sensors

MDPI

Article

Traceability Management System Using Blockchain Technology and Cost Estimation in the Metrology Field

Naoki Takegawa * and Noriyuki Furuichi

National Metrology Institute of Japan (NMIJ), National Institute of Advanced Industrial Science and Technology (AIST), 1-1-1, Umezono, Tsukuba 305-8563, Ibaraki, Japan
* Correspondence: takegawa-naoki@aist.go.jp

Abstract: Metrological traceability is essential to ensure the reliability of calibration tests. Calibration certificates usually include information on only one upper-level reference standard. As metrological traceability is multi-layered, generally there is no method available for end users to instantly confirm the traceability from the reference standard to a primary standard. This study focuses on the Ethereum blockchain, which has both tamper resistance and high availability, as a digital data management method. To improve the transparency and reliability of calibration tests, a smart contract that traces back to the primary standard is proposed. Consequently, it is confirmed that end users can instantly obtain traceability information. In addition, the execution of smart contracts requires transaction fees. Here, the calculation of the transaction fees is organized, and the traceability management system is discussed from a cost-effective perspective in the field of metrology.

Keywords: measurement; traceability; management; blockchain; operating cost

Citation: Takegawa, N.; Furuichi, N. Traceability Management System Using Blockchain Technology and Cost Estimation in the Metrology Field. *Sensors* **2023**, *23*, 1673. https://doi.org/10.3390/s23031673

Academic Editors: Maurizio Talamo and Christian H. Schunck

Received: 12 January 2023
Revised: 29 January 2023
Accepted: 30 January 2023
Published: 3 February 2023

1. Introduction

The introduction describes metrological traceability and examines the benefits of its management and visualization system. It also surveys the previous literature on digital calibration certificate (DCC) and the use of blockchain, which are related technologies for digitizing metrological traceability. The overview of this research and the contents of the chapters are provided.

1.1. Issues Related to Traceability Management in the Field of Metrology

In manufacturing, accurate measurement is indispensable for achieving the required quality and improving productivity. Calibration of equipment with reference standards is important in ensuring the reliability of measurement results, and the establishment of metrological traceability is required in international standards, such as ISO 10012 [1] and ISO 17025 [2]. Metrological traceability is defined in ISO/IEC Guide 99:2012 VIM [3] as "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". A calibration certificate issued by an accredited calibration laboratory is a stand-alone proof of metrological traceability and usually includes information on only one upper-level reference standard. Therefore, as metrological traceability is multi-layered, there is no immediate way for end users to ascertain the traceability from a device under test (DUT) to a primary standard in general. Note that the results in a certificate are metrologically traceable in the above situation. Takatsuji et al. [4] highlighted the existence of certificate holders who require details of metrological traceability and proposed the visualization of metrological traceability. Miličević et al. [5] presented the concept of a traceability system for electrical energy measurement based on blockchains. Although the management and visualization system of metrological traceability is important and expected to improve the reliability and transparency of calibration tests, there are several

issues related to (1) the digital format and (2) the digital security of calibration information in its construction.

1.2. Calibration Information as Digital Data and Digital Calibration Certificate (DCC)

To organize the handling of calibration information as digital data, studies on DCC have been conducted [6–8]. Hackel et al. [9] mentioned the necessary content for DCC and proposed XML as a data format. Mustapää et al. [10] discussed the contribution of DCC to the uncertainty, completeness, and authenticity of measurement data and introduced applications of DCC such as smart cities. Ačko et al. [11] summarized the SmartCom (communication and validation of smart data in IoT networks) project adopted by EMPIR of EURAMET, which aims to develop a digital format, and presented the interim progress of SmartCom, including the DCC format. Gadelrab et al. [12] conducted an exhaustive survey study on DCC. In addition, CIPM is actively undertaking a project [13] called Digital-SI to establish a metadata format that conforms to SI units.

1.3. Digital Security of Calibration Information and Blockchain Technology

In recent years, the use of blockchain as a highly robust and highly available database in the industrial sector has increased [14–18]. Compared with the usual centralized databases, the advantages of blockchains are considered to be the tamper resistance, elimination of single points of failure, high availability, and savings in human costs. Andoni et al. [19] reviewed the current business cases and presented blockchain solutions for the energy industry. Zhou et al. [20] summarized the global development of peer-to-peer energy trading and introduced blockchains supporting the trading. Leng et al. [21] investigated the contribution of blockchains to achieving sustainability from the perspective of the manufacturing system and product lifecycle management. Chen et al. [22] designed an efficient and secure data collection framework in the smart grid by integrating fog computing and blockchain. Iftikhar et al. [23] studied recent research based on blockchains in the IoT for privacy protection. Suvarna et al. [24] focused on the concept of cyber–physical production systems (CPPSs) and proposed applying blockchains to CPPS to secure data sharing in decentralized systems.

In metrological transactions, the tamper resistance of calibration information is important because there is an economic incentive to tamper with the information on measuring instruments. When traceability management and visualization are implemented as a system, high system availability and elimination of single points of failure are also required. Therefore, blockchain has attracted attention as a useful tool in the field of metrology [25–27]. Blockchains can be broadly classified into private and public chains based on the presence or absence of an administrator. Table 1 presents a summary of private and public blockchains. Hyperledger Fabric (HF) [28] is a private chain that is being considered for use in metrology. Moni et al. [29] used HF to connect peers between the national metrology institute in Germany and Brazil to identify and authenticate smart meters. Melo et al. [30,31] compared the blockchain with existing paper- and cloud-based data management and examined the throughput and latency of HF applied to smart meters. Yurchenko et al. [32] proposed a model for a secure smart meter system using HF and cryptography. Peters et al. [33,34] proposed a use of blockchain in legal metrology and verified the confidentiality of decentralized meters combining HF and homomorphic cryptography.

