International Journal of Innovative Research and Scientific Studies, 7(4) 2024, pages: 1509-1517

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

PLCBlox: Using blockchain-based audit trails to generate secure PLC commands

Andrew R. Short[1*], Theofanis G. Orfanoudakis[2], Helen C. Leligou[3]

[1,3]*Department of Industrial Design and Production Engineering, University of West Attica, Greece.*
[2]*School of Science and Technology, Hellenic Open University, Greece.*

Corresponding author: Andrew R. Short (*Email: ashort@uniwa.gr*)

Abstract

This research paper discusses security issues with current deployments of Programmable Logic Controllers (PLCs) and Supervisory Control and Data Acquisition Systems (SCADA) in the industry and proposes a solution that enables PLC devices to query a blockchain infrastructure for commands and setpoints. The blockchain assumes a dual role in this context: serving as an immutable audit trail database as well as a trusted source for critical commands and setpoints. In contrast to the conventional paradigm, this novel approach does not require write access at the PLC level, thus minimizes its attack surface and helping to protect against known and zero-day vulnerabilities often used in cyberwarfare, such as in the case of the notorious Stuxnet worm. Applications that enforce the logging of user operations for Good Manufacturing Practices (GMP) or compliance purposes use the blockchain network as an audit trail database for user actions. Any attempt to maliciously circumvent the logging operation would not affect the operation of a critical process. Additionally, a prototype implementation developed as part of this research finds that modern PLC devices are more than capable of interacting with private Ethereum blockchain nodes. The required libraries and user code consume a small percentage of available resources, while the duration of a complete request-response cycle measured around 22msec. The authors anticipate that PLCBlox can be used as a drop-in replacement for applications requiring higher security standards and logging enforcement, such as nuclear power plants or other critical infrastructure.

Keywords: Blockchain, Industry 4.0, PLC, SCADA, Ethereum, Security, Smart contracts.

DOI: 10.53894/ijirss.v7i4.3449
Funding: This research is supported by the University of West Attica (Grant number: 13/21-03-2024).
History: Received: 28 December 2023/**Revised:** 29 April 2024/**Accepted:** 17 May 2024/**Published:** 22 August 2024

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Institutional Review Board Statement: Not applicable.
Publisher: Innovative Research Publishing

1. Introduction

In the era of Industry 4.0 and the ongoing digital transformation, Supervisory Control and Data Acquisition Systems (SCADA), Human-Machine Interface Devices (HMI), and Programmable Logic Controllers (PLCs) play essential roles in reshaping industrial processes and operations. SCADA systems serve as data hubs that aggregate data from various sensors and machines. HMI devices provide the operator with the ability to interact with complex systems and make informed decisions. A wide range of devices and systems can communicate with PLCs. They serve as the "brains" of automation, orchestrating processes and responding to real-time data. PLCs have limitations in terms of computing resources and processing power, which can make them less suitable for heavy computational tasks compared to more powerful computing platforms. Designed primarily for real-time control and automation in industrial environments, they prioritize reliability, determinism, and stability over raw computing power.

SCADA, HMI, and PLCs collectively enable data-driven decision-making by providing real-time insights into operational performance, equipment health, and quality metrics, and are integral components of the digital transformation in Industry 4.0.

1.1. Audit Trail Logs

Certain industries, such as the pharmaceutical, biotechnology, and medical device industries, are required to apply regulations such as those described by the Food and Drug Administration (FDA) in 21 CFR Part 11 [1]. This regulation outlines the criteria under which electronic records and signatures are considered trustworthy, reliable, and legally equivalent to paper records and handwritten signatures. An audit trail is defined as “a secure, computer-generated, time-stamped electronic record that allows reconstruction of the course of events relating to the creation, modification, and deletion of an electronic record”[2]. In more detail, the logging process should record the user’s identity, time-stamps, and actions. Additionally, the system should be resilient to tampering and preserve the recorded information for compliance.

Figure 1 depicts a typical architecture that describes the information flow within the components of an industrial application.

