



Forwarding Metrology with an IoT and Blockchain Approach: The Gas Pumps Use Case

Gabriel Estevam de Oliveira   [Universidade Federal de Santa Catarina | gabriel.estevam@posgrad.ufsc.br]


Pedro Henrique de Sena Trombini Taglialenha  [Universidade Federal de Santa Catarina | pedro.taglialenha@grad.ufsc.br]

Luis Felipe Fabiane  [Universidade Federal de Santa Catarina | luis.fabiane@grad.ufsc.br]

Thaís Bardini Idalino  [Universidade Federal de Santa Catarina | thais.bardini@ufsc.br]

Martín Vigil  [Universidade Federal de Santa Catarina | martin.vigil@ufsc.br]

Jean Everson Martina  [Universidade Federal de Santa Catarina | jean.martina@ufsc.br]

 Universidade Federal de Santa Catarina, Campus Florianópolis, R. Eng. Agrônomo Andrei Cristian Ferreira, s/n, Trindade, Florianópolis - SC, 88040-900.

Received: 03 October 2024 • **Accepted:** 12 February 2025 • **Published:** 24 May 2025

Abstract Volumetric fraud at gas pumps is a serious and ongoing issue, leading to substantial financial losses for consumers. Recognizing the severity of this problem, regulatory agencies in Brazil have introduced new gas pumps equipped with digital certification. This initiative is part of a broader strategy to integrate digital certification into measuring instruments, starting with gas pumps, as a proactive measure to counteract fraud. Additionally, Brazilian agencies are developing a mobile application that will allow users to access refueling data and perform their own inspections. In this context, we aim to further advance the topic by proposing a system that enhances the smart capabilities of metrology. We introduce the adoption of blockchain technology to establish consumer communities and promote metrology within IoT and cloud computing landscape. Our proposal allows users to share their refueling data, facilitating more active gas pump inspections with less dependence on regulatory agencies. We propose utilizing the user data in an evaluation system that cross-references the data and applies statistical methods to detect both volumetric fraud and fuel tampering. The system is designed to generate a ranking of gas pumps with the highest potential of being fraudulent, providing insights to both regulatory agencies and consumers. By leveraging blockchain technology, we can securely record user data and deliver the evaluation service in a transparent and decentralized manner. Finally, we apply statistical techniques to address the issue of trusting external data incorporated into the blockchain, which is commonly referred to as the oracle problem in the literature. Our simulation results demonstrate that, by using only refueling and vehicle data, we can achieve fraud detection accuracy of 89% in scenarios that closely resemble real-world conditions.

Keywords: Blockchain, Metrology, IoT, Cloud Computing, Measuring instruments, Gas pumps.

1 Introduction

Metrology is the science concerned with the measurement of physical events occurring in the real world [Fanton, Jean-Pierre, 2019]. Legal Metrology, in turn, is responsible for ensuring the accuracy and compliance of measuring instruments utilized across various metrological applications [Rodrigues Filho and Gonçalves, 2015]. This specific branch of metrology deals with standardizing and regulating instruments such as gas pumps, digital scales, and energy meters to maintain their precision and reliability in both commercial and regulatory contexts [ASMETRO-SI, 2024].

Despite varying specifications, each measuring instrument fundamentally serves the same purpose: measuring physical quantities. For example, a gas pump measures the volume of fuel delivered into the tank of a vehicle, a digital scale determines the mass of a product purchased by a consumer, and an energy meter tracks electricity consumption within a network over a specific period. In all these scenarios, commercial transactions or financial compensations are directly tied

to the products being measured. Consequently, ensuring the accuracy and precision of the data obtained from measuring instruments is of critical importance. Sellers aim to avoid dispensing more than what has been sold, while customers seek assurance that they are receiving no less than the quantity for which they have paid. In fuel trading, even minor deficits can result in financial losses amounting to billions [Estadão, 2024].

In response to these challenges, the Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro) has initiated efforts to modernize legal measuring instruments in Brazil, starting with gas pumps [Indio, 2021]. Digital certification represents a transformative advancement for these new gas pumps. Through the use of digital signatures, key properties such as integrity, authenticity, and non-repudiation are ensured for refueling data. The verification of integrity determines whether the refueling data from the gas pump has been tampered with, the verification of authenticity confirms the specific gas pump that generated the data, and non-repudiation ensures that the gas station owner can be held

accountable for the data generated.

Another notable feature of the new gas pumps is the integration of Bluetooth Low Energy for open communication. This allows anyone with a compatible device, such as a smartphone, to download data from a gas pump directly. This capability facilitates the development of innovative applications that can utilize these data. For instance, customers can share data to establish evaluation service systems, enhancing transparency not only for gas pumps but also for other legal measuring instruments that could benefit from this technology.

The data generated by these systems can provide insights and facilitate decision-making. Consequently, a smart network of measuring instruments could offer customers a higher quality of service, such as improved fraud detection in gas pumps or a comprehensive fuel quality assessment system. But even in scenarios where the instruments are not connected, such as lacking Bluetooth connectivity, users can still manually enter the data without compromising the smart features of the system.

Within this framework of intelligent systems, blockchain technology emerges as a means to enable connectivity among these systems. Essentially, blockchains are distributed ledgers that record transactions. A network of independent nodes validates the transactions against a shared database. Consequently, the system supports the operation of decentralized applications without requiring the intervention of third parties. Blockchains allow all transactions to be recorded in a transparent and verifiable manner, accessible to all parties involved. Additionally, rather than centralizing data storage within a single regulatory entity, blockchain decentralizes it across all participants. This decentralization allows each participant to maintain a copy of the blockchain and engage in a consensus protocol.

The contribution of this work is to apply blockchain to facilitate the creation of user communities for measuring instruments, thereby promoting active oversight in exchange for improved service quality. More specifically, we propose a method for detecting volumetric fraud and fuel tampering in gas pumps using refueling and vehicle data. These data are transmitted to a Hyperledger Fabric network, where a gas pump evaluation algorithm based on vehicle fuel efficiency has been implemented. To validate this method, we conducted an experiment simulating distinct real-world scenarios. Our results demonstrate that this method can detect fraudulent gas pumps with a precision of up to 81.6% and an accuracy of 89% in scenarios that closely resemble actual operational environments. This initial effort demonstrates that it is possible to enhance fraud detection through a blockchain-based system.

The remainder of the article is organized as follows. Section 2 introduces fundamental concepts, followed by a systematic review in Section 3. In Section 4, we describe the Brazilian use case upon which our study is based, while Section 5 outlines our proposal and Section 6 details its implementation. Section 7 presents our experiments, with discussions in Section 8, and conclusions in Section 9.

2 Background

In this section we present fundamental concepts such as measuring instruments, legal metrology, IoT & cloud computing, and blockchain technology, providing the necessary background to understand our contributions.

2.1 Measuring instruments

Measuring instruments are devices used to determine a magnitude, quantity, or size under observation [Inmetro, 2020]. They operate on principles specific to the physical quantity they measure, such as distance, temperature, pressure, or electrical current, ensuring accuracy and precision in data collection. These tools are essential across many areas, including commerce, health, safety, environmental protection, and law enforcement, particularly within the scope of Legal Metrology. In commerce, examples include scales, water meters, taxi meters, and gas pumps. In the healthcare sector, clinical thermometers and blood pressure meters are commonly used. For safety applications, devices such as Tachographs, vehicle speed meters, and breathalyzers are essential. Environmental measurements utilize instruments like vehicle gas analyzers, opacimeters, and vehicle inspection modules. Additionally, instruments like vehicle speed meters and gas analyzers are also used for inspection effects, such as in the enforcement of laws and regulations. Instruments subject to metrological control typically feature labels indicating the validity of their last metrological verification.

2.2 Legal Metrology

The International Organization of Legal Metrology defines Legal Metrology as the branch of metrology concerned with measurement units, measurement methods, and measuring instruments in relation to mandatory technical and legal requirements [Inmetro, 2024a]. It aims to ensure public assurance regarding the safety and accuracy of measurements.

Legal Metrology encompasses a crucial function within all levels and sectors of a nation. It governs the use of measurement instruments that are subject to regulatory oversight, aiming to disseminate and maintain harmonized measurements and units. Moreover, it supervises and examines instruments and measurement methods. This governmental effort in legal metrology primarily protects both the consumer, as the buyer of measured products and services, and the seller, as the provider. The accuracy of measurement instruments, especially in commercial activities, is often beyond the verification capability of the involved parties, particularly those without the technical means to perform such checks.

Legal Metrology originated from the need to ensure fair trade, playing a pivotal role in enhancing trade efficiency by maintaining trust in measurements and reducing transaction costs. This is primarily achieved through regulatory measures that ensure a reliable level of measurement accuracy. Measurement instruments are typically held by one of the trading partners, and accessible even when the other party is absent. Today, not only are commercial activities subject to governmental oversight in developed countries but measurement instruments used in official activities, medical fields,

drug manufacturing, occupational safety, environmental and radiation protection are also subject to mandatory metrological oversight.