One public chain that is being considered for use the field of metrology is Ethereum [35,36]. Gavin [37] released the first yellow paper outlining the technical specifications of Ethereum. Ethereum is explained in detail in Section 2 and beyond. Iqbal et al. [38] addressed issues related to trust in IoT systems and proposed tracking, management, governance, and access control of smart vehicles using Ethereum. Shah et al. [39] proposed the management of calibration information using Ethereum and examined the effect of the number of calibrators and calibration hierarchy on the time to obtain traceability in the Ethereum blockchain. Santis et al. [40] proposed a combination of blockchain and physical unclonable function-based authentication protocols for an auditing system for metrological traceability. The system for voltage and current

measurements used Ethereum as the blockchain technology and Node.js as the web interface. Peterek and Montavon [41] proposed the IOTA [42,43] blockchain, a public chain, as a database of hash values of measured data.

Table 1. Comparison of private and public chains.

	Private Chains	**Public Chains**
Consensus building	Consensus-building costs (fees and time) are generally small.	Consensus-building costs (fees and time) are generally significant.
Robustness	The possibility exists that data may be tampered with by certain participants. A single point of failure may exist.	For the cost of consensus building, the likelihood of data being falsified by a particular participant is generally low.
Chain participants	Specific (licensed individuals and companies)	Unspecified
Application examples in the field of metrology	HF [26,30–34,44]	Ethereum [26,38–40,45–47], IOTA [41]

1.4. Contents of This Study

As described in Section 1.1, the management and visualization system for metrological traceability in this study is expected to improve the reliability and transparency of calibration tests. Therefore, the above system is constructed using blockchain, which has been attracting attention in the field of metrology. The digital format of calibration information is beyond the scope of this study, as there are numerous studies and projects on this topic. An important concept in this study is the recognizable traceability path (RTP), which is defined as the path from a DUT to a primary standard that can be recognized by end users (Figure 1). In Figure 1, the traceability hierarchy is set to 4 as an example. However, in practice there are simpler or more complex cases than this case. Additionally, examples of standards in the flow measurement field corresponding to each hierarchy are provided. By using the RTP, end users can easily know metrological traceability. Although the RTP mainly focuses on information in calibration certificates that is metrologically traceable, a system such as the RTP can also be explored for other information that requires traceability management and visualization.

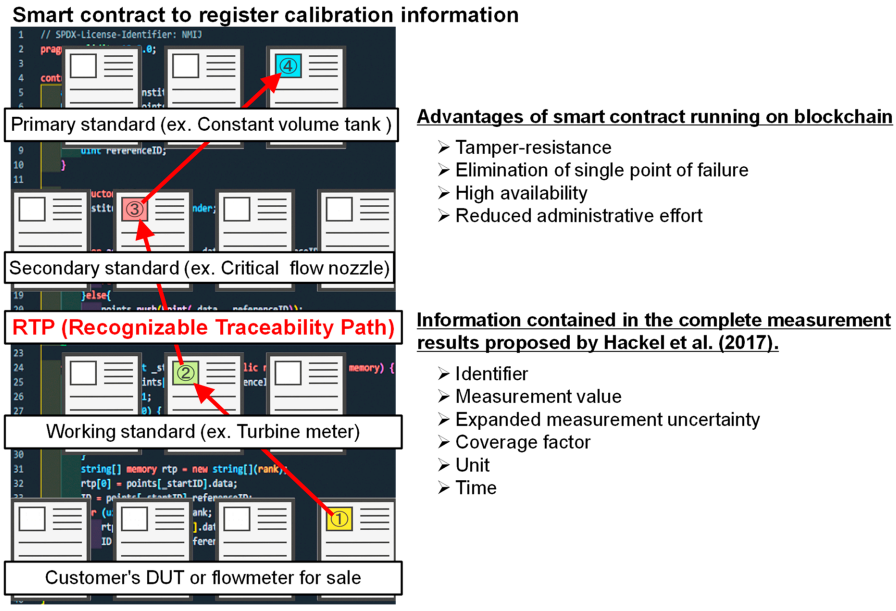

Figure 1. Conceptual diagram of the RTP using a smart contract. Hackel et al. [9] mentioned the necessary content for DCC.

Section 1 summarizes the management and visualization system of metrological traceability and the adoption of blockchains in the field of metrology. In Section 2, a simple system for the RTP is created using the Ethereum blockchain, which is extremely difficult to tamper with. There are only a few studies in the field of metrology that have written a blockchain program and verified its operation. Section 3 estimates the cost of recording information on the Ethereum blockchain and examines the Ethereum-based traceability management and visualization system from an economic cost perspective. There is a debate about whether to choose private or public chains, such as HF or Ethereum, respectively. An important indicator for choosing between private or public chains is the cost of the chain (Table 1). However, to the best of the authors' knowledge, there is no study in the field of metrology that examines the economic feasibility of using blockchain to manage digital data.

