ACTA IMEKO
ISSN: 2221-870X
March 2023, Volume 12, Number 1, 1 - 7

Automated calibration and DCC generation system with storage in private permissioned Blockchain network

Cristian Zet[1], Gabriel Dumitriu[2], Cristian Fosalau[1], Gabriel Constantin Sarbu[3]

[1] *Gheorghe Asachi Technical University of Iasi, Bd. D. Mangeron 67, 700050 Iasi, Romania*
[2] *Individual Enterprise GCD, Str. Hlincea nr. 27, 700714, Iasi, Romania*

ABSTRACT
Digital technologies have proved their usefulness in instrumentation and measurements since many years, becoming a "must have". The use of microprocessors and microcontrollers in measuring instruments became a common practice, bringing the advantage of signal and information processing at the instrument level, digital interfaces, remote control, software update and calibration. Thus, the instrument can be calibrated and verified being connected in an automated calibration system which can carry all the process without the operator interference and to generate in the end the calibration certificate. The paper presents the possibility of joining the automated calibration system and the creation of a Digital Calibration Certificate (DCC) with the Blockchain technology for storing and validation. As benefits there are the traceability of the DCC, the impossibility of altering the information and the preservation of the full history in the digital wallet.

Section: RESEARCH PAPER

Keywords: Blockchain technology, Digital Calibration Certificate (DCC), Virtual instrument, automated test system, data acquisition, uncertainty

Citation: Cristian Zet, Gabriel Dumitriu, Cristian Fosalau, Gabriel Constantin Sarbu, Automated calibration and DCC generation system with storage in private permissioned Blockchain network, Acta IMEKO, vol. 12, no. 1, article 16, March 2023, identifier: IMEKO-ACTA-12 (2023)-01-16

Section Editor: Daniel Hutzschenreuter, PTB, Germany

Received November 20, 2022; **In final form** February 14, 2023; **Published** March 2023

Funding: This work was supported from project POC 351/390027/08.09.2021 European Structural Funds.

Corresponding author: Cristian Zet, e-mail: czet@tuiasi.ro

1. INTRODUCTION

Calibration is defined by VIM (JGCM200:2012) as the *"operation that, under specified conditions, in a first step, establishes a relation between the quantity values with measurement uncertainties provided by measurement standards and corresponding indications with associated measurement uncertainties"*. It is usually accomplished after the instrument gets out from the production line or at regular time intervals during the instrument's life time. Calibration is often considered by companies as being the process of measuring the offset and the gain errors [1], [2] and trimming the analog circuitry in order to correct these errors, being confused with the adjustment process. During the factory adjustment, the correction values are stored in the nonvolatile memory of the instrument and they are used during operation to directly correct the indication. Later, the errors change in time due to aging and with temperature, making these values invalid after a time period, requiring a new adjustment. Depending on the needs, the instrument must be checked at least once a year, but it can be even earlier (6 or 3 month) if necessary.

Modern instruments are programmable via the built-in interfaces, like USB or GPIB [3]. A software control loop can control several instruments in order to get an automated test system. If one or more of the instruments have no interface, the process can be only partially automated using video processing [4], on single range or function, while switching ranges/functions are performed manually. The commercially available remote control software from the producer is not suitable in most cases for metrological purposes [1], and hence custom software must be developed for each instrument.

In [3], an automated calibration system for electrical sources and measuring instruments like Digital Multimeters (DMMs) has been described. It is intended for several well known instruments like calibrators (Fluke 5720A or Wavetek 9100) or DMMs (Fluke 8506, Fluke 8846, HP 3458). The software is built in LabView and allows controlling the calibration system, eliminates the human errors and performs statistical processing.

In [2], an automated measuring station for the determination of calibration intervals for DMMs is presented. The authors are using a standard device and a verified instrument, both equipped

with communication interfaces. The test is performed every 2 month interval up to 1 year.

In [5], authors present an automated calibration system for DMMs without a Communication Interface. They are using video processing to "read" the numbers provided on 7 segment displays. The process is partially automated, the operator's task being to change the ranges and functions.

In [6] it is shown that the calibrations can be performed on site based on travelling standards, without requiring the presence of any specialized personnel from the metrology lab. Such situation needs an Internet connection to automatically and securely send the calibration data on a server.

There are several approaches described above, but for any of them the software is a custom design one, being fully automated or partially automated, depending on the instruments. Despite this, an automated system can be endowed with the feature to automatically create the DCC. As long as the data is recorded in the system in the digital format, the software can automatically create the calibration certificate, according to the issuer regulations. In most cases the data can be saved in local files with various formats, human readable or machine readable.

