How Blockchains can improve Measuring Instruments Regulation and Control

Wilson Melo Jr, Luiz F. R. C. Carmo
National Institute of Metrology,
Quality and Technology, RJ, Brazil

Alysson Bessani, Nuno Neves
LaSIGE, Faculdade de Ciências
Universidade de Lisboa, Portugal

Altair Santin
Pontifical Catholic University of Parana
Curitiba, PR, Brazil

***Abstract*—In the last years, measuring instruments have become quite complex due to the integration of embedded hardware and software components and the increasing aggregation of new features. Consequently, metrological regulation and control require more efforts from notified bodies, becoming slower and more expensive. In this work, we evaluate how blockchains can help to overcome such challenges. We propose a conceptual model for implementing measuring instruments in a distributed blockchain-based architecture, and compare it with traditional measuring instruments and distributed measuring models discussed in previous works. We also develop a security analysis, demonstrating that blockchains-based measuring systems can impact how measuring instruments are used in consumer relations, at the same time that improve security and simplify metrological regulation and control. At the end, we point out the main challenges, suggesting alternatives and potential research lines for future works.**

I. Introduction

Measurement instruments (MI) are used in a diversity of applications including industry, commerce, energy, transportation, medical care and environment protection [1]. Only in Europe, MI are responsible for an annual turnover of more than 500 billion Euros [2]. In developing countries, the demand for MI has increased substantially due to the adoption of technologies and methods well established in developed countries [1]. MI also can be seen as elementary building blocks for new technologies such as internet of things and cyber physical systems (e.g., smart grids) [1], [2], [3], [4], [5], [6].

MI are nowadays quite complex, since they are strongly based on embedded electronic and software and are often connected and accessible by the Internet [2], [3]. That creates security gaps which can be explored with malicious intent [4], [5]. Legal metrology is responsible for promoting MI metrological assurance, establishing security requirements and technical activities such as type approval, verification and metrological supervision [1]. However, the increasing complexity of MI affects such activities substantially. Type approval requires more efforts while verification can involve use cases which are hard to reproduce inside labs. In turn, metrological supervision becomes difficult due to the high number of MI different models and versions, the capillarity of their deployment and the limited resources owned by regulation agencies.

We work with the hypothesis that such difficulties should be overcome with alternative approaches that simplify MI design while employing strategies for decentralizing metrological supervision. Such idea finds many aspects in common with a new trendy technology: *blockchains* [7]. A blockchain can be described as a distributed data structure which assures information integrity and authenticity while providing a platform for executing self-enforce software procedures, called *smart contracts* [8]. Blockchain solutions have been very successful in financial applications (e.g., Bitcoin and Ethereum), which motivates innovative ideas using blockchains in different applications and knowledge areas [7], [8].

In this paper we discuss how blockchains can improve measuring applications, evaluating two main aspects: *distributed measuring* (DM) and *decentralized surveillance*. We start from preliminary concepts already consolidated in MI regulation and control. Then we explore ideas related to the integration of MI in Distributed Measuring Systems (DMS), proposing a blockchain-based model. Such aspects result in an innovative concept that dissociates the measurement service from the measurement quantity while improves MI security and makes metrological assurance simpler and less expensive.

Our main contributions can be summarized as follows:

- We introduce the idea of DM using blockchains and describe its advantages when compared to traditional MI and other DM models. To the best of our knowledge, we are the first to describe a blockchains-based DMS.
- We propose an architectural model for implementing our idea, showing that MI and blockchains enable a new business model where the measuring process is seen as an independent service, which reduces conflict of interests.
- We develop a security analysis, showing that our model improves MI security since it constrains the attacker capabilities, thus simplifying MI regulation and control.

II. Background

A. Legal metrology and MI reliability

Legal metrology embraces MI regulation and control. It is crucial to assure the measurements correctness, having a significant impact over countries competitiveness [1]. Legal metrology protects the economic system and regulates consumer relations, while enhancing MI public reliability [6].