2.3 IoT & Cloud Computing

Internet of Things (IoT) refers to distributed systems that integrate sensing, transmission, and computation [Khan and Yuce, 2019]. Since they are fundamentally based on data collection and transmission, IoT can be seen as extending the role of measuring instruments. Similarly, measuring instruments can be considered IoT devices if they meet the connectivity requirements. Some key IoT applications include healthcare, smart cities, smart agriculture, and automotive systems [Khan and Yuce, 2019]. Therefore, although IoT devices may not be subject to the same regulations as legal measuring instruments, concerns about measurement accuracy remain, particularly in critical applications such as healthcare or high-demand markets, including energy smart meters.

IoT devices are characterized by being connected and requiring minimal human intervention, often becoming transparent to the user. They are also characterized by having restricted hardware and a focus on low energy consumption, which implies limited computational power [Tripathy and Anuradha, 2018]. Furthermore, IoT systems generate vast amounts of data, often called Big Data, and rely on cloud computing for data processing. Cloud computing not only handles the computational processing but also serves as a platform for monitoring and making the data accessible [Khan and Yuce, 2019]. In this work, blockchain will take on the role of cloud computing, receiving, storing, and ensuring security requirements, in addition to supporting the computational processes needed.

2.4 Blockchain

Blockchain technology is a distributed data structure that forms a chain of data blocks, maintained by a network of nodes adhering to a consensus protocol. This structure ensures that each block is linked to its predecessor through cryptographic hashes contained in the block headers, along with timestamps and data compilations. Together, cryptographic hashes and timestamps ensure the integrity and chronological order of data stored in the blockchain.

Blockchains operate on a peer-to-peer network where each participating node stores a copy of the entire chain. This decentralization ensures that no single node or authority controls the transaction data, thereby increasing the security and transparency of the data recorded. Nodes in the network use public key cryptography to secure transactions; the private key signs transactions, ensuring their authenticity, while the public key is used for verification by other nodes [Nakamoto, 2008]. Transactions are triggered by nodes performing various operations, such as transferring assets. Once a transaction is proposed, it must be validated by other nodes through a process that involves checking the transaction against the current state of the blockchain and the network consensus rules [Xu *et al.*, 2017].

To make these validations, blockchain employs consensus mechanisms such as Proof of Work (PoW) or Proof of

Stake (PoS) to maintain uniform agreement across the network on the validity of transactions. These mechanisms require nodes to perform specific tasks, whether computational in the case of PoW or ownership-based in PoS, to validate transactions and create new blocks. This process secures the network by ensuring that all nodes agree on the state of the ledger and also prevents fraudulent activities such as double-spending and unauthorized data changes [Alsunaidi and Al-haidari, 2019].

Blockchain technology can also be categorized into permissionless and permissioned systems. Permissionless blockchains, such as Bitcoin and Ethereum, are open to anyone for participation in activities like transaction validation and block creation, promoting transparency and resistance to censorship. In contrast, permissioned blockchains restrict network activities to a select group of authorized participants, making them suitable for business contexts where privacy, governance, and performance are fundamental [Reijsbergen *et al.*, 2022].

Beyond its original application of cryptocurrencies, blockchain technology has been applied for a wide range of uses across various sectors. These applications extend from enhancing supply chain transparency to securing sensitive medical data and enabling the execution of automated legal agreements through smart contracts. These contracts are self-executing contracts with the terms of the agreement directly written into code, which automatically enforce and execute the terms based on underlying transactions [Christidis and Devetsikiotis, 2016].

3 Systematic Literature Review of Blockchain applications in Metrology

The adoption of blockchain in metrology offers significant potential to improve the security, reliability, and efficiency of metrological processes, especially in the context of gas pumps. However, research in this field is still in its early stages, highlighting the need for a thorough overview of blockchain applications in metrology. To fill such a gap, this section presents a systematic review of the use of blockchain in metrology.

3.1 Methodology

We conducted a systematic review using the method of Kitchenham and Charters [2007] and were guided by the following research questions:

1. What are the main proposals for the application of blockchain in metrology? and;
2. How can blockchain be used to add value to metrological systems?

The search was conducted in the main databases of the computing field (IEEE, Science Direct, ACM Digital Library, Springer Link, and Google Scholar) using the keywords Blockchain and Metrology, combined with synonyms and related terms. The search string was applied to the

databases in March 2024 and returned 1,930 non-duplicates. Only articles published in journals and conference proceedings were considered.

By the inclusion criteria, papers that addressed the integration between blockchain and metrological objects were included, but not only within legal metrology; it also encompassed smart meters and IoT, provided that they brought some contribution to the theme. Additionally, another criterion was the capacity to add value or intelligence to a final application through information extraction. Therefore, we ruled out papers concerning only the security of data. Out of the 1,930 articles, 51 were selected based on their titles. Of these, 21 were chosen after abstract review. In the end, after a thorough reading, only 8 papers are concretely related to the theme, and these are presented in the following subsection.

3.2 Related Works

This section presents studies that, as in our work, use blockchain to prevent frauds or ensure the integrity of metrological data or similar applications. Also, a comparison with our work is provided at the end of this section. Table 1 summarizes the main features of both the related works and our approach. The works are presented as follows.

An approach centered on directly verifying the core measurement algorithm within legally supervised measuring instruments, as opposed to traditional integrity checks targeting the entire software stack, was introduced by Peters *et al.* [2020]. The authors employ secure storage (e.g., permissioned Blockchains) and trusted computing hardware with sensors to facilitate confidential and computationally efficient checks of the core algorithm during each measurement cycle. This approach reduces the need for comprehensive software stack verification, offering a significant security improvement for software-controlled devices used in legally regulated measurement scenarios.

A blockchain-based security system for smart meters, integrating PoS consensus mechanisms with Advanced Encryption Standard (AES) techniques, was proposed by Singhal *et al.* [2023]. Their focus is on preserving privacy within smart grids by enabling secure data sharing and transaction validation, as well as energy-efficient data protection. To optimize blockchain storage for smart meter data, the authors introduce a data pruning technique, enhancing resource efficiency.

In a similar context, Tahir Bokhari *et al.* [2019] proposed a blockchain-based solution for secure metering and fraud prevention within IoT-connected metrology systems. The system includes the design of both a blockchain testbed and a specialized revalidation protocol to ensure the integrity of metering data. The authors also investigate external revalidation methods, propose a lightweight validation protocol, and analyze consensus algorithm suitability to optimize security and reduce the risk of utility theft.

To address the challenges of fuel dispensers surveillance, Melo *et al.* [2021] developed a methodology that combines IoT-based metering devices with blockchain technology. The authors introduce a Distributed and Decentralized Surveillance Framework that leverages smart fuel meters and

a blockchain infrastructure to monitor fuel dispensers. To mitigate measurement uncertainties, the work employs statistical techniques grounded in the Law of Large Numbers. The researchers implement a secure fuel measurement data storage mechanism using the Hyperledger Fabric blockchain platform. Smart contracts are used to facilitate real-time monitoring and data analysis.

Singh *et al.* [2022] proposed a reputation model designed to mitigate insider attacks in smart metering infrastructures, utilizing blockchain for decentralized attack identification. The proposed model addresses threats such as false data injection, energy fraud, denial of service, and data disclosure attacks by authenticating devices and validating transactions efficiently. By customizing the Go Ethereum implementation, the model demonstrates security effectiveness in handling post-authentication attacks. The use of permissioned Proof of Authentication blockchain enhances security and scalability for lightweight smart metering applications.

To enhance smart grid security against False Data Injection (FDI) attacks, Reijnders *et al.* [2022] proposed an incentive mechanism for blockchain-based data sharing among operators. Although the majority of the work focuses on security, we analyzed it because it uses blockchain to mitigate a specific type of fraud related to metrology. The work addresses a realistic threat model where operators may be compromised, leading to potential data manipulation. The proposed solution involves operators forming a consortium to share data on a tamper-evident blockchain, enabling the detection of FDI attacks through redundant measurements. The implementation includes optimizations such as offline computation, caching, and multithreading to enhance performance and scalability. The mechanism incentivizes operators to upload accurate data while penalizing deficits, ensuring the integrity of grid operations. Additionally, the study explores the practical implications of operator size on the effectiveness of the proposed solution and discusses potential future enhancements, such as replacing the existing mechanisms with more efficient algorithms.

Singh *et al.* [2023] introduced Logicontract, a framework that integrates Quantum Key Distribution (QKD) methods with a vote-based consensus algorithm to establish a quantum-secured, permissioned blockchain. The research develops a quantum-resistant lottery protocol and a scalable consensus protocol, coupled with a logic-based scripting language for smart contracts that enables precise execution of contract logic. Incorporating QKD-enhanced digital signatures significantly fortifies the blockchain against quantum threats, crucial for the integrity of transactions in metrology-related applications such as energy trading and advanced metering infrastructure. Moreover, the introduction of a structured scripting language allows for detailed and secure implementation of contracts that could be applied to metrological processes, improving the traceability and reliability of measurements within Industry 4.0 frameworks.

In the context of distributed measuring systems, Melo Junior *et al.* [2019] conducted a technical analysis focusing on the design of an architectural model that leverages blockchain for securing measurement instruments and addressing regulatory challenges. The authors introduce secure interfaces for legally relevant software functions, addressing

Table 1. Related work comparison.