There are several formats and several approaches in the literature for creating a DCC [7]. There are various information to be recorded in the certificate and various users of it. The certificate must respect norms and regulations and maintain traceability. An analysis of digital formats reveals several advantages for Blockchain based DCCs. In [8] the authors describe the possibility of generating the DCC from Excel, taking benefits from the programming environment built in. In [9], the authors present several variants of saving the DCC in pdf format for various fields like VNA, electrical energy, or acoustics. The pdf file may have attached the digital calibration certificate.

In [10], the authors describe how to make DCC in XML format with 4 layers: administrative, results, individual information and optional attachment (pdf), considering the case of sensor networks. The digital signature is also considered.

For using DCCs, an infrastructure is needed [11] that must be distributed [12]. Security issues must be provided that prevent the information to be altered.

An internal report from NIST makes a detailed analysis of Blockchain overview with respect to the metrology area, emphasizing the benefits and the weaknesses [13]. A Blockchain system is not exactly immutable, requiring governance that must be trusted. The data recorded must correspond to the real world. Transactions that are not yet included in a block are vulnerable to attacks and vulnerable to malicious users.

Some applications for the Blockchain technology have been emphasized in [14]: decentralized audit trail (the instrument communicates that the calibration parameters are not proper anymore), parameters update with agreement from the user, public keys for manufacturers and NMIs, or billing system.

In conclusion, according to this short analysis, calibration is one of the activities requesting traceability, allowing the connection with the primary standards, the needs of DCCs and the advantages of using the Blockchain technology in metrology. The present paper brings as novelty the direct generation of the DCC during an automated calibration together with saving it as a Blockchain transaction. A short description of the used Blockchain network is presented in Section 2, followed by the description of the hardware and software application performing the automated calibration, DCC generation and its embedding in the Blockchain in Section 3 and ending up with some results in Section 4 and conclusions in Section 5.

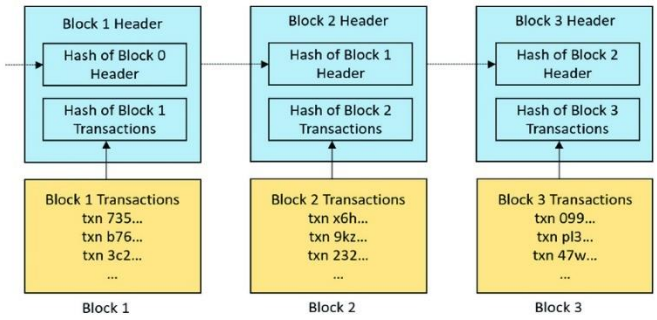

Figure 1. Blockchain block simplified.

2. BLOCKCHAIN NETWORK ARCHITECTURE AND SPECIFIC TRANSACTION BLOCKS

As per IBM's definition, Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network.

All these transactions are stored in blocks of data, using complex cryptography functions. Each block contains a cryptographic hash of the previous block, a timestamp, and the transaction data (generally represented as a Merkle tree) as in Figure 1. Once a transaction is executed, all the data remain in the Blockchain permanently. You cannot alter, modify, copy or delete it but you can only distribute it.

In order to migrate the Digital Calibration Certificate on Blockchain, we built a private permissioned Blockchain infrastructure with 3 private full nodes, an API and a web platform acting as smart asset management tool like in Figure 2. A full node can be seen as a server in a decentralized network. It keeps the consensus between other nodes and verifies the transactions. It also stores a copy of the Blockchain, thus being able to securely enable custom functions such as instant send and private transactions.

Our Blockchain is based on the X15 algorithm, a hybrid between POW (Proof of Work) and POS (Proof of Stake) consensus mechanism [15]. Thanks to its energy efficiency, it can even run on a Raspberry PI2. POS is a type of consensus mechanism used in blockchain networks for validating transactions and creating new blocks.

When using PoS, instead of miners competing to solve complex mathematical problems to create new blocks (as in PoW based networks), validators are chosen to create new blocks based on the amount of cryptocurrency they hold and are willing to "stake" (i.e. lock up) as collateral.

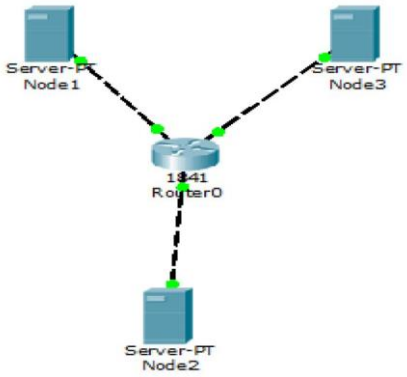

Figure 2. Local Blockchain node simplified.