Usually, legal metrology regulations are defined by government agencies or international committees. Once a regulation directive is approved, it traditionally establishes a set of requirements and activities for providing MI metrological

assurance [1]. Activities are classified in two levels. The first level is related to legal control and includes MI type approval, validation and verification. The second level activities covers metrological supervision, including quality, marketing and field surveillance. Activities can be executed by different parties according to the directives adopted in regulation. Usually, notified bodies[1] are designated to assert MI conformity in both activity levels [2], [6].

When one talks about electronic and software controlled MI, legal metrology activities can demand more complex procedures and specialized knowledge. Usually, regulation adopts security requirements and good practices from well consolidated technical standards [2], [5], [9]. The *OIML*[2] *D 31(E)* document and *WELMEC*[3] *Software Guide 7.2* are probably the more widespread standards for software controlled MI design, deployment and inspection. Both documents are taken as reference by metrological agencies, notified bodies and manufacturers in different countries [3], [5].

The majority of security issues with MI are associated to economic undue advantages taken by attackers, which are interested in the measured physical quantity value. A classical example occurs in the commerce of measured goods where vendors and consumers have conflicting interests[1]. Malicious vendors can try to maximize profits while malicious consumers can try to minimize prices by tampering measurements. Measurement frauds against MI (such as scales, energy meters and fuel pumps) are very common in developing countries [3], [9]. Attacks can also intend to steal sensitive information and intellectual property [3], [6]. In some cases they even threat people physical integrity (e.g., tampering measurements related to medical procedures) [4].

B. Distributed measuring

Distributed measuring (DM) is a concept supported by previous works. Boccardo et al. [4] describes a strategy to simplify MI type approval and supervision activities related to medical MI. That consists in signing sensing raw data immediately after analog-to-digital (AD) conversion. Such approach suggests that part of the measurement computing can be done externally to the MI hardware core due to the use of a digital signature for checking sensing data integrity and authenticity. In turn, Peters et al. [5] describes a MI security framework using virtual machines to get separation among *legally relevant* (LR) and *non-legally relevant* (NLR) software.[4] The authors propose different virtual machines to execute LR and NLR functions and define secure interfaces for communicating among them. Such approach is presented as an alternative to improve security and reduce MI complexity. Additionally, it enables virtualization using different hardware cores and consequently allows the implementation of *Distributed Measuring Systems* (DMS). Lastly, a DM architecture using cloud computing is discussed by Oppermann et al. [6]. The authors present advantages related to IT infrastructure cost-savings and the possibility of MI manufacturers to offer modern interconnected devices and features. In contrast, they also point out problems related to communication security, data management and reliability. Broadly speaking, they assert that the following challenges need to be addressed:

- DM instruments must be as secure as their classical counterparts.
- Large amounts of data will be accumulated in distributed repositories, requiring proper treatment.
- If distributed service providers are considered untrustworthy, then data security is very difficult to assure.

C. Blockchains

Blockchain is an emerging technology which has called attention of stakeholders in different industry segments. Initially associated to crypto-currency markets due to Bitcoin popularity [7], blockchain-based architectures have been proposed for a wide set of application areas including sensors networks, internet of things, smart cities, among others [7], [8], [10].

Conceptually, a blockchain can be regarded as a distributed append-only data structure (designated as *ledger*) which is replicated and shared among a set of network peers [8]. This structure consists of a sequence of blocks where block n is cryptographically linked to the block $n-1$ using a hash function. Consequently, block n can not be changed without also modifying all subsequent blocks $n+i, ..., n+k$ [11]. Being a decentralized model, blockchains availability does not depend on third parties, which can greatly save costs [7]. In turn, integrity and availability are ensured by consensus among the peers, preventing the whole chain from being modified and requiring an agreement about any block to be appended to the ledger [11], [12]. Blockchain platforms can be classified as *permissionless*, when anybody can join to the network and participate in the network consensus, or *permissioned*, when consensus is achieved by a set of known and identifiable peers [12], [10]. Usually, permissioned blockchains consensus protocols expend less computational resources and can reach better transaction latency and throughput [11].