Article	Blockchain	Blockchain Role	Metrology In- tegration	Fraud Prevention
[Peters <i>et al.</i> , 2020]	Generic	Software integrity, measurement accuracy	Smart meters	Indirect; system integrity to prevent tampering
[Singhal <i>et al.</i> , 2023]	Not explicit Proof-of-Stake blockchain	Secure meter data, privacy	Smart meters	Indirect; enhances security and privacy
[Tahir Bokhari <i>et al.</i> , 2019]	Ethereum, custom TCP-based protocol	Validate meter accuracy, security	Smart meters	Reduces tampering, enhances billing accuracy
[Melo <i>et al.</i> , 2021]	Hyperledger Fabric with BFT consensus	Monitor dispenser accuracy, automate	IoT devices in vehicles	Detects tampering using statistical analysis
[Singh <i>et al.</i> , 2022]	Custom Permissioned Ethereum	Mitigate attacks, secure reputation	Smart meters	Insider attacks prevention, reputation management
[Reijsbergen <i>et al.</i> , 2022]	Private Hyperledger Fabric	Incentivize sharing, enhance security	Smart meters	Indirect; combat false data injection
[Singh <i>et al.</i> , 2023]	Ethereum	Secure metering infrastructure	Smart meters	Indirect; unauthorized access and data tampering
[Melo Junior <i>et al.</i> , 2019]	Hyperledger Fabric	Distributed measuring, MI security	Sensor network	Constrains attacker capabilities, measurement security
This work	Hyperledger Fabric	Create a user community for active surveillance	Gas pumps	Detects tampering using statistical analysis

challenges in traditional measuring instruments. They discuss the advantages of cloud-based architecture in terms of cost savings and enhanced device connectivity. A case study utilizing the Hyperledger Fabric platform demonstrates the practicality of the proposed blockchain-based approach in measuring vehicle speed. Additionally, a quantitative comparison between traditional Measuring Infrastructure (MI) and blockchain-based solutions offers insights into the potential benefits and limitations of the new system.

Our work addresses the persistent issue of volumetric fraud at gas stations by utilizing blockchain, focusing specifically on gas pumps in Brazil. We propose the application of blockchain technology to establish consumer-independent communities. In our proposal, blockchain is used to record measured data and apply statistical methods for fraud detection. The statistical methods allow us to identify data tampering, false data injection, and fraudulent activities. This approach provides a distinct advantage by directly facilitating the automatic detection of gas pump volumetric fraud and fuel tampering, thus potentially streamlining inspection and audit processes in legal metrology. Moreover, this targeted application enhances fraud detection accuracy and regulatory compliance, aspects not specifically addressed by other studies. The practical application to a real-world use case adds more credibility to our proposed method than the other approaches. The simulation reinforces the reliability of the experimental results and demonstrates the effectiveness of the solution. With our work, we demonstrate the potential benefits of integrating blockchain into legal metrology, making the supervision process more effective and efficient. Finally, Fraud detection benefits not only consumers but also supervisory bodies, supply chains, fuel distributors, and federal agencies in the fight against tax evasion and corruption.

In comparison, our work enhances the value of metrological data recorded on the blockchain. We apply techniques to improve data reliability and extract useful information for the final application. Melo *et al.* [2021] present a similar approach, evaluating fraud at gas pumps using metrologi-

cal data. However, their method relies on additional equipment installed in vehicles, significantly reducing its usability, whereas our approach utilizes only existing data. Furthermore, compared to Melo *et al.* [2021], we provide a more in-depth application of statistical methods for fraud detection and build a more robust simulation. Similarly, Singh *et al.* [2022] and Reijsbergen *et al.* [2022] also addressed the prevention of tampering and false data injection, as we do. However, they rely on a reputation system or an incentive mechanism based on rewards, respectively, to ensure data trustworthiness, whereas we rely solely on the data itself. In contrast to Singhal *et al.* [2023], we do not focus on data privacy, since it may hinder data aggregation and limit the transparency required to apply verification methods. Peters *et al.* [2020] focus on checking the software of instruments, which we believe is insufficient, since sensors or data channels may remain vulnerable. Tahir Bokhari *et al.* [2019] are constrained by costs and performance on the Ethereum blockchain, indicating that public blockchains remain a challenge for this type of application. Singh *et al.* [2023], in addition to also using Ethereum, focus primarily on establishing a secure infrastructure to receive data rather than on the content of the data itself, as we do. The same applies to the work of Melo Junior *et al.* [2019].

In summary, most of the work focuses on systems that use smart meters, highlighting the importance of this area. Blockchain emerges as an infrastructure that enables data sharing and transparency. All studies on fraud prevention contribute to enhancing data reliability, either directly or indirectly. Privacy is also a key issue for certain applications, while performance and scalability are concerns for the majority.

4 The Brazilian Use Case

According to a report by Peduzzi [2021], Inmetro detects approximately 20,000 frauds in gas pumps every year, which result in financial losses exceeding 20 billion reais annually.

Such frauds typically involve tampering with the flow meter components of gas pumps. Consequently, consumers receive less fuel than indicated on the pump display, effectively paying for more fuel than they actually receive.

The issue of gas pump fraud is longstanding [Oyama, 2019], yet it remains unresolved to this day. A national inspection initiative, titled as *Operação Petróleo Real*, uncovered widespread occurrences of gas pump fraud across multiple states in Brazil [Inmetro, 2021]. Inmetro approved a regulation to standardize the digital certification of gas pumps [Inmetro, 2024b], which aims to combat fraud in gas pumps. Digital certification ensures that the signal transmitted by the flow meter is accompanied by a digital signature, guaranteeing data integrity and helping to prevent volumetric distortion. In recent years, Inmetro and the *Instituto Nacional de Tecnologia da Informação* have established a partnership to support the digital certification of metrological instruments [Correio Braziliense, 2021]. This technology is expected to become available soon, offering significant benefits to consumers.

However, there are some points to consider. Inmetro [2022] establishes that gas pump inspections occur annually. While this frequency may be insufficient for addressing a highly active “fraud market”, it is understandable that increasing the frequency of inspections poses challenges for regulatory agencies, both in Brazil and globally. Inspections conducted by regulatory agencies require specialized personnel, incur significant costs, and disrupt gas station operations due to the temporary deactivation of gas pumps. Another consideration is fuel tampering, which involves mixing other substances into the fuel and is not addressed by the digital certification.

The efforts made by regulatory agencies, particularly Inmetro, to modernize measuring instruments and mitigate fraud in gas pumps, are commendable. However, we believe that there is still room for improvement. In this work, we aim to take these efforts further by proposing a method to detect fraud more efficiently and less dependent on regulatory agencies.

5 The Blockchain-Based System to Detect Frauds on Gas Pumps

This section presents our proposal for detecting fraud in refueling events. The proposal involves creating a platform where consumers can share their refueling data. By cross-referencing data from the consumer community and applying statistical techniques, we aim to identify discrepancies that may indicate potential fraud.

The key elements of the proposal are as follows: integration of measuring instruments and data acquisition, data sharing and storage, and the fraud detection method. These components are described in detail below.

5.1 The measuring instrument

Our case study focuses on the Brazilian gas pumps, which are to be equipped with digital certification and Bluetooth

communication following Inmetro Ordinance No. 264 Inmetro [2024b]. The communication protocol for these new gas pumps is detailed in Inmetro [2024c]. According to the protocol, all refueling data will be made available via Bluetooth. Among the data provided, we are particularly interested in the refueled volume, which will be used to evaluate gas pumps and detect volumetric fraud. In scenarios where gas pumps do not have Bluetooth connectivity, data can be manually entered by users without compromising the effectiveness of the fraud detection method.

5.2 User data

Our proposal involves the collection of specific data reported by users, namely the vehicle model and odometer readings for each refueling event. To obtain these data, we proposed using a mobile application that collects refueling data transmitted by the gas pump via Bluetooth and allows the user to input the odometer reading. An application designed for this purpose is currently under development [Peduzzi, 2021]. By enabling users to register their vehicle model in advance, the only data required from the user at the time of refuel will be the vehicle odometer.

5.3 Using blockchain to record data

We propose to use blockchain technology to record data. In this approach, the metrological data emitted by gas pumps, along with user data, are transmitted to a blockchain, ensuring transparency for all recorded data. Both gas pump and user data are publicly recorded, allowing any interested party to access, monitor, and maintain the data. The only data that users enter are the vehicle model and odometer, which are not sensitive data. This approach eliminates database centralization, making the data available for queries by anyone, including regulatory agencies, thereby facilitating inspections and audits. We also assume that the majority of users provide the correct vehicle model and odometer readings; otherwise, the method may yield inaccurate results. However, minor errors are tolerated by the method.

To maintain the blockchain nodes, we propose a network composed of parties interested in improving service quality. As noted by Melo *et al.* [2021], numerous stakeholders have a vested interest in preventing fraud at gas pumps. Initially, this could include the national metrological institutions and regulatory agencies. Additionally, fuel distributors and retailers might participate to promote themselves as trustworthy companies. Users may also be inclined to join the network to ensure they are not adversely affected.

