Journal of Network and Computer Applications 175 (2021) 102914

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Field surveillance of fuel dispensers using IoT-based metering and blockchains

Wilson S. Melo Jr. [a,*], Luiz V.G. Tarelho [a], Bruno A. Rodrigues Filho [a], Alysson N. Bessani [b], Luiz F.R.C. Carmo [a,c]

[a] National Institute of Metrology, Quality and Technology, Rio de Janeiro, Brazil
[b] LaSIGE, Faculdade de Ciências, Universidade de Lisboa, Lisboa, Portugal
[c] Federal University of Rio de Janeiro, Brazil

ARTICLE INFO

Keywords:
IoT-based metering
Blockchains
Legal metrology
Field surveillance

ABSTRACT

The field surveillance of fuel dispensers is an activity of Legal Metrology that checks these measuring instruments' correct behavior. However, it constitutes a complex challenge because malicious entities can tamper with fuel dispensers to get undue economic advantages. This paper proposes a distributed and decentralized solution. We use IoT-based vehicle simple meters to estimate the fuel amount in refilling events. Although these estimates can be inaccurate, we explore properties of the Law of the Large Numbers to evaluate the fuel dispenser's accuracy. We also use blockchains to avoid collusion attacks and provide a truly distributed and decentralized surveillance solution that implements statistical surveillance analysis as smart contracts. We develop a case study based on the vehicular fleet and fuel dispensers in São Paulo, Brazil. We perform our experiment using the Hyperledger Fabric platform with Byzantine fault-tolerant consensus. In a hypothetical scenario where vehicular meters present error rates below 5%, and each vehicle refuels more than ten times on average, we can identify tampered fuel dispensers with sensitivity and specificity over 95%. We also demonstrate that our blockchain deployment can support a workload of 600 concurrent clients with a throughput higher than 350 tps and latency lower than 1 s. These results attest to our framework suitability in terms of accuracy and performance. They provide promising perspectives on using our idea in the metrological surveillance of other measuring instruments.

1. Introduction

Fuel dispensers (or fuel/petrol pumps) are measuring instruments which play a crucial role in the trading of fuel as a consumable good. In most places in the world, fuel stations and consumers trade fuel based on measurements from fuel dispensers. The transaction relies on the assumption that the fuel dispenser is a precise, accurate, and reliable measuring instrument. Directives promoted by regulatory agencies and metrological supervision activities introduced by Legal Metrology are often employed for assuring this assumption (Rodrigues Filho and Gonçalves, 2015). However, evidence indicates that frauds against fuel dispensers are a growing and widespread practice, especially in developing countries (Beteto et al., 2016; Luchsinger et al., 2008; Leitão et al., 2014; Narwade and Patil, 2016; Rodrigues Filho and Gonçalves, 2016). One of the most common frauds is known as *low pump*, and it occurs when the fuel dispenser delivers a fuel amount lower than the informed to the consumer (Beteto et al., 2016). Leitão et al. (2014) present empirical evidence that these frauds result in a measuring error of 6%–8% of the correct fuel amount. Narwade and Patil (2016) corroborate these findings on estimating than 8% of the fuel sold in India is adulterated. Moreover, Rodrigues Filho and Gonçalves (2016) report that, in Brazil alone, frauds related to fuel dispensers result in economic losses in the order of USD 300 million per year.

The main problem associated with these frauds is the difficulty in proceeding with metrological supervision activities, in particular, *field surveillance* (Joint Committee For Guide, 2012). Although Legal Metrology usually designates notified bodies for inspecting fuel dispensers, this action is not sufficient (Melo et al., 2019). The high number

* Corresponding author.
E-mail addresses: wsjunior@inmetro.gov.br, wsmelojunior@gmail.com (W.S. Melo), lvtarelho@inmetro.gov.br (L.V.G. Tarelho), bafilho@inmetro.gov.br (B.A. Rodrigues), anbessani@di.ul.pt (A.N. Bessani), lfrust@inmetro.gov.br (L.F.R.C. Carmo).
URL: https://www.di.fc.ul.pt/%7Ebessani (A.N. Bessani).

https://doi.org/10.1016/j.jnca.2020.102914
Received 19 June 2020; Received in revised form 11 September 2020; Accepted 14 November 2020
Available online 28 November 2020
1084-8045/© 2020 Elsevier Ltd. All rights reserved.

of instruments spread over extensive geographic areas constitutes a challenge in logistics and inspection costs. Also, many frauds employ sophisticated mechanisms that explore electronics and software features of the instrument (Leitão et al., 2014). These mechanisms can be activated and deactivated remotely, making fraudulent behavior stealthy and hard to detect. Although there are several entities interested in solutions against such cheating (e.g., honest fuel station owners, fuel manufacturers, regulation agencies, and civil representatives) (Beteto et al., 2016; Oppermann et al., 2018), these frauds are very profitable (Rodrigues Filho and Gonçalves, 2016). That increases the chance of collusion among dishonest fuel vendors and corrupted entities which should expose this fraudulent practice.

We understand that the challenge of making fuel dispensers' field surveillance efficient demands the use of new technologies and innovative ideas (Oppermann et al., 2018; Peters et al., 2018; Rodrigues Filho and Gonçalves, 2016). Firstly, we need a solution to gather measuring information freely, without the need of waiting for notified bodies' actions. As an initial step, we can conceive a fuel dispenser as a *smart fuel meter*, i.e., an Internet of Things (IoT) device. Metering is already one of the leading applications related to IoT solutions (Kassab and Darabkh, 2020), because smart meters can easily integrate features such as sensing (i.e., perception) and communication (i.e., network and data transmission) (Sandrić and Jurčević, 2018; Thiel, 2018). However, a smart fuel dispenser is useless if we cannot trust its information. Thus we could use other IoT devices to "estimate" and confirm the provided fuel measurements. In practice, these "secondary" meters would implement a type of *online field surveillance*. Finally, we need to store information in a reliable, immutable data repository. On doing that, we assure we can audit, evaluate, and validate any measurement from a fuel dispenser. Although a centralized data store solution could meet these technical requirements, the possibility of collusion among dishonest parties indicates that we do not have a trusted third party. The fraud profitability incentives dishonest entities to offer bribes and undue advantages in attacks to get the control of a centralized solution. In this scenario, we glimpse that distributed ledger technologies can play a vital role in providing secure storage, high availability, and mainly protection against collusion frauds (Dai et al., 2019; Makhdoom et al., 2019; Zheng et al., 2017).

In this paper, we propose an IoT-based distributed and decentralized solution to improve fuel dispensers' field surveillance. Our idea consists of using IoT-based vehicular fuel meters that perform additional fuel measuring in each refuel event, and make this information available in a distributed data storage. Besides, we propose the use of permissioned blockchains (Vukolić, 2017; Xiao et al., 2020; Zheng et al., 2017) to store information. Blockchain is a distributed append-only data structure that assures information integrity by consensus among its participants, while automatizes workflows by implementing self-executable code (i.e., smart contracts) (Christidis and Devetsikiotis, 2016). Since we have different stakeholders interested in preventing frauds in fuel dispensers, their effort in maintaining a blockchain for metrological surveillance constitutes a robust solution against collusion attacks. The following research questions guided our efforts in this work:

- **Q1:** Is it feasible to perform the field surveillance of fuel dispensers without depending on inspections done by notified bodies?
- **Q2:** Can we implement effective field surveillance strategies from information provided by simple IoT fuel meters installed in vehicles?
- **Q3:** Does blockchain constitute a suitable solution against collusion attacks which are common in frauds related to fuel measurement?

The main contributions of this paper are the following:

- We present an *IoT-based strategy* to perform the field surveillance of fuel dispensers using simple, smart fuel meters whose measurement uncertainty is unknown. We propose a statistical approach based on the *Law of Large Numbers* (LLN) (Evans and Rosenthal, 2004) to deal with the fuel meters *measurement uncertainty*. This result is significant and has several applications in the Legal Metrology field. We also discuss the available technologies for obtaining fuel measurements from a vehicle's tank in refueling events.
- We propose a blockchain-based *Distributed and Decentralized Surveillance Framework* where drivers can contribute to field surveillance actively and spontaneously (Section 3). The blockchain poses as a suitable alternative because it offers natural protection against collusion attacks.
- We implement a *case study* that instantiates our framework to meet the demand from fuel dispensers surveillance in São Paulo state, Brazil. We use the *HyperLedger Fabric* (Androulaki et al., 2018) blockchain platform to store measurements from fuel dispensers and vehicles. We also implement a statistical surveillance strategy using smart contracts. Finally, we present an experiment that evaluates our strategy efficiency and performance.

This paper is organized as follows. After this Introduction, Section 2 presents elementary concepts and related works. Section 3 describes our framework proposal and its component's details. Section 4 discuss security issues, presenting an attack model and the respective countermeasures. Section 5 brings a case study that demonstrates practical aspects of our proposal. Section 6 presents complementary discussions about advantages, drawbacks and limitations. Section 7 presents the conclusion of our work.

2. Preliminaries

2.1. Legal metrology

Legal Metrology is responsible for the control of measuring instruments that impact both the economy and society (Rodrigues Filho and Gonçalves, 2015). In practice, it acts as a third-party assessor to make a measurement reliable. One can describe the levels of control in Legal Metrology as (VIM, 2012):

1. Legal control of measuring instruments, which comprises type approval and both initial and subsequent verification of devices used on the market;
2. Metrological supervision, which are activities aiming to check the accordance of devices to metrology laws and regulations, and includes market and field surveillance;
3. The operations comprising examination and demonstration of conformity to a court for legal penalties, previously known as metrological expertise.

Despite the levels of control in Legal Metrology, measuring instruments are always subject to metrological frauds. In these situations, a dishonest seller can intentionally influence the instrument performance, impacting on its accuracy due to a component of uncertainty against the buyer. In the fuel market, a simulation showed that for a 10% volume fraud and 1% fraudulent devices on the market, the economic losses are represented by approximately USD 300 million per year (Rodrigues Filho and Gonçalves, 2016). Frauds also imply an unfair competition to the honest seller that does not use fraudulent procedures.

