DOI: 10.2507/32nd.daaam.proceedings.075

BLOCKCHAIN-BASED METROLOGICAL TRACEABILITY

Almira Softic, Nermina Zaimovic Uzunovic & Samir Lemes

This Publication has to be referred as: Softic, A[lmira]; Zaimovic Uzunovic, N[ermina] & Lemes, S[amir] (2021). Blockchain-based Metrological Traceability, Proceedings of the 32nd DAAAM International Symposium, pp.0522-0526, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-33-4, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/32nd.daaam.proceedings.075

Abstract

Calibration of measuring instruments is common requirement for quality control, and calibrated instrument has to be traceable. Metrological traceability is the property of the measurement result relating it to a stated reference standard through an unbroken chain of comparisons with stated uncertainties. The data integrity of the traceability chain is vulnerable, as digital calibration certificates can potentially be altered. This paper evaluates how blockchain technology could be used to prevent data alteration and improve data integrity in calibration certificates. This is of great importance in digital quality infrastructure for innovative products and services in Industry 4.0.

Keywords: Metrological Traceability; Blockchain; Industry 4.0; Digital Calibration Certificate.

1. Introduction

The International vocabulary of metrology (VIM) [1] defines metrological traceability as the "property of a measurement result whereby the result can be related to a reference through a documented unbroken chain of calibrations, each contributing to the measurement uncertainty". The International Laboratory Accreditation Cooperation (ILAC) considers the elements for confirming metrological traceability to be an "unbroken metrological traceability chain to an international measurement standard or a national measurement standard, a documented measurement uncertainty, a documented measurement procedure, accredited technical competence, metrological traceability to the SI, and calibration intervals" [2].

The metrological traceability chain is defined in [1] as a "sequence of measurement standards and calibrations used to relate a measurement result to a reference". The calibration hierarchy defines the metrological traceability chain used to establish the metrological traceability of a measurement result to a measurement unit. The reference is the international definition of a measurement unit through its practical realization [1]. It is necessary to establish such a chain of traceability where each step is described, and the uncertainty connected with each step is evaluated to maintain the metrological traceability for quality control. Ačko et al. in [3] analysed some novel approaches to assuring traceability of in-process measurements by using robust and thermal invariant multi-purpose material standards and a mobile simulator to emulate shop floor environmental conditions. The traceability of the measurements guarantees end users' confidence in the correctness of measurement results, ensuring customer protection and product quality. The requirements of ISO 17025:2017 standard in its latest revision [4] introduced the concept of risk-based thinking, following the ISO 9000 series of standards for quality management.

The lack of metrological traceability identifies potential risks in calibration and testing laboratories [5]. The overwhelming digitalization and upcoming Industry 4.0 automation introduce some new risks, introducing potential breaches of information integrity. The calibration and accreditation system relies on a well-established hierarchy of accredited calibration laboratories, making this process error-proof to a certain extent. For example, around 10.000 calibrations to a national standard are performed in Germany each year, 100.000 calibrations to reference standards and millions of calibrations to working standards [6]. To address the risk of data integrity breach and eliminate the risk of compromising calibration certificates, the Physikalisch-Technische Bundesanstalt (PTB) introduced the concept of a Digital Calibration Certificate (DCC), which serves for the electronic storage, the authenticated, encrypted and signed transmission and the uniform interpretation of calibration results in Germany. The information integrity is based on the official national electronic signature and time stamps.

It is estimated that there are 850 million measuring instruments on the EU market [7], which are responsible for a share of 4 % to 6 % of the European GDP, equivalent to 660 to 990 billion euros per year. Each year, almost 350 million measuring instruments are being in the European market [7]. Emerging digital technologies, such as embedded systems, cloud computing, big data, Internet of Things (IoT), and cyber-physical systems, opened some new challenges for instruments that are using distributed and cloud-based data storage and processing. There is a need to establish a digital quality infrastructure for European Union and even globally. Smart data and smart services could be connected with databases and infrastructure through a "European Metrology Cloud" [7], ensuring that all measurements are reliable and traceable to protect the customer and the end-user, as European directives within the New Approach regulate it. However, the concept presented in [7] could be centralized, distributed or hybrid, making sure that appropriate surveillance and quality control mechanisms are in place. This research evaluates how blockchain could improve data integrity and prevent data alteration in calibration certificates. To open the space for this technology, it is important to establish the link between the legal metrology, software engineering and to leverage the two previously unrelated engineering disciplines.

