METROLOGIA
2023

Blockchain network to conformity assessment bodies

E G Machado[1], R T R Gomes[2], E V A Martins[1], I L Vieira[3], E L Madruga[1] and W S Melo Jr.[1]

[1] National Institute of Metrology, Quality and Technology, Duque de Caxias, 25250-020, Brazil
[2] Fluminense Federal University, Niteroi, 24210-310, Brazil
[3] Auge Tech, Rio de Janeiro, 22420-040, Brazil

edugmac@gmail.com

Abstract. We have developed a blockchain network for conformity assessment bodies. This system aims to assure the integrity of results from distributed measurement systems used by these organizations. To evaluate the functionality of the proposed blockchain solution, we conducted a case study simulating a force measurement instrument (brake tester) and the blockchain network using Hyperledger Fabric platform. The simulation results demonstrated that the method is applicable in real-world conditions and that blockchains show potential for providing robust and reliable solutions in managing and safeguarding data from distributed measurement systems used by conformity assessment bodies.

1. Introduction

The world is immersed in the age of information and automation, where the physical and cyber realities are increasingly interconnected. Metrology is undergoing a digital transformation too [1]. Measurement systems are responsible for gathering information about physical quantities and providing data for decision-making by conformity assessment bodies. Certification and inspection organizations utilize measurement instruments integrated into computer systems in various scenarios. Distributed Measurement Systems (DMS) are a special case of measurement instruments. Generally, DMS consist of multiple measurement or processing units interconnected through a network. DMS have the capability to perform measurements in remote and distinct locations, add or remove nodes without altering the entire network structure, and share resources among nodes, thus reducing costs and optimizing equipment usage. Therefore, they are flexible measurement systems used by notified bodies to approve or reject products under analysis. The assessment provided by these bodies is economically strategic.

As a result, DMS used in conformity assessment bodies are targeted for attacks with the aim of manipulating measurements to gain financial benefits. Implementing the appropriate cybersecurity measures is a requirement to ensure the reliability and security of data [2]. The cybersecurity of measurement instruments is a challenge for smart meters and a major concern in the present [3]. Fraudulent measurements can lead to unfair commercial transactions, financial losses, and risks to public safety [4]. In this context, blockchain technology has been considered a promising solution to ensure the integrity and security of measurement data. Blockchains can provide a decentralized and trustworthy storage environment for recording and verifying measurements, preventing fraud, and ensuring information traceability. Additionally, data captured by measurement instruments can be processed in a distributed manner using smart contracts [5], making it more challenging to protect from attacks.

The overall objective of this work is to propose a blockchain-based solution that provides additional levels of cybersecurity for DMS used by conformity assessment bodies. Our focus is to explore how blockchain can enhance cybersecurity in distributed measurement systems. We conduct experiments to test our proposed model's effectiveness and performance. This research aims to advance metrology and protect measurement systems used by conformity assessment bodies. We develop applications to safeguard measurement data in critical distributed systems that are vital to the economy and society. The ultimate goal of this work is to promote trust and transparency in the conducted measurements, essential to ensure quality, safety, and fairness in various domains.

2. Related Works

Blockchain is a peer-to-peer network formed by different organizations for the secure storage of information. This technology emerged in 2008 with the creation of Bitcoin. It offers a decentralized and secure alternative to the financial market [6]. It consists of a chain of information blocks that store multiple transactions. Each new block added to the network references the previous ones, forming a distributed and immutable ledger. New blocks are validated through a mechanism called consensus. Cryptographic techniques are applied to ensure data authenticity and integrity. Currently, it finds applications in various projects across different sectors. Smart contracts act as computer programs executed on the blockchain network, combining computational protocols with user interfaces to enforce the terms of the contract. This technology can be used to process and store data from DMS.

Distributed Measurement Systems (DMS) can be defined as arrangements for performing monitoring and measurement tasks, where each node possesses computational and communication capabilities [7]. They find applications in various sectors, such as automotive, aviation, astrophysics, and communication systems [8, 9] to measure quantities such as the energy of a vehicular impact, aircraft altitude, velocity, among others.

Brake testers are DMS used by accredited inspection bodies to assess the braking system of vehicles [10]. They have ten sensors that measure vertical and braking force. Their processing system performs calculations to obtain measurements of braking efficiency and imbalance for the service and parking brakes of inspected vehicles. The results are used to assess compliance with the NBR 14040-6 standard and issue the Vehicle Safety Certificates (CSV). The Brazilian National Traffic Department reported that nearly 2 million CSVs were issued in 2021 [11].