2.2. IoT-based technologies for fuel measurement

2.2.1. How modern fuel dispensers work

An electronic fuel dispenser pumps the fuel from an underground tank passing into a measurement transducer, responsible for the measurement, throughout the nozzle, under the control of a solenoid valve, to the car tank (Leitão et al., 2014; Luchsinger et al., 2008). The measurement transducer consists of a mechanical axis integrated into a *pulser*, which converts the movement of the axis in electronic pulses. Consequently, the number of pulses is proportional to the measured

volume. Fig. 1 shows a typical fuel dispenser measurement transducer.

Under normal circumstances, fuel dispensers are very precise and accurate measuring instruments. Some fuel dispenser models also include features to increase information security (e.g., pulsers can provide the measurement's digital signature) (Melo et al., 2020). Besides, fuel dispensers also present a high automation level. They commonly integrate with payment or data gathering systems (Beteto et al., 2016). Due to their embedded technologies, modern fuel dispensers are in practice fuel smart meters, and we can classify them as IoT devices.

Fuel dispensers are subject to subsequent verification, i.e., they are periodically tested and compared to volume standards by applying procedures based on general recommendations (OIML, 2007; VIM, 2012). They are also subject to metrological *field surveillance*. The equipment is tested randomly in the field, and notified bodies check its compliance with legal requirements. According to the International Organization of Legal Metrology (OIML, 2007), the test of accuracy comprises testing the instrument in different flow rates using a standard capacity measure. For example, in Brazil, tests follow the recommendation of using a 20 L standard, and the maximum permissible error is 0.5%, for both maximum and minimum flow rate. Devices that do not fulfill the requirements are rejected and shall be removed from use. In Mexico, notified bodies adopt the same maximum permissible error of 0.5% in field surveillance, although other processes (e.g., type approval) can demand error rates no higher than 0.25% (Luchsinger et al., 2008).

2.2.2. *Measuring fuel in vehicles*

Vehicles' fuel amount estimate is an essential requirement in different applications. We find examples in telemetry, driver evaluation, fleet monitoring, and fuel theft prevention, among others (Ahmed et al., 2017; Massoud et al., 2019; Obikoya, 2014; Patil et al., 2017; Skog and Handel, 2014). Table 1 summarizes a comparison among some relevant works in terms of application, sensing technology, connectivity, and metrological accuracy.

In the majority of countries, vehicles must exhibit fuel measurement to the driver. The main reason is for preventing drivers from running out of fuel. Vehicles do that by using different instruments, from simple analogic fuel gauges to modern digital displays embedded in the vehicle's panel. Besides, vehicles' fuel amount estimates can be helpful to implement more sophisticated features. Different IoT applications can easily integrate vehicle's fuel meters to improve engine performance (Skog and Handel, 2014), guide drivers in best conduction practices (Massoud et al., 2019), or remotely monitor a vehicular fleet (Ahmed et al., 2017; Obikoya, 2014; Sheth and Rupani, 2020).

Level sensors are the most common technology behind vehicles' fuel meters (Obikoya, 2014). There are also more sophisticated instruments that use non-intrusive technologies like ultrasonic sensors (Ahmed et al., 2017; Patil et al., 2017). Some hybrid strategies can combine different sensors to estimate fuel amount, e.g., level and ultrasonic sensors (Patil et al., 2017), or even pressure ("etape") sensors (Ahmed et al., 2017). In industry, the decision about which technology to use is usually price oriented. Most of the time, vehicle manufacturers do not specify precise or accurate embedded sensors in their projects. Recent works proposing low-cost vehicles' fuel meters report measuring errors usually lower than 5% (Ahmed et al., 2017; Obikoya, 2014; Patil et al., 2017).

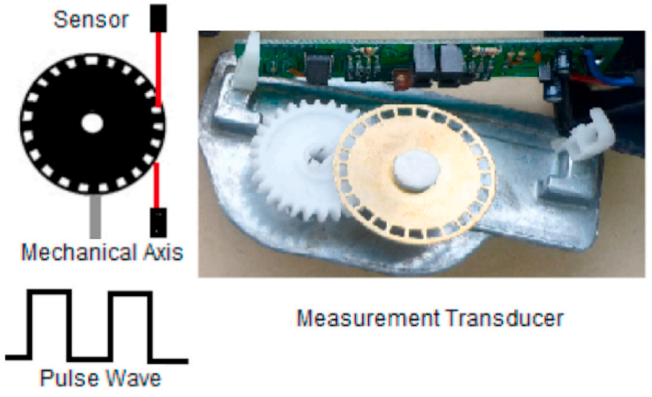

Fig. 1. Principle of a measurement transducer and a real device, adapted from Leitão et al. (2014).

Table 1
Comparison among works related to technologies to estimate the fuel amount in vehicle's tanks.

	Application	Technology	Connectivity	Error
Ahmed et al. (Ahmed et al., 2017)	Prevent fuel stolen from tower sites	ultrasonic "etape" (pressure)	Ethernet(R-Pi)	3%–0.2%
Massoud et al. (Massoud et al., 2019)	Eco-driving (driver assistance)	OBD sensor	Bluetooth (OBD-II)	N.A.
Obikoya (Obikoya, 2014)	Monitor fuel level of any tank	level sensor	GSM	<0.5%
Patil et al. (Patil et al., 2017)	Monitor fuel level in vehicle tanks	Ultrasonic flow sensor	Ethernet (R-Pi)	5%–2%
Skog and Handel (Skog and Handel, 2014)	Estimate instantaneous fuel consumption	OBD sensor	Bluetooth (OBD-II)	<10%

The existence of a transport layer is one of the premises to perform vehicles' fuel amount estimates using IoT devices. In this context, OBD (Onboard Diagnostics) Protocol is an alternative to obtain information from vehicle's embedded sensors (Massoud et al., 2019; Skog and Handel, 2014). OBD interfaces have been a mandatory requirement in vehicles produced in the USA and Europe for the last 15 years. Nowadays, one can obtain low-cost OBD monitoring devices on the Internet for less than USD 10.[1] Furthermore, smart sensors with communication features are also a suitable solution (Ahmed et al., 2017) for sending fuel measurements directly to a monitoring application. When necessary, GSM modems and smartphones can work as gateways to provide connectivity among sensors and the Internet (Obikoya, 2014).

2.3. *Blockchains*

Blockchain is an emerging technology which has called the attention in different industry segments (Dai et al., 2019; Makhdoom et al., 2019; Zheng et al., 2017). Recently, Legal Metrology was also pointed out as a potential area to develop blockchain-based solutions (Melo et al., 2019, 2020; Peters et al., 2018, 2020). Conceptually, one can regard a blockchain as a distributed append-only data structure (designated as *ledger*), which is replicated and shared among a set of network peers (Dai et al., 2019). By avoiding central points of control, blockchains availability does not depend on third parties, which can significantly save costs (Zheng et al., 2017). Blockchain also ensures integrity and availability by consensus among the peers, preventing the whole chain from being modified and requiring an agreement about any new block in the ledger (Xiao et al., 2020). A blockchain can virtually store any digital asset, from data to self-executing scripts, usually defined as *smart contracts* (Christidis and Devetsikiotis, 2016). That makes blockchain not only a data storage architecture but also a complete distributed platform for automated workflow.

We can classify blockchain platforms as *permissionless* when anybody can join the network and participate in the consensus, or *permissioned* when the network achieve consensus from a set of known and identifiable peers (Vukolić, 2017). Usually, permissioned blockchains

[1] https://www.amazon.com/s?k=obd2+wireless.

consensus protocols expend less computational resources and can reach better transaction latency and throughput (Sousa et al., 2018; Xiao et al., 2020). Hyperledger Fabric (or only Fabric) is an example of an open source platform for implementing permissioned blockchains (Androulaki et al., 2018). It provides a flexible architecture that accommodates different mechanisms to implement consensus and validation of transactions (Sousa et al., 2018). Fabric also supports smart contracts (called chaincodes) and can deal with more than 2000 transactions per second (Androulaki et al., 2018), being one of the leading blockchain platforms in terms of performance.

2.4. Related works

After presenting preliminary concepts, we now discuss the works directly related to our proposal. We consider three main groups: a) works that talk about field surveillance practices, b) works related to IoT fuel meters and c) works that discuss blockchain-based solutions to store IoT data.

Rodrigues Filho and Gonçalves (2015) presents a systematic review that addresses field surveillance as a critical activity in the context of Legal Metrology. Field surveillance is essential to prevent fraud involving tampering with measurements (Esche and Thiel, 2015; Narwade and Patil, 2016; Rodrigues Filho and Gonçalves, 2016). However, field surveillance practices are still very dependent on non digitalized procedures, especially when we consider fuel dispensers (Leitão et al., 2014; Luchsinger et al., 2008; Rodrigues Filho and Gonçalves, 2016). In 2008, Luchsinger et al. (2008) described a procedure to evaluate fuel dispensers that, even after ten years, is still similar to the procedures adopted by most notified bodies in the world. Leitão et al. (2014) argue that these practices can be considered obsolete in the face of the growing level of sophistication exhibited in the electronic frauds reported in the Brazilian fuel dispensers. The same paper presents empirical evidence that these frauds result in a measuring error of 6%–8% of the correct fuel amount. Narwade and Patil (2016) corroborate these findings on estimating than 8% of the fuel sold in India is adulterated. Moreover, Rodrigues Filho and Gonçalves (2016) report that, in Brazil alone, frauds related to fuel dispensers result in economic losses in the order of USD 300 million per year. So exists a shared sense among different authors (Beteto et al., 2016; Leitão et al., 2014; Rodrigues Filho and Gonçalves, 2016; Thiel, 2018) that Legal Metrology must urgently promote new field surveillance solutions based on novel digital technologies. However, only a few works present practical solutions that contemplate field surveillance. An example is the *European Metrology Cloud* (Thiel, 2018), a long term project that proposes the integration of different Legal Metrology services in a secure cloud computing architecture. These services shall include managing legal processes, measurement storage, monitoring systems, logging of legally relevant activities, and even the execution of legally relevant software in the cloud.