When a validator wants to create a new block, they must first stake a certain amount of cryptocurrency, which acts as a form of collateral. The more cryptocurrency a validator stakes, the higher their chances of being chosen to create a new block.

Once a block is created, the validator receives a reward for their work, proportional to the amount they staked. If a validator is found to be acting maliciously or attempting to cheat the system, their stake can be taken away as a penalty and his work is excluded from that specific block. It uses 15 hashing algorithms that are consecutively carried out one after another. We also built its associated Windows and Linux wallets from which we can natively monitor all the transactions. The infrastructure has been built to run on P2P Port: 10218 and accept commands only on RPC Port: 20208. This specific Blockchain feature also adds an extra layer of security.

Some APIs were built using the opensource jsonRPCClient.php - a simple php class that implements Json RPC client over raw tcp.

The asset management tool works in parallel with the LabView Dashboard and allows the user to create a Blockchain identity for the measurement instrument. Basically, it uses a specific function, "getnewaddress" from jsonRPCClient.php in order to remotely connect to the main wallet and store the instrument's details (such as name and serial) as metadata in a single transaction. The Blockchain address attached to the instrument is converted to a QR code for a better portability. This process is basically the creation of the smart asset on our infrastructure. Then, we use the newly created Blockchain identity to initiate transactions. Each transaction generates a unique transaction id (Figure 3). We use the "sendtoaddress" function and store the metadata in the "comment" argument, part of the function. The "comment" argument is kept in the main public wallet; it is not distributed over the network. This means that the only way you can see the metadata is by typing the correct transaction, which is a unique identifier. So, even though all transactions are public, the content of the DCC can be verified only if you have a valid transaction id. This type of architecture restricts any fraudulent transactions.

The traceability aspect of the whole system is given by the fact that we can trace back in time every transaction and identify each measurement. This can be done directly from the wallet (as a native feature) or by accessing our smart asset management tool. Using the "listtransactions" function, we developed a method which allows us to check the previous calibration/measurements of the same instrument. This is achieved natively, from the wallet and also from our Web asset management tool. Having this functionality, it allows the system to have a full history of calibration/verification of the same instrument and also

Figure 3. Blockchain transaction details.

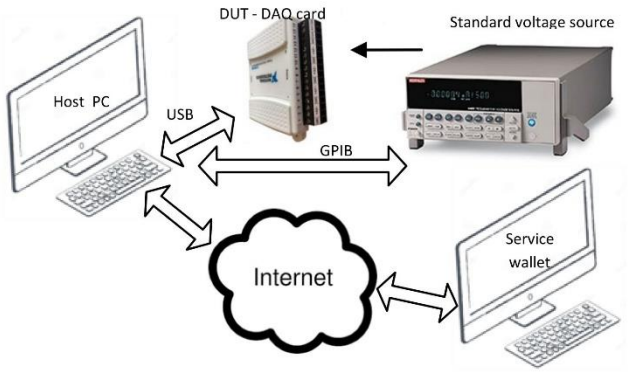

Figure 4. The schematic of the calibration system.

providing a secure method of storing and sharing data, protecting it from unauthorized access or modifications. This specific aspect also helps to reduce the cost of creating, maintaining, and distributing physical certificates.

The LabView side of the project uses HTTPClient.lvlib to connect to the Blockchain API. It also collects the measured values and sends them to a specific address as metadata. The data is formatted as .XML before embedding it to Blockchain, which offers an alternative in future verification.

We designed the system in such a way that once the Labview application runs, it automatically correlates the serial number of the Data Acquisition card with its associated Blockchain wallet address. We achieved this by using the "getaccountaddress" native function that returns the wallet address of a previous created account. All these actions happen on the wallet, being stored locally on the main wallet.

This particular approach offers an extra degree of anonymity and low-cost of transactions in the peer-to-peer (P2P) Blockchain network compared to those in the real world.

3. DESCRIPTION OF AUTOMATED CALIBRATION SYSTEM – HARDWARE AND SOFTWARE OVERVIEW

For proving that it is possible to store the DCC as a transaction using Blockhain technology, an automated calibration system has been created to perform both the measurement and the DCC generation, as shown in Figure 4. It consists of standard source and the DUT, both connected to a host PC running the specific software developed in LabView.

The DUT is a multifunction NI USB 6008 data acquisition card. It has 8 analog inputs with 2 types of input connections: differential (DIFF) and single ended (RSE). The technical data for the DAQ card are listed in Table 1. It provides a resolution of 12 bits on the differential input and 11 bits on single ended input and relatively high maximum permissible errors. The DAQ is connected at the host PC using the USB interface.

