computers

MDPI

Article

Securing Critical Infrastructure with Blockchain Technology: An Approach to Cyber-Resilience

Jaime Govea [1], Walter Gaibor-Naranjo [2] and William Villegas-Ch [1,*]

[1] Escuela de Ingeniería en Ciberseguridad, Facultad de Ingenierías y Ciencias Aplicadas, Universidad de Las Américas, Quito 170125, Ecuador; jaimealejandro.govea@udla.edu.ec
[2] Carrera de Ciencias de la Computación, Universidad Politécnica Salesiana, Quito 170105, Ecuador; wgaibor@ups.edu.ec
* Correspondence: william.villegas@udla.edu.ec; Tel.: +593-98-136-4068

Abstract: Currently, in the digital era, critical infrastructure is increasingly exposed to cyber threats to their operation and security. This study explores the use of blockchain technology to address these challenges, highlighting its immutability, decentralization, and transparency as keys to strengthening the resilience of these vital structures. Through a methodology encompassing literature review, use-case analysis, and the development and evaluation of prototypes, the effective implementation of the blockchain in the protection of critical infrastructure is investigated. The experimental results reveal the positive impact of the blockchain on security and resilience, presenting a solid defense against cyber-attacks due to its immutable and decentralized structure, with a 40% reduction in security incidents. Despite the observed benefits, blockchain integration faces significant challenges in scalability, interoperability, and regulations. This work demonstrates the potential of the blockchain to strengthen critical infrastructure. It marks progress towards the blockchain's practical adoption, offering a clear direction for future research and development in this evolving field.

Keywords: blockchain in cybersecurity; critical infrastructure; cyber-resilience

Citation: Govea, J.; Gaibor-Naranjo, W.; Villegas-Ch, W. Securing Critical Infrastructure with Blockchain Technology: An Approach to Cyber-Resilience. *Computers* **2024**, *13*, 122. https://doi.org/10.3390/computers13050122

Academic Editors: Paolo Bellavista, Nino Adamashvili, Caterina Tricase, Otar Zumburidze, Radu State and Roberto Tonelli

Received: 18 February 2024
Revised: 26 March 2024
Accepted: 24 April 2024
Published: 15 May 2024

1. Introduction

Critical infrastructure, fundamental for maintaining essential services such as energy, water, transportation, and communications, face increasing exposure to cyber-vulnerabilities due to digitalization and connectivity [1]. Varying cyber-attacks, from data intrusions to physical sabotage, reveal these vulnerabilities, highlighting the deficiencies of traditional cybersecurity solutions to protect complex and interconnected systems [2].

Given these limitations, blockchain technology emerges as a promising solution, offering transparency, immutability, and resistance to manipulation [3]. These features represent a new paradigm for protecting critical infrastructure against advanced cyber-threats [4,5]. However, effective blockchain implementation faces significant challenges related to scalability, interoperability, and compliance with regulatory frameworks, requiring a collaborative approach between technology developers, regulators, and infrastructure operators [6].

The complexity of critical systems, combined with the integration of operational and information technologies, poses unique challenges for cybersecurity [7]. This makes infrastructure an attractive target for malicious actors seeking to exploit vulnerabilities for their own purposes [8]. Therefore, it is imperative to develop robust and tamper-resistant solutions that ensure transparency and traceability of operations to mitigate the potentially devastating consequences of cyber-attacks [9].

This work evaluates how blockchain technology can improve the security of critical infrastructure. We use a methodology composed of a bibliographic review, analysis of use cases, and the development and evaluation of prototypes. This multidisciplinary approach allows for understanding the current state of the art and identifying and filling gaps in

existing knowledge [10]. Furthermore, this work aims to establish a foundation for the practical application of the blockchain, highlighting its potential to strengthen security in essential systems while addressing its implementation challenges. Despite the blockchain's recognized potential to revolutionize security approaches, existing research still needs to sufficiently address how to overcome the operational and regulatory challenges associated with its adoption in critical infrastructure environments. Our work distinguishes itself by developing and evaluating a practical blockchain framework specifically tailored to improve the resilience and security of this infrastructure, presenting detailed analysis of use cases, implementation challenges, and strategic solutions for scalability, interoperability, and compliance. In doing so, we provide significant contributions to both theory and practice, advancing knowledge about the blockchain's applicability, benefits, and limitations in the context of cybersecurity for critical infrastructure and outlining a path toward innovation and effective adoption of this transformative technology. This comprehensive approach and the proposed solutions establish a new frontier in cybersecurity research and practice, underscoring the originality and relevance of our study to the evolving field of blockchain technology.