Works describing technologies to create simple IoT fuel meters are also related to our work. We examined in detail five of these works and summarized them in Table 1. We selected these works because they are related to fuel amount measuring, and their methodologies present substantial detail. In the present work, we do not develop any new IoT fuel meter device. So we use those works to demonstrate that these devices are used in different applications, offer connectivity resources, and delivers fuel measurements with estimate precision. There is a diversity of sensor's technology at affordable prices. Massoud et al. (2019) and Skog and Handel (2014) develop their solution using their own vehicle's embedded sensor. Also, the measuring error presented in these works is lower than 5% in most cases. Ahmed et al. (2017) and Patil et al. (2017) present more consistent results, pointing out a measuring error between 5% and 2%. We take this error as a reference for our experiment in Section 5. The literature also presents some works that use vehicles' fuel measurement to prevent frauds related to fuel adulteration (Narwade and Patil, 2016; Rocher et al., 2018). Narwade and Patil, (2016) use sensors to measure fuel density and viscosity and so discover if there is an odd chemical mixture. In Rocher et al. (2018), the authors use light sensors to infer if a vehicle tank contains a specific kind of dyed fuel. Although both works bring interesting approaches, they do not deal with the fuel amount problem, and are not directly related to our needs.

We also analyzed works related to the use of blockchains to store and protect data from IoT devices. The recent works of Makhdoom et al. (2019) and Dai et al. (2019) survey different blockchain-based IoT applications, including smart manufacturing, smart grids, supply chain management, healthcare, and intelligent vehicles. This combination includes several challenges. According to Makhdoom et al. (2019), IoT centric consensus, scalability, and performance are some of the gaps that blockchain-based IoT applications need to care about. Dai et al. (2019) emphasizes that data traceability and reliability are two of the main advantages of combining IoT and blockchains. Christidis and Devetsikiotis (2016) give another motivation to put these technologies together: smart contracts enable the automation of several existing, time-consuming workflows in a cryptographically-verifiable manner. Wang and Zhang (2019) discuss the use of blockchains to deal with data integrity verification in large-scale IoT systems. The authors argue that blockchains can be an alternative to trusted third auditors (TTA). Despite the blockchains' problems of large computational and communication overhead, they also develop a blockchain-based solution for checking data integrity that outperforms TTA-based solutions. In the scope of Legal Metrology, few works propose blockchain-based applications to deal with measuring instruments and their data. We can cite works that use the Fabric platform to test applications related to measuring and sensing physical quantities. Melo Jr. et al. (Melo et al., 2019) implement a distributed speed meter measuring system, exploring Fabric endorsers' features to achieve better performance and reduce regulatory costs. Peters et al. (2020) and Yurchenko et al. (2020) also use Fabric to implement smart contracts together with functional encryption to assure the privacy of sensitive data from smart energy meters. To the best of our knowledge, there are no works proposing field surveillance strategies using blockchain-based solutions.

3. Distributed and Decentralized Surveillance Framework

3.1. The challenges related to field surveillance

Any trade transaction of measured goods can involve conflict of interests. Usually, a vendor has a measuring instrument $\mathcal{M}_k$, which is supposed to be reliable and regulates the transaction by informing the correct measurement. However, different factors can compromise $\mathcal{M}_k$'s precision and accuracy (e.g., defects, misbehavior, or even fraud attacks). That is why Legal Metrology introduces *field surveillance* actions. Usually, a *notified body* $\mathcal{N}$ is responsible for verifying each measuring instrument $\mathcal{M}_k$ and attesting its correct behavior. $\mathcal{N}$ is also responsible for discarding measuring instruments which do not satisfy precision and accuracy criteria, applying penalties when she finds evidence of mismanagement or malicious behavior.

The field surveillance of fuel dispensers faces several practical challenges. First, they require *in loco* inspection at the instrument's deployment site. This scenario becomes quite expensive because fuel dispensers are geographically spread and can be deployed in remote places. Also, fuel trading is related to very profitable frauds that can impose more challenging scenarios (Beteto et al., 2016). Malicious entities can try to corrupt notified body representatives, offering bribes and convincing them to overlook inspection. Furthermore, a modern fuel dispenser can be a target of sophisticated fraud mechanisms that implement stealthy malicious behavior (Leitão et al., 2014). Such attacks are harder to spot in conventional inspection procedures.

3.2. An IoT-based distributed and decentralized solution

Field surveillance of fuel dispensers can be more effective when it integrates new information technologies (Rodrigues Filho and

Gonçalves, 2016; Thiel, 2018). Thus we propose an IoT-based distributed and decentralized surveillance solution which uses vehicles' fuel tanks to provide information about fuel dispensers accuracy. Fig. 2 depicts our idea. Fuel station owners and drivers represent vendors (v) and consumers (c). $\mathcal{M}_k$ correspond to a modern fuel dispenser (i.e., a smart fuel meter) with expected high accuracy and precision that belongs to a fuel vendor v_n. Each consumer c_m has an IoT-based *vehicular fuel meter* (VFM) device $\mathcal{S}_l$ whose accuracy and precision are unknown. Our strategy relies on the communication of these IoT devices with a distributed and decentralized data storage service $\mathcal{D}_s$, which keeps the record of any performed fuel trading and enables metrological field surveillance on the fly. In practice, $\mathcal{D}_s$ is a blockchain held by independent stakeholders, which can include other fuel station owners, government agencies, notified bodies, and entities representing consumer interests. The blockchain $\mathcal{D}_s$ stores measurement records, which are the fuel measurements from fuel dispensers ($\mathcal{M}_k$) and vehicle tanks ($\mathcal{S}_l$), together with any complementary information. Authorized stakeholders can access such measurements and implement data analysis as smart contracts, contributing to surveillance in a comprehensive manner.

The main reason for using blockchains is because they offer natural protection against collusion attacks. Although centralized solutions can perform better, they depend on the existence of a trusted third party. Frauds related to fuel dispensers tampering are very profitable, which motivates collusion attacks among malicious entities. Any possible trusted third party (even notified bodies and legal authorities) could have its representatives compromised for bribes and undue advantages offered by an attacker. Thus the field surveillance of fuel dispensers poses as a suitable case for using blockchain-based solutions, according to the directives given by Wust and Gervais (2018). Besides, being a distributed solution, blockchains present high availability and can also automatize surveillance workflows in smart contracts.

We assume two necessary conditions to implement the DDSF:

1. **Different stakeholders want to assure the reliability of each trade transaction.** This premise is very realistic since dishonest fuel trading affects not only the directly involved parts (i.e., vendors and consumers). This practice also harms several other actors related to the business chain. That can include other vendors who have losses due to unfair competition, government agencies that need to worry about more restrictive supervision policies, notified bodies that have more efforts with field surveillance procedures, and the society in general once the trade relations are under suspicion.
2. **Each consumer has her own VFM $\mathcal{S}_l$.** Measuring instruments with high precision and accuracy are expensive. That is one of the main reasons why, in consumption relations, the fuel dispenser $\mathcal{M}_k$ usually belongs v_n. However, c_m usually want to be sure that $\mathcal{M}_k$ is measuring correctly. So we assume that c_m wants to and has enough resources for using $\mathcal{S}_l$ to verify $\mathcal{M}_k$.

3.3. Requirements of each component

We now describe the requirements of each main DDSF component. These requirements help to understand our proposal.

3.3.1. The fuel dispenser $\mathcal{M}_k$

We assume $\mathcal{M}_k$ as a smart fuel dispenser like the one described in Section 2.2.1. This device implements connectivity features. It can connect to the Internet and write transactions into the blockchain. Under ordinary circumstances (i.e., no malicious behavior), the fuel dispenser $\mathcal{M}_k$ is a highly precise and accurate device.

The fuel dispenser $\mathcal{M}_k$ also needs a unique ID (e.g., a private cryptographic key). It uses the ID to identify each refuel transaction. We assume that this procedure consists of a challenge/response protocol. For instance, $\mathcal{M}_k$ can generate the refuel transaction ID by signing the timestamp and a nonce using its private key. $\mathcal{M}_k$ provides the transaction ID at the beginning of each transaction, publicly. It can be a QRCode exhibited in a display, for instance. The ID also associates the fuel dispenser with its physical location or deployment site.

The fuel vendor deploys $\mathcal{M}_k$ in a fuel station that offers a stable operational environment. Consequently, we assume that $\mathcal{M}_k$ is plenty of resources in energy and connectivity services.

3.3.2. The vehicular fuel meter $\mathcal{S}_l$

We assume the VFM $\mathcal{S}_l$ as a simple IoT-based fuel meter. It has the same general features of the IoT devices discussed in Section 2.2.2. Usually, the VFM can present two sub-modules: the sensing module and the gateway module. The sensing module is the part responsible for getting the fuel measurement. The gateway module connects with the sensing module and sends transactions to the blockchain. The gateway module also implements the user interface. This interface treats events related to refuels' start and provides useful information to the driver, like the fuel measurements from each previous refilling. The gateway also knows how to get the transaction ID provided by the fuel dispenser. For instance, if this ID is a QRCode, the gateway has a camera that decodes it and initiates the refueling event.