A blockchain can store virtually any digital asset, from data to self-executing scripts, usually defined as *smart contracts*. Ethereum [8] is probably the most well-known blockchain implementation supporting that. That makes blockchain not only a data storage architecture but also a complete distributed platform for proper and distributed automated workflow [8]. Once smart contracts are executed at every network peer in an independent and automatic manner, software integrity is achieved from blockchains integrity as a whole.

III. Defining MI Security Scope

In this work, we want to evaluate the security level of different measuring systems models and so point out advantages and drawbacks of each model. We are specially interested in MI reliability and the required efforts for providing MI metrological assurance. Metrological requirements and activities are very

[1]Notified bodies are public or private parties organized for verifying MI.

[2]OIML is the International Organization of Legal Metrology.

[3]WELMEC is the European committee to promote cooperation in the field of legal metrology.

[4]OIML D 31(E) and WELMEC 7.2 uses LR to designate any component which can affect measuring final results, while NLR can not do that.

particular for different MI classes. However, an elementary set of requirements and activities are representative to a most of software controlled MI in terms of security properties. Knowing that, we define our MI security scope based on a generic attack model and its respective metrological assurance framework. Both are described as follows.

A. Attack model

We consider a simple attack model that can be formulated from MI use cases, accordingly to OIML D 31(E) and WELMEC 7.2 guides. MI are targeted by malicious entities trying to get undue economical advantages by tampering with measurements. Basically, the attacker capability consists in changing MI expected behavior, tampering any LR component and compromising measurements reliability.

We assume the attacker could be any entity with access to the MI components or sensitive features, at any moment of its lifecycle. That includes manufacturers, vendors, clients and other entities. Malicious manufacturer staff (e.g., a malicious programmer) can inject software vulnerabilities and backdoors, "selling" them to other potential attackers. Once a MI is deployed, vendors and clients can have access to its resources, exploring eventual failures and misbehaviors or changing sensitive parameters related to MI precision. Furthermore, modern MI usually provide interfaces for loading software upgrades and improvements. Such features can be explored by malicious vendors and clients for loading tampered LR software or for modifying critical parameters.

In opposite, we establish that an attacker can not compromise tamper-proof hardware devices, neither cryptographic primitives and communication protocols from algorithms recognized as secure. In addition, we also define that an attacker can not launch collusion attacks with more than a fraction of peers that integrates the network. The exact value of this fraction depends on the blockchain implementation [12].

B. Basic Metrological Assurance Framework (BMAF)

We also assume the existence of a Basic Metrological Assurance Framework (BMAF) tailored to implement MI regulation and control, which works as a countermeasure to the previously described attack model. Despite BMAF explicits a minimal set of requirements and activities, its conception is very realistic since its statements can be found in regulation directives implemented in several countries [2], [3], [4], [9].

Our BMAF sets the following protection requirements:

- **R1**: MI have reliable physical sealing to protect physical components such as sensors and electronic circuits;
- **R2**: MI implement acceptable mechanisms for LR software identification and integrity checking by notified bodies during MI supervision;
- **R3**: MI implement secure mechanisms for LR software loading that accept only software modules signed by manufacturers and responsible notification bodies.

In turn, BMAF also establishes the following control and supervision activities:

- **A1**: MI type approval includes MI hardware and software detailed analysis, LR software source code inspection and conformity assessment regard to the MI protection requirements;
- **A2**: MI validation and verification of all relevant MI use cases identified during type approval;
- **A3**: MI supervision by periodic inspection in both manufacturing site and application field. Activities must include MI seal verification and LR software identification and integrity check.

IV. Blockchains in Measuring Systems

In this section, we compare three different measuring systems models: the traditional MI, a cloud-based measuring system and our blockchain-based measuring system model (see Figure 1). For each model we describe the applicable supervision activities, using different sized icons to represent the expected magnitude of effort and cost associated with it.