The programmable voltage source Keithley 6487 (a picoammeter with built-in voltage source) is connected to the PC through the GPIB interface and it is driven using SCPI commands. In order to demonstrate the feasibility of an automated verification and DCC generation system, a virtual instrument has been developed in LabView. It is designed to

Table 1. NI USB 6008 absolute accuracy specifications (25°C) in mV.

Input type	± 20 V	± 10 V	± 5 V	± 4 V	± 2.5 V	± 2 V	± 1.25 V	± 1 V
RSE	-	14.7	-	-	-	-	-	-
DIFF	14.7	7.73	4.28	3.59	2.56	2.21	1.70	1.53

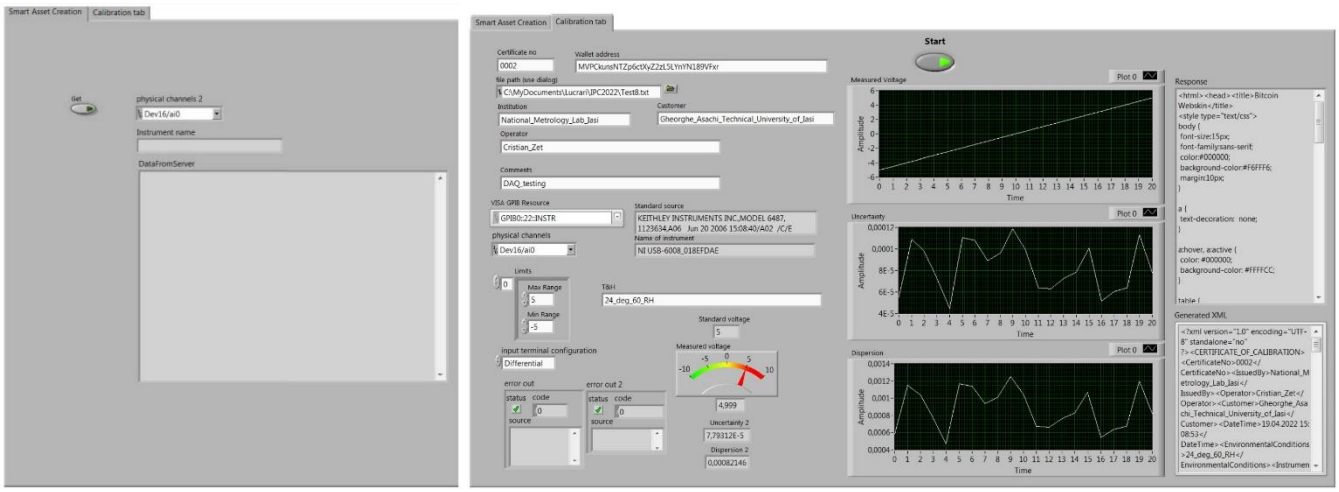

Figure 5. The front panel of the virtual instrument: left - The "Create smart asset" Tab; right - the Calibration Tab.

allow the creation for each instrument of its own identity in the specified wallet. If it has not already one, it must be set up and run the verification process. At the end, the resulting data must be saved in the Blockchain network as transactions. The data is also saved in readable format in local .txt files. The process is not really fully automated, as the operator must change the input connection when the RSE connection is tested.

The front panel of the VI is presented in Figure 5. If the instrument to be calibrated is not yet registered as a smart asset or it was not verified before using the system, the operator can choose the tab "Smart asset creation". In Labview, each data acquisition device gets a device number which can be found in the Measurement and Application Explorer . After inserting the "Device no", the program will query the device and will get its serial number and board name. It will concatenate the two strings, will call the Blockchain platform to create a wallet for the device using the "getnewaddress" API and will return the wallet address as shown in Figure 5 left (like MMZo6BKSvw JhMJZ2vvGMGyaA8fexGwmE4C). The new address will appear also in the wallet application. The user has to copy this and paste it in the corresponding field in the Calibration tab.

Moving to the "Calibration tab" (Figure 5. right), the operator must fill in the fields for the certificate header, as for example: the certificate number (Certificate no), the certificate issuer name (Institution), the operator name (Operator), the customer name (Customer) and the comments field (Comments). The header can be customized following the lab wishes and regulations with various fields. Next, the operator must setup the connection type (input terminal configuration), the scale limits (Limits) for each desired scale and GPIB address of the standard source. The environmental conditions can be specified as an input field (T&H). If the room is environmentally controlled or they can be measured using a remote environment monitor station, the values can be automatically inserted into the field. Before starting the instrument, the operator has to fill in the wallet address of the instrument to be verified (Wallet address), if it already has one, or paste it after it was created in the "Smart asset creation" tab. Once the DUT and the standard source are connected and all the control fields are filled in, the operator can start the verification process by pressing the button "Start".