The communication between the sensing and the gateway is flexible. We assume that it can happen in different ways. The gateway module can integrate with different sensing modules and work in three different modes, with different reliability levels. These modes are:

- **Measured by the vehicle system:** the gateway connects to the vehicle (i.e., using OBD technologies) and gets the fuel amount estimate provided by the vehicle's embedded computer. This mode can require an OBD adaptor (if the vehicle does not offer a Bluetooth interface) and perhaps some specialized training (or service) to configure the client.
- **Measured by smart sensors:** the gateway connects to a smart sensor installed into the vehicle's fuel tank. The smart sensor provides

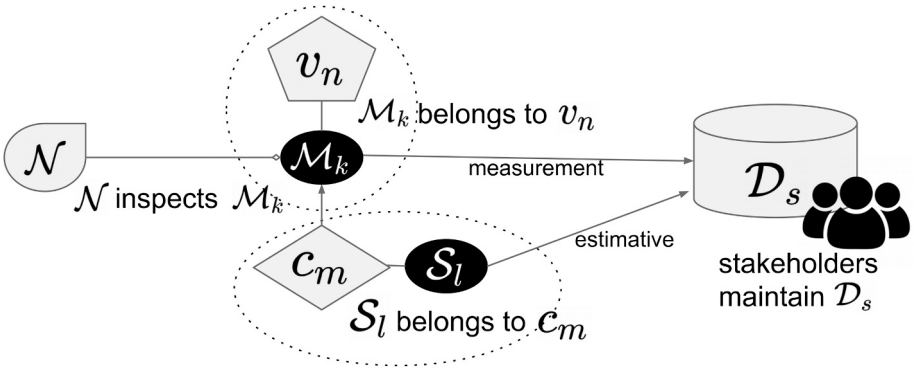

Fig. 2. The Distributed and Decentralized Surveillance Framework (DDSF).

highly accurate measurement and can also sign it, attesting its authenticity. This mode is the most expensive one, and its deployment usually requires specialized service.

- **Informative:** the gateway provides an interface where the driver types the measurement informed by the vehicle's fuel gauge/panel. This mode does not require a sensing module, and it is the cheapest. However, it is very imprecise and subject to measurement and typing errors.

One must notice that the described modes impact information reliability. Even when there are no frauds, the collecting mode can compromise information due to its imprecision. For instance, in the Informative mode, the user can type a wrong measurement and provide spurious information. However, we understand that this flexibility can promote DDSF adoption. Since the gateway informs the blockchain about the collecting mode, we can adopt different information treatments. Measurements provided without the driver's intervention are more reliable and can be prioritized in statistical surveillance analysis.

We define that the VFM can also inform, besides its measurement, the measurement provided by the fuel dispenser. The driver knows this information once he/she has requested the refuel and paid for it. Although this information is also subject to typing error (or even malicious use), it can aggregate more possibilities in terms of surveillance. For instance, we can compare the measurement informed to the driver by the fuel dispenser after the refilling with the measurement sent to the blockchain.

3.3.3. The data storage $\mathcal{D}_s$

We assume $\mathcal{D}_s$ as a permissioned blockchain that enables smart contracts to implement field surveillance analysis. Also, we choose a permissioned blockchain because they deliver better performance when compared to permissionless blockchains.

Each stakeholder engaging in assuring the reliability of the transactions contributes with a respective number of peers (i.e., physical or virtual machines). The set of peers compose the blockchain network. A small group of peers, with members from different stakeholders, constitute the consensus quorum. The diversity of organizations in the consensus is the key to protect against collusion attacks. The information in the ledger is public to all the blockchain participants. The vehicles are anonymous. We cannot identify their transactions in the blockchain. The fuel dispensers are identifiable only, but their IDs are exposed only in case of a proven fraudulent behavior and eventual prosecution by a court.

Any stakeholder can implement smart contracts with field surveillance analysis and strategies. The blockchain can execute these smart contracts on any complete transaction. Stakeholders can consult the ledger, audit information, and request legal measures whenever they find traces of fraud.

3.4. The transaction model

We propose the DDSF in a way where drivers and fuel vendors are invited to contribute voluntarily. This concept takes advantage of common sense that honest entities have a strong motivation against fraud. That is why we call it *free model* (Fig. 3). Firstly, the fuel dispenser $\mathcal{M}_k$ and the VFM $\mathcal{S}_l$ need to agree on the transaction ID that identifies the refueling event. This agreement happens at the beginning of the refueling. As we described previously, $\mathcal{M}_k$ generates the ID.

When the refilling finishes, $\mathcal{M}_k$ and $\mathcal{S}_l$ need to send their fuel measurements to the blockchain $\mathcal{D}_s$ in independent transactions linked by the same ID. The fuel dispenser $\mathcal{M}_k$ always knows when to do that because it controls the fuel flow. On the other hand, the VFM $\mathcal{S}_l$ needs to detect the event. It monitors the event by analyzing a sudden fuel amount positive variation (refuel start), followed by a period of stability (refuel stop) or a slow decrease (indicating that the vehicle is consuming fuel again). This monitoring produces a delay of the VFM when compared to the fuel dispenser. However, the VFM does not need to send the refilling measurement immediately (this is one of the advantages of the free model). He can wait for the refuel stop detection (something no longer than 5 min, for instance), and then write the information into the blockchain. Finally, the blockchain $\mathcal{D}_s$ implements a smart contract and invokes it whenever the ledger indicates two transactions with the same ID. This last step consolidates both transactions, making the measurement record available to stakeholders.

The free model can produce three distinct scenarios. The best one is when the vendor and driver contribute to the system, sending their measurements. The other scenarios occur when only one of them sends their measurement. If only the vendor informs the fuel dispenser measurement $\mathcal{M}_k$, this information does not have a practical use because one does not have the vehicle measurement for comparing. In opposite, when only the driver informs the VFM $\mathcal{S}_l$ measurement, he/she could also include the fuel dispenser measurement. Although these measurement record would seem suspicious (i.e., the driver can cheat with the fuel dispenser measurement), it is yet useful for statistical analysis. We discuss these questions in detail in Section 4.

3.5. Dealing with measurement uncertainty

The precision and accuracy of $\mathcal{S}_l$ have a remarkable impact on the DDSF idea. In other words, the *metrological uncertainty* associated with $\mathcal{S}_l$ requires some care when we use the measurements from $\mathcal{S}_l$ to implement statistical data analysis. We rely on the *Law of Large Numbers* (LLN) (Evans and Rosenthal, 2004) to deal with this uncertainty. The LLN states that, in an experiment where the number of samples of a random variable (identically distributed) increases, their average converges strongly to their theoretical value.

Yang and Ha (2013) proved that the convergence of the LLN on probability space is equivalent to convergence in uncertain measures whenever their relevant universe is finite. One can reduce the standard

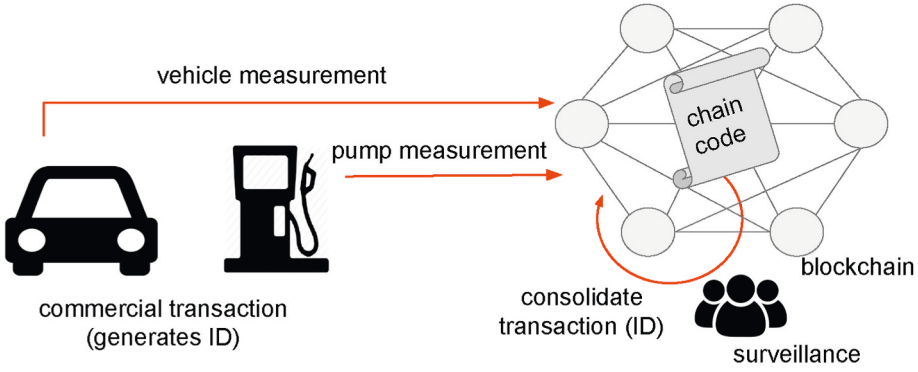

Fig. 3. The DDSF implementation for fuel dispensers field surveillance.

deviation of the mean to the number of repeatable and reproducible measurements performed to estimate the dispersion of the measures. The findings of Yao and Gao (2015) and Sheng et al. (2018) corroborate this idea and also demonstrate that the convergence of the mean value by applying LLN allows the use of the mean value as representative of the measurement distribution. Our idea consists in using the LLN as suggested by these authors. In this manner, we apply such theorem to the $\mathcal{S}_l$ measurements.

Although $\mathcal{S}_l$ is, by definition, an instrument with a high uncertainty value, a large number of measurements must have an average, which converges to the theoretical mean. By assuming that $\mathcal{S}_l$ error is identically distributed around the real measured quantity, we have that a large number of samples from $\mathcal{S}_l$ can be used to evaluate $\mathcal{M}_k$ reliability.

For each fuel trading transaction involving a fuel dispenser $\mathcal{M}_k$ and an embedded VFM given by S_l, we update the VFM uncertainty estimate $\mu_{\mathcal{S}_l}$ in the n-th refuel event by using the measurements $m(\mathcal{M}_k, n)$ and $m(\mathcal{S}_l, n)$, according to the equation:

$$\mu_{\mathcal{S}_l}(n) = \frac{(n-1) \times \mu_{\mathcal{S}_l}(n-1) + m(\mathcal{M}_k, n) - m(\mathcal{S}_l, n)}{n} \tag{1}$$

where $\mu_{\mathcal{S}_l} = 0$ when $n < 1$.

After a sufficient number of samples, the VFM estimate uncertainty $\mu_{\mathcal{S}_l}$ converges to the correct VFM uncertainty value due to the LLN (Evans and Rosenthal, 2004). The more events we compute, the more precise the uncertainty estimate is.

When the uncertainty estimate becomes a stable value (i.e., new refuel events change the uncertainty estimate with a negligible correction), we can use it to detect outliers. We mark each outlier event in the blockchain as a case of suspicious measurement. We consider as outlier any refuel event where the difference between the fuel dispenser measurement and the VFM measurement (i.e., the measurement uncertainty estimate) satisfies the following inequation:

$$|m(\mathcal{M}_k, n) - m(\mathcal{S}_l, n)| > K_1 \mu_{\mathcal{S}_l}(n) \tag{2}$$

where K_1 correspond to a dispersion constant to determine outlier events.

Once we have the outliers list, we implement a second level analysis based on the same idea used to detect event outliers. If a fuel dispenser is related to a significant number of suspicious events (i.e., it is a frequent outlier), we consider it as a possible tampered instrument. We decide that by using the frequency information in the outliers list. Let $F = \{f_{\mathcal{M}_1}, f_{\mathcal{M}_2}, \ldots, f_{\mathcal{M}_k}\}$ be the set with the frequencies which count the number of suspicious events related to each fuel dispenser $\mathcal{M}_k$, the decision about if $\mathcal{M}_k$ is a possible tampered instrument is given by:

$$f_{\mathcal{M}_k} > mean(F) + K_2 std(F) \tag{3}$$

where $mean(F)$ and $std(F)$ are respectively the mean and the standard deviation of the values in F and K_2 correspond to a dispersion constant to determine outlier frequencies.