Previous work has been conducted concerning the cybersecurity of distributed measuring and blockchain networks. A secure architecture for measurement instruments with embedded computer systems was proposed by [12]. However, the processing of sensor data to obtain measurement results occurs in a centralized manner within the instrument itself. In attack scenarios where the attacker has direct access to the measurement instrument, it becomes an easy target. The approach suggested by [5] proposes to process information from sensors and generate a consolidated measurement value within a blockchain network environment, using smart contracts. This strategy increases the security level of DMS while simplifying the model approval of new instruments by regulatory agencies. Furthermore, [13] developed a blockchain network targeted for national metrology institutes, aiming to implement applications and activities within the context of legal metrology. However, this network is specifically designed for research applications involving meters and does not include processes related to accredited bodies.

In this work, the goal was to combine and extend the findings of previous research efforts. Blockchain was chosen as the solution due to the absence of a trusted third party available to store the generated data, and because there are multiple eligible candidates capable of participating in the network.

3. Blockchain Network for Conformity Assessment Bodies

This work describes the development of a blockchain network tailored for conformity assessment bodies. It offers a solution that ensures transparency and integrity of measurement data for notified organizations. Additionally, it shifts the processing of measurements to the blockchain network. The blockchain network comprises conformity assessment bodies and regulatory authorities. It is a permissioned network, enabling authentication of its participants. The use of blockchain technology is particularly advantageous when there is no trusted third party available to store and validate information or when technical or economic infeasibility exists for such a setup. While National Metrology Institutes (NMI) could serve as a trusted third party, the costs of storing and auditing measurement results from conformity assessment bodies are prohibitively high. Moreover, blockchain operates as a collaborative network, where participants send and store information within the chain. In general, incentives are provided to encourage participants to contribute to the network. However, participating in the blockchain of conformity assessment bodies might be a requirement for accreditation, which serves as a sufficient incentive. Figure 1 illustrates an overview of how participants interact within the network.

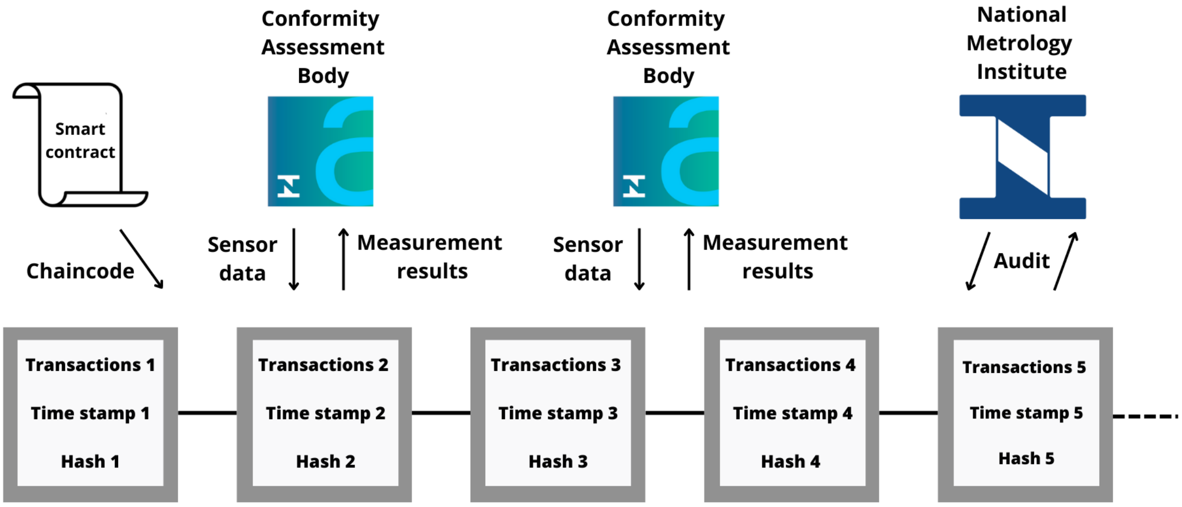

Figure 1. Scheme of the Blockchain Network for Conformity Assessment Bodies.

Typically, sensor data serves as the input for a measurement but often requires some processing, such as performing calculations to obtain the result of a derived quantity. The blockchain network stores sensor data from distributed measurement systems and, through smart contracts, performs the necessary calculations to aggregate the sensor information and carry out the measurement realization. DMS inherently possess connectivity between their elements. While this feature increases the attack surface, it also enables the instrument to connect to platforms like the blockchain network. This processing is particularly relevant in DMS because, in many cases, it is necessary to gather information from different sensors to achieve the measurement's objective. For instance, in the case of the brake tester, it aggregates the vertical force information from sensors on each side of vehicle inspected and then performs calculations involving braking force to determine the desired parameters, such as efficiency and imbalance. In conventional instruments, this measurement realization typically occurs in a centralized manner, making it a critical target for cyber-physical attacks.