The first task is to read the instruments IDs and serial numbers directly from their firmware, which will be added to the certificate. After the instruments are initialized with the working parameters, the process is started. Depending on the number of points per scale and on the number of scales the process will take a while. For the present approach we set a number of 20 points per scale and 8 scales. The sampling frequency is set to 1 kHz and $n = 1000$ samples to acquire. The acquired values are processed for each test point in order to calculate the arithmetic mean and the standard deviation:

$$U_{\text{mean}} = \frac{1}{n}\sum_{k=0}^{n} U_k\,,\quad s(U_k) = \sqrt{\frac{1}{n}\sum_{k=0}^{n}(U_k - U_{\text{mean}})^2} \tag{1}$$

where U_k are the measured values for a single test voltage, while the type A uncertainty is calculated as the experimental standard deviation of the mean value:

$$u_{\text{A}} = s(U_{\text{mean}}) = s(U_k)/\sqrt{n}\,. \tag{2}$$

Type B evaluation of the measurement uncertainty may also be characterized by standard deviations, which will be evaluated from the probability density functions based on experience or other information, as reported in GUM [Evaluation of measurement data—Guide to the expression of uncertainty in measurement, JCGM 100:2008]. The combined uncertainty and the expanded uncertainty are calculated as:

$$u_{\text{C}} = \sqrt{u_{\text{A}}^2 + u_{\text{B}}^2}\,, u_{\text{E}} = k \cdot u_{\text{C}}\,, \tag{3}$$

where k is the coverage factor ($k = 2$ for a probability of 95%). In the current application, only the type A uncertainty is considered as resulting from the experimental verification.

The virtual instrument flow is presented in Figure 6. After the initial setting of various parameters, it runs 3 loops. The inner one takes the measurements for each test point 1000 times and calculates the uncertainty, the middle one runs for each test point and the outer one runs for each range. The data is written in the local file after each test point, while the transaction containing the DCC is sent after each range.

The header of the Calibration certificate has to be flattened into XML string. Because that some special characters are not allowed in this format of Blockchain, they have to be removed from the instrument identification string and replaced with underscores or dots.

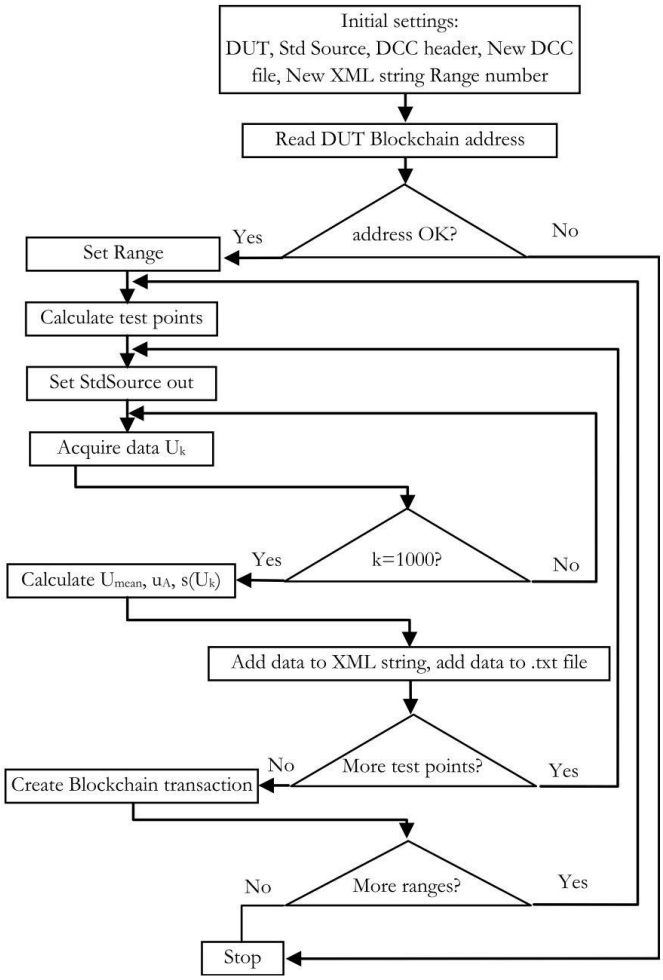

Figure 6. The virtual instrument flow diagram.