4. Security analysis

4.1. Attack model

In a typical scenario involving fuel dispensers and vehicles, we assume that an attacker's primary objective is to get undue economic advantages. He does that by tampering with fuel measurements. Initially, one can consider suspicious any one of the parts involved in the commercial transaction. However, in a simplified manner, we identify malicious drivers and fuel vendors as potential attackers. Malicious fuel vendors take advantage of cases when the fuel measurement is higher than the correct value. On the other hand, a fuel measurement lower than the correct amount benefits malicious drivers. Also, a scenario including a surveillance system (i.e., a system that evaluates fuel dispensers' accuracy and correct behavior) introduces a second attack goal: compromising this system. For instance, malicious drivers can target the surveillance system, aiming to create false suspicions about a fuel dispenser, harming this device's owner.

Regarding attack capabilities, a malicious fuel vendor is supposed to be more resourceful than a malicious driver. The fuel vendor is the formal owner of the devices involved in a commercial transaction (e.g., fuel dispenser, payment systems). The fuel vendor can control and modify these devices' features, compromising the measurements' accuracy and reliability. Besides, fuel measurement frauds are very profitable for malicious vendors. This undue advantage motivates the conception of sophisticated attacks involving different fraud strategies. Malicious drivers also can tamper with measurements. However, they are limited when compared to fuel vendors. Although the driver has total control over the vehicle measuring system, the fuel dispenser controls the commercial transaction. Any tampered measurement coming from the vehicle does not result in an economic advantage. One can consider exceptional cases where the driver can hack fuel dispensers or payment systems. However, reports of similar practices are very uncommon, so we remove it from our analysis.

Attacks targeting the surveillance system require some specific resources. We foresee two basic strategies: a) the attacker provides incorrect information in a manner that the surveillance system does not detect the measurement frauds, and b) the attacker compromises the surveillance system by tampering with the stored measurements. Both strategies depend on collusion among fuel vendors, drivers, and even other stakeholders. Collusion attacks are typically expensive. Also, these attacks would result in economic advantages only for fuel vendors. That reduces the incentives for malicious drivers to take part in the collusion. However, a possible attack approach is to falsify refueling events. For instance, a malicious driver can forge several measurements, creating fake refuel events. He then sends the information to the surveillance system, claiming that the fuel station did not report it.

4.2. Countermeasures

We claim that the DDSF offers natural protection against several scenarios related to the described attacks. We show that by evaluating the security features provided by the DDSF in four main attack classes: measurement tampering, information denying, information forging, and collusion.

4.2.1. Measuring tampering

The main attack against a measuring instrument consists of tampering with measurements (i.e., replace a correct measurement for a fraudulent one). The DDSF tries to detect fraud by comparing measurements from the fuel vendor and the driver. Besides, although both the entities can still tamper with measurements, such practice may be exposed later by analyzing data in the blockchain using statistical tools.

4.2.2. Information denying

Information denial might happen when either the fuel vendor or the driver decides to omit information about a trading transaction. Malicious fuel vendors can deliberately do this to hide fraudulent refillings. On the other hand, we notice that drivers do not have any advantage in omitting information. Notwithstanding, they eventually may not have the necessary resources to do that or decide not to contribute to the system. There is a practical manner of dealing with this situation: DDSF can consider as suspicious any transaction informed only by the driver. So honest fuel vendors will send their measurements whenever possible to avoid auditing. This approach is convenient because fuel vendors usually have plenty of resources to send their information to the system. However, that also introduces a new class of attacks, which consists of forging false transactions.

4.2.3. Information forging

Information forging happens when the attacker creates information about a false trading transaction. Primarily, this kind of attack aims to compromise DDSF credibility. Information from false transactions can affect statistical analysis and impact DDSF efficiency. Both the fuel vendor and driver can try this attack. Fuel vendors do not have any advantage in doing that. If a fuel vendor simulates a trading transaction, he does not harm any consumer. In contrast, he can have problems with other authorities investigating if the amount of trading fuel corresponds to the paid taxes. In turn, drivers can forge transactions to spoil DDSF or even harm a correct fuel vendor's reputation. However, an attack launched by only one driver is not enough to compromise statistical analyses. We can also easily spot transactions forged by the same driver, invalidating the chances of a regular driver to undertake such attacks. Finally, we consider one last possibility: a resourceful attacker can personify different drivers by creating fake profiles or even stealing legitimate drivers' identification. Despite its chances of success, this attack is remarkably costly. Countermeasures can include analyzing drivers' behavior and the existence of a formal process to accept and identify drivers who want to join DDSF.

4.2.4. Collusion attacks

Collusion attacks are common in the context of fuel trading transactions. The main reason is fraud profitability, as we mentioned before. Malicious fuel vendors can corrupt legal authorities and can even form cartels that control fuel prices and disseminate measurement frauds on a large scale. In the DDSF, collusion attacks only occur after the fuel vendor and driver sending their respective measurements. These attacks will succeed if they compromise the blockchain security premises. Happily, blockchains drastically reduce the possibility of a specific entity to take control of the network. A blockchain forces an attacker to control the majority of the peers that integrate the consensus quorum. The more organizations participate in the blockchain consensus, the more expensive the collusion attack becomes. Once any information is stored, it is virtually impossible to modify or remove it. These features make blockchains a unique technology to store information used to detect and prevent measurement frauds.

4.3. Privacy concerns

In terms of privacy, we understand that DDSF can make use of techniques of data anonymization. This approach can protect consumers' identities and avoid attacks trying to link any sensitive information to a specific person. Anonymization mechanisms have been developed consistently in the last years, with applications in different areas that demand privacy requirements (Alcaide et al., 2013). This work's scope does not include the discussion of these mechanisms, but as a minimum requirement, we assume the ID of consumers will be pseudonymized.

5. Case study: a DDSF practical application

In this section, we develop a practical case study that uses Hyperledger Fabric to implement DDSF. We simulate the behavior of fuel dispensers and vehicles by using metrological field surveillance data from the Inmetro.[2] We consider that our implementation needs to meet the demand of vehicles refueling in São Paulo state, Brazil. São Paulo is the biggest federated state in Brazil, with a population of approximately 45 million people and a vehicular fleet of more than 30 million vehicles. These numbers are expressive in demonstrating that we can compare São Paulo with countries like the United Kingdom, Mexico, and Spain, in terms of the number of vehicles.

In 2015, São Paulo had a total 8849 fuel stations (Beteto et al., 2016). By assuming that each fuel station can manage one refuel event per minute (i.e., the driver needs to park the vehicle, insert the fuel nozzle in the respective place, refuel the vehicle tank, and finally remove the vehicle before releasing the fuel dispenser to the next driver), we can estimate that all the fuel stations in São Paulo state can manage a demand of no more than 150 refuel events per second. Each refuel event generates two transactions (vendor and consumer measurements), so we estimate a demand of 300 transactions per second (tps) in the blockchain.

5.1. Data simulation

We start our experiment by simulating random refuel events. Each event has its respective measurements from the fuel dispenser and the VFM. Both measurements are subject to a statistical error. We model the fuel dispenser error by using real data from field surveillance inspections done in 2017. Regarding the VFM, we assume that its error is random and uniformly distributed in a range between $-v_{Err}$ and $+v_{Err}$, being v_{Err} the measurement error associated with the VFM uncertainty.

Table 2 summarizes the data used to simulate the fuel dispenser error for correct and tampered instruments. We take data from 187,849 periodic inspections of fuel dispensers. An inspection procedure consists in measuring a standard refuel of 20 L and comparing the measured value with the reference value. In Brazil, the fuel dispensers regulation[3] defines the permissible error between −100 and 50 ml (in 20 L). In the set of inspected instruments, the measurement error has a mean of 9.7 ml and a standard deviation of 48.3 ml. We use this information to simulate fuel dispensers that are supposed to inform correct measurements. A total of 8857 fuel dispensers exceed the limits of error. However, we are interested in instruments whose the measurement error could be indicative of fraudulent behavior. So we consider in our simulation only the cases where the error is higher than 200 ml (1%). This group corresponds to 111 fuel dispensers. In this group, the measurement error presents a mean of 417.4 ml, and its standard deviation is 398.9 ml. We use this information to simulate fuel dispensers that are supposed to be tampering with the measurements. There is an important point here. The percentage of instruments considered as suspicious of fraudulent behavior is remarkably low. However, we have reasons to assume that the percentage of fraud cases is much higher than that. The available inspection data comes from periodic inspections, which correspond to situations where the notified body plans the inspection, and the fuel station manager knows about it. Under these circumstances, many malicious vendors modify tampered instruments before the inspection, removing any evidence of fraud (Leitão et al., 2014).

Our simulation generates refilling events by considering scenarios with different numbers of vehicles and fuel dispensers. In each scenario, we assign a different measurement uncertainty to the VFM. We also assume different tampered fuel dispensers percentages. A high number of tampered fuel dispensers increases false positives and false negatives rates. The same thing happens when the VFM has high uncertainty.

We use the simulated refuel events to submit transactions to the blockchain. We assume that both fuel dispensers and vehicles inform their measurements in different transactions, following DDSF. Every

Table 2
Statistical description of inspection data with error measurement's mean and standard deviation (in ml).

	number	*mean*(*err*)	*std*(*err*)
Inspected instruments	187,849	9.7	48.3
Inst. with error >200 ml	111	417.4	398.9

[2] Inmetro is the Brazilian NMI (National Metrology Institute) responsible for measuring instruments type approval, market and field surveillance.

[3] http://www.inmetro.gov.br/legislacao/rtac/pdf/RTAC002514.pdf.

time a transaction is complete (i.e., the blockchain receive both the expected measurements), the respective smart contract starts the statistical analysis described at Section 3.5.