2. Building a Traceability Management System Using a Smart Contract

2.1. Smart Contract of Ethereum

The Ethereum blockchain has a feature called a smart contract [48,49] that automatically executes contracts (programs), allowing for complex processing. Applications using smart contracts are examined in detail by Hewa et al. [50]. For instance, smart contracts have been used to develop various services, such as decentralized finance (DeFi) and non-fungible token [51], which is proof of the uniqueness of digital art. Smart contracts are often written in a programming language called Solidity [35]. The smart contract on the RTP described below is written in Solidity and their behavior is checked on Ropsten, Ethereum's test network. The behavior is also confirmed on another test network, Goerli.

2.2. Preparations Required to Execute Smart Contract

There are many methods for deploying and using smart contracts written in Solidity on the Ethereum network. One method is to use Go Ethereum (Geth), a node operation software developed by the Ethereum Foundation, and another method is to use an integrated development environment called Remix, which allows the creation, compilation, and deployment of smart contracts in a web browser. Unlike the above methods, this study implements and uses smart contracts, employing Truffle, INFURA, and web3.js, which are relatively easy and highly flexible. Truffle is the de facto standard framework for Ethereum application development and can compile and deploy smart contracts. INFURA, an Ethereum node hosting service, makes it possible to connect to the Ethereum network without downloading Ethereum nodes such as Geth. web3.js is a JavaScript library and can be used to access deployed smart contracts. Figure 2 illustrates these relationships.

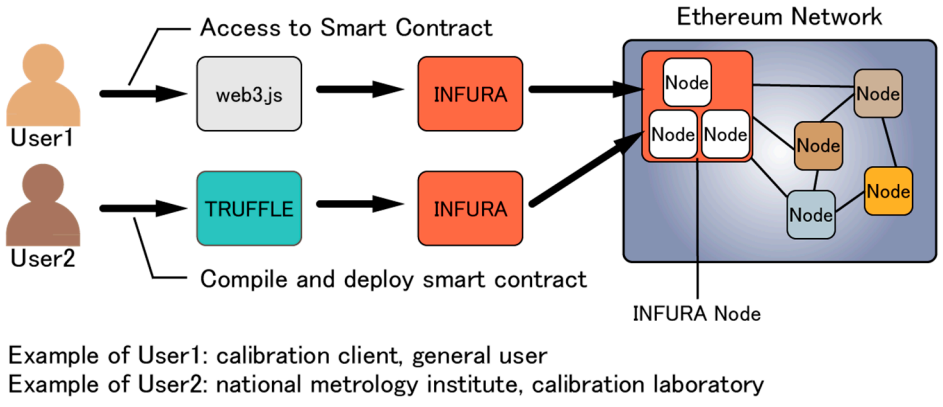

Figure 2. Method of creating and using smart contracts in this study.

2.3. Smart Contract on the RTP

An overview and program of a simple smart contract on the RTP are depicted in Figure 3 and Algorithm 1. There are two types of functions in Algorithm 1. One is "function add" that records data such as a DUT or reference standard in the Ethereum blockchain, and the other is "function RTP" that references the RTP from a DUT to a primary standard. "constructor()" is executed when a smart contract is deployed and records the address of the smart contract issuer. This grants access to "function add", which is described next only to the smart contract issuer. This is necessary to resolve user authentication issues such as verifying the identity of national metrology institutes and calibration laboratories.

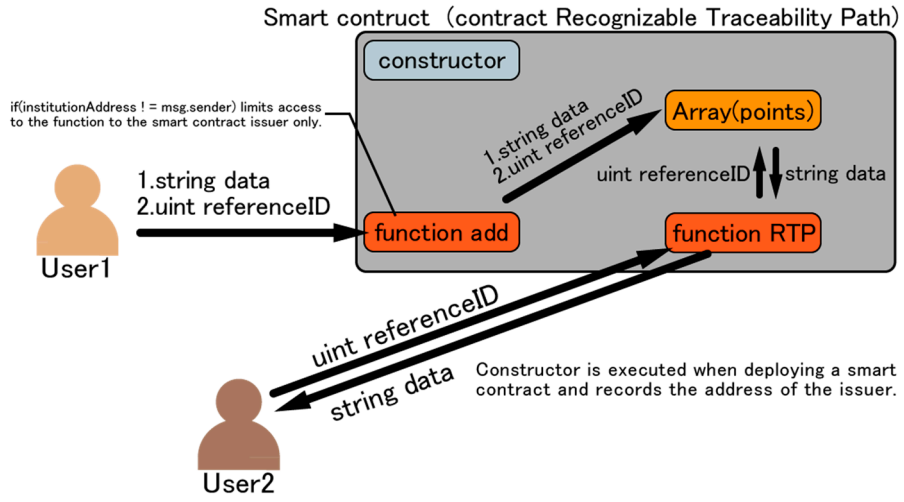

Figure 3. Overview of smart contract on RTP in this study.

"function add" records the two arguments, "string data" and "uint referenceID", on the Ethereum blockchain. "referenceID" indicates the ID with which the information on one upper-level reference standard is linked. Transaction fees must be paid when using "function add" because of the data writing process involved. According to Hackel et al. [9], there are six types of information to be recorded as string data: identifier, measurement value, expanded measurement uncertainty, coverage factor, unit, and time. If six items are recorded as RTP data, it is desirable to prepare six types of variables ("string data") to store data. The data recorded in the smart contract should be limited to what can be disclosed to the outside world, and information that cannot be disclosed should be recorded as hash values. "function RTP" allows the end user to enter the ID of a DUT and receive RTP information as the return value. In the case of data for reference only, no transaction fees are incurred. To make this clear, the function modifier "view" is used in "function RTP".