4. RESULTS

In our experiment 10 DAQ cards were tested for all measuring ranges on the differential input and for the single range on the RSE input. Their DCCs were saved in the Blockchain network as transactions. Each tested scale has its own DCC embedded in one transaction.

The results are presented in Table 2 for differential input base scale ± 10 V, for the lowest scale ± 1 V and for RSE input.

Maximum values from all 10 tested DUTs for each test point for the combined uncertainty are presented. As it can be seen, the values are below 6.35 mV, which is lower than the absolute accuracy value of 7.73 mV given by the producer for the base scale ± 10 V. For the lowest scale, ± 1 V, the combined uncertainty is maximum 1.15 mV, slightly under the absolute accuracy limit of 1.53 mV given by the producer. This might be produced by the standard source whose lowest output scale is ± 10 V and the accuracy according to the datasheet is 0.1% of output voltage + 1 mV. This means that for 1 V output voltage,

Table 2. NI USB 6008 absolute accuracy specifications (25 °C) in mV.

Scale factor	-1	-0.8	-0.6	-0.4	-0.2	0	0.2	0.4	0.6	0.8	1
DIFF ± 10 V	6.35	5.19	4.04	2.89	1.73	0.58	1.73	2.89	4.04	5.19	6.35
DIFF ± 1 V	1.15	1.04	0.92	0.81	0.69	0.58	0.69	0.81	0.92	1.04	1.15
RSE ± 10 V	6.35	5.19	4.04	2.89	1.73	0.58	1.73	2.89	4.04	5.19	6.35

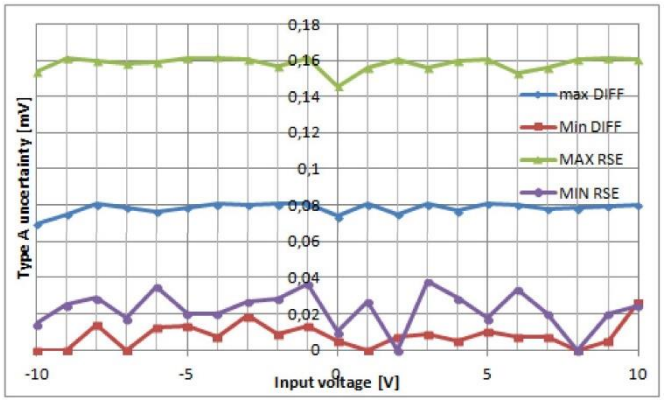

Figure 7. Type A uncertainty for the base scale ± 10 V.

the absolute accuracy is maximum 2 mV. For the RSE input the values are under the limit of 14.7 mV.

The behaviour of the maximum and minimum Type A uncertainties are depicted in Figure 7. The DIFF series represents the behaviour of the differential input for the base scale ± 10 V, while the RSE series is the behaviour for RSE input. The minimum limit is for both below 40 μV, while the maximum type A uncertainty is double for RSE (160 μV) than DIFF. As resulted the Type A uncertainty is much lower than the type B uncertainty.

5. CONCLUSIONS

Usually, the structure of National Metrology Institutes (NMI) involves a central unit and a number of territorial subsidiaries. Each one can be possess an own wallet in the private permissioned Blockchain infrastructure. Each wallet is associated to a node located at subsidiary or at the central entity. They all make up the Blockchain network (Figure 8). The nodes in the network are constantly synchronizing in between, as long as the Internet connection is available. If for some nodes the connection is temporarily broken, after its restoration, the node will send the transactions realized in the meantime in the network and each node will validate each transaction. As a closing takeaway, here are 5 benefits for metrological applications using blockchain:

- Improved security and authenticity: Blockchain technology ensures that once a certificate is added to the Blockchain, it cannot be altered or tampered with, providing a tamper-proof and secure method of recording and sharing calibration data.

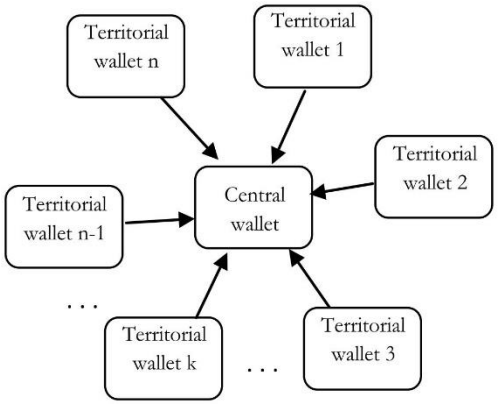

Figure 8. The Metrology Blockchain network.

- Traceability: Blockchain allows for the tracking of the calibration certificate throughout its lifecycle, providing transparency and traceability which can be useful for regulatory compliance and quality control.