5.2. Blockchain implementation

We use HyperLedger Fabric 1.1[4] in our experiment. We develop a blockchain network where organizations representing stakeholders cooperates for implementing the DDSF solution. Each organization provides a corresponding number of peers that constitutes the blockchain network. Some organizations also take part in the *orderer consortium* (i.e., a group of peers that performs the blockchain consensus). We make use of the BFT (Byzantine Fault-Tolerant) orderer described in (Sousa et al., 2018).

Fig. 4 depicts our blockchain architecture. We consider two independent organizations (Org 1 and Org 2) that correspond to entities interested in supporting DDSF (e.g., notified bodies, fuel distributors). Each one provides a set of 4 ordinary peers and two consensus peers. The blockchain network accepts transactions from clients who are essentially vendors (i.e., fuel station owners) or consumers (i.e., drivers). We assume that every refuel event generates a unique event ID (e.g., the fuel dispenser can exhibit a QR Code). Both clients use this ID to identify their transaction and send their measurements to the DDSF network.

5.3. Experimental evaluation

Before presenting our experiment results, we discuss some specific parameters which are relevant to our analysis:

- E is the number of refuel events, i.e., the number of simulated samples of measurements pairs (fuel dispenser and VFM measurements).
- D is the number of distinct fuel dispensers.
- D_f is the percentage of fuel dispensers simulated as tampered instruments.
- V is the number of distinct vehicles (and consequently, distinct VFMs).
- v_{Err} is the VFM measurement error limit value.

The parameter E impacts directly on results because it determines the LLN applicability in our study. The parameters D and V have an essential influence on the results, once they determine the proportion between fuel dispensers and vehicles. Lastly, D_f and v_{Err} are crucial because they establish the universe of tampered instruments as so as the VFM's necessary accuracy to exploit the fraudulent behavior.

We organize our experiment in three rounds. On each round, we vary one specific parameter of interest and set the others. We modify the parameter of interest in a determined range, by assigning individual values. For each value, we execute 100 consecutive simulations, implementing the field surveillance in each simulation with the statistical analysis described in Section 3.5. We implement our analysis procedure as a smart contract in Fabric. In the end, we evaluate our method efficiency using the statistical measures of *sensitivity* (i.e., the proportion of actual positives that are correctly identified) and *specificity* (i.e., the proportion of actual negatives that are correctly identified) (Dangeti, 2017).

Since our experiment is multi-variable, for each simulation round, we need to variate only the parameter of interest and fix the others. We define the fixed values based on the following conjectures. We fix $D = 100$ to make it easier to calculate the percentage of tampered instruments, and $V = 1{,}000$ as the minimum number of distinct VFMs to evaluate the convergence. Larger values would be more representative of the population, but this sampling condition allows us to simulate 2,000 to 10,000 refilling events. The increasing of these values should lead to simulations of 100,000 to 1,000,000 events, which would not be practical in terms of computing simulations. However, this condition is enough to represent scenarios where the adherence of drivers does not need to be higher to prove the usefulness of the model. This argument also justifies why we define $E = 10000$ when we need to fix it. Finally, we define the parameters $D_f = 5\%$ and $v_{Err} = 5\%$ because these are average values described in the literature, as discussed in Section 2.

The plots at Fig. 5 shows the sensitivity and specificity of each experiment round. We discuss each one of them in the following:

- **Round #1 (modifying E):** The results demonstrate how the number of events affects our analysis and the convergence properties of the LLN. The sensitivity presents poor measures at the beginning and increases significantly after 5000 events (or samples). The other parameters are fixed as $D = 100$, $D_f = 5\%$, $V = 1{,}000$, and $v_{Err} = 5\%$.
- **Round #2 (modifying v_{Err}):** The value of v_{Err} is related to the VFM accuracy and impacts directly the sensitivity of our analysis. One can see that it decreases fast when $v_{Err} > 5\%$. Instruments with lower accuracy will require a larger number of measurements to present some useful result. However, as we discussed in Section 2.2.2, the assumption of $v_{Err} \leq 5\%$ is very realistic. The other parameters are fixed as $E = 10{,}000$, $D = 100$, $D_f = 5\%$, and $V = 1{,}000$.
- **Round #3 (modifying D_f):** The results seem to indicate that the analysis is robust with different percentages of tampered fuel dispensers. Although specificity is slightly compromised when we have a low percent of frauds (which increases the number of false positive cases), our analysis heuristic presents a good performance. We obtain the best trade-off when considering a rate of 7% of tampered fuel dispensers. The other parameters are fixed as $E = 10{,}000$, $D = 100$, $V = 1{,}000$, and $v_{Err} = 5\%$.

After checking these results, we confirm that the statistics heuristic used to detect tampered fuel dispensers performs fairly well. However, as expected, it requires a significant number of refuel events samples. We get our best trade-off when considering a minimal of 10,000 samples from 1000 distinct vehicles. This result implies that each vehicle refuels an average of 10 times. This number is quite realistic in terms of practical implementations. If a driver refuels his vehicle once or twice a week, a real-world application would collect the required amount of samples in less than two months.

5.4. Blockchain performance

We also evaluate the blockchain performance, by following a methodology similar to the one used in (Melo et al., 2019; Peters et al., 2020). We generate a workload of concurrent clients that simulates transactions from fuel vendors and drivers. The client instances try to send transactions continually, while we evaluate the blockchain performance in terms of latency (in seconds) and throughput (in tps). Fig. 6 shows our findings. The throughput rate increases until we have 600 concurrent clients. From this point on, throughput decreases slightly while latency increases.

The best trade-off points out a throughput of around 400 tps to the proposed network configuration. This performance meets the demanded of 300 tps previously associated with the refuel events in São Paulo state. An important aspect is that the proposed network infrastructure is not expensive. Furthermore, other peers could be easily added to the solution to address specific issues related to the smart contract execution, once Fabric uses the concept of endorsers to do that (Androulaki et al., 2018; Peters et al., 2020).

6. Discussions

After evaluating the DDSF implementation and the results from our experiment, we discuss some questions that are quite relevant in real-world performance. This section brings an overview of our proposal

[4] https://hyperledger-fabric.readthedocs.io/en/release-1.1/.

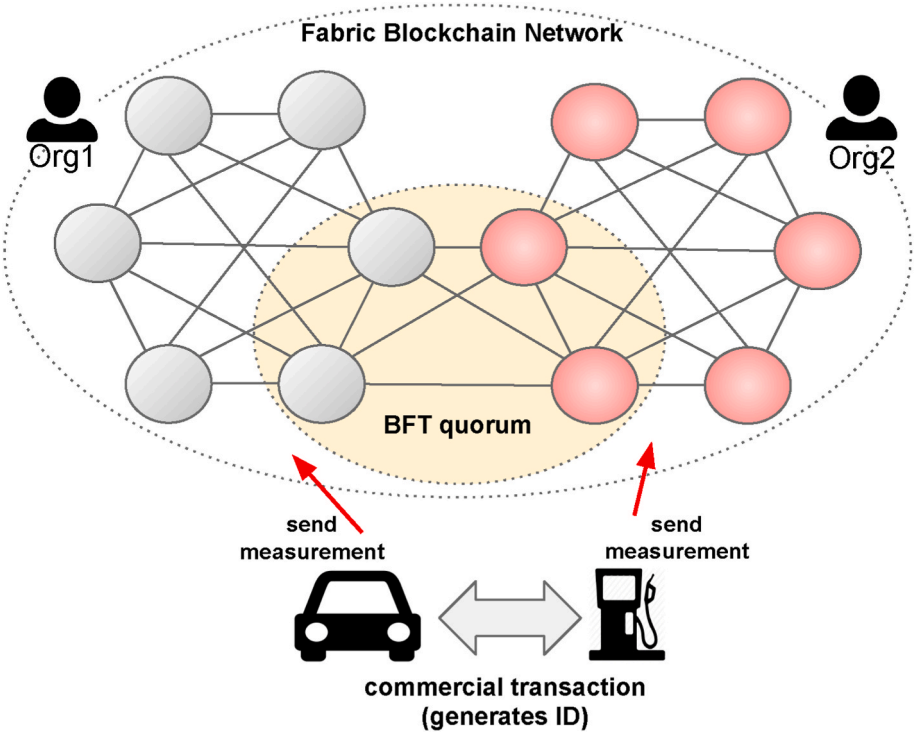

Fig. 4. The proposed blockchain architecture.

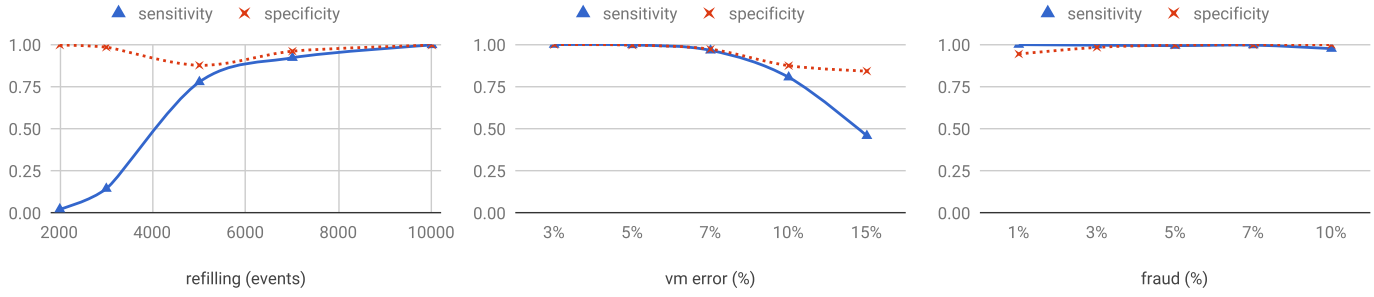

Fig. 5. Sensitivity and specificity rates in the tests round #1 (modifying E), round #2 (modifying v_{Err}), and round #3 (modifying D_f), respectively.