In this study, calibration clients and end users are assumed as User 1 using "function RTP", and national metrology institutes and accredited calibration laboratories are assumed as User 2 using "function add". An example of RTP information received by User 1 is depicted in Figure 4, revealing the actual acquisition of pre-registered data from Ropsten (Ethereum's test network) by a local server built on node.js through web3.js and INFURA. The calibration information in Figure 4 corresponds to "string data" in Algorithm 1, and the data are stored in each traceability hierarchy. Information registered on Ropsten using Algorithm 1 is obtained through web3.js and INFURA and reflected in node.js. Traceability hierarchy 1 describes the calibration information on a primary standard, and 4 describes the calibration information on a DUT.

Algorithm 1: Smart contract on the recognizable traceability path (RTP) written using Solidity in this study.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract RecognizableTraceabilityPath {
    address public institutionID;
    Point[] public points;
    struct Point {
        string data;
        uint referenceID;
    }

    constructor() {
        institutionID = msg.sender;
     }

    function add(string memory _data, uint _referenceID) public {
        if(institutionID != msg.sender){
            revert();
        }else{
            points.push(Point(_data, _referenceID));
        }
    }

     function RTP(uint _startID) view public returns(string[] memory) {
        uint ID = points[_startID].referenceID;
        uint rank = 1;
        while(ID != 0) {
            rank++;
            ID = points[ID].referenceID;
        }
        string[] memory rtp = new string[](rank);
        rtp[0] = points[_startID].data;
         ID = points[_startID].referenceID;
        for (uint i = 1; i < rank; i++) {
             rtp[i] = points[ID].data;
            ID = points[ID].referenceID;
        }
        return rtp;
    }
}
```

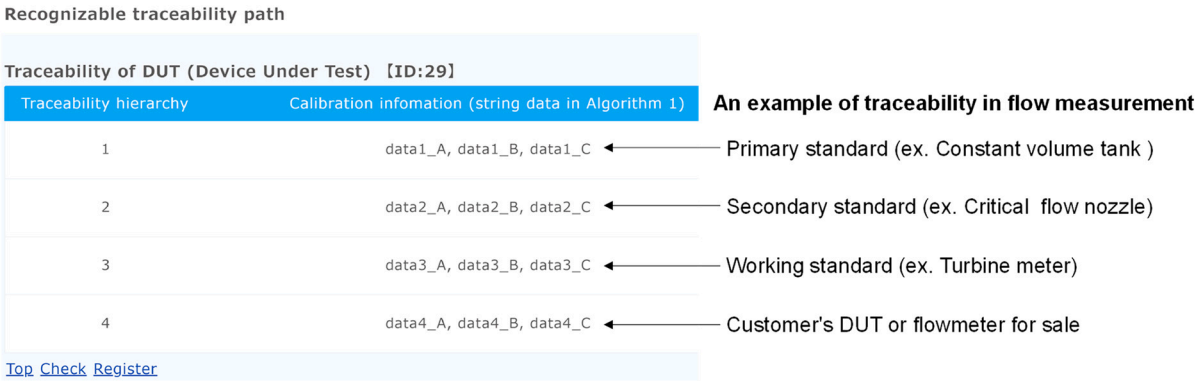

Figure 4. An example of the RTP received by an end user.

3. Cost Estimation of the RTP

3.1. Overview of Transaction Fees

Section 3 estimates the costs associated with the RTP proposed above and discusses the economic feasibility of managing calibration information using Ethereum, a public chain. To deploy and execute a smart contract on Ethereum, a transaction must be issued and a fee called "gas" must be paid. The transaction fees are paid to the miner, who tends to record transactions with high transaction fees in the blockchain. This gas-based transaction fee is represented by the following equation:

$$gas(eth) = gas\ price(eth/gas) \times gas\ usage(gas) \quad (1)$$

The gas price is set by the transaction issuer based on the congestion of the Ethereum network. The gas usage varies depending on the content of the program to be executed by the smart contract. Therefore, to estimate the cost of a smart contract for the RTP, it is necessary to estimate the gas price and gas usage.

3.2. Gas Price

The gas price can be set by the transaction issuer. Setting a higher gas price increases the likelihood that the transaction is recorded in the blockchain more quickly. Therefore, the gas price setting depends on the urgency of transaction approval. The gas price comprises three components: Base Fee Per Gas, Priority Fee Per Gas, and Max Fee Per Gas. For more details, please refer to EIP-1559 [52]. As an indication of the gas price, you can use web3.eth.getGasPrice() of web3.js, a JavaScript library, to obtain the median gas price set in multiple transactions in the past. Figure 5a depicts the time variation in the gas prices obtained from web3.eth.getGasPrice() observed in the main network of Ethereum. The units of gas price are expressed in Gwei (=10^{-9} ETH). The gas price is affected by various factors, such as the congestion of Ethereum's main network, etc. Therefore, it is extremely difficult to predict future gas prices even though it is possible to know the current appropriate gas prices. It is not necessary to pay for the gas price depicted in Figure 5a at each time, where users can set their gas price as low as not less than Base Fee Per Gas. Figure 5b is the gas price converted to the dollar notation by multiplying Figure 5a with the price of Ethereum, providing an intuitive gas price. The gas prices represented in Figure 5a or Figure 5b multiplied by the gas usage is the transaction fee on Ethereum's main network.

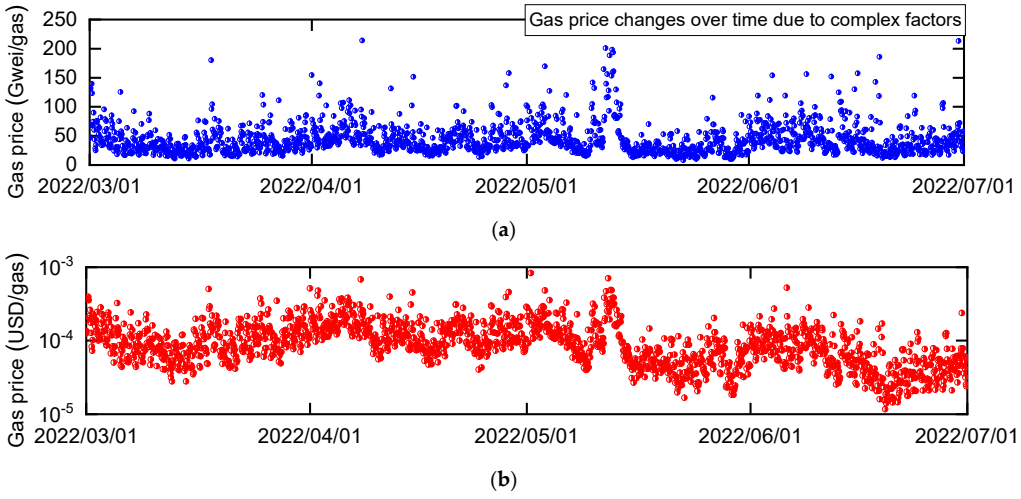