A. Traditional MI

Traditional MI can be seen as dedicated computers calculating measurements of a physical quantity (e.g., size, weight, speed). They include sensors for interfacing with the physical world and AD converters for gathering data, besides other LR and NLR components, which are usually software modules. Sensors and AD converters are also LR components, being usually immutable hardware components (Figure 1-A).

Although LR and NLR software separation is a well-known concept, many MI manufacturers do not adopt such practice. The claimed reasons are costs, computational resources restrictions or the existence of a legacy software. As a paradox, despite their complexity, traditional MI software modules are usually monolithic systems. That affects metrological assurance activities substantially, making MI regulation and control more expensive and complex, due to the follow aspects:

- Type approval can demand MI hardware and software evaluation and checking against a set of reliability requirements. Once LR and NLR are usually tightly coupled, notified bodies leading type approval need to evaluate and attest th compliance of all software modules. In some cases, LR software source code must be inspected for assuring their correctness.
- Software validation and verification can become more difficult due to the diversity of MI use cases, being many of them hard to reproduce out of the real measurement environment.
- Metrological supervision requires that notified bodies have sufficient staff to proceed with MI surveillance activities in both manufacturing and field. Albeit physical seals can be helpful to protect physical components, they are innocuous to protect software components.

Due to their complexity, the activities also demand a highly qualified professional profile, complementary checking and greater supervision staff proficiency. These factors contribute to make MI regulation and control a very expensive and time consuming process.

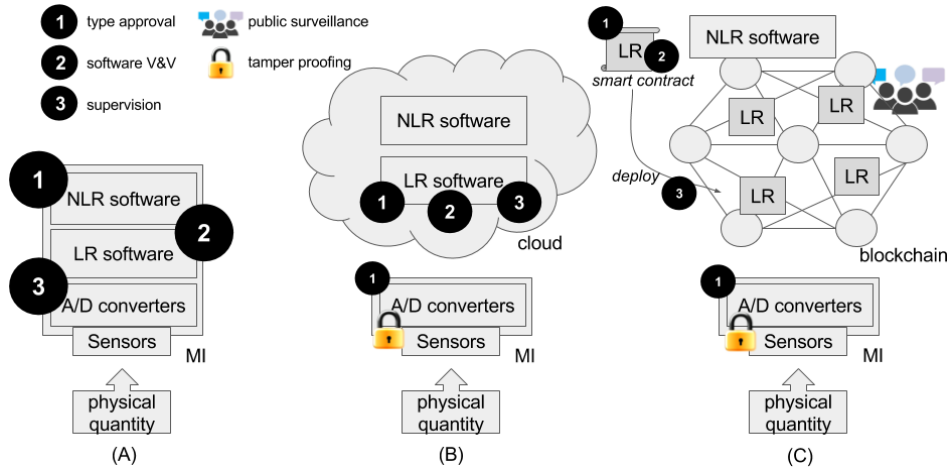

Fig. 1. Comparing measuring models: (A) Traditional MI; (B) Cloud Measuring System; (C) Blockchain Measurement System

B. Cloud-based Measuring System

When LR and NLR components are properly separated in independent modules, one could run these modules in different hardware sets connected by well-defined interfaces. Such architecture leads to a DMS. For evaluating its properties, we take a cloud computing MI model inspired in [6]. In this model, LR and NLR software are running as cloud services, outside of MI physical set (Figure 1-B). We assume MI communicates with the cloud services using a secure channel (e.g., TLS) and that side channel attacks are infeasible.

When traditional and cloud models are compared, one can observe that the distributed architecture simplifies MI devices. MI practically do not include software components anymore once both LR and NLR software modules are running in the cloud. In practice, MI is now set up as a blend of sensors, AD converters and a communication interface that ables MI to send sensing raw data to the cloud measuring system. Basically, the MI could be designed only based on hardware components (e.g., smart sensors, cryptographic chips), although one should consider that some elementary software could be necessary. In any case, a significantly amount of software is moved to the cloud and works as a service. Consequently, LR and NLR software can be scaled accordingly to the demand.