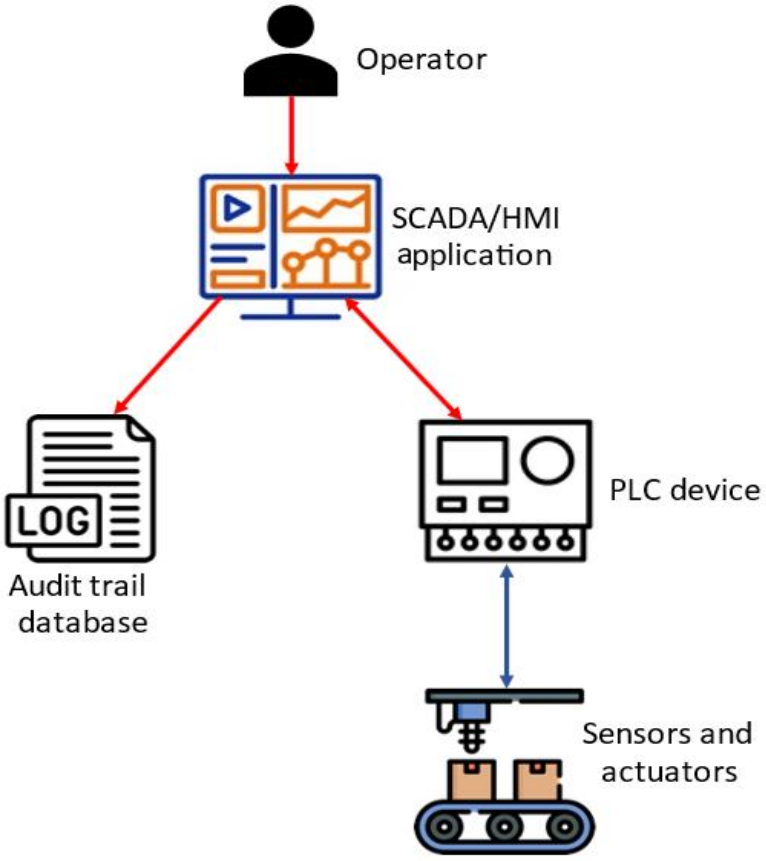

Figure 1.
Typical architecture of industrial applications built upon SCADA/HMI and PLC devices.

1.2. Security Considerations

As these systems become more interconnected, cybersecurity is critical. Industry 4.0 initiatives emphasize robust cybersecurity practices to protect against cyber threats and data breaches.

Many industrial control systems, including SCADA and PLCs, have long lifecycles that can span decades. This means that older hardware and software versions are still in operation, even after newer, more secure alternatives have become available. Some manufacturers discontinue support, focusing their efforts on newer products. This leaves users of these legacy systems without access to security patches. In some cases, upgrading to newer SCADA or PLC systems may not

even be feasible due to compatibility issues with existing infrastructure, cost constraints, or the need for extensive reconfiguration. Smaller organizations or those with limited resources may struggle to keep pace with technology updates and may continue to use older SCADA and PLC systems. Even when updates are available, organizations may be reluctant to apply them for fear of disrupting critical processes.

In 2010, a highly sophisticated computer worm was discovered that gained international attention for its unprecedented level of complexity and its specific target: industrial control systems, particularly Siemens programmable logic controllers (PLCs) at the Iranian nuclear program. Once deployed, Stuxnet does not require Internet access for command-and-control. Instead, it's design involves injecting rouge code into PLC devices [3]. We have also thoroughly documented many other exploits that compromise legacy SCADA systems [4].

SCADA systems operate by sending data (such as setpoint updates, operator commands) directly to the PLC device, and naturally, the devices are required to allow such incoming connections. This requirement forms a large attack vector due to the security issues arising from compromised SCADA systems, malware. Because of these security concerns, such deployments usually reside on isolated internal networks without internet connectivity.

1.3. Proposed Scheme

This paper presents a distinctive contribution by introducing PLCBlox, a novel approach that facilitates the integration of Programmable Logic Controllers (PLCs) with blockchain networks. The unique aspect of this research lies in the nature of the direct interface between a PLC device and a blockchain node, enabling a machine or industrial process to autonomously utilize a smart contract as a trusted source of setpoint updates and commands. Furthermore, security-sensitive operations typically handled by the SCADA system, such as user authentication and authorization, are now handled by the blockchain network, which is inherently more secure and robust. While existing literature discusses blockchain applications in various domains, including industrial applications, the specific exploration of PLCs interacting with blockchain networks, as presented in PLCBlox, remains an unexplored area, opening avenues for further investigation and validation.

Furthermore, due to the immutability attributes of blockchain networks, all historical users' actions are permanently recorded and can be read from previous blocks, in effect forming an audit trail database. Ultimately, the paper demonstrates that a malicious user or software cannot circumvent blockchain logging, as the smart contract's data serves as the sole source of commands and setpoints. This policy enforcement aspect improves security even more.

The motivation behind the development of PLCBlox, is its use in mission critical applications where higher security standards are required. Such applications may include critical infrastructure that may be more targeted by malicious actors such as nuclear power plants as well as in organizations requiring the enforcement of audit trail logs, such as in drug manufacturing industries.