Figure 5. Time variation in gas price on Ethereum's main network. The transaction fee is determined by the gas price and gas usage. Gas prices change over time due to various factors. Gas usage depends on the throughput of smart contracts (type and number of opcodes executed). (**a**) Gas price (Gwei/gas). (**b**) Gas price (USD/gas).

3.3. Gas Usage

Languages such as Solidity that describe smart contracts on Ethereum are compiled into bytecode and opcode that are executed by the Ethereum Virtual Machine in the node. The gas usage is determined by the arithmetic operations performed in the opcode. For example, addition of two elements (ADD) consumes three gas; multiplication of two elements (MUL) consumes five gas; obtaining block height (NUMBER) consumes two gas, and obtaining balance (SELFBALANCE) consumes five gas in the opcode. All the above opcodes are static gas costs; the opcodes whose gas cost varies depending on the amount of data handled are called dynamic gas costs. For more information on each opcode, please refer to the Ethereum Yellow Paper (Berlin) [53]. The gas usage required to execute "function add", which records the calibration information described in Algorithm 1, can be estimated by examining the opcodes used. In this study, "function add" is executed on Ropsten (Ethereum's test network) to extract the opcode operations with large gas usage and verified the dominant factors in transaction fees.

The results of the validation reveal that when "string data" and "uint referenceID" are recorded on Ropsten in Algorithm 1, the gas usage is 72,572. The two opcodes with the highest gas costs are TRANSACTION and SSTORE, as depicted in Figure 6. TRANSACTION consumes 21,000 gas as the minimum cost of issuing a transaction. SSTORE consumes 22,100 gas as the cost of recording data (cold access) on each Ethereum node. In the program described here, SSTORE is used twice because two data, "string data" and "uint referenceID", are recorded (44,200 gas). TRANSACTION and two SSTOREs account for approximately 90% of the total gas usage of 72,572 gas. This ratio is similar when the number of variables (number of "string data") increases. From this, it is possible to estimate the overall gas usage from the number of times SSTORE are used, i.e., the number of variables. Note that recording more than 256 bits of data in "string data" may cause the gas usage to fluctuate.

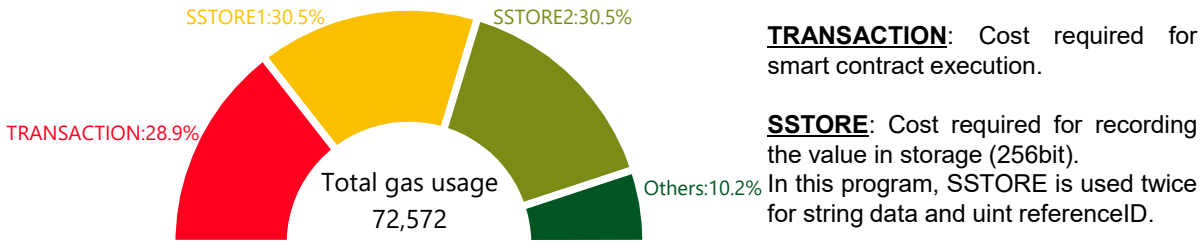

Figure 6. Breakdown of gas usage in a transaction.

3.4. Feasibility of RTP Using Ethereum in the Field of Metrology

According to the Physikalisch-Technische Bundesanstalt (PTB) report [9], the number of calibration certificates issued is estimated to be approximately 10,000 per year by PTB and approximately 100,000 per year by accredited calibration laboratories in Germany. In addition, the National Metrology Institute of Japan (NMIJ) issues approximately 700 calibration certificates per year (jcss calibration: 500, calibration and testing service except jcss: 200), excluding those in the field of legal metrology, and approximately 610,000 calibration certificates [54] are issued by accredited calibration laboratories in Japan. As mentioned above, the number of calibration certificates issued by each national metrology institute is enormous, and it is unrealistic to manage all the information in a public chain, which requires transaction fees. For a single measurement, the cost of recording the six items proposed by Hackel et al. [9] on the Ethereum blockchain using the smart contract described in Algorithm 1 is estimated. As the majority of the gas usage is accounted for by one TRANSACTION and six SSTOREs, the usage is estimated to be approximately 170,000 gas based on Section 3.3. The necessary transaction fees for a single measurement can be estimated by multiplying this gas usage by the median gas price of 37 Gwei/gas (Figure 5a) or 0.000089 USD/gas (Figure 5b). For reference, as of 2022, the NMIJ's fee for

issuing a certificate for calibration and testing service except jcss is 1300 JPY for Japanese text and 2300 JPY for English text (excluding tax).

The data recording on a blockchain is expected to improve the reliability and added value of the measurement system, as exemplified by the traceability management and visualization system (i.e., the RTP) proposed in this study. Therefore, companies and research institutions should conduct a cost–benefit analysis before recording data on a blockchain. Blockchain usage may be appropriate for valuable data with high calibration costs (e.g., flow meter calibrations with large bore under high flow rates and calibration of cryogenic thermometers) because of the need to pay transaction fees at the time of using a public chain (Ethereum). Moreover, important standards that are frequently referenced, such as national and primary standards, would also be worth registering on the blockchain. If the transaction fee is an issue in the use of blockchain, utilizing a private chain such as HF rather than a public chain such as Ethereum would reduce costs. However, tamper resistance and other factors need to be considered when using a private chain. On public chains, practical applications for lowering transaction fees are also underway. For instance, Layer2 technologies such as Lightning Network [55,56] and proof-of-stake [57,58] alternatives to proof-of-work [59] are being developed.