Figure 1 illustrates the proposed architecture. The frame Blockchain Network on the right side represents the permissioned blockchain, which is composed of participating nodes. The frame Actors on the left side identifies the actors responsible for data collection. And, the frame Blockchain Application on the center highlights the application processes that transmit data to the blockchain.

The steps depicted in the Figure 1 are described below:

- **Step 1:** The User accesses its Device, submits their vehicle information, and initiates a refuel reading.

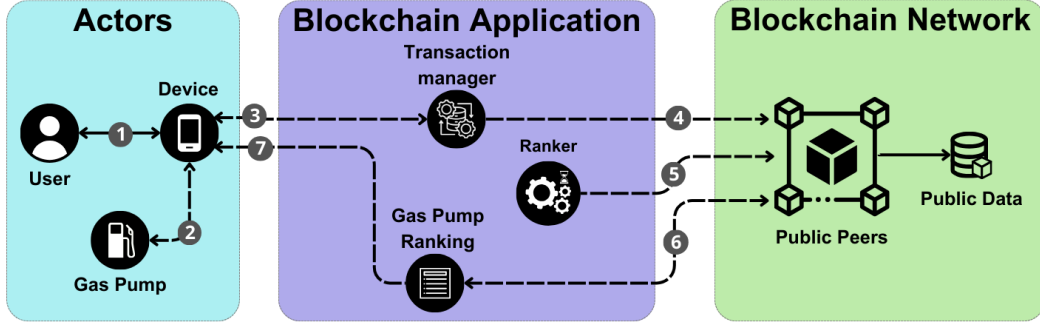


Figure 1. System architecture and communication diagram.

- **Step 2:** The Device collects refueling data from the Gas Pump.
- **Step 3:** The Device sends the data to the Blockchain Application, which prepares a blockchain transaction with the received data.
- **Step 4:** The Blockchain Application transmits the transaction to the Blockchain Network.
- **Step 5:** The Ranker requests the Blockchain Network to update the ratings of Gas Pumps.
- **Step 6:** The Blockchain Application retrieves the updated Gas Pump ranking.
- **Step 7:** The Blockchain Application sends the Gas Pump ranking to the Device.

5.4 Rating metrics

To support the fraud detection scheme, we propose a method for evaluating vehicles' efficiency and gas pumps' trustworthiness. This method is based on calculating the efficiency of vehicle fuel consumption and evaluating the quality of the fuel dispensed by the gas pumps. If the vehicle efficiency is close to or exceeds the expected efficiency for its model, it will positively influence the gas pump evaluation. Conversely, if the vehicle efficiency is below the expected efficiency for its model, it will negatively impact the gas pump evaluation. The parameters and formulas for evaluating vehicle efficiency and gas pumps are outlined below.

- A set V of vehicles.
- A set F of gas pumps.
- A set $E = \{E_v | v \in V\}$ of the expected efficiency for each vehicle v of set V .
- A set $S = \{S_{fv} | f \in F, v \in V\}$ of the refueled volumes by vehicle v at gas pump f .
- A set $D = \{D_s | s \in S\}$ of the distances driven since the last refueling event s .

For a vehicle v , we can obtain its efficiency as:

$$VE_v = \frac{1}{E_v} \frac{\sum_{f=1}^{|F|} S_{fv}}{\sum_{f=1}^{|F|} D_{sfv}}$$

A $VE_v \approx 1$ indicates that the vehicle v performed near its expected efficiency; a $VE_v < 1$ indicates that the performance of vehicle v was worse than expected; and, a $VE_v > 1$ indicates that the performance of vehicle v exceeds expectations.

From the vehicle rating, it is possible to obtain the gas pump evaluation. The gas pump rating is calculated as the weighted average of the vehicles rating, where the weight is determined by the amount of fuel each vehicle received from the gas pump. The formula for calculating the gas pump rating is as follows:

$$VF_f = \frac{\sum_{v=1}^{|V|} VE_v S_{fv}}{\sum_{v=1}^{|V|} S_{fv}}$$

Similarly to the vehicle, a $VF_f \approx 1$ indicates that gas pump f provides the expected volume of fuel. Values above 1 indicate that the gas pump provides more fuel than expected, while below 1 indicate that the gas pump provides less fuel than expected.

5.5 Frauds detection

By examining the vehicles and gas pump evaluations, it is evident that the rating is directly proportional to the fuel efficiency of the vehicles. Consequently, if a gas pump dispenses less fuel than indicated, the efficiency of vehicles refueled at the gas pump is likely to decrease. This results in a lower vehicle rating and consequently in the gas pump rating. Similarly, the presence of tampered fuel can also lead to decrease vehicle efficiency and gas pump rating.

Therefore, by utilizing the ratings, we can classify gas pumps with the lowest values as likely fraudulent, creating a ranking system. The threshold to identify fraudulent gas pumps can be estimated by using historic inspection data, for example. However, the primary objective of this ranking is to guide inspection efforts, facilitating more effective targeting and mitigation of fraud.

6 Implementation

For our proof of concept, we implemented the blockchain infrastructure using Hyperledger Fabric on a test network hosted on a single laptop. Our benchmark hardware consists of a computer equipped with 16 GB of RAM and an 11th Gen Intel Core i7-1165G7 processor running at 2.8 GHz with eight cores. This laptop hosts all the Blockchain network peers and organizations instances, all of which are containerized using Docker. We structured the network with containers assigned to two distinct organizations, each comprising their respective peers. Each peer functions as both endorser and committer. It receives client transactions, endorses them

after executing the respective chaincode, and commits them to the ledger.

In our setup, we utilized a channel structure provided by Hyperledger Fabric. This channel functions as a private communication medium, accessible only to authorized participants who can view the transaction data. We adopted the default endorsement policy, which requires endorsements from peers of both organizations. This ensures that transactions are validated by multiple independent peers.

6.1 Chaincode

For our blockchain application, we implemented a chaincode, which serves as the Hyperledger Fabric equivalent of a smart contract. This chaincode manages transactions between gas pumps and vehicles, ensures continuous tracking of vehicle refuel and consumption, and also supports periodic evaluation of gas pumps. The chaincode is designed to provide the following key functionalities:

- **Entity Management:** The chaincode enables the registration and management of gas pumps and vehicles within the blockchain network. It captures essential details about each entity.
- **Transaction Recording:** The chaincode records essential information about refueling events, associating each transaction with the corresponding vehicle and gas pump. This includes tracking the quantity of refueled, the odometer readings of vehicles, and the cumulative refuels associated with each gas pump. By maintaining only this transactional data, the chaincode ensures a streamlined process focused on monitoring the refuels and supporting the rating process.
- **Performance Evaluation:** The chaincode enables the evaluation of performance metrics for both vehicles and gas pumps. This evaluation process is based on the calculations detailed in Section 5.4.
- **Query:** The chaincode provides querying capabilities that allow stakeholders to retrieve and analyze specific data from the ledger.

7 Performance Evaluation

In this section, we present the experiments conducted in two parts. In the first part (Section 7.1), we present a simulation to evaluate the fraud detection method, and in the second part (Section 7.2), we present experiments to evaluate our blockchain-based implementation.

7.1 Fraud Detection Method

In order to validate the proposed methodology for detecting fraud at gas pumps, we modeled a simulation of the refueling scenario. In this scenario, we assume that users will actively contribute to the metrological ecosystem by transmitting data from each refueling event to a decentralized blockchain network. Specifically, the users will submit the odometer reading and the volume of fuel dispensed after each refueling. This input is crucial for the creation of a ranking system, as

discussed in section 5.5, which aims to identify and categorize gas pumps based on their accuracy and reliability.

The simulation is conducted to explore the efficacy of this system within a controlled environment. To do this, we generate a dataset replicating the refueling events over the course of one year as faithfully as possible. This dataset allows us to assess the efficacy and accuracy of the fraud detection method. The setup, execution, and evaluation of the experiment are detailed in the subsequent subsections. The findings are intended to determine whether the proposed system can effectively identify fraudulent pumps, thus enhancing consumer trust and regulatory compliance during refueling events.

7.1.1 Scenario

For this simulation, we chose the road fuel market in Brazil as the base scenario, reflecting the specific context of the use case presented. The data utilized are from the year 2022, which was the year with the most available data to substantiate the simulation. Each piece of data was carefully validated to ensure the simulation accurately mirrors real-world conditions. The data are as follows:

- Total amount of gas stations: 43,266¹.
- Total amount of fuel sold by type in the year: Table 2².

Table 2. Total fuel sold in 2022 by type.

Fuel type	Total (liters)
Gasoline (commercial)	45,955,600,000
Ethanol (hydrous)	15,986,400,000
Diesel	65,466,400,000

- Vehicles active in the year (electric vehicles do not apply to this experiment and we ruled out hybrid vehicles for the sake of simplicity): Table 3³.

Table 3. Vehicles active in 2022.

Vehicle category	Units
Automobiles	63,100,342
Light commercials	10,244,844
Trucks	3,732,698
Bus	729,830
Motorcycles	30,263,233

- Volumetric fuel deficit: customers receive, on average, 3%⁴ less fuel on all their purchases over the course of a year.