The reset of the paper is organized as follows: Section II outlines the benefits of using a blockchain network as a secure audit trail database and documents related work. Section III describes our approach that builds upon related work in order to enable a PLC device to query the blockchain network and discusses motivation, challenges, and the benefits in terms of security improvements as well as audit log enforcement. Section IV analyses the prototype implementation developed in order to verify feasibility and collect performance indicators and metrics related to calculating the required resources. The results are discussed in Section V, followed by the conclusions in Section VI.

2. Blockchain-Based Audit Trail Databases

Blockchain networks make a great medium for auditing trail databases. The most compelling reasons are the following:

1. Compliance: For industries subject to regulatory compliance, blockchain-based audit trail logs can simplify compliance efforts by providing a tamper-resistant and easily auditable record of activities.
2. Immutability: Once recorded on the blockchain, data becomes nearly impossible to alter or delete. Each new block in the chain contains a cryptographic hash of the previous block, creating a secure and immutable ledger. This feature ensures that audit trail logs remain tamper-proof, providing a reliable historical record of activities.
3. Security: Blockchain networks employ strong cryptographic techniques to secure data. Public and private keys, digital signatures, and consensus mechanisms help protect the integrity of audit trail logs. Unauthorized access and alterations are exceedingly difficult, if not impossible.
4. Permanent Records: Blockchain technology allows for the indefinite storage of audit trail logs. This ensures that historical data is always accessible for compliance, forensic analysis, and trend monitoring.
5. Traceability: Blockchain provides a detailed history of data changes and transactions. Each entry in the audit trail can be traced back to its origin, making it easier to identify the source of any unauthorized actions or anomalies. We can map each action, such as a setpoint change, to a singular user in the context of audit trails.

2.1. Related Word

For the reasons outlined above, researchers are actively developing blockchain-based audit trail database solutions. Some notable examples are mentioned below:

Researchers introduced Block Trail, an innovative blockchain architecture, in a recent study to address the space and time complexity challenges inherent in traditional blockchain systems [5, 6]. They employed a hierarchical structure in Block Trail, utilizing the nature of transactions to partition the system into multiple layers capable of processing transactions simultaneously. This architectural approach aimed to reduce space overhead and accelerate the validation

process by minimizing the number of active replicas. The researchers also implemented additional security measures in Block Trail to strengthen defense capabilities and facilitate the detection of faulty replicas.

Researchers Regueiro, et al. [7] enhanced current audit trail solutions by developing a blockchain-based mechanism that prioritizes security and usability. They leveraged blockchain's intrinsic security features, including integrity, traceability, availability, and non-repudiation, to ensure a high level of security in audit trails. To enhance usability, they incorporated a blockchain monitor, isolating users from the complexities of blockchain use. The resulting prototype contributes to more reliable, secure, and user-friendly audit trails, with identified improvements over existing methods. The mechanism is designed for general-purpose use, applicable across various ecosystems.

Authors Suzuki and Murai [8] have proposed a scheme using blockchain technology for applications requiring strict access control and auditing, such as medical record queries. Potential tampering renders traditional server-side logging insecure, prompting the proposal of a blockchain-based request-response channel for client-server systems. A proof-of-concept system is implemented on a public blockchain testbed, showcasing the feasibility of blockchain transactions as an auditable communication channel. The authors suggest broad applicability, including shared key delivery mechanisms content encryption key delivery, and envision extending the scheme to smart contracts for multi-party conditional schemes and access delegation in healthcare systems.

Researchers Pourmajidi and Miranskyy [9] address the challenge of log tampering in cloud solutions by proposing a blockchain-based log system named Logchain. They emphasize the critical nature of logs during incidents and propose immutability through blockchain to ensure the integrity of log data. Logchain, or Log Chain as a Service (LCaaS), cryptographically seals logs and adds them to a hierarchical ledger, preventing tampering and providing an immutable platform for log storage. The system aims to establish trust among cloud participants (providers and users) by offering verifiable logs through a hierarchical ledger.

Factom, introduced in a whitepaper by Snow, et al. [10] addresses the scarcity of trust in the global economy by offering a precise, verifiable, and immutable audit trail, reducing the need for blind trust and enhancing efficiency. Factom introduces a solution by leveraging blockchains to lock in data, providing a distributed and independently auditable mechanism. While Bitcoin's blockchain is a trusted, immutable data store, Factom extends blockchain technology to businesses without the complexities associated with cryptocurrencies.