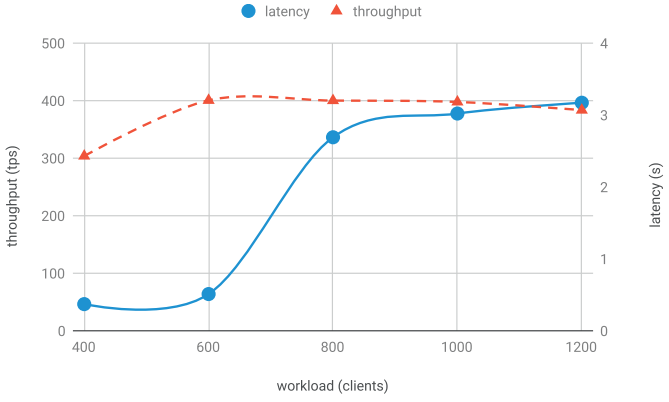

Fig. 6. Performance results in terms of transactions throughput and latency.

practical aspects, advantages, drawbacks, and limitations.

6.1. Practical aspects

We demonstrated the possibility of practical field surveillance of fuel dispensers by using innovative tools. Indeed, our proposal successfully combines IoT devices with digital ledgers (i.e., blockchains) to compose a solution for a classical activity in Legal Metrology. We claim that the DDSF meets one of the Legal Metrology main tendencies: optimize its activities using new technologies. We justify our claim by comparing the DDSF with some European Metrology Cloud strategies. The Metrology Cloud emerges from the idea that information must be available as soon as possible to improve decision making.

The practical implementation of the DDSF demands an agreement among the different stakeholders interested in promoting it. In Brazil, this group includes all the supply chain related to fuel distribution, besides the government and authorities responsible for coordinating legal metrology activities. The Brazilian scenario is particularly complex due to the country's extension and its political organization in federated units. On the other hand, we consider that smaller countries can find more agility in implementing these ideas. For instance, we believe that the European Metrology Cloud could take advantage of incorporating aspects of the DDSF model since the cloud specification already includes a metrological blockchain and connectivity among smart meters.

Fuel vendors and drivers can demand additional incentives to take part in a practical DDSF implementation. We remember that the first group is already under legal control since fuel dispensers receive periodic inspections from notified bodies. Indeed, fuel vendors need to pay

the expenses related to these inspections. So if the participation in the DDSF can reduce the inspections periodicity (e.g., semi-annually to annually), vendors will have a natural incentive to do that. Drivers' motivation depends on more effective incentives. Besides the natural motivation in avoiding fraud (nobody likes to be stolen), drivers will demand an affordable easy-of-use IoT device (the VFM) and a functional smart application to send their measurements to DDSF. More than that, they will need the perception that the system works and is efficient in restrain frauds.

6.2. Technical advantages

To the best of our knowledge, there are no similar works in literature reporting field surveillance solutions using technologies as IoT devices and distributed storage systems. We can only compare our solution with traditional processes that use people to inspect instruments and centralized databases to store inspection reports. Although that could be an uneven comparison, we can discuss our approach's technical aspects that we consider advantageous.

Perhaps the main technical achievement of our solution is to demonstrate how to inspect a highly accurate measuring instrument (i.e., fuel dispenser) using measurements from less accurate devices (i.e., VFMs). The Legal Metrology essentially determines that one must have a more precise instrument (usually called standard) to evaluate any ordinary measuring instrument. This procedure is what a notified body's representative does in an inspection (i.e., he needs a standard). We demonstrated (by relying on the LLN) that we can perform field surveillance using the VFM readings of a large group of vehicles. This idea introduces a new concept in Legal Metrology activities, which can save costs and report inspections continually (since we have enough drivers sending their VFM measurements).

We claim that another technical advantage is the option for using blockchains. As we already discussed before, the fuel measurements' reliability is one of the main concerns in field surveillance. Collusion among malicious entities is a recurrent thread because fraud involving fuel is very profitable. These entities can corrupt notified body representatives, offering bribes and convincing them to overlook inspection. Since notified bodies and even the legal authority cannot be assumed as always reliable, a centralized solution is not secure. Blockchains can address scenarios where stakeholders cannot find a trusted third party, providing trust among the involved parties (e.g., fuel vendors, drivers, and legal authorities).

We also need to emphasize the low implementation cost of our idea. As we discussed previously, the use of an app by drivers and the acquisition of devices to interface with the vehicle are not expensive. We also demonstrate that a blockchain network composed of eight machines is enough to support the demand related to a fleet of around 30 million vehicles, as is in São Paulo, Brazil. Besides, the use of smart contracts to implement surveillance strategies is straightforward and improves transparency.

6.3. Limitations and drawbacks

Our proposal also presents its limitations and drawbacks. One of the limitations regards our experiment assumptions. The experiment simulates tampered fuel dispensers with a particular behavior. It assumes that malicious instruments generate tampered measurements every time. In practice, the behavior of a compromised fuel dispenser can be more stealthy. For instance, a malicious vendor can activate and deactivate an electronic fraud on a fuel dispenser in a specific schedule (e.g., frauds are active on the weekends because there are more drivers and low probability of inspections). However, we do not see this limitation as a drawback. In our implementation, we used an elementary statistical analysis that presented satisfactory results. On the other hand, since we store the measurements in a distributed and decentralized ledger, any authorized stakeholder can implement smart contracts to proceed with different surveillance strategies. One can address different particular cases of malicious behavior using specific surveillance strategies. In practice, the DDSF enables different possibilities to detect and prevent fraud in measuring instruments.

A particular concern in the DDSF is the blockchain performance. When we compare the blockchain with a centralized solution, it is evident that the second performs better. Besides, the DDSF does not aggregate any novel feature to the blockchain platform to improve performance. It only uses a Hyperledger Fabric network instance to implement the storage layer. However, we argue that the blockchain's performance drawbacks are justified by its reliability properties. As we discussed before, reliability is the main reason to propose blockchains usage in the DDSF.

7. Conclusion

This paper presented a practical idea to implement the metrological surveillance of fuel dispensers using a blockchain-based distributed and decentralized solution. Our solution uses many fuel measurements from simple vehicular IoT-based meters to perform the fuel dispenser inspection, relying on the Law of Large Numbers. We also described all the steps in the DDSF conception. The framework takes advantage of the blockchains to store measurements reliably while enables surveillance practices by using smart contracts.

Now we revisit the research questions we proposed in the Introduction. About the first question, we conclude that we can perform the field surveillance of fuel dispensers without depending on inspections done for a third party. We demonstrate that we can get positive results in collecting information from drivers without checking the fuel dispenser integrity.

Regarding our second research question, we answer it with the results from our statistical analysis. In a hypothetical scenario where VFMs present error rates lower than 5%, and each vehicle refuels more than ten times on average, we can identify tampered fuel dispensers with sensitivity and specificity over 95%. The number of refillings per vehicle is very realistic. Since a driver refuels his vehicle once or twice a week, the DDSF would start to provide useful surveillance information in one or two months.

Finally, we can answer our third research question with our blockchain performance results. We demonstrate that our blockchain deployment can support a workload of 600 concurrent clients with a throughput higher than 350 tps and latency lower than 1 s. This performance meets the demand imposed by a scenario like São Paulo state, with 30 million vehicles and almost 9000 fuel stations. We recall that we used a small network composed of only eight peers. This result also indicates that DDSF is a low-cost alternative.

Our work's next steps are to create a complete prototype for Brazil's drivers and develop a more sophisticated analysis to proceed with field surveillance. These ideas also include developing an app for smartphones and specifying devices to interface with the vehicles using the OBD standard.

The next steps in our work are the creation of a complete prototype for drivers for a real pilot and the development of more sophisticated analysis to proceed with field surveillance. These ideas also include the development of an app for smartphones, and the specification of devices able to interface with the vehicles by using the OBD standard.

CRediT author statement

Wilson S. Melo Jr: Conceptualization of this study, Methodology, Software, Writing - Original Draft. Luiz V. Tarelho: Methodology, Formal analysis, Writing - Review & Editing. Bruno A. Rodrigues Filho: Data curation, Writing, Methodology, Formal analysis. Alysson N. Bessani: Resources, Writing - Review & Editing, Supervision, Project administration. Luiz F. R. C. Carmo: Supervision, Project administration.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledge

This work was partially supported by FCT through project Threat-Adapt (FCT-FNR/0002/2018), and the LASIGE Research Unit (UIDB/00408/2020 and UIDP/00408/2020).

References

Ahmed, A.A.I., Mohammed, S.A.E., Satte, M.A.M.H., 2017. Fuel management system. In: 2017 International Conference on Communication, Control, Computing and Electronics Engineering (ICCCCEE), pp. 1–7. https://doi.org/10.1109/ICCCCEE.2017.7867671.

Alcaide, A., Palomar, E., Montero-Castillo, J., Ribagorda, A., 2013. Anonymous authentication for privacy-preserving IoT target-driven applications. Comput. Secur. 37, 111–123. https://doi.org/10.1016/j.cose.2013.05.007.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S.W., Yellick, J., 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, pp. 1–15. https://doi.org/10.1145/3190508.3190538 arXiv:1801.10228.

Beteto, A., Melo, V., Dias, E., 2016. Fuel reselling: electronic documents and tax surveillance. Int. J. Econ. Manag. Syst. 1, 163–168.

Christidis, K., Devetsikiotis, M., 2016. Blockchains and smart contracts for the internet of things. IEEE Access 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339.

Dai, H.N., Zheng, Z., Zhang, Y., 2019. Blockchain for internet of things: a survey. IEEE Internet of Things Journal 6, 8076–8094. https://doi.org/10.1109/JIOT.2019.2920987 arXiv:1906.00245.

Dangeti, P., 2017. Statistics for Machine Learning. Packt Publishing Ltd.

Esche, M., Thiel, F., 2015. Software risk assessment for measuring instruments in legal metrology. In: Proceedings of the Federated Conference on Computer Science and Information Systems, pp. 1113–1123. https://doi.org/10.15439/2015F127.

Evans, M.J., Rosenthal, J.S., 2004. Probability and Statistics: the Science of Uncertainty. Macmillan.

International Organization of Legal Metrology (OIML), 2007. RECOMMENDATION 117-1 - Dynamic Measuring Systems for Liquids Other than Water.