¹<https://www.gov.br/anp/pt-br/centrais-de-conteudo/publicacoes/anuario-estatistico/arquivos-anuario-estatistico-2023/anuario-2023.pdf>

²<https://www.gov.br/anp/pt-br/centrais-de-conteudo/publicacoes/sinteses/scc/2023/>

³<https://www.fenabreve.org.br/anuarios/Anuario2022.pdf>

⁴<https://www.saopaulo.sp.gov.br/spnoticias/operacao-olhos-de-lince-ipem-sp-fiscaliza-postos-na-capital-e-gde-sp/>

⁵<https://agenciabrasil.ebc.com.br/economia/noticia/2021-04/celulares-podem-ajudar-no-combate-fraudes-em-bombas-de-combustiveis>

- Fraudulent gas pump shortfall: a fraudulent gas pump dispenses, on average, 10%⁶ less fuel on a refuel transaction.

To complement the data, we assumed some estimates established by crossing related data, which are shown below:

- Gas stations have on average 12 gas pumps each⁷, which totals approximately 519.192 gas pumps across the entire scenario.
- Gas pumps dispense only one fuel type and the number of each type of gas pump is proportional to the total fuel sold.
- Dual-fuel vehicles do not change the fuel type during the period.
- Vehicles with the same type of fuel travel on average the same distance.
- The refueled volume is on average half the tank capacity.

This allows us to create distinct consumption profiles for each vehicle type and fuel variety, as shown in Table 4. The total number of vehicles within each profile was calculated to distribute fuel consumption while maintaining the average distance traveled by each fuel type. For efficiency and tank capacity, the best-selling vehicle of 2022 within each profile was used as a reference^{8 9 10}.

Normal and continuous distributions were used to model user and environmental behavior, such as how often a user refuels, at which gas pump, and the volume refueled. The normal distribution consists of values that create a 'bell-shaped' curve, while continuous distributions represent events with the same probability of occurring. Additionally, it is expected that not all users will submit their refueling data. Therefore, a user adoption percentage was incorporated to reflect the actual proportion of users who have adopted the system and actively sent their refueling data. Consequently, the dataset is structured into three distinct sets, which are described below:

- Gas Pumps dataset: it defines the gas pumps with the fuel types Gasoline, Ethanol, and Diesel. We determined the number of gas pumps for each fuel type based on the fuel sales proportion shown in Table 2. Also, we used two normal distributions to quantify the volumetric shortfall of each gas pump. Figure 2 depicts the distribution of the volumetric gas pump's shortfall. The first peak represents non-fraudulent gas pumps, with a shortfall around zero and a tolerance percentage of -0.5% to +0.5%. The second peak represents fraudulent gas

pumps, with a fluctuation around the gas pump shortfall (a parameter of the simulation) with a range extending from -20% to +20% of this peak. We calculated the number of fraudulent and non-fraudulent gas pumps to align with the overall volumetric fuel deficit specified in the simulation.

- Vehicles dataset: it defines the vehicle's profiles, based on the data provided in Table 4. We calculated the number of vehicles of each profile proportionally to the values on the table and the user adoption percentage (parameter of the simulation).
- Refuels dataset: it defines the refueled volume, vehicle and gas pump involved in the refuel, and vehicle odometer. We used the following steps to generate the dataset:
 1. The number of refuels performed by each vehicle was dictated by a normal distribution with the average calculated proportionally to the profile, with a range between zero and two times the average.
 2. A continuous distribution selected the gas pumps of each refueling event, giving each equal opportunity to gas pumps at every refueling event.
 3. The refueled volume at each refueling event followed a normal distribution, with an average of half the vehicle's tank capacity, ranging from zero to full capacity.
 4. The fuel consumed since the last refueling was determined using a normal distribution centered on half of the residual volume (i.e., volume remaining in the tank after the last refueling), with its range extending from a minimal consumption to the total residual volume. The minimal consumption is set such that the tank does not overflow during the next refueling.
 5. A dynamic consumption rate was calculated to adjust the actual fuel efficiency, which is influenced by the gas pump shortfall and a random coefficient reflecting different driving behaviors (e.g., more or less economic driving). This coefficient fluctuates around the expected profile efficiency by plus or minus 20% on a normal distribution.
 6. The odometer reading for each vehicle at the time of refuel was calculated by multiplying the fuel consumed and the dynamic consumption rate.
 7. After each refuel, the dynamic consumption was recalibrated as a weighted average of the efficiency of the volume refueled and the residual fuel before the refuel.
 8. Finally, the vehicle odometer was updated to reflect the distance traveled based on the consumed fuel and the recalculated dynamic consumption.

Furthermore, we anticipate that user behavior may inadvertently or deliberately compromise the data integrity. Accordingly, we incorporated two categories of data discrepancies into the analysis. Firstly, we assumed that 10% of the users who adopted the system might forget to record and transmit their data 10% of the time. Secondly, we assumed intentional data manipulation by 5% of the users, where they deliberately alter the vehicle odometer readings by up to 20%, either increasing or decreasing the values.

⁶<https://oglobo.globo.com/economia/quadrilhas-usam-chips-para-alterar-volume-em-bombas-de-combustivel-21518786>

⁷<https://www.saopaulo.sp.gov.br/spnoticias/operacao-olhos-de-lince-ipem-sp-fiscaliza-postos-na-capital-e-gde-sp/>

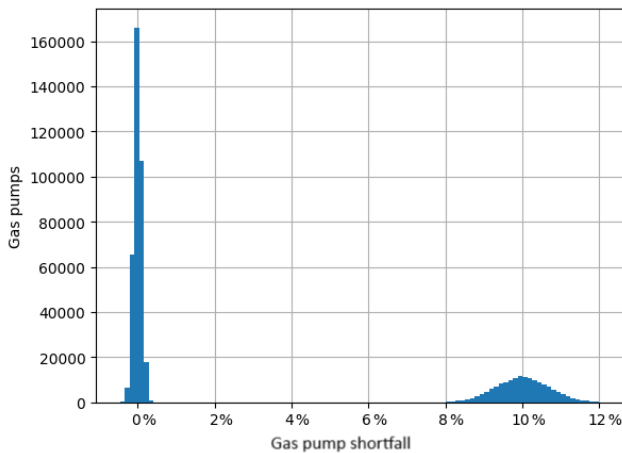
⁸<https://autopapo.uol.com.br/noticia/carros-mais-vendidos-2022/>

⁹<https://blog.fretebras.com.br/voce-sabe-quais-foram-os-caminhoes-mais-vendidos/>

¹⁰<https://www.motoo.com.br/emplacamentos/motos-mais-vendidas/2022/>

Table 4. Consumption profiles.

Profile	Units	Average efficiency (km/L)	Tank capacity (L)
Automobiles with Gasoline	46,587,851	14.10	50.00
Automobiles with Ethanol	14,615,548	10.30	50.00
Automobiles with Diesel	1,841,923	12.30	55.00
Light commercials with Gasoline	4,002,530	13.20	55.00
Light commercials with Ethanol	1,302,644	9.40	55.00
Light commercials with Diesel	4,939,711	12.10	55.00
Trucks with Diesel	3,732,698	1.56	495.00
Bus with Diesel	729,830	3.30	300.00
Motorcycles with Gasoline	30,263,233	35.00	16.10

Figure 2. Distribution of the volumetric gas pump's shortfall.

The selection of users who forget or manipulate follows continuous distributions, randomly selecting 10% and 5% of users for each case, respectively. Regarding the manipulation percentage, a normal distribution centered around 20% was used, ranging from 0% to 40%, along with a sign indicating whether the manipulation is positive or negative. In practice, this results in a bimodal distribution with two bell-shaped curves: one centered at +20% and the other at -20%. The resulting value is then multiplied by the efficiency of the vehicles belonging to the users who manipulate the data during refueling.

The code that generates the simulation is available at https://anonymous.4open.science/r/GasPumpsUseCase_Simulation-24B0/GasPumpsUseCase_Simulation.ipynb.

7.1.2 Results

After constructing the simulation, we conducted three experiments to: 1) evaluate the effectiveness of the method in detecting fraudulent gas pumps; 2) measure the impact of user adoption on fraud detection; and 3) assess the efficiency threshold of the method by varying the number of gas pumps classified as fraudulent. The experiments are detailed as follows.

In the first experiment, we assessed the ability of the proposed method to detect fraudulent gas pumps. The test focused on observing variations in the outcomes by systematically altering the scenario parameters. We chose to vary

the volumetric fuel deficit and gas pump shortfall parameters, based on the estimates shown in the previous section. The estimates point to a fuel deficit of 3% and a gas pump shortfall of 10%, but we also questioned whether the method could detect fraud of lower values. Due to the method being based on statistical discrepancies, smaller shortfalls tend to be more difficult to detect. So, we varied the fuel deficit to values of 1% and 3%, and the gas pump shortfall to values of 3%, 5%, and 10%. Additionally, we assume levels of user adoption of 1%, 5%, and 10%, which we estimated to be reasonable values in the real scenario.