Recent work by Schmid, et al. [11] addresses security and privacy issues in the Internet of Things (IoT) networks, particularly focusing on Programmable Logic Controller (PLC) systems. Acknowledging the potential of blockchain technology to enhance security, resilience, and trustless authentication in IoT ecosystems, the paper proposes a novel approach. The suggested model adds a proof-of-work-based blockchain to the PLC IoT ecosystem. This makes it easier to send and store binary data from PLC networks safely. The authors highlight the security challenges of integrating blockchain into IoT systems and suggest evaluating alternative consensus mechanisms, managing storage requirements, and exploring integration with emerging technologies like edge computing and machine learning for improved efficiency. They also emphasize the importance of interoperability and standardization efforts for broader adoption.

Researchers Vick, et al. [12] have explored the integration of blockchain technology, specifically Solana, into Industrial Robot Control Systems using a virtual PLC that interfaces with the Unified Architecture protocol developed by the OPC Foundation (OPC UA). They propose a software gateway connecting Solana Blockchain Cluster and the OPC UA server, enabling data exchange between blockchain and industrial equipment. The smart contract deployed on Solana implements control logic, demonstrated by driving an Industrial Robot Handling Process in a laboratory setting. Test results reveal varying runtimes for different steps, influenced by network latency and transaction processing. The cost analysis shows acceptable expenses for implementing a trusted third-party industrial robot control service on Solana. The blockchain ensures end-to-end data security, allowing the secure deployment of third-party control services as smart contracts. Additional data security measures are recommended for communication between the gateway client, shopfloor, and automation system operator, especially when not in the same segment or location.

A recent study by Loss, et al. [13] addresses the regulatory challenges faced by pharmaceutical manufacturing in Brazil, particularly the requirements set by the Brazilian Health Regulatory Agency that mandate that pharmaceutical systems ensure the integrity, security, and traceability of product information to safeguard consumers. The paper proposes a blockchain-based microservice for audit trail management, aiming to automatically record and secure all pharmaceutical system operations, ensuring data immutability. The paper presents a case study that showcases the suitability of the proposed microservice in pharmaceutical systems. The results indicate the microservice's capability to handle 100 to 200 simultaneous users with good throughput, making it suitable for small or medium-sized companies.

3. Description of PLCBlox

The solution presented in this article builds upon the related work presented in the previous section in order to enable PLC devices to query blockchain-based audit trail databases as a source for parameters and commands. This approach offers improvements to typical HMI and SCADA applications and, to our knowledge, has not yet been researched.

3.1. Principle of Operation

For reading and displaying process data (information flow from CPU to HMI), the procedure remains unchanged, i.e., the CPU is read by the HMI device using vendor specific libraries. In order to update values (parameters or commands) in the CPU area, the user (operator) must first commit a transaction on the blockchain network using his wallet. The CPU asynchronously queries a blockchain node for sets of parameters and setpoints. When changes are identified, they are applied inside the device’s user memory.Figure 2 depicts the complete workflow.

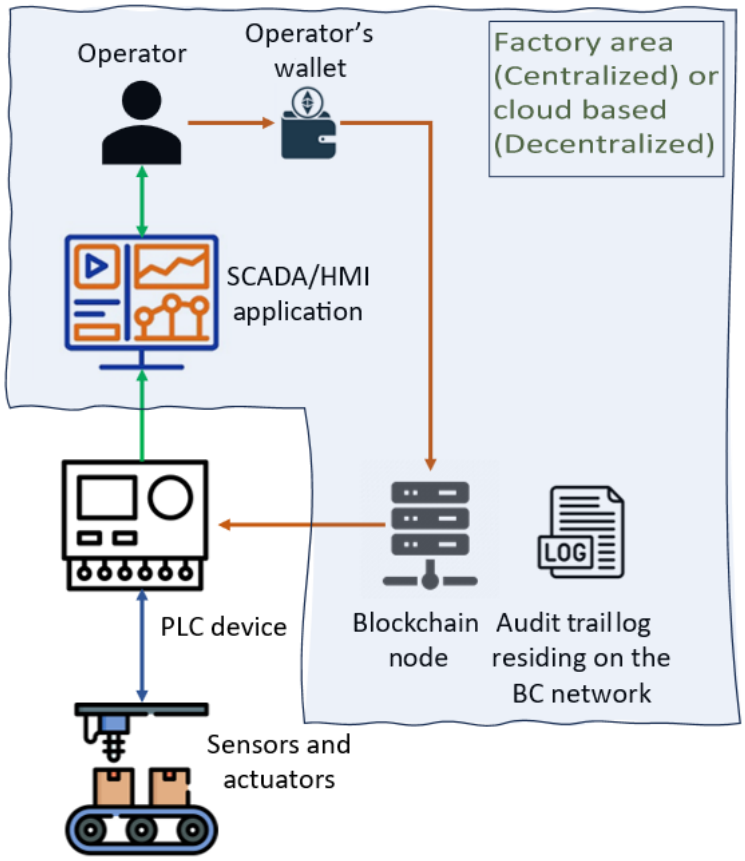

Figure 2.
Flow of information within PLCBlox.