2. Digital metrology

A novel concept of digital metrology primarily intended for IoT devices is presented in [8], which relies on a digital calibration certificate (DCC) and a Digital Twin concept. They proposed using the X.509 certificate to cryptographically bound a measurement device with supporting authentication of the instrument's identity. X.509 is a cryptography standard frequently used in electronic signatures used to define the format of public-key certificates. This standard relies on certificate authorities, making it unsuitable for decentralized systems. The use of false certificates issued through illegal compromise of certification authorities was reported by national security services, such as Dutch certification authority DigiNotar [9].

A blockchain-based system for metrological purposes is mentioned in [10], where a vehicle speed measuring system was implemented using the Hyperledger Fabric blockchain platform. They compared three different measuring system models: the traditional measuring instruments, a cloud-based centralized and hierarchical measuring system, and distributed and decentralized blockchain-based measuring system model. The biggest advantage of the blockchain-based model is the fact that the measuring process as a cloud-based service is supported by resources owned and managed by anyone who has no interest to alter the measured quantity. The quantitative assessment showed that blockchain-based measurements are less costly but highly rely on internet connectivity.

A similar concept, evaluated on the CMM dataset, was presented in [11]. They fully implemented the dual digital traceability of the metrological data approach using X.509 certification standard and SHA-256 hashing algorithm to represent the instrument calibration and cryptographically sign measurements on record level. Dual digital traceability has been successfully implemented in a software prototype, allowing publicly stored fingerprints of a measurement record able to validate invalid or retracted calibration certificates and unwanted modification. The system was tested using IOTA cryptocurrency distributed infrastructure (https://www.iota.org/).

Aimagmbetova et al. in [12] discussed how metrological traceability is achieved in the Internet of Measurement (IoM) concept. Without going into details, they concluded that there is a need to perform remote measurements and calibration using centralized databases, but the risk of jeopardizing information security opens the space for multistage cryptographic hash functions. These functions are used to protect the data in a distributed chain of encrypted blocks. The data encryption and data checks are performed by special users of the IoM network called miners, like those in blockchain-based cryptocurrencies. Anto and Nugraha in [13] designed a system of Blockchain-based technology for Digital Multimeter calibration used to improve the data integrity and to prevent potential data manipulation (tampering-data) for Digital Multimeter calibration results. The most important advantage that motivated that research is the possibility of storing track-record of previous calibration data and losing calibration records.

3. Blockchain

Blockchain, at first used only for cryptocurrencies, is a concept emerging in many different areas, providing data integrity and reliability by utilizing distributed data processing and cryptographic techniques. It is already well established in the supply chain processes [14], but it opens its path into other disciplines of Industry 4.0, such as distributed CAD environments: ERP, BIM, PDM, PLM [15]. In order to describe how it can be leveraged to support metrological traceability, there is a need to explain the concepts behind the blockchain briefly.

The blockchain relies on three IT concepts: peer-to-peer networking, public-key cryptography, and distributed consensus based on the resolution of a random mathematical challenge [15]. This technology creates fixed-size blocks of information using cryptographic hash functions. These blocks are added to an array called blockchain in a way that every new block has the same size but contains irreversibly encrypted information about all its predecessors. The blockchain contains the encrypted version of the complete history of changes of all blocks.

Fig. 1 shows how blocks in the blockchain are signed and verified. The entire process is based on cryptography based on private and public keys. Each transaction in the chain is verified by the previous block owner's public key and signed by his private key. The hash function ensures data integrity as it is irreversible and has no inverse function. The accredited laboratories 1, 2 and 3 have different vertical levels, from working (industrial), national, regional, to international. As these laboratories also act as nodes in the network, they are also distributed horizontally. The nature of the blockchain provides the error-proof traceability of calibration certificates and procedures.

Each data transaction (calibration that needs metrological traceability) is accompanied by the timestamp, making the data also temporally identifiable and traceable. The process relies on the consensus of the nodes, and each case of altered or invalid data is easily detected and excluded from the chain. The nonce is an arbitrarily chosen string, changed multiple times until the hash value of the block header is below the predefined target value. This process is called mining, and it is performed by the nodes of the network. Only if the solution is valid, the block is included in the blockchain, and the transaction considered complete.