- Reduced cost and efficiency: Blockchain-based digital certificates can help reduce the cost of creating, maintaining, and distributing physical certificate and increasing efficiency.

- Better accessibility: Digital certificates stored on the Blockchain can be easily accessed and shared, eliminating the need for physical certificates, reducing risks of loss or damage.

- Greater standardization: The use of Blockchain technology in creating DCCs can also help promoting standardization and consistency in metrology, as data stored on the Blockchain can be easily shared and compared across different organizations.

When a new instrument is calibrated by an entity in territory, it must have its own identity in the entity wallet. Its identity can be created as a unique label in the entity wallet. This will correspond to an own address in the wallet for the instrument (Figure 9). Each transaction is sent inside the same wallet, but the transactions are visible in the whole network.

If the instrument has been calibrated before, it already has a label and respectively an address. The calibration software is checking the existence of the label corresponding to its name and serial number. It interrogates the instrument, gets its name and serial number and then asks the wallet for its address. If there is not a match, it returns an error and the operator has to create the address. If the calibration software finds a match, it uses that address for the following transactions.

Each transaction contains a DCC for a single range. This has been chosen in the present approach because the comment field that carry the DCC information is limited to a number of characters. The DCC is structured as an XML format being stored in the comment of the transaction. For the verification of an instrument with multiple functions and scales, there will be several transactions (Figure 10). In our case, there are 9 transactions for each instrument (9 available scales).

In conclusion, the Blockchain technology shows promising possibilities for metrological applications. It can securely store the DCC, can keep all the certificates issued for an instrument and can assure the traceability as long as the standard has its own address which might have a DCC in the network. The DCC can be generated without the intervention of the operator, with custom software, guaranteeing the validity of the results, minimizing the possibility to fake them.

On the other hand, we plan for future upgrades including a full audit of the calibration process, meaning that every local and national authorized authority can release a DCC for any instrument/standard device. This way one can trace back in time and check how a specific instrument has been authorized by a local authority and follow the traceability chain.

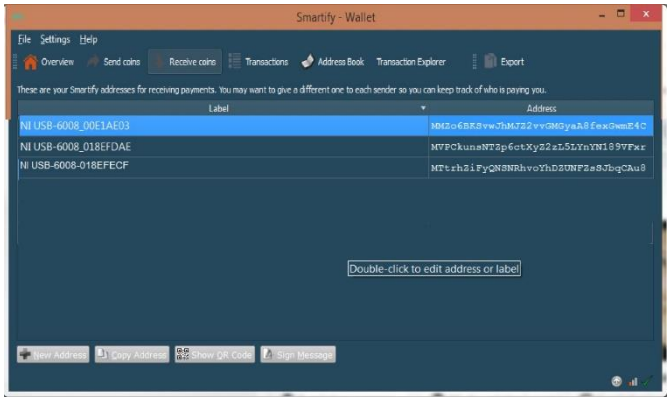

Figure 9. How the instruments get their own labels/address.

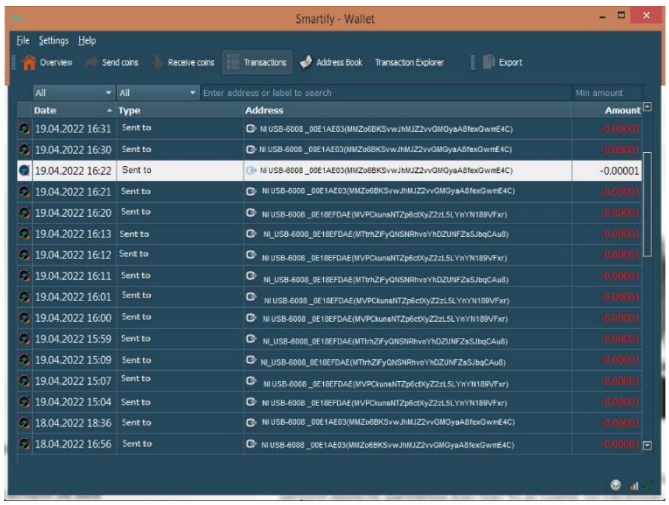

Figure 10. The transaction list containing multiple transactions for 1 address.

A second aspect of future upgrades includes a secure login feature for the Web Asset management tool that manages the enrolment in our private-permissioned infrastructure and also access to read/write data. This basically translates into a simple background check of the provided identification data and allocation of a wallet address.