Despite the connectivity DMS increases the attack surface, by integrating DMS into a blockchain network, the processing and validation of measurements can occur in a distributed and secure manner. Utilizing smart contracts, the blockchain can facilitate the collaborative processing of data from various sensors while ensuring its integrity and preventing unauthorized alterations. This approach significantly enhances the DMS security and safeguards against potential cyber-physical attacks that target centralized measurement processing systems. In the blockchain network for conformity assessment bodies, the measurement processing occurs using smart contracts that run the chaincode. This decentralized approach allows multiple entities to participate in the measurement calculations, thereby mitigating attacks that aim to tamper with the software responsible for the measurement realization. Additionally, different versions of smart contracts can be registered on the ledger, ensuring the integrity of the involved code.

The blockchain network is utilized to preserve the integrity of measurement results. While conventional instruments store results in local memories or centralized servers, in our model, each participant in the network has a copy of the measurement results, accessible according to the established business rules for the network. Consequently, the success of attacks attempting to tamper with the already calculated results would require substantial computational power or extensive participation in the network, making the attack more costly than the benefits intended to be obtained.

Moreover, measurements can be queried and audited through smart contracts to identify possible inconsistencies or fraud. This enhances transparency and accountability within the network, ensuring that the measurement data remains reliable and trustworthy. The blockchain distributed nature and the use of smart contracts for measurement processing and validation contribute to the overall system's robustness and security, making it resilient against fraudulent activities or unauthorized alterations.

3.1. Simulation of Brake Testers

Accredited vehicle inspection bodies employ the brake tester as a measurement instrument to assess the conformity of brakes in vehicles, particularly those transporting hazardous goods or powered by compressed natural gas. Due to the nature of these vehicles, such inspections are deemed critical to ensure their safe operation on public roads. The brake tester traditionally comprises ten load cell-type sensors, two of which measure braking force, while the remaining eight measure vertical force. The overall braking efficiency (1) and braking imbalance per axle (2) are calculated using the following equations, where "i" represents each vehicle wheel and "n" denotes the total number of wheels.

$$\text{braking efficiency} = \frac{\sum_{i=1}^{n} \text{braking effort}}{\sum_{i=1}^{n} \text{vertical effort}} \tag{1}$$

$$\text{braking imbalance} = \frac{\text{higher brake effort - lower brake effort}}{\text{higher brake effort}} \tag{2}$$

Given its critical role in the inspection process, the brake tester becomes a primary target for cyber-attacks. Malicious actors seek to gain undue advantage through fraudulent activities. Examples of such attacks include tampering with calculation parameters or sensor sensitivity and manipulating the centralized database stored on each instrument's server. These potential frauds pose a threat to the integrity of measurements conducted by the brake tester, compromising its ability to ensure the safety of inspected vehicles.

We implemented a prototype[1] which reproduces a blockchain network using the HyperLedger Fabric platform version 2.2 LTS. This network is permissioned and composed of conformity assessment bodies and the Brazilian National Institute of Metrology, Quality and Technology. A smart contract receives vertical and braking force data from all brake tester sensors, aggregates this information, and performs distributed calculations for braking efficiency and imbalance measurement. Additionally, the smart contract records the inspection result, indicating whether the vehicle has been approved or rejected

[1] https://github.com/rafaeltiribas/braketester-smart-contract

according to normative parameters. The system is capable of differentiating between light and heavy vehicles, as well as identifying those with more than two axles, which affects the measurement calculations. Both service and parking brakes are measured. The inputs and outputs of the program are stored in the distributed ledger, ensuring measurement integrity and making the results auditable.

A JSON file was generated containing the test data obtained from a real brake test. This file was then replicated multiple times, creating new transactions that were written to the blockchain. The test time was one minute. The objective was to determine how many identical transactions from a real test the simulation environment could record on the network, generating new blocks. Additionally, we aimed to verify if the smart contract produced the same results as the calculations performed in the real test. As the test involved real data, the information used was treated as confidential.

Furthermore, the simulation was performed to verify whether the blockchain network for conformity assessment bodies can handle the transaction volume compatible with the number of issued CSVs. A standard microcomputer, with 16 GB of RAM and an Intel i7 processor, was used for this test. The results showed an average of 97 brake tests registered per minute, which translates to over 15 million tests per year. The test was conducted and demonstrated acceptable performance for the limited computational environment of the simulation. Scalability tests on dedicated computers for deployment show that the infrastructure based on Hyperledger Fabric is capable of recording up to 3500 transactions per minute [14]. This quantity exceeds the 2 million per year CSVs that were issued, according to [11]. Therefore, the network demonstrates its ability to handle the necessary transactions for conformity assessment bodies effectively.