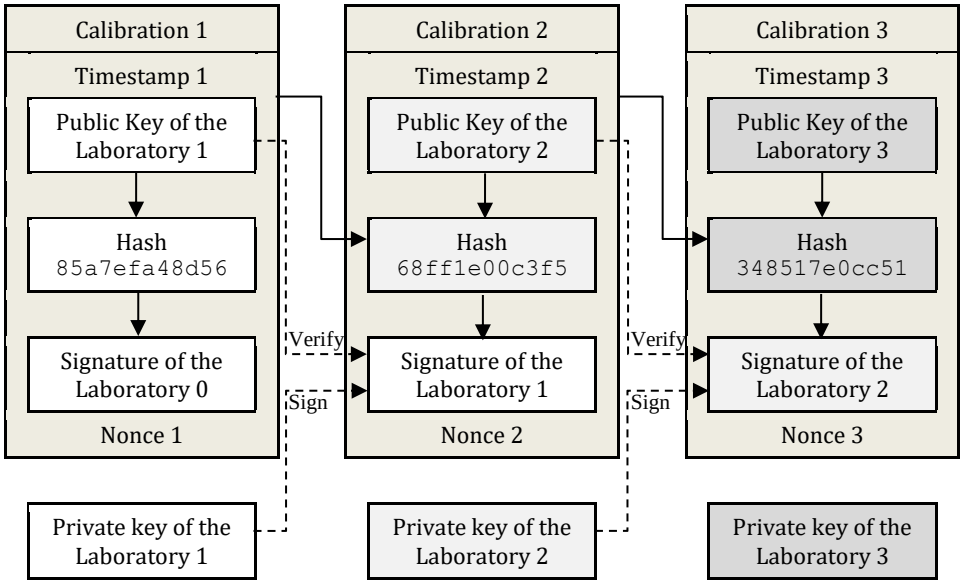

Fig. 1. The signing and verification in the blockchain, modified from [15]

The blockchain is prone to alterations, as any change in any phase of data transfer irreversibly alters the final output. This feature makes it a state-of-the-art digital tool to ensure data integrity. The blockchain relies on mathematical functions (hash functions), which create the fixed-size bit-string output (hash). It is practically impossible to guess the length of the hash by decrypting the blockchain. The hash algorithm produces a unique output as a unidirectional function having no inverse function. The blockchain uses these hash functions to encrypt information and to digitally sign the information from all previous steps. Cryptocurrencies Bitcoin and Ethereum use SHA-256 (secure hash algorithm), developed in 2001 by the National Security Agency (NSA) in the USA.

The list of currently used cryptographic hash functions includes 128–320-bit RACE Integrity Primitives Evaluation Message Digest (RIPEMD), Merkle tree-based 128–512-bit message digest algorithm (MD5, MD6), 224–512-bit secure hashing algorithm (SHA-2 also known as SHA-256 or SHA-512, SHA-3), 224–512-bit BLAKE (BLAKE2, BLAKE3), Russian 256, 512-bit Streebog, etc. These hash functions can contain more different algorithms, and they are implemented in programming languages as classes.

The top feature of the blockchain is the fact that information stored in the blockchain can never be altered or lost. The blockchain replicates into the same number of copies as there are nodes in the network. The blockchain also stores the complete history of all previous states of information stored. In that way, anyone could check the final state validity simply by using the same hashing algorithm to all information from the beginning to the end.

Bucci et al. in [16] tackled the problem of privacy if blockchain technology is used for the purpose of distributed measurement systems, especially in the European Union where GDPR (General Data Protection Regulation) is used. They also emphasized the problem of network bandwidth and connectivity, as it plays a crucial role in the overall performance of the system.

Takatsuji et al. in [17] demonstrated how blockchain technology could be used to improve visualization of metrological traceability. As only the first higher standard is shown in the calibration certificate, the end-user lacks the data about the traceability to an international standard, making space for immutability and falsification of calibration standards. As the traceability chain could be long, there is a possibility that the highest-level calibration in the traceability chain was performed a long time ago. Blockchain can overcome this by using timestamps which are included in each block and secured with hash functions. Zhu et al. in [18] explained how blockchain is superior to classic electronic signatures and digital certificates, as it disables data alteration. Peters et al. in [19] raised an issue of how could embedded devices handle the huge amount of data in a blockchain, ignoring the fact that data is stored in a cloud, and only a digital signature is stored locally.

There is no doubt that blockchain is an emerging technology, which can be used in many metrological disciplines, from distributed measuring systems to calibration certificate management.