C. Blockchain-based Measuring System

Now we introduce the *blockchain model* (Figure-1-C). We consider that MI basically generate and store reliable measurements of physical quantities while managing the interests of different involved parties (e.g., consumption relations). Thus measurements can be seen as *transactions* whose values must be protected against tampering and unintentional changes [2]. Such aspects make DM a typical use case for blockchains applications.

As a first and intuitive insight, we devise a distributed ledger storing reliable measurement transactions which can be checked by any involved party. In addition, the blockchain also would support the execution of LR (and even NLR) software using smart contracts, which process information from sensors and generate a consolidated measurement value. The integrity of measurements and LR software (as smart contracts) is preserved by blockchain implicit properties [7]. The ledger accounting enables the management of cumulative consumption transactions, such as energy and gas metering. If a financial blockchain platform is used, it can integrate billing and payment functions. That is an interesting additional resource when compared to the cloud model.

We can glimpse a practical implementation of such DMS in the following example related to energy measuring. Smart meters can be designed in a straightforward way: a tamper-proof hardware with only (1) voltage and current sensors; and (2) a module able to sign sensors' raw data and send them as a blockchain transaction. In the blockchain network, the peers invoke a smart contract that implements all remaining LR computation (i.e., signal processing, noise reduction, values integration, etc.). The blockchain ledger stores the final measurement. In turn, the cumulative energy consumption is obtained by querying each meter's stored measurements.

There is a crucial difference between blockchain and cloud models: the liability of the distributed services. In most use cases, MI belong to one of the parties interested in the measurement computing result. Energy and fuel are classical examples where MI are owned by the vendors of the goods. In the cloud model, one can expect that the cloud services will also be held by one of the interested parties. On the other hand, the blockchain is a truly decentralized architecture, being held potentially by several parties. Thus it is expected that a blockchain model will require the contribution of different parties interested in the measurement activities, and consequently it need to be idealized following a different philosophy.

In the blockchain model, we devise measuring as *a service offered by someone without any interest in the measured quantity*. This is remarkably distinct to the traditional scenario where a vendor provides MI for measuring and is rewarded proportionally to the measurement. This idea fits perfectly in the blockchain architecture. Smart contracts can be used for computing measurements based on sensing information.

TABLE I
TRADITIONAL MI, CLOUD MODEL AND BLOCKCHAIN MODEL SECURITY ANALISYS SUMMARY

	Traditional MI	Cloud Model	Blockchain Model
R1	Required	Required (tamper proofing).	Required (tamper proofing).
R2	Required	Required only for LR software in the cloud.	Unnecessary, LR smart contracts have integrity enforced due to blockchain properties.
R3	Required	Required only for LR software in the cloud.	Unnecessary, LR smart contracts are signed by notified bodies and checked by blockchain peers on deployment.
A1	Necessary	Necessary, but the evaluation of LR software in the cloud is expected to be easier than MI embedded software.	Necessary, but the evaluation of LR smart contracts is easier than the other models.
A2	Necessary	Necessary, but MI use cases is reduced and V&V tests can be performed without the need of field tests.	Necessary, but MI use cases is reduced and V&V tests can be performed without the need of field tests.
A3	Necessary	Partially necessary, since periodical inspections take place only in data centers where cloud servers are hosted.	Unnecessary, LR smart contracts have integrity enforced due to blockchain properties.

However they are coded by different parties that do not have conflicts of interests related to the measured quantity. Whatever the measurement result, these parties shall be rewarded by a fixed value. That motivates new players to compete by more efficient measuring algorithms once as faster they execute, more credits they earn. Additionally, such strategy creates incentives for keeping the blockchain network since that becomes profitable. One could say that such concept is an innovative idea once it breaks with the manner how MI are traditionally used in consumer relations. Furthermore, it creates a new market for players who want to offer computing services for measuring.

The blockchain model also enables a set of complementary activities involving MI market and field surveillance that can be done by checking measurements inserted in the distributed ledger. Besides notified bodies, any entity representing society interests, consumers, goods providers, among others, can take part in additional supervision activities. We call that *public surveillance*. Such efforts can include smart contracts for generating redundant measurements for counter-proofing, or statistical analyses against the ledger looking for fraud evidence or patterns, for instance.