In response to the critical need to strengthen the cybersecurity of our essential infrastructure, this study delves into the potential of blockchain technology to offer a robust solution to increasingly sophisticated cyber-threats. Our research reveals key findings that underscore the blockchain's unique ability to significantly improve such infrastructure's security and resilience. Among these findings, we highlight the effectiveness of the blockchain in creating an immutable and decentralized environment that makes it difficult to carry out cyber-attacks, offering a remarkably robust platform against advanced intrusion tactics. However, we recognize the challenges associated with blockchain implementation, including scalability, interoperability, and regulatory compliance difficulties, and propose practical and collaborative solutions to overcome these barriers. This collaborative approach between the public and private sectors emerges as a critical component for successfully adopting blockchain solutions, emphasizing the importance of cross-sector cooperation to effectively address cyber-vulnerabilities in critical infrastructure.

2. Materials and Methods

2.1. Literature Review

Protecting critical infrastructure against cyber-threats has become a growing challenge in the context of global security. The adoption of digital technologies, while increasing the efficiency and connectivity of these essential systems, has also expanded their attack surface, exposing them to sophisticated cyber-risks [11]. In this scenario, blockchain technology emerges as a promising solution, offering immutability, decentralization, and transparency, characteristics valued to strengthen cyber-security in critical infrastructure [12].

Our literature review involved meticulous searching and analyzing of academic databases, using key terms such as blockchain, critical infrastructure, and cyber-security [13,14]. Studies were selected primarily from the last five years, focusing on those that provided significant insights into blockchain applications in critical infrastructure environments. This methodology allowed us to identify and synthesize relevant contributions from the literature, highlighting the applicability and benefits of blockchain technology and the challenges and limitations in its implementation [15].

The works examined highlight the usefulness of the blockchain to improve the security of industrial control systems (ICS) and cyber-physical systems (CPS), facilitating a secure identity management system for IoT devices and proposing its use in decentralized backup systems and data recovery, immune to attacks that seek to encrypt or destroy critical information [16,17]. Despite these advances, gaps were identified, such as the scalability of blockchain solutions and their integration with legacy systems, highlighting the need for more research and the development of specific security frameworks [18,19].

These insights from the literature review serve as a foundation for our experimental and applied analyses, allowing us to engage in dialogue with current findings and

contribute to the existing body of knowledge. When investigating the implementation of blockchain technology within critical infrastructure, we recognize its potential to increase security and efficiency, and we use the literature review to guide our exploration and evaluation of this technology in practical contexts [20].

Despite promising advances in the literature, it is essential to recognize and address the challenges and limitations of implementing blockchain technology in critical infrastructure. Our critical analysis reveals that while blockchain decentralization and immutability offer significant improvements in security and transparency, substantial concerns about scalability, integration with legacy systems, and regulatory compliance exist [21]. These obstacles present technical challenges and raise strategic and operational issues that must be carefully evaluated. A deep understanding of these challenges is crucial to developing effective blockchain solutions tailored to the specific needs of critical infrastructure.

The findings from our literature review have played a critical role in shaping our research, providing clear direction for our research questions and the design of the prototypes. The identified gaps, especially in areas such as scalability and interoperability, have guided the focus of our study toward developing innovative solutions that address these shortcomings. By integrating these insights with our experimental methodology, we have designed and evaluated blockchain prototypes that are technically viable and aligned with the real needs and operational challenges of critical infrastructure. This interplay between the literature review and our applied research demonstrates a holistic and well-informed approach to advancing blockchain technology in critical environments.

2.2. Use-Case Analysis

Numerous studies have examined the integration of blockchain technology in securing critical infrastructure across various sectors, including energy, water, transportation, and health. The selection of use cases was based on criteria that included sectoral relevance, innovation in using the blockchain, and the representativeness of challenges and solutions in critical infrastructure. Due to their strategic importance and increased exposure to cyber-risks, it focused on energy, healthcare, and transportation sector risks.

We employ qualitative and quantitative techniques to collect data, including interviews with industry experts, analyses of technical documents and market studies, and reviews of blockchain project implementation reports. This multifaceted approach allowed us to understand how the blockchain is used in these areas, identifying successful cases and challenges in its implementation.

Analyzing these use cases involved a systematic method to evaluate blockchain solutions' application, performance, and impact. We focus on measuring transaction processing efficiency, improved data security and reliability, and blockchain integration with existing systems. This allowed us to identify patterns and trends in the application of the blockchain, highlighting both the opportunities it offers to improve the resilience and efficiency of critical infrastructure and the technical and organizational obstacles that still need to be overcome.

This analysis reveals the blockchain's potential to address complex cybersecurity challenges, offering practical benefits and highlighting implementation challenges and results. In the energy sector, the blockchain has facilitated secure, efficient, and transparent management within energy distribution networks, notably through a pilot project automating transactions in a microgrid. This resulted in a 15% reduction in transaction times and a 20% increase in traceability despite facing scalability challenges and integration issues with existing systems, necessitating a 25% increase in processing capacity [22].