Joint Committee For Guides In Metrology, 2012. International Vocabulary of Metrology – Basic and General Concepts and Associated Terms (VIM). https://doi.org/10.1016/0263-2241(85)90006-5.

Kassab, W., Darabkh, K.A., 2020. A–Z survey of Internet of Things: architectures, protocols, applications, recent advances, future directions and recommendations. J. Netw. Comput. Appl. 163, 102663. https://doi.org/10.1016/j.jnca.2020.102663.

Leitão, F.O., Vasconcellos, M.T., Brandão, P.C.R., 2014. Hardware and software countermeasures on high technology fraud at fuel dispensers under the scope of legal metrology. In: IX Simposio Internacional Metrologia 2014, pp. 1–10. Havana.

Luchsinger, H., Cajica, C., Maldonado, M., Castelazo, I., 2008. Are gas pumps measuring up? The Mexican experience. NCSLI Measure 3, 62–68.

Makhdoom, I., Abolhasan, M., Abbas, H., Ni, W., 2019. Blockchain's adoption in IoT: the challenges, and a way forward. J. Netw. Comput. Appl. 125, 251–279. https://doi.org/10.1016/j.jnca.2018.10.019.

Massoud, R., Bellotti, F., Berta, R., De Gloria, A., Poslad, S., 2019. Eco-driving profiling and behavioral shifts using IoT vehicular sensors combined with serious games. In: IEEE Conference on Computational Intelligence and Games, CIG, pp. 1–8. https://doi.org/10.1109/CIG.2019.8847992. IEEE.

Melo Jr., W.S., Bessani, A., Neves, N., Santin, A.O., Carmo, L.F.R.C., 2019. Using blockchains to implement distributed measuring systems. IEEE Trans. Instrum. Meas. 68, 1503–1514. https://doi.org/10.1109/TIM.2019.2898013.

Melo Jr., W.S., Machado, R.C.S., Peters, D., Moni, M., 2020. Public-key infrastructure for smart meters using blockchains. In: 2020 IEEE International Workshop on Metrology for Industry 4.0 and IoT, Rome, Italy, p. 7. https://doi.org/10.1109/MetroInd4.0IoT48571.2020.9138246.

Narwade, R., Patil, V., 2016. IOT: fuel quality and quantity, estimation of fuel adulteration and fuel quantity accuracy. SAE Technical Papers. https://doi.org/10.4271/2016-28-0219, 2016-Febru.

Obikoya, G.D., 2014. Design , construction , and implementation of a remote fuel-level monitoring system. EURASIP J. Wirel. Commun. Netw. 2014, 1–10.

Oppermann, A., Toro, F.G., Thiel, F., Seifert, J.P., 2018. Secure cloud computing: reference architecture for measuring instrument under legal control. Security and Privacy 1, 1–26. https://doi.org/10.1002/spy2.18.

Patil, S., Jagtap, H., Ippar, S., Vidhate, V., More, S., Biswas, P., 2017. Gasoline fraud buster. Int. J. Comput. Eng. Res. Trends 4, 444–448.

Peters, D., Wetzlich, J., Thiel, F., Seifert, J.p., 2018. Blockchain applications for legal metrology. In: IEEE International Instrumentation and Measurement Technology Conference, Houston, Texas, USA, p. 6. https://doi.org/10.1109/I2MTC.2018.8409668.

Peters, D., Yurchenko, A., Melo, W., Shirono, K., Usuda, T., Seifert, J.P.P., Thiel, F., 2020. IT security for measuring instruments: confidential checking of software functionality. In: Advances in Intelligent Systems and Computing, vol. 1129. Springer, Cham, pp. 701–720. https://doi.org/10.1007/978-3-030-39445-5_51. AISC.

Rocher, J., Taha, M., Parra, L., Lloret, J., 2018. IoT Sensor to detect fraudulent use of dyed fuels in smart cities. In: 2018 5th International Conference on Internet of Things: Systems, Management and Security, IoTSMS 2018. IEEE, pp. 86–92. https://doi.org/10.1109/IoTSMS.2018.8554631.

Rodrigues Filho, B.A., Gonçalves, R.F., 2015. Legal metrology, the economy and society: a systematic literature review. Measurement 69, 155–163. https://doi.org/10.1016/j.measurement.2015.03.028.

Rodrigues Filho, B.A., Gonçalves, R.F., 2016. Measuring the economic impact of metrological frauds in trade metrology using an Input-Output Model. IFIP Adv. Inf. Commun. Technol. 488 https://doi.org/10.1007/978-3-319-51133-7.

Sandrić, B., Jurčević, M., 2018. Metrology and quality assurance in internet of things. In: 2018 1st International Colloquium on Smart Grid Metrology, pp. 1–6. https://doi.org/10.23919/SMAGRIMET.2018.8369849. SmaGriMet 2018.

Sheng, Y., Shi, G., Qin, Z., 2018. A stronger law of large numbers for uncertain random variables. Soft Computing 22, 5655–5662.

Sheth, M., Rupani, P., 2020. Smart fleet monitoring system in Indian armed forces using internet of things (IoT). In: International Conference on Communication, Computing and Electronics Systems. Springer, Singapoure, pp. 573–580. https://doi.org/10.1007/978-981-15-2612-1_55.

Skog, I., Handel, P., 2014. Indirect instantaneous car-fuel consumption measurements. IEEE Trans. Instrum. Meas. 63, 3190–3198. https://doi.org/10.1109/TIM.2014.2315739.

Sousa, J., Bessani, A., Vukolić, M., 2018. A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform. In: 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 51–58. https://doi.org/10.1145/3152824.3152830.

Thiel, F., 2018. Digital transformation of legal metrology - the European Metrology Cloud. OIML Bulletin 59, 10–21.

Vukolić, M., 2017. Rethinking permissioned blockchains. In: Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts - BCC '17, pp. 3–7. https://doi.org/10.1145/3055518.3055526.

Wang, H., Zhang, J., 2019. Blockchain based data integrity verification for large-scale IoT data. IEEE Access 7, 164996–165006. https://doi.org/10.1109/ACCESS.2019.2952635.

Wüst, K., Gervais, A., 2018. Do you need a blockchain?. In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE, pp. 45–54. https://doi.org/10.1109/CVCBT.2018.00011.

Xiao, Y., Zhang, N., Lou, W., Hou, Y.T., 2020. A survey of distributed consensus protocols for blockchain networks. IEEE Commun. Surv. Tutorials EAA 1–27. https://doi.org/10.1109/COMST.2020.2969706 arXiv:1904.04098.

Yang, L., Ha, M., 2013. Laws of large numbers for uncertain variables. In: 2013 6th International Conference on Biomedical Engineering and Informatics. IEEE, pp. 765–772.

Yao, K., Gao, J., 2015. Law of large numbers for uncertain random variables. IEEE Trans. Fuzzy Syst. 24, 615–621.

Yurchenko, A., Moni, M., Peters, D., Nordholz, J., Thiel, F., 2020. Security for distributed smart meter: blockchain-based approach , ensuring privacy by functional encryption. In: Proceedings of the 10th International Conference on Cloud Computing and Services Science - CLOSER, pp. 292–301. https://doi.org/10.5220/0009377702920301.

Zheng, Z., Xie, S., Dai, H.N., Wang, H., 2017. Blockchain challenges and opportunities : a survey. Int. J. Web Grid Serv. 1–24. https://doi.org/10.1504/IJWGS.2018.095647.

Wilson S. Melo Jr. is a Researcher and active Lecturer at the Brazilian National Institute of Metrology, Quality, and Technology (Inmetro). He holds a Ph.D. in Computer Sciences from the Federal University of Rio de Janeiro (UFRJ). He has more than 20 years of experience with software development and testing projects. His main expertise regards software for industrial applications, especially solutions related to measurement, control, patterns recognizing, and cybersecurity.

Luiz V. Tarelho received a Ph.D. in Nuclear Technology-Applications by IPEN-USP in 2001. He was a researcher at IPEN-CNEN from 1998 to 2008 in the area of Lasers and Applications. In 2008, he became a researcher at the National Institute of Metrology, Quality, and Technology where he works with the applications of optics and spectroscopy in the standardization and dissemination of the quantities of the International System of Units. From 2008 to 2011 he developed projects for the standardization and dissemination of the length quantity. As of 2011, he developed projects in time and frequency metrology to achieve standardization and dissemination by electro-optical methods. Currently, he works in the Division of metrology for Information and Communication Technologies and uses quantum optical metrology for applications in cryptography and cybersecurity.

Bruno A. Rodrigues Filho is a Ph.D. in Industrial Engineering and an expert in legal metrology, whose research is mainly focused on numerical methods to understand the impact of metrology activities in both society and economy. Dr. Rodrigues Filho is a Researcher at Inmetro, the National Metrology Institute in Brazil, and carrying out activities as research in legal metrology processes, accreditation, and conformity assessment. He also is responsible for a project aiming to implement a proficiency testing of sphygmomanometer in Brazil. The researcher is also a member of the International Organization of Legal Metrology Technical Subcommittee TC 3/SC 5 Conformity Assessment.

Alysson N. Bessani is an Associate Professor of the Faculty of Sciences of the University of Lisboa, Portugal, and a member of LASIGE research unit. He holds a Ph.D. in Electrical Engineering from UFSC (Brazil) and was a visiting professor in Carnegie Mellow University (2010) and a visiting researcher in Microsoft Research Cambridge (2014). He is the co-author of more than 100 peer-reviewed publications on dependability, security, Byzantine fault tolerance, and cloud. More information about him can be found at http://www.di.fc.ul.pt/bessani.

Luiz F. R. C. Carmo received a Ph.D. degree in Computer Science in 1994, from the LAAS/CNRS, Toulouse III – France. Presently, he is a Senior Specialist in Computer Sciences of the Brazilian Institute of Metrology, Technology, and Quality (Inmetro). He is an active lecturer of both the Doctoral programs in Computer Sciences of UFRJ and in the Metrology of Inmetro. His research interests include information security and embedded systems.