By varying these parameters, we observed the effects on the accuracy and precision of detecting fraudulent gas pumps. Accuracy tells us how many fraudulent gas pumps were detected, while precision tells us how well the method correctly classifies the gas pumps as either fraudulent or non-fraudulent. In practice, precision is not only about detecting fraudulent gas pumps but also avoiding the false accusation of legitimate gas pumps as fraudulent. For example, an accuracy of 60% means that 60% of all gas pumps were classified correctly. By contrast, a precision of 60% means that, among the gas pumps identified as *possibly* fraudulent, only 60% are actually fraudulent, while the remaining 40% have been incorrectly classified as such.

With this approach, we could obtain a comprehensive understanding of how different degrees of shortfalls and user engagement impact the method's effectiveness in identifying fraudulent activities within the gas pump's refuel process. To assess this effectiveness, it is necessary to compare the results against the baseline of random selection (i.e., randomly inferring which gas pumps are fraudulent). For example, in the scenario with a fuel deficit of 1% and a gas pump shortfall of 3%, 33.3% of the gas pumps are fraudulent. Therefore, randomly selecting gas pumps would result in an accuracy of 33.3%. Table 5 shows the results. The scenario with a fuel deficit of 3% and a gas pump shortfall of 3% is not valid because it would require all gas pumps to be fraudulent to achieve the total deficit. Therefore, the line representing this scenario is indicated with a dashed mark in the table.

In all scenarios, the accuracy of the method overcomes the baseline. However, we observed some noteworthy points. The smaller the gas pump shortfall, the smaller the accuracy. This occurs because the fraudulent gas pumps are less discrepant and, therefore, more difficult to detect. Conversely, scenarios with a higher number of fraudulent gas pumps achieve the greatest precision values. That indicates that the

Table 5. Fraud Detection Outcomes Across Potential Scenarios.

Fuel Deficit	Gas Pump Shortfall	Accuracy	Adoption 1%		Adoption 5%		Adoption 10%	
		Baseline	Acc.	Prec.	Acc.	Prec.	Acc.	Prec.
1%	3%	33.3%	61.3%	41.9%	68.2%	52.3%	72.5%	58.7%
	5%	20.0%	73.9%	34.7%	80.9%	52.3%	84.8%	62.0%
	10%	10.0%	87.2%	36.0%	92.6%	63.2%	94.6%	73.1%
3%	3%	-	-	-	-	-	-	-
	5%	60.0%	62.5%	68.8%	73.2%	77.7%	78.8%	82.3%
	10%	30.0%	73.0%	55.1%	84.6%	74.3%	89.0%	81.6%

quantity of fraudulent gas pumps does not pose a challenge to the method.

As expected, higher user adoption leads to greater accuracy and precision. That occurs because more data are available to support the analysis. Nevertheless, we went further to explore the effects of varying adoption levels in the next experiment.

In the second experiment, we systematically adjusted the adoption level from 0.1% to 100% and measured the accuracy and precision. The aim was to observe how increasing user participation impacts the efficacy of the fraud detection system. We chose the scenario with a fuel deficit of 3% and a gas pump shortfall of 10% because they are potentially closer to the real-world scenario. The results are shown in Figure 3. At an adoption level of 0.1%, accuracy begins at 62.9%, while precision starts at 37.81%.

Analyzing the results, we observed that an adoption level of just 1% allowed us to achieve a precision rate exceeding 50%, but more surprisingly, it reached an accuracy of over 73%, which is more than 40% higher than the accuracy baseline. This level of participation underscores a guideline for achieving good effectiveness for the system.

The progression of the adoption implies a rapid improvement in the accuracy and precision initially, particularly noticeable as adoption percentages rise from 1% to around 20%. This reflects substantial gains in the method's ability to detect and correctly classify fraudulent pumps as more data become available.

Following this rapid growth phase, the increase in accuracy and precision rates begins to plateau, progressing more slowly and gradually as it nears 100%. This trend suggests diminishing returns on detection effectiveness improvements, highlighting that while higher levels of user participation continue to enhance system capabilities, the most significant leaps in effectiveness are achieved relatively early in the adoption spectrum.

Finally, in the third experiment, we aimed to determine the threshold of the method's effectiveness by varying the number of gas pumps classified as fraudulent. After evaluating the gas pumps, the method generates a ranking based on their ratings, where gas pumps with the lowest scores are the most likely to be fraudulent. The method uses a cutoff point to classify the gas pumps as fraudulent. This cutoff is estimated based on the fuel deficit and gas pump shortfall. For example, in the scenario with a fuel deficit of 3% and a gas pump shortfall of 10%, it is estimated that 30% of the gas pumps are fraudulent. We refer to the percentage of this cutoff as the positivity parameter. When the number of gas pumps classified as fraudulent is equal to the method's esti-

mate, we say the positivity is 100%.

However, we questioned whether it would be possible to achieve better results by adjusting this parameter. Thus, we varied the positivity parameter in one of the previous scenarios. We chose the scenario with a fuel deficit of 1%, a gas pump shortfall of 3%, and an Adoption level of 1%, which previously yielded low outcome metrics. Figure 4 shows the result.

We analyze both graphs, focusing on values from 100% downward along the x-axis. As positivity percentages decreased from 100% to 30%, we observed a clear increase in both accuracy and precision. This trajectory highlights that with a lower cutoff for classification, it is more certain that a gas pump classified as fraudulent is indeed fraudulent. Additionally, as the cutoff decreases, fewer non-fraudulent gas pumps are mistakenly classified as fraudulent, but also fewer fraudulent gas pumps are detected. This underlines the necessity of finding a reasonable compromise between the number of pumps detected and maintaining high precision to ensure the reliability of the fraud detection system.

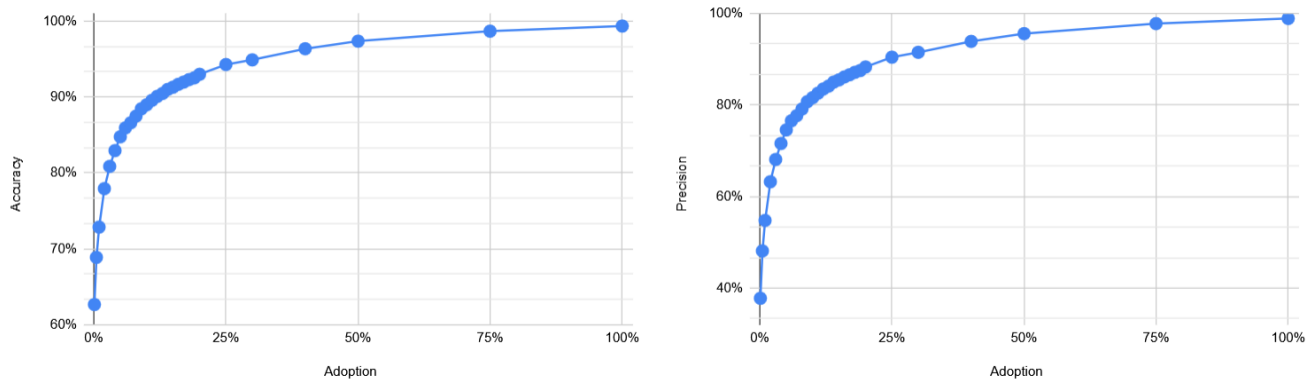
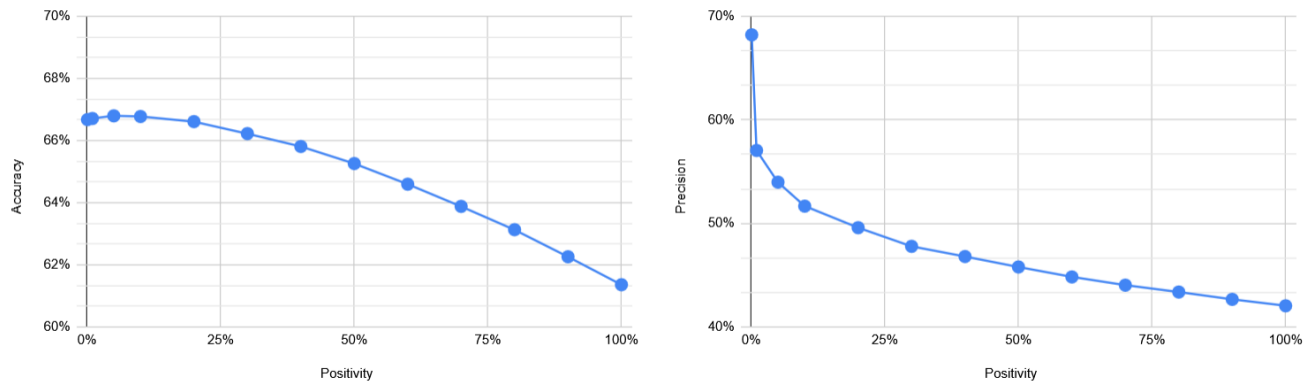
7.2 Blockchain implementation

To evaluate our blockchain infrastructure, we conducted a series of experiments using Hyperledger Caliper¹¹, a benchmark tool designed to measure the performance of blockchain solutions. Our objective was to assess performance metrics while executing key operational functions, such as records creation, evaluations, and queries.