4. Conclusions

This study focuses on the Ethereum blockchain, which is both tamper-resistant and highly available, as a method of managing digital data in the field of metrology as only a few studies have clearly identified the economic costs of blockchains. This study then proposes the RTP that can be accessed by end users using smart contracts to improve the transparency and reliability of calibration tests. Only a few existing studies have created smart contracts and verified their operation. While describing the development environment and procedures in detail, this study works on the management and visualization of the traceability path. As a result, the recording of data on the blockchain ("function add" in Algorithm 1), the retrieval of data from the blockchain ("function RTP" in Algorithm 1), and the verification of the output as the RTP (Figure 4) are confirmed. Furthermore, using Ethereum, the transaction fee of executing smart contracts is estimated. The calculation of the transaction fee requires gas prices and gas usage. First, the required gas prices are recorded (2022/03~2022/07) and clarified on Ethereum's main network. Then, calculation method of the gas usage is explained in detail, and the opcodes of TRANSACTION and SSTORE account for 90% of the gas usage in the smart contract for the present RTP. In addition, the traceability management system is verified from an economic cost perspective. The basic cost of executing smart contracts on Ethereum is described so that everyone can reproduce it. This study makes a valuable contribution to the literature by presenting a decision method based on economic costs in an era where there is debate in the field of metrology about choosing between private and public chains such as HF and Ethereum, respectively.

Author Contributions: N.T.: Conceptualization, Methodology, Draft preparation, Visualization. N.F.: Supervision, Validation, Writing—reviewing and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data that support the findings of this study are available from the corresponding authors upon reasonable request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. *ISO 10012*; Measurement Management Systems–Requirements for Measurement Processes and Measuring Equipment. International Organization for Standardization: Geneva, Switzerland, 2003.
2. *ISO 17025*; General Requirements for the Competence of Testing and Calibration Laboratories. International Organization for Standardization: Geneva, Switzerland, 2006.

3. Joint Committee for Guides in Metrology. *International Vocabulary of Metrology—Basic and General Concepts and Associated Terms (VIM)*, 3rd ed. Available online: https://www.bipm.org/en/committees/jc/jcgm/publications (accessed on 29 January 2023).
4. Takatsuji, T.; Watanabe, H.; Yamashita, Y. Blockchain technology to visualize the metrological traceability. *Precis. Eng.* **2019**, *58*, 1–6. [CrossRef]
5. Miličević, K.; Tolić, I.; Vinko, D.; Horvat, G. Blockchain-Based Concept for Digital Transformation of Traceability Pyramid for Electrical Energy Measurement. *Sensors* **2022**, *22*, 9292. [CrossRef] [PubMed]
6. Marques, M.; Sousa, J.A.; Ribeiro, L. Calibration 4.0–Information system for usage of digital calibration certificates. In Proceedings of the 19th International Congress of Metrology (CIM2019), Paris, France, 24–26 September 2019; p. 01002.
7. Boschung, G.; Wollensack, M.; Zeier, M.; Blaser, C.; Hof, C.; Stathis, M.; Blattner, P.; Stuker, F.; Basic, N.; Toro, F.G. PDF/A-3 solution for digital calibration certificates. *Meas. Sens.* **2021**, *18*, 100282. [CrossRef]
8. Bruns, T.; Nordholz, J.; Röske, D.; Schrader, T. A demonstrator for measurement workflows using digital calibration certificates (DCCs). *Meas. Sens.* **2021**, *18*, 100208. [CrossRef]
9. Hackel, S.; Härtig, F.; Hornig, J.; Wiedenhöfer, T. The digital calibration certificate. *PTB-Mitt.* **2017**, *127*, 75–81.
10. Mustapää, T.; Nikander, P.; Hutzschenreuter, D.; Viitala, R. Metrological challenges in collaborative sensing: Applicability of digital calibration certificates. *Sensors* **2020**, *20*, 4730.