Contrary to traditional HMI systems, the user authentication and authorization tasks are now coordinated by the blockchain network, the smart contract, and the user's wallet. Moreover, by leveraging the underlying technology of blockchain, aspects of the audit trail database are self-contained in the smart contract's storage area. These concepts are summarized in Table 1.

Table 1.
Key differences between typical industrial application architectures and PLCBlox.

Function	Typical architectures	PLCBlox
User authentication	Local windows accounts, domain controller accounts, accounts configured in SCADA application	User's wallet
User authorization	Local windows groups, domain controller groups, groups configured in SCADA application	Smart contract
Audit logs	Audit trail database	Blockchain
Source of device (PLC) commands and setpoints	Commands and setpoints/Parameters are sent from the SCADA/HMI application to the PLC	The PLC device queries the blockchain for commands and new setpoints/Parameters
Required permissions on PLC device	Read/Write	Read only

3.2. Improvements

In addition to improvements in terms of scalability and secure audit logs already demonstrated by researchers in the related work section, PLCBlox by itself offers advantages in the following areas:

3.2.1. Security Improvements on the PLC Device

PLCBlox does not require write access to the PLC device. The PLC device initiates updates of command statuses and setpoints during the blockchain node's querying operation. It is therefore possible to completely disable write access at the device level. This fact alone leads to a smaller attack surface, rendering many known and zero-day attacks and unusable [3, 14].

3.2.2. Security Improvements at the Application Layer (SCADA/HMI)

An attack on the device hosting the user application could circumvent the user authentication and authorization checks, allowing anyone to control the end device. Even further, a malicious threat actor could use the compromised operating system as an attack vector, bypass the SCADA software entirely, and use vendor-specific libraries to communicate with the end device directly, as in the case of the Stuxnet worm [3]. Because PLCBlox disables write access, the SCADA/HMI application cannot directly control the PLC. Any compromise of its software components would not affect the behavior of the PLC. Moreover, the authentication and authorization tasks are now coordinated by the blockchain network, which is an inherently more secure platform.

3.2.3. Audit Trail Enforcement

A compromised or malfunctioning SCADA system could be altered in such a way that all components are functional except the audit trail logging aspects. In such a scenario, a malicious user (e.g., rogue employee) would be able to execute commands and alter setpoints without his actions being recorded. Any attempt to bypass the audit trail would prove meaningless with PLCBlox, as it is the only source for command and setpoint updates.

4. Prototype Implementation

PLC devices are considered unsuitable for performing higher-level tasks such as blockchain transactions due to their limited resources. Their work memory (equivalent to Random Access Memory in computers) ranges from a few Kbytes to 32Mbytes for very large systems, and code storage is usually also limited. The process of querying a blockchain node does not have high computational requirements, such as those associated with the creation of signed transactions. Instead, predefined Application Programming Interface (API) calls are used, such as those in the form ofJavaScriptObject Notation Remote Procedure Calls (JSON-RPC) documented for the Ethereum network[1]. Due to the resource limitations of PLC devices, a prototype implementation was necessary to first verify the feasibility of the solution, record real-world performance indicators, and provide the basis for further development.

The complete design of PLCBlox solution consists of four elements, namely, the PLC application, an Ethereum private blockchain network, a smart contract, and an Ethereum-compatible wallet. A complete list of hardware and software tools used for the development and execution of PLCBlox implementation is summarized in the following Table 2.

Table 2.
List of hardware and software tools.

Component	Tools
Development of PLC demo application and reference blockchain node client	Siemens TIA portal V18 - integrated development environment (IDE) for Siemens PLC devices
PLC device	Siemens S7-1511-1PN
HMI device for acquiring results	HMI TP900 comfort panel (Simulated HMI panel)
Blockchain network	Ganache private Ethereum blockchain environment
Authentication	MetamaskEthereum wallet
Ethereum smart contract	Remix IDE (Solidity programming language)

4.1. PLC Application

The PLC application code incorporates a newly created library for interfacing with the Ethereum node. It also incorporates a demo application, which serves as an illustrative example of streamlined industrial process, and supplementary code for gathering performance indicators. The Ethereum interface library provides essential functions for executing Hypertext Transfer Protocol (HTTP) API requests and implements the Ethereum "eth_call" client-side JSON API.