4. Metrological traceability

From the very beginning, the concept of metrological traceability was intended to be centralized, assuring that any measurement result is traceable to the highest-level standard. On the contrary, blockchain is decentralized by its nature, and it is not obvious that this technology can be used to support metrological traceability. Table 1 summarizes what should be taken into account to utilize the blockchain as a means to make calibration certificates non-repudiable and traceable to the international standard.

Metrological traceability			**Blockchain**
The interlaboratory comparison relies on a network of laboratories. The higher number of comparisons, the higher confidence in measurement results.	😐	😐	Blockchain relies on a high number of network nodes. The higher number of nodes, the better information security.
Measuring instrument traceable to a highest calibration reference standard	😐	😐	Unchangeable information stored in a distributed network of nodes
An unbroken chain of comparisons of instrument's measurements	😐	😐	A continuous chain of encrypted data blocks
Calibration certificates (also digitally signed)	😐	😐	Encrypted digital certificates stored in the cloud
Strictly vertically centralized hierarchical structure	😐	😐	Still, a vertically centralized hierarchical structure, reinforced with a horizontal network of nodes
Calibration certificates could be falsified	☹	☺	Calibration certificates cannot be falsified
Fixed calibration intervals	☹	☺	Flexible calibration intervals
Slow and expensive system of checking authenticity and integrity of the calibration certificates	☹	☺	Automated and fast system of checking authenticity and integrity of the calibration certificates
Low dependence on internet connectivity and bandwidth	☺	☹	High dependence on internet connectivity and bandwidth

Table 1. Relations between the metrological traceability and the blockchain

The statements presented in Table 1 reveal that the only weakness in blockchain-based metrological traceability is high dependence on internet connectivity and high requirements for computational resources. The advantages prevail, and it is plausible to expect that blockchain will find its way into this area of use. Measurement and instrumentation will benefit if metrological traceability is supported by a distributed ledger of information about calibration certificates.

5. Conclusion

The general requirement for each measuring instrument is a calibration certificate, stating that the measurement results are reliable, accurate, and within prescribed measurement uncertainty interval. The calibrated instrument has to be traceable to the highest level of the reference standard, and this chain should be verifiable and prone to alterations. However, these certificates can be easily falsified and it is very important to provide their integrity.

Blockchain is an emerging digital technology constantly finding new applications towards Industry 4.0 and cyber-physical systems. Initially used only as a basis for cryptocurrencies, its capability to ensure data integrity and authenticity made it an unavoidable tool to secure any information which needs a high level of information security. Its nature makes this technology a reliable solution for the problem of calibration certificate data integrity.

Recent practices opened the path for blockchain to be used in distributed digital measurements, sensors in smart devices, the Internet of Things and all instruments requiring calibration. It is not enough to have surveillance, auditing and legal mechanisms against falsification of calibration certificates. These certificates can be reinforced with blockchain-based infrastructure made of accredited laboratories.

These laboratories would appoint a part of their computational resources to verify the cryptographic hash functions in the same way the cryptocurrency miners verify the financial transactions or smart contracts. International metrology infrastructure still does not support the implementation of this concept, but there are some initiatives at the national level, where authorities recognized the need to increase the level of digitization of metrology infrastructure.

In the near future, the national metrological institutions should first get familiar with the blockchain technology, then implement a pilot project with one type of measuring instrument, and finally provide a legal framework to make blockchain-based calibration certificates digitally traceable.

6. Acknowledgments

The publication of this paper is supported by the University of Sarajevo, Mechanical Engineering Faculty.

7. References

[1] JCGM 200:2012 International vocabulary of metrology - Basic and general concepts and associated terms (VIM), 3rd edition, Joint Committee for Guides in Metrology (JCGM).

[2] ILAC P10:07/2020: ILAC Policy on Metrological Traceability of Measurement Results. International Laboratory Accreditation Cooperation (ILAC). Available online from https://ilac.org/?ddownload=123220 29.5.2021

[3] Acko B, Klobucar R, Acko M (2015) Traceability of In-process Measurement of Workpiece Geometry, In: Procedia Engineering, Vol.100, pp 376-383, ISSN 1877-7058, DOI: 10.1016/j.proeng.2015.01.381

[4] Standard ISO/IEC 17025:2017 General requirements for the competence of testing and calibration laboratories. The International Organization for Standardization (ISO).