11. Ačko, B.; Weber, H.; Hutzschenreuter, D.; Smith, I. Communication and validation of metrological smart data in IoT-networks. *Adv. Prod. Eng. Manag.* **2020**, *15*, 107–117. [CrossRef]
12. Gadelrab, M.S.; Abouhogail, R.A. Towards a new generation of digital calibration certificate: Analysis and survey. *Measurement* **2021**, *181*, 109611. [CrossRef]
13. CIPM Task Group on the Digital SI (CIPM-TG-DSI). Available online: https://www.bipm.org/en/committees/ci/cipm/wg/cipm-tg-dsi (accessed on 29 January 2023).
14. Chen, C.L.; Zhu, Z.P.; Zhou, M.; Tsaur, W.J.; Wu, C.M.; Sun, H. A Secure and Traceable Vehicles and Parts System Based on Blockchain and Smart Contract. *Sensors* **2022**, *22*, 6754. [CrossRef]
15. Ai, Y.; Chen, C.L.; Weng, W.; Chiang, M.L.; Deng, Y.Y.; Lim, Z.Y. A Traceable Vaccine Supply Management System. *Sensors* **2022**, *2*, 9670.
16. Guo, X.; Zhang, G.; Zhang, Y. A Comprehensive Review of Blockchain Technology-Enabled Smart Manufacturing: A Framework, Challenges and Future Research Directions. *Sensors* **2023**, *23*, 155. [CrossRef] [PubMed]
17. Zubaydi, H.D.; Varga, P.; Molnár, S. Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review. *Sensors* **2023**, *23*, 788. [CrossRef] [PubMed]
18. Tyagi, A.K.; Dananjayan, S.; Agarwal, D.; Thariq Ahmed, H.F. Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0. *Sensors* **2023**, *23*, 947. [CrossRef] [PubMed]
19. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* **2019**, *100*, 143–174. [CrossRef]
20. Zhou, Y.; Wu, J.; Long, C.; Ming, W. State-of-the-art analysis and perspectives for peer-to-peer energy trading. *Engineering* **2020**, *6*, 739–753. [CrossRef]
21. Leng, J.; Ruan, G.; Jiang, P.; Xu, K.; Liu, Q.; Zhou, X.; Liu, C. Blockchain-empowered sustainable manufacturing and product lifecycle management in industry 4.0: A survey. *Renew. Sustain. Energy Rev.* **2020**, *132*, 110112. [CrossRef]
22. Chen, S.; Yang, L.; Zhao, C.; Varadarajan, V.; Wang, K. Double-blockchain assisted secure and anonymous data aggregation for fog-enabled smart grid. *Engineering* **2020**, *8*, 159–169. [CrossRef]
23. Iftikhar, Z.; Javed, Y.; Zaidi, S.Y.A.; Shah, M.A.; Iqbal Khan, Z.; Mussadiq, S.; Abbasi, K. Privacy preservation in resource-constrained IoT devices using blockchain—A survey. *Electronics* **2021**, *10*, 1732. [CrossRef]
24. Suvarna, M.; Yap, K.S.; Yang, W.; Li, J.; Ng, Y.T.; Wang, X. Cyber–Physical Production Systems for Data-Driven, Decentralized, and Secure Manufacturing—A Perspective. *Engineering* **2021**, *7*, 1212–1223. [CrossRef]
25. Barbosa, C.R.H.; Sousa, M.C.; Almeida, M.F.L.; Calili, R.F. Smart Manufacturing and Digitalization of Metrology: A Systematic Literature Review and a Research Agenda. *Sensors* **2022**, *22*, 6114. [CrossRef]
26. Miličević, K.; Omrčen, L.; Kohler, M.; Lukić, I. Trust model concept for IoT blockchain applications as part of the digital transformation of metrology. *Sensors* **2022**, *22*, 4708. [CrossRef] [PubMed]
27. Zakaret, C.; Peladarinos, N.; Cheimaras, V.; Tserepas, E.; Papageorgas, P.; Aillerie, M.; Piromalis, D.; Agavanakis, K. Blockchain and Secure Element, a Hybrid Approach for Secure Energy Smart Meter Gateways. *Sensors* **2022**, *22*, 9664. [CrossRef] [PubMed]
28. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; pp. 1–15.
29. Moni, M.; Melo, W., Jr.; Peters, D.; Machado, R. When Measurements Meet Blockchain: On Behalf of an Inter-NMI Network. *Sensors* **2021**, *21*, 1564. [CrossRef] [PubMed]
30. Melo, W.; Carmo, L.F.; Bessani, A.; Neves, N.; Santin, A. How blockchains can improve measuring instruments regulation and control. In Proceedings of the 2018 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Houston, TX, USA, 14–17 May 2018; pp. 1–6.
31. Melo, W.S.; Bessani, A.; Neves, N.; Santin, A.O.; Carmo, L.F.R.C. Using blockchains to implement distributed measuring systems. *IEEE Trans. Instrum. Meas.* **2019**, *68*, 1503–1514. [CrossRef]

32. Yurchenko, A.; Moni, M.; Peters, D.; Nordholz, J.; Thiel, F. Security for Distributed Smart Meter: Blockchain-based Approach, Ensuring Privacy by Functional Encryption. In Proceedings of the 10th International Conference on Cloud Computing and Services Science (CLOSER 2020), Online, 7–9 May 2020; pp. 292–301.
33. Peters, D.; Wetzlich, J.; Thiel, F.; Seifert, J.P. Blockchain applications for legal metrology. In Proceedings of the 2018 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Houston, TX, USA, 14–17 May 2018; pp. 1–6.
34. Peters, D.; Yurchenko, A.; Melo, W.; Shirono, K.; Usuda, T.; Seifert, J.P.; Thiel, F. IT security for measuring instruments: Confidential checking of software functionality. In Proceedings of the Future of Information and Communication Conference, San Francisco, CA, USA, 5–6 March 2020; pp. 701–720.