We configured Hyperledger Caliper to run four simultaneous processes distributed across eight CPU cores. In the experiment, we executed multiple rounds, with each round performing a different chaincode functionality. The parameters for each round were set to simulate peak and intensive operational conditions. For measuring purposes, we use 1,000 transactions across 10 rounds to record gas pumps and vehicles, 10,000 across 10 rounds for refueling records, and 100 transactions across 10 rounds to execute gas pump evaluations and query operations. Table 6 shows the results.

Gas Pump and Vehicle records functions are triggered only once for each entity, as each gas pump and vehicle has a single record on the chaincode. A Refuel record, however, is triggered every time a refueling event occurs, or at least when the user has adopted the system. Both record tests achieved a throughput of over 300 transactions per second, while the Gas Pump and Vehicle records required no more than 200 milliseconds on average latency. The Refuel record exhib-

¹¹<https://www.hyperledger.org/projects/caliper>

Figure 3. Effects on accuracy and precision as adoption increases in the scenario with a fuel deficit of 3% and a gas pump shortfall of 10%.**Figure 4.** Effects on accuracy and precision as positivity decreases.**Table 6.** Performance measurement of the chaincode functions on the blockchain network with Caliper.

Test Name	Average Latency (s)	Throughput (TPS)
Gas Pump record	0.13	319.74
Vehicle record	0.19	330.91
Refuel record	4.72	318.28
Gas Pump evaluation	1.883	28.57
Query	0.01	937.94

ited the highest average latency, at nearly 5 seconds. However, this is not a bottleneck when we consider that a gas refuel operation typically takes approximately five minutes, including vehicle parking and payment.

For the Gas Pump evaluation test, which involves generating the ranking of gas pumps, the results showed a relatively low throughput. However, this operation need not be run immediately after users refuel their cars. For example, conducting it once a week is sufficient to ensure that every gas pump in the system is adequately assessed. Finally, for the Query functions, there is no predicted demand, and they do not interfere with the system's operation. Despite this, they exhibit the best throughput and latency metrics because they are read-only operations.

8 Discussion

We now discuss some key aspects of our system, such as how data was obtained, handled, stored, and processed, as well as the results achieved using the fraud detection method.

In the context of obtaining data, some methods have been considered for collecting and transmitting information from gas pumps. One of the approaches involves embedding a software module directly into the gas pump control system, which would automatically collect and transmit data of all refueling events to the blockchain. This method offers the advantage of full automation and complete data coverage, as every refueling event would be recorded. However, this implementation would require cooperation from both regulatory agencies and gas pump manufacturers.

A more feasible approach might involve consumer-driven data collection. By utilizing a mobile application, consumers could collect and transmit refuel transaction data to the blockchain themselves. This method would facilitate data collection and also allow consumers to complement the information with additional details, such as the vehicle's odometer reading and model, which are useful for fuel quality analysis. An advanced evolution of this approach could involve integrating the data collection process directly with the vehicle. The vehicle could automatically detect when a refueling occurs and then collect and transmit the data to the blockchain. This could be done with an interoperable module, similar to that proposed by de Araújo Sousa *et al.* [2021], installed by the vehicle owner. This method would also ensure complete

data coverage, at least for users who adopted the system, as every refueling event would be recorded once the equipment is installed in the vehicle.

An important consideration when obtaining data and inserting them into the blockchain is the oracle problem. Traditional blockchains, such as Hyperledger Fabric, Bitcoin, and Ethereum blockchains, exhibit passive behavior. This means that they cannot retrieve external data by themselves. An active external agent is always required to provide the data that will be recorded on the blockchain. These agents are known as blockchain oracles. Caldarelli [2020], however, cautions about the centralization that can occur with the introduction of these agents, as well as the risk of data tampering and manipulation.

In our case, two approaches were used to mitigate this issue. The first approach is based on digital certification. For instance, in the case of Brazilian gas pumps, data are digitally signed to ensure their integrity and authenticity. Once data are recorded on the blockchain, all parties involved can verify that it has not been modified. However, this method is centralized, as it relies on trustworthy certification authorities. Furthermore, not all countries have regulations for measuring instruments that include digital certification.

The second approach, however, is entirely decentralized and does not depend on the specificities of the scenario. This approach involves cross-referencing data from users. The method of fraud detection is based on statistical metrics and, therefore, does not rely on isolated values but rather on their aggregate. During the experiments, the interquartile range method was employed to detect and eliminate counterfeited data, whether added intentionally or not. Data of this nature were introduced into the simulation, and the method successfully identified them with an accuracy of over 90% in all cases. Moreover, even after removing outlier data, due to the fraud detection method being based on average values, it is resilient to isolated instances of counterfeit data.

Given that we are utilizing blockchain technology, we need to incentivize stakeholders to engage with the system. On one hand, regulatory agencies might prefer traditional centralized databases due to their lower cost and greater control. On the other hand, gas station owners may face a conflict of interest, whereas full transparency could help honest retailers distinguish themselves as reliable, it could disadvantage those engaged in fraudulent activities. To address this, we proposed a streamlined ledger architecture aimed at minimizing costs while preserving the benefits of blockchain technology. The primary entities interested in maintaining a peer within our ledger are likely to be regulatory agencies and involved companies, such as fuel retailers. These stakeholders require a high degree of confidence in the integrity of refueling service within the market or under their brand.

With reduced data requirements and a limited number of peers, storage, and distribution challenges are minimized. Additionally, we recognize that end-users might have an interest in maintaining a node within the blockchain network. This prospect underscores the importance of keeping the ledger lean and efficient.

To encourage end-user participation, the system was designed to require minimal computational resources. A basic AWS EC2 instance can effectively handle the storage and

validation tasks required for peers. A configuration with 2 CPUs, 2 GB of RAM, and a stable network connection, utilizing Elastic Block Store for storage, is sufficient for those interested in contributing to the ledger. The cost of maintaining this instance in South America is approximately \$35 per month,¹² but may be lower if users opt for EC2 on-demand. These values were collected in August 2024.

Based on our research, we estimate that over 4 billion refueling events occur annually in Brazil. Given our system's capability to handle 318 TPS for refueling recording, it can theoretically support over 10 billion transactions per year, assuming continuous operation. This capacity significantly exceeds current market demands.

However, we must consider the system's capacity during peak hours. Under normal conditions, each refuel transaction takes approximately five minutes. In the same interval, the system can manage around 100,000 refuel transactions. In a worst-case scenario, where all gas pumps operate simultaneously, the system could face up to half a million refuels within the same five-minute window. If 10% of users adopt the system, they would utilize 50% of the system's capacity.

Although improbable, to mitigate a potential bottleneck, we propose modifying the endorsement policy to distribute transaction validation across a subset of peers. This strategy would preserve the system's trust and integrity while significantly increasing its transaction-processing capacity. Additionally, implementing a load-balancing mechanism could further improve the system's ability to manage high transaction volumes effectively.

In the context of gas pump evaluation, our system operates at a lower throughput due to the complexity of the evaluation method, which requires ratings from every vehicle that has used the gas pump. A throughput of 28 evaluations per second is considered sufficient, as real-time updates of the rankings are not required. By scheduling these evaluations during off-peak hours, we can maintain system performance and keep the gas pump ranking up-to-date without overloading the system's resources. Considering the potential scenario of a half million gas pumps, the system would require approximately five hours to complete all evaluations. To optimize hardware utilization, gas pumps could be grouped into six clusters, with each group scheduled for evaluation sequentially on different days during less busy hours, such as 4 A.M. With this approach, we guarantee that every gas pump is evaluated weekly.

Finally, the results of the method evaluation showed an accuracy of nearly 90% in detecting fraud in the estimated Brazilian scenario, covering both volumetric fraud and fuel tampering. However, the method not only classifies the gas pumps as potentially fraudulent but also generates a ranking based on their evaluations, which we believe is the most valuable outcome. We envision two primary uses for this ranking. First, regulatory agencies can use it to support active surveillance, focusing on gas pumps that are more likely to be fraudulent. And second, a more valuable approach is the use of the gas pump ranking to advise users about suspicious gas pumps. This can automatically incentivize gas pump owners

¹²AWS EC2 price calculator: <https://calculator.aws/#/estimate?id=67e346698ddcf51f98f6719f529ed669579754ef>

to comply with the regulations and maintain their gas pumps in optimal conditions.

9 Conclusions & Future work

In this work, we propose the integration between metrology and blockchain, intending to add value to data obtained from measuring instruments. The role of the blockchain is to allow user communities to share their data to achieve improved service quality. By cross-referencing user data, we propose to apply statistical methods to detect metrological frauds. In this way, the aim is to conduct more active and less intrusive inspections, with reduced dependence on regulatory agencies. The method was applied to the gas pump use case, a metrological application subject to persistent fraud. Using this technique, we can consistently detect volumetric fraud and assess fuel quality. Although we have presented a Brazilian use case, the method can be applied to any scenario, even if the instruments lack connectivity. Finally, we address the oracle problem by assigning the trust to the statistical methods used.