4. Conclusion

In conclusion, the development of a blockchain network tailored for conformity assessment bodies represents a significant step towards enhancing the integrity and security of measurement data. By utilizing smart contracts and distributed processing, the network ensures that measurement realization occurs in a collaborative and tamper-resistant manner, mitigating cyber-attacks and fraudulent activities.

The implementation of a prototype using the HyperLedger Fabric platform demonstrated the practical viability of the network. The smart contract successfully aggregated data from brake tester sensors, performed distributed calculations, and recorded inspection results on the ledger, guaranteeing data integrity and auditability. Furthermore, the performance test showcased the network's capability to handle a substantial volume of transactions, surpassing the number of issued CSV. This confirms the network's effectiveness in real-world conditions and its ability to support the requirements of conformity assessment bodies.

Overall, the blockchain network for conformity assessment bodies provides a reliable and transparent environment for preserving measurement integrity, facilitating trust between stakeholders, and ensuring the safety and fairness of inspections. This technology can play a crucial role in advancing metrology and protecting critical distributed measurement systems used by conformity assessment bodies, ultimately benefiting the economy and society as a whole. As the field of cybersecurity and metrology continues to evolve, blockchain technology stands at the forefront as a promising solution to safeguard measurement data and promote trust in various industries and sectors.

References

[1] Thiel F, Esche M, Grasso Toro F, et al. The European Metrology Cloud. EDP Sciences, 2017, p. 09001.

[2] Lombardo L. Distributed Measurement Systems: Advantages and Challenges of Wireless Sensor Networks. *IEEE Instrum Meas Mag* 2022; 25: 21–28.

[3] Rastogi S. *Internet of Things based Smart Electricity Meters*. 2016.

[4] Souza RP de. *Um arcabouço tecnológico para detecção de possíveis serviços fraudulentos em organismos de avaliação da conformidade*. Tese de Doutorado, Universidade Federal do Rio de Janeiro, 2017.

[5] Melo Jr. WS, Bessani A, Neves N, et al. Using Blockchains to Implement Distributed Measuring Systems. *IEEE Trans Instrum Meas* 2019; 68: 1503–1514.

[6] Nofer M, Gomber P, Hinz O, et al. Blockchain. *Business and Information Systems Engineering* 2017; 59: 183–187.

[7] Lamonaca F, Carni DL, Grimaldi D, et al. Mobile object to speed up the synchronization of IoT network. *2017 IEEE International Workshop on Measurement and Networking, M and N 2017 - Proceedings*. Epub ahead of print 2017. DOI: 10.1109/IWMN.2017.8078356.

[8] Druzhinin Y, Sokolov V. Features of data collection at strict schedule in distributed measurement system with ring structure. *Proceedings of 2017 10th International Conference Management of Large-Scale System Development, MLSD 2017*. Epub ahead of print 2017. DOI: 10.1109/MLSD.2017.8109612.

[9] Wiesner A, Kovacshazy T. Distributed Measurement System for Performance Evaluation of Embedded Clock Synchronization Solutions. *2022 23rd International Carpathian Control Conference, ICCC 2022* 2022; 293–298.

[10] Machado EG, Wojciechowski RB, Corrêa I, et al. Comparação de frenômetros de diferentes organismos de inspeção acreditados. In: *VI Congresso Internacional de Metrologia Mecânica (2021)*. Rio de Janeiro, pp. 1–8.

[11] Senatran. Anuário 2021, https://www.gov.br/transportes/pt-br/assuntos/transito/conteudo-Senatran/estatisticas-senatran/anuariosenatran2021.pdf (2022, accessed 11 July 2023).

[12] Peters D, Peter M, Seifert JP, et al. A secure system architecture for measuring instruments in legal metrology. *Computers* 2015; 4: 61–86.

[13] Moni M, Melo W, Peters D, et al. When measurements meet blockchain: On behalf of an inter-nmi network. *Sensors* 2021; 21: 1–24.

[14] Pajooh HH, Rashid M, Alam F, et al. Hyperledger fabric blockchain for securing the edge internet of things. *Sensors (Switzerland)* 2021; 21: 1–29.

Acknowledgments

This work was partially supported by Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro (FAPERJ), grants E-26/205.266/2022 and E-26/260.179/2023.