The demo application assumes that the PLC device is in charge of a machine, necessitating one temperature setpoint and one command to configure the operation mode. Consequently, it is imperative to retrieve the following two variables from the smart contract:

- Operation Mode: This variable indicates the machine's intended operational state.
- Temperature: This variable represents the setpoint for the desired process temperature.

4.2. Smart Contract

The smart contract runs on the blockchain network and communicates with the PLC device through the blockchain node. It processes users' requests for updating process parameters, which are received in the form of transactions. It also needs to support the authentication and authorization functionality that would otherwise be handled by the SCADA device.

4.2.1. Authentication and Authorization

To showcase the authorization capabilities of PLCBlox, the smart contract incorporates distinct authorization levels outlined as follows:

[1] Ethereum JSON-RPC API - https://ethereum.org/en/developers/docs/apis/json-rpc/.

- *Administrator*: The user deploying the smart contract by default assumes this role. This user is able to assign other users to roles, but cannot modify any other variables.
- User: Users are restricted to modifying the machine's 'operationMode' variable exclusively.
- SuperUser: A super-user has the capability to alter both variables, namely 'operationMode' and 'Temperature'.

The smart contract employs three variables (admin, user, and superuser) to store the public addresses of users corresponding to their designated roles. Authentication relies on the inherent functionality of the blockchain network and the user's wallet. New requests reach the smart contract in the form of transactions that are signed with the user's wallet, utilizing the associated private key. The smart contract then verifies these transactions against known public keys, permitting functions to execute in accordance with the specified authorization level.

4.2.2. Functions

The smart contract provides the following functions to facilitate interaction with the PLC and enable user interactions:

- ChangeUser and ChangeSuperUser: These functions are invoked by the admin to assign user and super-user permissions, respectively. The function parameters pass the blockchain network address of a new user.
- SetTemperature: Super users utilize this function to modify temperature setpoints. The function parameter receives the new setpoint value.
- SwitchON and SwitchOFF: Users or superusers can call these functions to modify the desired operation mode.

4.3. Project Repository

In order to lay the groundwork for further research and development, all components of PLCBlox have been uploaded to GitHub[2], namely:

- Controller-side code includes open-source communication libraries, the newly developed Ethereum client-side RPC library, and the demo process application.
- Smart Contract source code (bloxtrail.sol).

5. Results

Developing the prototype implementation has been a vital phase of the research, serving as a testing ground to evaluate feasibility and performance and to record resources consumed.

The complete solution, has been successful in verifying the complete feature set shown in Table 1, namely user authentication, authorization, the usage of the blockchain network as an audit trail database, as well as the interface between a PLC device and an Ethereum node. Crucially, it showcases the ability to update a set of setpoints and commands without necessitating direct controller access.

As previously discussed, PLC devices have limited resources. The most important metrics are the size of the actual code as well as the size of work memory. Work memory is the equivalent of RAM in computers but is a fraction of its size. The implementation specifically uses a controller with 300kb of work memory. Although the source code storage can be extended by means of an SD card, the work memory cannot. The prototype implementation, including all necessary libraries, consumes 260kb of storage, as well as 14,5kb of work memory (5% of available).

Regarding the performance and in order for the results to better reflect real-world conditions, the CPU and blockchain network (Ganache) were located in separate locations and were connected through the internet across a link with a moderate network latency of 12ms. Additionally, the Ethereum node calls were configured to run in a loop, so as soon as one call finishes, the next one starts immediately. Each call duration is measured by the CPU, and an HMI device was configured to display the results. An example of 100 measurement points is shown in Figure 3. The calculation of each measurement point occurs after the completion of the Ethereum node call, reflecting its duration. In summary, each call was completed within a timeframe of 17-28ms with a mean value of 22ms. Subtracting the baseline network latency (12ms with no network load), we can attribute an average cycle duration of 10ms to CPU computation and delays in the Ethereum network protocol.

[2]PLCBlox GitHub repository - https://github.com/andshort/PLCBlox.