In future work, we plan to advance the practical implementation for obtaining data from measuring instruments. This includes exploring possibilities to obtain some data independently of users, such as through devices embedded in the measuring instruments that send the data directly to the blockchain. Furthermore, we aim to explore the method to mitigate fraud in other metrological applications using blockchain, such as energy meters.

Declarations

Acknowledgements

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001. Also, the study had the support of Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro).

Authors' Contributions

All authors contributed equally to the development of the work. All authors read and approved the final manuscript.

Competing interests

The authors declare no conflicts of interest.

Availability of data and materials

The code that generates the simulation and evaluates the method is available at: <https://github.com/GabrielEstevam/ArtigoBMCs>.

Acronyms

AES Advanced Encryption Standard.

CPS Cyber-Physical Systems.

FDI False Data Injection.

Inmetro Instituto Nacional de Metrologia, Qualidade e Tecnologia.

IoT Internet of Things.

MI Measuring Infrastructure.

PoS Proof of Stake.

PoW Proof of Work.

QKD Quantum Key Distribution.

References

- Alsunaidi, S. J. and Alhaidari, F. A. (2019). A survey of consensus algorithms for blockchain technology. In *2019 International Conference on Computer and Information Sciences (ICCIS)*, pages 1–6, Sakaka, Saudi Arabia. IEEE. DOI: 10.1109/iccisci.2019.8716424.
- ASMETRO-SI (2024). Inmetro inaugura a geração de objetos metrológicos 4.0. Available at: <https://asmetro.org.br/portalsn/2023/02/28/inmetro-inaugura-a-geracao-de-objetos-metrologicos-4-0/>. Accessed 6 January 2024.
- Caldarelli, G. (2020). Understanding the blockchain oracle problem: A call for action. *Information*, 11(11). DOI: 10.3390/info11110509.
- Christidis, K. and Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303. DOI: 10.1109/ACCESS.2016.2566339.
- Correio Braziliense (2021). Inmetro lançará certificação digital para evitar fraude em bombas de combustíveis. Available on: <https://www.correiobraziliense.com.br/economia/2021/06/4929848-inmetro-lancara-certificacao-digital-para-evitar-fraude-em-bombas-de-combustiveis.html>. Accessed 29 September 2024.
- de Araújo Sousa, L. E., Stopiglia, F. S., de Mello Filho, L. V. F., Guimarães, D. H. P., and de Moraes Gomes Rosa, M. T. (2021). Prototype proposal for control and inspection of gas stations. In Iano, Y., Arthur, R., Saotome, O., Kemper, G., and Borges Monteiro, A. C., editors, *Proceedings of the 5th Brazilian Technology Symposium*, pages 357–366, Cham. Springer International Publishing. DOI: 10.1007/978-3-030-57566-3_35.
- Estadão (2024). Brasil bate recorde de venda de combustível em 2021, puxado por diesel e gasolina. Available at: <https://www.infomoney.com.br/minhas-financas/brasil-bate-recorde-de-venda-de-combustivel-em-2021-puxado-por-diesel-e-gasolina/>. Accessed 6 January 2024.
- Fanton, Jean-Pierre (2019). A brief history of metrology: past, present, and future. *Int. J. Metrol. Qual. Eng.*, 10:5. DOI: 10.1051/ijmqe/2019005.
- Índio, C. (2021). Ex-vereador é preso em esquema de desvio de combustíveis no rio. Available at: <https://agenciabrasil.ebc.com.br/geral/noticia/2021-01/ex-vereador-e-preso-em>

- esquema-de-desvio-de-combustiveis-no-rio. Accessed 29 September 2024.
- Inmetro (2020). Definição de instrumentos de medição. Available at: <https://www.gov.br/inmetro/pt-br/assuntos/vigilancia-de-mercado/fiscalizaveis/instrumentos-de-medicao>. Accessed 29 May 2024.
- Inmetro (2021). Operação petróleo real: órgãos delegados do inmetro em todo país saem em campo para combater fraudes em bombas de combustíveis. Available at: <https://www.gov.br/inmetro/pt-br/centrais-de-conteudo/noticias/operacao-petroleo-real-orgaos-delegados-do-inmetro-em-todo-pais-saem-em-campo-fiscalizando-bombas-de-combustiveis-para-combater-fraudes>. Accessed 29 September 2024.
- Inmetro (2022). Portaria nº 227, de 26 de maio de 2022. Available at: https://www.ipem.pr.gov.br/sites/default/arquivos_restritos/files/documento/2022-06/portaria_227_26_05_2022_bombas_medidoras_nova_julho_2022.pdf. Accessed 27 July 2024.
- Inmetro (2024a). Metrologia legal - definição e objetivo. Available at: <http://inmetro.gov.br/metlegal/definicao.asp>. Accessed 13 May 2024.
- Inmetro (2024b). Portaria nº 264. Available at: <http://www.inmetro.gov.br/legislacao/rtac/pdf/RTAC002778.pdf>. Accessed 5 January 2024.
- Inmetro (2024c). Protocolo de comunicação serial para verificação de integridade de software em instrumentos de medição. Available at: <http://www.inmetro.gov.br/metlegal/docDisponiveis.asp>. Accessed 1 May 2024.
- Khan, J. Y. and Yuce, M. R. (2019). *Internet of Things (IoT): Systems and Applications*. Jenny Stanford. Book.
- Kitchenham, B. and Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. 2. Available at: https://www.researchgate.net/profile/Barbara-Kitchenham/publication/302924724_Guidelines_for_performing_Systematic_Literature_Reviews_in_Software_Engineering/links/61712932766c4a211c03a6f7/Guidelines-for-performing-Systematic-Literature-Reviews-in-Software-Engineering.pdf.
- Melo, W. S., Tarelho, L. V., Rodrigues, B. A., Bessani, A. N., and Carmo, L. F. (2021). Field surveillance of fuel dispensers using iot-based metering and blockchains. *Journal of Network and Computer Applications*, 175:102914. DOI: 10.1016/j.jnca.2020.102914.
- Melo Junior, W., Bessani, A., Neves, N., Santin, A., and Carmo, L. (2019). Using blockchains to implement distributed measuring systems. *IEEE Transactions on Instrumentation and Measurement*, 68:1503–1514. DOI: 10.1109/TIM.2019.2898013.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Available on: <https://bitcoin.org/bitcoin.pdf>. Accessed 29 May 2024.
- Oyama, J. □. (2019). Chip para fraudar abastecimento em posto é acionado por controle remoto. Available at: <https://sindcomb.org.br/2019/10/25/chip-para-fraudar-abastecimento-em-posto-e-acionado-por-controle-remoto/>. Accessed 23 May 2025.
- Peduzzi, P. (2021). Celulares podem ajudar no combate a fraudes em bombas de combustíveis. Available on: <https://agenciabrasil.ebc.com.br/economia/noticia/2021-04/celulares-podem-ajudar-no-combate-fraudes-em-bombas-de-combustiveis>. Accessed 29 September 2024.
- Peters, D., Yurchenko, A., Melo Junior, W., Shirono, K., Usuda, T., Seifert, J.-P., and Thiel, F. (2020). *IT Security for Measuring Instruments: Confidential Checking of Software Functionality*, pages 701–720. DOI: 10.1007/978-3-030-39445-5_1.
- Reijsbergen, D., Maw, A., Dinh, T. T. A., Li, W.-T., and Yuen, C. (2022). Securing smart grids through an incentive mechanism for blockchain-based data sharing. DOI: 10.1145/3508398.3511504.
- Rodrigues Filho, B. A. and Gonçalves, R. F. (2015). Legal metrology, the economy and society: A systematic literature review. *Measurement*, 69:155–163. DOI: 10.1016/j.measurement.2015.03.028.
- Singh, J., Sinha, A., Goli, P., Subramanian, V., Shukla, S., and Vyas, O. (2022). Insider attack mitigation in a smart metering infrastructure using reputation score and blockchain technology. *International Journal of Information Security*, 21. DOI: 10.1007/s10207-021-00561-8.
- Singh, Y., Datta, A., Shandilya, S., and Shandilya, S. K. (2023). Securing advanced metering infrastructure using blockchain for effective energy trading. pages 27–38. DOI: 10.1007/978-3-031-34222-6_3.
- Singhal, D., Ahuja, L., and Seth, D. A. (2023). Posmeter: proof-of-stake blockchain for enhanced smart meter data security. *International Journal of Information Technology*. DOI: 10.1007/s41870-023-01653-5.
- Tahir Bokhari, S., Bakhshi, T., Aftab, T., and Nadir, I. (2019). Exploring blockchain-secured data validation in smart meter readings. DOI: 10.1109/INMIC48123.2019.9022772.
- Tripathy, B. K. and Anuradha, J. (2018). *Internet of Things (IoT): Technologies, Applications, Challenges, and Solutions*. CRC Press. Book.
- Xu, X. et al. (2017). A taxonomy of blockchain-based systems for architecture design. In *2017 IEEE International Conference on Software Architecture (ICSA)*, pages 243–252, Gothenburg, Sweden. IEEE. DOI: 10.1109/icsa.2017.33.