V. SECURITY ANALYSIS

In this section, a security analysis is done by comparing the measuring models discussed in the previous section, considering the attacks and the metrological assurance framework BMAF previously described. We demonstrate how BMAF requirements and activities are impacted when applied on traditional MI and DMS. Table I depicts such analysis.

Initially we evaluate the traditional MI security. In this scenario, one should note that BMAF requirements and activities are necessary to prevent attacks. As already discussed at Section IV-A, the efforts required for proceeding with traditional MI control and supervision activities are distinguished. Type approval and software validation and verification need to comprise all components and software modules. In turn, supervision also requires experienced surveillance technicians to implement inspection and software integrity checks.

When the cloud model is analyzed, one notes that MI become simpler because LR and NLR software are now running in the cloud. At same time, that reduces capabilities of a typical attacker (e.g., consumers do not have physical access to MI software interfaces anymore). The BMAF protection requirements are still necessary, however R2 and R3 requirements are applied on LR software cloud implementation. Supervision activities are also impacted, requiring less efforts to be executed. In A1, the type approval of LR software running in the cloud is expected to require less efforts than embedded software evaluation. Activity A2 is also made simpler once tests can now be performed using interface stubs, without the need of real MI physical environment. In turn, A3 also becomes less expensive because LR software identification and integrity check are executed against cloud servers which are far fewer in number than deployed MI. Finally, field surveillance for checking MI physical seals can also be eliminated. If we assume simplified MI as immutable instruments, they can be conceived as tamper proofing devices. That approach could eliminate the need for verifying MI seals as it implies that the MI will be permanently damaged and any attack trying to explore such vulnerability will not succeed.

Lastly, we evaluate the blockchain model. In addition to presenting the same characteristics of the cloud model, the blockchain security properties also affect BMAF requirements and activities. LR software is now a smart contract whose the deployment rules can be enforced for requiring developers and notified bodies attestation, something that automatically satisfies R3 and makes its regulation unnecessary. Once deployed, LR software is distributed among the network peers and it can not be changed anymore. Blockchain peers can not execute a different smart contract code otherwise blockchain security assumptions will be violated. In consequence, R2 also becomes unnecessary. In terms of activities, although A1 and A2 are still necessary, they should became much simpler when compared to the required effort in the other models. That is because the structure of smart contracts limits significantly the complexity resulting from having different technologies, software components and programming languages, while im-

posing software separation. Finally, A3 becomes unnecessary in a blockchain network due to the same reasons as R2.

We conclude that while DM already reduces attackers capabilities, such reduction is more accentuated in the blockchain model. Once LR software is produced by players which are exempted from conflict of interests, many activities related to assure software correctness and integrity are made simpler of even unnecessary. The blockchain security properties plays an important role in this context.

VI. Challenges Ahead

Although blockchains-based DMS is a promising approach, there are some challenges that need to be addressed for their use. The main ones as discussed as follow:

- **The measurement Big Data:** MI usually manipulate a high amount of data. In a large scale scenario (e.g., energy meters in a smart grid), MI can update their measurements faster, generating lots of transactions. A network connecting millions of meters may generate a transaction load unfeasible to be processed by existing blockchains implementations. Benchmark tests in Sousa et al. [11] indicate that the best available blockchain platforms are able to reach a peak around of 2000 transactions/second. Such performance is certainly not enough to meet the demand for measurements on a smart grid, for instance. As a possible solution, aggregated measurements can be used for reducing transactions in a blockchain implementation. Smarter MI can also be tried for determining transactions on demand. Another idea is to use *transaction endorsers*, a concept introduced by HyperLedger Fabric [10], [11]. Endorsers can execute complex measuring computing, leaving only validation tasks for regular peers.
- **Measuring and privacy:** Measurements assigned to a specific person allow to infer information about her habits and lifestyle. In a blockchain with public ledger, this problem becomes more serious. One needs to establish an acceptable trade-off between privacy and efficiency. Depending on the application scenario, privacy can require more sophisticated mechanisms for protecting or obfuscating identities, such as pseudonyms or identity protection layers. Permissioned blockchains can also constitute a suitable alternative once they contemplate an access control layer built into blockchain nodes [10], [12]. Access policies can be constrained in such a manner that they satisfy privacy rules and restrictions.
- **Communication issues:** Although we consider MI as connected devices, communication can be a problem in applications demanding real-time decisions. That is a restriction for any DMS over asynchronous networks. Thus blockchain-based measuring is not proper for all MI applications. Furthermore, attacks aiming communication (e.g., DDoS) represent an additional risk, although fully distributed systems as blockchains are more resilient to such attacks than conventional cloud architectures.
- **Oracles authentication:** External information providers are usually called *oracles* in blockchain architectures. In the described model, MI sensors can be seen as oracles since they are responsible for providing information from the physical world. Despite the fact that sensors are small components which can be protected using physical seals, sensors authentication can be necessary to assure measuring reliability.