We also believe that data portability and authenticity is crucial in delivering a DCC, hence we plan a third module that facilitates a digital signature of the exported certificate as PDF file. This feature stores the private key of the digital signature certificate on Blockchain, eliminating the need of hardware security modules (HSM).

The working module requires a small adjustment in order to comply to the European Commission eIDAS Regulation - https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation.

ACKNOWLEDGEMENT

This work was supported from project POC 351/390027/08.09.2021 European Structural Funds.

REFERENCES

[1] National Instruments Corp, Calibration Procedure, 322314B-01, February 2000.

[2] C. De Capua, D. Grillo, E. Romeo, The Implementation of an Automatic Measurement Station for the Determination of the Calibration Intervals for a DMM, IEEE Symposium on Virtual Environments, Human-Computer Interfaces and Measurement Systems, La Coruna, Spain, 10-12 July 2006, pp. 58-62. DOI: 10.1109/VECIMS.2006.250790

[3] H. M. Abdel Mageed, A. M. El-Rifaie, Automatic Calibration System for Electrical Sourcing and Measuring Instruments, 12th International Conference on Environment and Electrical Engineering, Wroclaw, Poland, 5-8 May 2013, pp. 30-34. DOI: 10.1109/EEEIC.2013.6549578

[4] F. Martín-Rodríguez, E. Vázquez-Fernández, Á. Dacal-Nieto, A. Formella, V. Álvarez-Valado, H. González-Jorge, Digital Instrumentation Calibration Using Computer Vision, ICIAR 2010, Part II, LNCS 6112, pp. 335–344, Springer-Verlag Berlin Heidelberg 2010, 978-3-642-13774-7.

[5] G. Grzeczka, M. Klebba, Automated Calibration System for Digital Multimeters Not Equipped with a Communication

Interface, MDPI Sensors 2020, 20, 3650.
DOI: 10.3390/s20133650

[6] A. Carullo, M. Parvis, A. Vallan, Security Issues for Internet-Based Calibration Activities, IEEE Instrumentation and Measurement Technology Conference Anchorage, Alaska, USA, May 21-23, 2002. pp. 817-822.
DOI: 10.1109/IMTC.2002.1006947

[7] M. S. Gadelrab, R. A. Abouhogail, Towards a new generation of digital calibration certificate: Analysis and survey, Measurement 181 (2021) 109611.
DOI: 10.1016/j.measurement.2021.109611

[8] D. Röske, A visual tool for generating digital calibration certificates (DCCs) in Excel , Measurement: Sensors, Volume 18, December 2021, 100175.
DOI: 10.1016/j.measen.2021.100175

[9] G. Boschung, M. Wollensack, M. Zeier, C. Blaser, Chr. Hof, M. Stathis, P. Blattner, F. Stuker, N. Basic, F. Grasso Toro, PDF/A-3 solution for digital calibration certificates, Measurement: Sensors, Vol. 18, December 2021, 100282, 4 pp.
DOI: 10.1016/j.measen.2021.100282

[10] T. Mustapää, P. Nikander, D. Hutzschenreuter and R. Viitala, Metrological Challenges in Collaborative Sensing: Applicability of Digital Calibration Certificates, Sensors 2020, 20, 4730.
DOI: 10.3390/s20174730

[11] C. Brown, T. Elo, K. Hovhannisyan, D. Hutzschenreuter, P. Kuosmanen, O. Maennel, T. Mustapaa, P. Nikander, T. Wiedenhoefer, Infrastructure for Digital Calibration Certificates, 2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT, 03-05 June 2020, Rome, Italy, pp. 485-489.
DOI: 10.1109/MetroInd4.0IoT48571.2020.9138220

[12] J. Schaerer; T. Braun, A Distributed Calibration Certificate Infrastructure, 4th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 27-30 September 2022, pp. 1-4.
DOI: 10.1109/BRAINS55737.2022.9909437

[13] D. Yaga, P. Mell, N. Roby, K. Scarfone, Blockchain Technology Overview, NISTIR 8202, October 2018, Internal Report 8202.
DOI: 10.6028/NIST.IR.8202

[14] D. Peters, J. Wetzlich, F. Thiel, J. P. Seifert, Blockchain Applications for Legal Metrology, IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Houston, TX, USA, 14-17 May 2018, pp. 1-6.
DOI: 10.1109/I2MTC.2018.8409668

[15] M. Sadek Ferdous, M. Jabed Morshed Chowdhury, M. A. Hoque, A. Colman, "Blockchain Consensus Algorithms: A Survey", shortcomarXiv: 2001.07091v2 [cs.DC] 7 Feb 2020. Online [Accessed 20230225]
https://arxiv.org/pdf/2001.07091.pdf