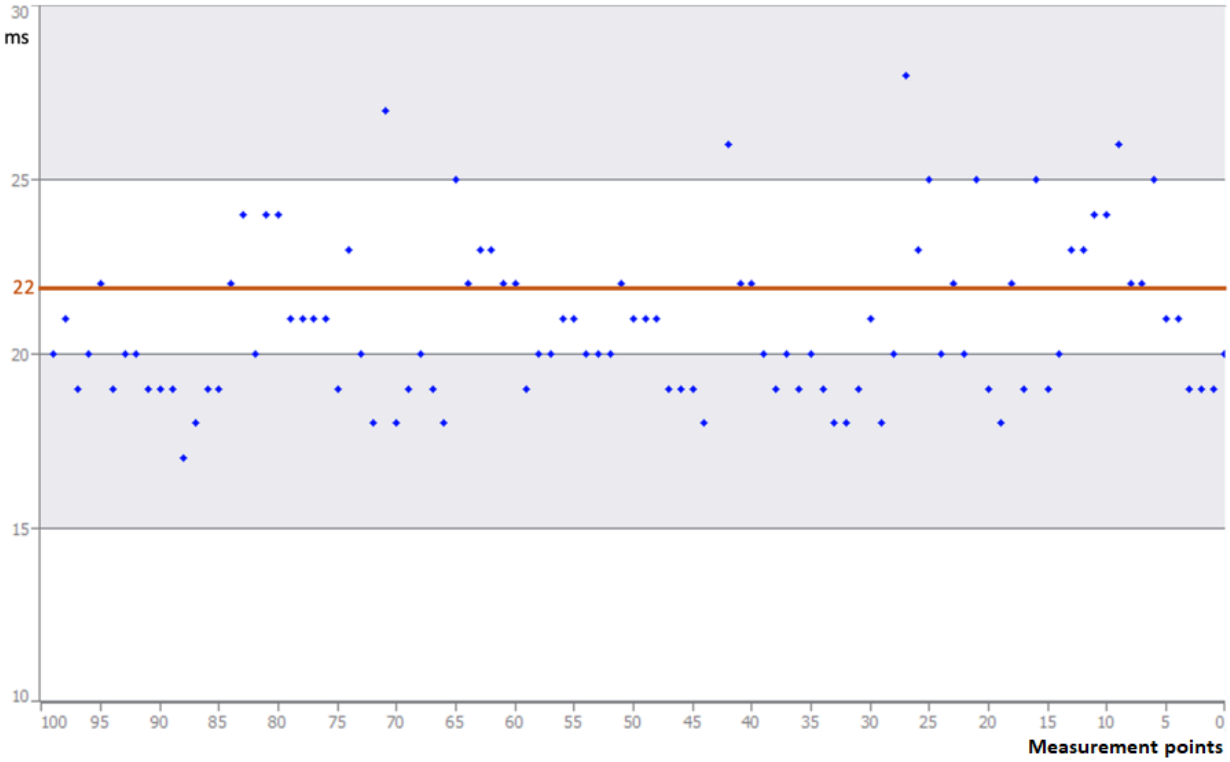

Figure 3.
Latency metrics over a period of 100 measurement points.

The resource utilization figures and performance indicators are summarized in Table 3. The list focuses primarily on the PLC device, as this would act as the bottleneck performance-wise.

Table 3.
Utilization figures and performance indicators.

Metric	Value
PLC code size on PLC device	260kb
Work memory (RAM)	14,5kb
Cycle duration (Request to response, end to end)	22ms
Throughput (Calculated)	45requests/Sec

6. Discussion

The innovative approach presented in this research has shown that modern PLC devices are able to interface with common blockchain nodes, opening new possibilities for added functionality and security improvements. Furthermore, it is demonstrated how PLCBlox can take advantage of the intrinsic tamperproof characteristics of an Ethereum network in order to facilitate the storage of audit trail records.

6.1. Security and Policy Enforcement (Audit Trail Logs)

Authentication and authorization tasks are now handled by the user's wallet and the smart contract, respectively. These two components, coupled with the underlying blockchain network operation, offer higher security standards, which have been proven by their use in the finance sector, especially when taking into account the security issues that exist in typical industrial deployments.

Furthermore, by requiring fewer access permissions on the PLC device (read only), it is impossible for an outside process to intentionally or unintentionally alter its data, effectively eliminating an attack surface that has been exploited over the years. Even further, due to the design, a compromised SCADA system would not be able to adversely impact the running process. Security requirements of these systems can therefore be relaxed.

The enforcement of the audit trail records, typically handled by the SCADA software on the end device, is now part of the system design. Moreover, there is no meaningful way to circumvent them, providing value to industries that require such policies.