VII. Conclusion

In this paper we discussed how blockchains can be used to support DMS. Due to their intrinsic security properties, blockchains can improve MI metrological assurance by imposing restrictions against potential attacks while reducing technical efforts related to regulation and control activities. Despite its promising application, blockchains pose several challenges that need to be faced. The main are related to the amount of data, privacy and oracles authentication. Future works shall bring experimental results and technical strategies for addressing and providing solutions for such difficulties.

Acknowledgment

This work was partially sponsored by the EU-BR SecureCloud project (MCTI/RNP 3rd Coordinated Call); and by the Coordination for the Improvement of Higher Education Personnel (CAPES), grant 99999.008512/2014-0, by FCT through project LaSIGE (UID/CEC/00408/2013).

References

[1] B. A. Rodrigues Filho and R. F. Gonçalves, "Legal metrology, the economy and society: A systematic literature review," *Measurement*, vol. 69, pp. 155–163, 2015.

[2] M. Esche and F. Thiel, "Software Risk Assessment for Measuring Instruments in Legal Metrology," in *Proceedings of the Federated Conference on Computer Science and Information Systems*, vol. 5, 2015, pp. 1113–1123.

[3] S. Camara, R. Machado, and L. F. Carmo, "A Consumption Authenticator Based Mechanism for Time-of-Use Smart Meter Measurements Verification," *Applied Mechanics and Materials*, vol. 241-244, no. February, pp. 218–222, 2012.

[4] D. R. Boccardo, R. C. S. Machado, S. M. Camara, C. B. do Prado, W. S. Melo, L. C. Ribeiro, and L. F. R. da Costa Carmo, "Software validation of medical instruments," *2014 IEEE International Symposium on Medical Measurements and Applications (MeMeA)*, no. October 2015, pp. 1–4, 2014.

[5] D. Peters, F. Thiel, M. Peter, and J.-P. Seifert, "A secure software framework for Measuring Instruments in legal metrology," *2015 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings*, pp. 1596–1601, 2015.

[6] A. Oppermann, J.-P. Seifert, and F. Thiel, "Secure Cloud Reference Architectures for Measuring Instruments under Legal Control," in *CLOSER 2016 - 6th International Conference on Cloud Computing and Services Science*, vol. 1, no. Closer, 2016, pp. 289–294.

[7] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain Challenges and Opportunities : A Survey," *International Journal of Web and Grid Services*, pp. 1–24, 2017.

[8] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[9] H. Luchsinger, C. Cajica, M. Maldonado, and I. Castelazo, "Are Gas Pumps Measuring Up? The Mexican Experience," *NCSLI Measure*, vol. 3, no. 2, pp. 62–68, 2008.

[10] M. Vukolić, "Rethinking Permissioned Blockchains," in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts - BCC '17*, 2017, pp. 3–7.

[11] J. Sousa, A. Bessani, and M. Vukolić, "A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform," *arXiv preprint arXiv:1709.06921*, 2017.

[12] M. Vukolic, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9591, pp. 112–125, 2016.