35. Dannen, C. *Introducing Ethereum and Solidity*; Apress: New York, NY, USA, 2017; Volume 1, pp. 159–160.
36. Atzei, N.; Bartoletti, M.; Cimoli, T. A survey of attacks on ethereum smart contracts (sok). In Proceedings of the International Conference on Principles of Security and Trust, Uppsala, Sweden, 22–29 April 2017; pp. 164–186.
37. Wood, E. A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 4836820.
38. Iqbal, R.; Butt, T.A.; Afzaal, M.; Salah, K. Trust management in social internet of vehicles: Factors, challenges, blockchain, and fog solutions. *Int. J. Distrib. Sens. Netw.* **2019**, *15*, 1550147719825820. [CrossRef]
39. Shah, R.; McIntee, M.; Nagaraja, S.; Bhandary, S.; Arote, P.; Kuri, J. Secure Calibration for Safety-Critical IoT: Traceability for Safety Resilience. *arXiv* **2019**, arXiv:1908.00740.
40. De Santis, L.; Paciello, V.; Pietrosanto, A. Blockchain-based infrastructure to enable trust in IoT environment. In Proceedings of the 2020 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Dubrovnik, Croatia, 25–28 May 2020; pp. 1–6.
41. Peterek, M.; Montavon, B. Prototype for dual digital traceability of metrology data using X. 509 and IOTA. *CIRP Ann.* **2020**, *69*, 449–452. [CrossRef]
42. Popov, S. The tangle. *White Pap.* **2018**, *1*, 30.
43. Silvano, W.F.; Marcelino, R. Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. *Future Gener. Comput. Syst.* **2020**, *112*, 307–319. [CrossRef]
44. Melo, W.S., Jr.; Tarelho, L.V.; Rodrigues Filho, B.A.; Bessani, A.N.; Carmo, L.F. Field surveillance of fuel dispensers using IoT-based metering and blockchains. *J. Netw. Comput. Appl.* **2021**, *175*, 102914. [CrossRef]
45. Kennedy, Z.C.; Stephenson, D.E.; Christ, J.F.; Pope, T.R.; Arey, B.W.; Barrett, C.A.; Warner, M.G. Enhanced anti-counterfeiting measures for additive manufacturing: Coupling lanthanide nanomaterial chemical signatures with blockchain technology. *J. Mater. Chem. C* **2017**, *5*, 9570–9578. [CrossRef]
46. D'Emilia, G.; Gaspari, A.; Natale, E.; Adduce, G.; Vecchiarelli, S. All-Around Approach for Reliability of Measurement Data in the Industry 4.0. *IEEE Instrum. Meas. Mag.* **2021**, *24*, 30–37. [CrossRef]
47. More, S.S.; Patel, N.; Parab, S.; Maurya, S. Blockchain based Tamper Proof Certificates. In Proceedings of the International Conference on Smart Data Intelligence (ICSMDI 2021), Tamil Nadu, India, 29–30 April 2021.
48. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
49. Wang, S.; Yuan, Y.; Wang, X.; Li, J.; Qin, R.; Wang, F.Y. An overview of smart contract: Architecture, applications, and future trends. In Proceedings of the 2018 IEEE Intelligent Vehicles Symposium (IV), Suzhou, China, 26–30 June 2018; pp. 108–113.
50. Hewa, T.; Ylianttila, M.; Liyanage, M. Survey on blockchain based smart contracts: Applications, opportunities and challenges. *J. Netw. Comput. Appl.* **2021**, *177*, 102857. [CrossRef]
51. Wang, Q.; Li, R.; Wang, Q.; Chen, S. Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. *arXiv* **2021**, arXiv:2105.07447.
52. Buterin, V.; Conner, E.; Dudley, R.; Slipper, M.; Norden, I.; Bakhta, A. EIP-1559: Fee Market Change for ETH 1.0 Chain. Available online: https://eips.ethereum.org/EIPS/eip-1559 (accessed on 29 January 2023).
53. Wood, E. A Secure Decentralised Generalised Transaction Ledger Berlin Version. Available online: https://ethereum.github.io/yellowpaper/paper.pdf (accessed on 29 January 2023).
54. National Institute of Technology and Evaluation. Number of Jcss Calibration Certificates Issued in fy 2019–2021. Available online: https://www.nite.go.jp/data/000049535.pdf (accessed on 29 January 2023). (In Japanese).
55. Poon, J.; Dryja, T. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Available online: https://lightning.network/lightning-network-paper.pdf (accessed on 29 January 2023).
56. Rohrer, E.; Malliaris, J.; Tschorsch, F. Discharged payment channels: Quantifying the lightning network's resilience to topology-based attacks. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Stockholm, Sweden, 17–19 June 2019; pp. 347–356.
57. Bez, M.; Fornari, G.; Vardanega, T. The scalability challenge of ethereum: An initial quantitative analysis. In Proceedings of the 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE), San Francisco, CA, USA, 4–9 April 2019; pp. 167–176.

58. Saleh, F. Blockchain without waste: Proof-of-stake. *Rev. Financ. Stud.* **2021**, *34*, 1156–1190. [CrossRef]
59. Gervais, A.; Karame, G.O.; Wüst, K.; Glykantzis, V.; Ritzdorf, H.; Capkun, S. On the security and performance of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 3–16.