6.2. Resource Overhead and Performance

It should be noted that the performance figures collected in the previous section reflect a mostly ideal setup due to the usage of a local Ethereum network node installation and the stable network connectivity. The authors argue that this setup more closely resembles typical deployments in industries that use on-premises audit trail database servers. Moreover, the small overhead delay imposed by the newly developed communication cycle should not be a concern for most industrial

applications. At the same time, PLCBlox's small PLC code footprint and RAM requirements leave most of its resources available for the operation of the main application.

6.3. Concerns when Running PLCBlox on a Pubilc Blockchain Network

We expect the solution to function on blockchain networks that share a similar RPC communications interface, such as the Ethereum Mainnet, but we must take into account the following factors: a) longer network delays attributed to both network latency as well as the fact that the blockchain node is simultaneously catering to a wider audience, b) reduced reliability due to the reliance on stable internet connectivity, c) costs incurred during the deployment of the smart contract and the creation of transactions (as would be the case when inserting audit trail entries) and d) privacy concerns arising from the fact that sensitive process information (process values, employee names or ids, justification of user actions) would be stored on a public medium. This research has not examined the use of PLCBlox in conjunction with public blockchain networks because it does not meet the requirements of most industrial use cases.

References

[1] U.S. Department of Health and Human Services Food and Drug Administration, "Part 11, electronic rec-ords; electronic signatures — scope and application," guidance for industry," Retrieved: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application. [Accessed 11-26-2023], 2023.

[2] U.S. Food & Drug Administration, "Computerized systems used in clinical trials," guidance for industry," Retrieved: https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/fda-bioresearch-monitoring-information/guidance-industry-computerized-systems-used-clinical-trials. [Accessed 11-26-2023], 2023.

[3] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy Magazine*, vol. 9, no. 3, pp. 49–51, 2011. https://doi.org/10.1109/MSP.2011.67

[4] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on SCADA systems: Secure protocols, incidents, threats and tactics," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1942–1976, 2020. https://doi.org/10.1109/COMST.2020.2987688

[5] A. Ahmad, M. Saad, M. Al Ghamdi, D. H. Nyang, and D. Mohaisen, "BlockTrail: A service for secure and transparent blockchain-driven audit trails," *In IEEE Systems Journal, Institute of Electrical and Electronics Engineers Inc*, pp. 1367–1378, 2022. https://doi.org/10.1109/JSYST.2021.3097744

[6] A. Ahmad, M. Saad, M. Bassiouni, and A. Mohaisen, "Towards blockchain-driven, secure and transparent audit logs," in *In Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, New York, NY, USA: ACM*, 2018, pp. 443–448.

[7] C. Regueiro, I. Seco, I. Gutiérrez-Agüero, B. Urquizu, and J. Mansell, "A blockchain-based audit trail mechanism: Design and implementation," *Algorithms*, vol. 14, no. 12, p. 341, 2021. https://doi.org/10.3390/a14120341

[8] S. Suzuki and J. Murai, "Blockchain as an audit-able communication channel," in *In Proceedings -Interna-tional Computer Software and Applications Conference, IEEE Computer Society*, 2017, pp. 516–522.

[9] W. Pourmajidi and A. Miranskyy, "Logchain: Blockchain-assisted log storage," presented at the In IEEE International Con-Ference on Cloud Computing, CLOUD, IEEE Computer Society, 2018.

[10] P. Snow, B. Deery, J. Lu, D. Johnston, and P. Kirby, "Factom: Business processes secured by immutable audit trails on the blockchain, Whitepaper, Factom, 2014," Retrieved: https://raw.githubusercontent.com/FactomProject/FactomDocs/master/Factom_Whitepaper.pdf. [Accessed 11-26-2023], 2014.

[11] P. Schmid, A. Schaffhäuser, and R. Kashef, "IoTBChain: Adopting blockchain technology to increase PLC resilience in an IoT environment," *Information*, vol. 14, no. 8, p. 437, 2023. https://doi.org/10.3390/info14080437

[12] A. Vick, W. Chen, and J. Krueger, "Using solana blockchain and OPC UA for trusted third party industrial robot control services," in *ISR Europe 2023; 56th International Symposium on Robotics*, 2023, pp. 332-337.

[13] S. Loss, L. Cardoso, N. Cacho, and F. Lopes, "Pharmaceutical audit trail blockchain-based microservice," in *In Proceedings of the 16th International Joint Conference on Biomedical Engineering Systems and Technologies, SCITEPRESS - Science and Technology Publications, Mar.*, 2023, pp. 368–375.

[14] X. Pan, Z. Wang, and Y. Sun, "Review of PLC security issues in industrial control system," *Journal of Cyber Security*, vol. 2, no. 2, pp. 69–83, 2020. https://doi.org/10.32604/jcs.2020.010045