[5] Vasilnakova, A. (2018). Risk management in accredited testing laboratories. In: Proceedings of the 29th DAAAM International Symposium, pp.1071-1075, B. Katalinic (Ed.), DAAAM International, ISSN 1726-9679, pp 1071-1075. DOI: 10.2507/29th.daaam.proceedings.153

[6] Hackel, S, Härtig, F, Hornig, J, Wiedenhöfer, T. (2017). The Digital Calibration Certificate. In: PTB-Mitteilungen 127 (2017), Heft 4. pp 75-81. ISSN 0030-834X. DOI: 10.7795/310.20170499

[7] Thiel, F, Esche, M, Grasso Toro, F, Peters, D, Oppermann, A, Wetzlich, J, Dohlus, M. (2017). A Digital Quality Infrastructure for Europe:The European Metrology Cloud. In: PTB-Mitteilungen 127 (2017), Heft 4. pp 83-97

[8] Mustapää, T, Autiosalo, J, Nikander, P, Siegel, J E & Viitala, R. (2020). Digital Metrology for the Internet of Things. In 2020 Global Internet of Things Summit (GIoTS), pp 1-6. IEEE. DOI: 10.1109/GIOTS49054.2020.9119603

[9] Zetter K. (2011). DigiNotar Files for Bankruptcy in Wake of Devastating Hack, Wired online magazine, Condé Nast. https://www.wired.com/2011/09/diginotar-bankruptcy/ 29.05.2021

[10] Melo, W S, Bessani, A, Neves, N, Santin, A O & Carmo, L F R C. (2019). Using Blockchains to Implement Distributed Measuring Systems. IEEE Transactions on Instrumentation and Measurement, ISSN: 1557-9662. pp 1-12. DOI: 10.1109/TIM.2019.2898013

[11] Peterek, M, & Montavon, B. (2020). Prototype for dual digital traceability of metrology data using X.509 and IOTA. CIRP Annals, 69(1), pp 449-452. DOI: 10.1016/j.cirp.2020.04.104

[12] Aimagmbetova, R Z, Ershov, I A, & Stukach, O V. (2017). Towards the problem of measurement traceability in the Internet of measurement concept. In: Dynamics of Systems, Mechanisms and Machines (Dynamics), pp 1-4. IEEE. DOI: 10.1109/Dynamics.2017.8239425

[13] Anto, I A F & Nugraha, I G B B. (2018). Blockchain-based for calibration of digital multimeter system design. In 2018 International Conference on ICT for Smart Society (ICISS), pp 1-6. DOI: 10.1109/ICTSS.2018.8549924

[14] Madhwal, Y & Panfilov, P (2017). Blockchain And Supply Chain Management: Aircrafts' Parts' Business Case, In: Proceedings of the 28th DAAAM International Symposium, pp.1051-1056, B. Katalinic (Ed.), DAAAM International, ISSN 1726-9679, pp 1051-1056. DOI: 10.2507/28th.daaam.proceedings.146

[15] Lemeš S. (2020). Blockchain-Based Data Integrity for Collaborative CAD, In: Mixed Reality and Three Dimensional Computer Graphics (B. Sobota, D. Cvetković, Eds.), IntechOpen. DOI: 10.5772/intechopen.93539

[16] Bucci, G, Ciancetta, F, Fiorucci, E, Fioravanti, A, Prudenzi, A & Mari, S. (2019). Challenge and future trends of distributed measurement systems based on blockchain technology in the european context. In IEEE 10th International Workshop on Applied Measurements for Power Systems (AMPS), ISSN: 2475-2304. pp 1-6. DOI: 10.1109/AMPS.2019.8897782

[17] Takatsuji, T, Watanabe, H & Yamashita, Y. (2019). Blockchain technology to visualize the metrological traceability. Precision Engineering, 58, pp 1-6. DOI: 10.1016/j.precisioneng.2019.04.016

[18] Zhu, Y, He, J, Yuan, K & Yang, Y. (2019). Research on Modify Protection of Metrology Electronic Certificate Based on Blockchain Technology. In 2019 14th International Conference on Computer Science & Education (ICCSE), pp 1020-1024. DOI: 10.1109/ICCSE.2019.8845467

[19] Peters, D, Wetzlich, J, Thiel, F & Seifert, J-P. (2018). Blockchain applications for legal metrology. 2018 IEEE International Instrumentation and Measurement Technology Conference (I2MTC). ISBN:978-1-5386-2222-3. DOI: 10.1109/i2mtc.2018.8409668