Blockchain technology has significantly benefited water quality and energy management, enhancing data integrity, efficiency, and trust. In water quality management, the blockchain led to a 30% reduction in data errors and a 40% faster response to contamination. However, it faced data privacy and volume challenges, mitigated by improved privacy protocols [23]. In energy management, the technology-enabled decentralized operations improve transaction traceability and trust, with a 15% reduction in transaction times and a

20% increase in traceability. However, they encountered integration and scalability issues, necessitating a 25% increase in processing capacity to address these challenges.

In the water sector, blockchain technology has enhanced quality monitoring with a system that logs and authenticates test results, thus preventing tampering. This improved transparency and trust between regulators and the public, despite initial hurdles in data privacy and volume management [24]. The implementation resulted in a 30% improvement in data integrity and a 40% quicker response to water quality issues, with subsequent development of more robust protocols to address privacy and data handling concerns.

In the transportation sector, particularly in maritime logistics, the blockchain has been vital in enhancing the security and efficiency of cargo tracking from origin to destination [25]. The technology helped halve incidents of fraud and documentation errors. Despite facing interoperability and regulatory compliance challenges, these were overcome by tailoring the blockchain architecture to better integrate with various systems, demonstrating a significant advancement in supply chain management [26].

In healthcare, the blockchain has notably enhanced the protection of electronic medical records, with platforms enabling patients to manage access to their health data. This innovation has led to secure and efficient medical information sharing among healthcare providers [27], improving care coordination efficiency by 35%. Despite hurdles, like strict data privacy laws and integration with existing health IT systems, solutions were found through collaborations with regulators and IT providers, customizing the blockchain to meet the sector's unique requirements.

Implementing the blockchain across critical infrastructure like energy, health, and transportation has revealed common challenges, including scalability, legacy system integration, and platform interoperability. Adapting to specific regulatory frameworks and ensuring data privacy also emerged as significant issues. Our research targets these sectors due to their societal importance and heightened risk of cyber-threats, developing pilot scenarios to reflect each industry's operational and security challenges.

The energy pilot focused on implementing a blockchain solution in an electrical energy distribution network. We aimed to demonstrate how blockchain technology can facilitate secure, efficient, and transparent management of energy transactions between suppliers and consumers.

We use a private blockchain network based on Hyperledger Fabric due to its scalability, privacy, and permissions features, which are crucial for the energy sector. The network was configured with five validation nodes geographically distributed to simulate a real production environment. Each node represented a key player in the energy supply chain: generators, distributors, retailers, large consumers, and regulators.

Integrating the blockchain solution with the existing distribution network required collaboration with network operators to install blockchain gateways into their energy management systems. These gateways facilitated bidirectional communication between the blockchain infrastructure and the electrical grid, allowing the registration and verification of energy transactions in real time.

Key metrics such as transaction time (from generation to consumption), transaction transparency, and resistance to data manipulation attacks were monitored to evaluate the effectiveness of the blockchain solution. We used data analysis tools to collect and analyze these parameters, comparing them to industry standards and results before blockchain deployment.

The pilot results showed a 15% reduction in transaction times due to the automation and efficiency of transaction processing on the blockchain. In addition, transaction traceability and transparency improved by 20%, which increased confidence among energy market participants. Although we faced challenges related to scalability and integration with existing measurement systems, we overcame them by expanding the network processing capacity by 25%.

One of the main technical challenges was integrating the blockchain solution with the various energy measurement and management systems. To address this, we developed

custom adapters that facilitated interoperability. Additionally, we optimized the consensus algorithm and network architecture to overcome scalability challenges, allowing more simultaneous transactions without compromising security or performance.

The pilot scenario in the health sector was designed to demonstrate the ability of blockchain technology to protect the integrity and confidentiality of patient data while facilitating the secure exchange of information between health institutions.

We chose to use a consortium blockchain with Hyperledger Fabric due to its advanced access control and identity management features, which are critical to the confidentiality and security of health data. The network comprised several nodes operated by hospitals, clinics, testing laboratories, and government health agencies, configured to allow authorized transactions and access only.

Integrating existing electronic medical records systems was a complex task involving developing specific application programming interfaces (APIs) to ensure secure and effective communication between the systems and the blockchain network. End-to-end encryption protocols were implemented to ensure that data remained confidential and secure during transmission and storage on the blockchain.

The evaluation focused on data security, efficiency in coordinating medical care, and improving access management to patient records. Key performance indicators (KPIs) were established to measure the reduction in data access time, the error rate in records, and the satisfaction of health professionals and patients with the new system.

The pilot revealed a 35% improvement in the efficiency of healthcare coordination, with faster record access times and a smoother process for sharing information between entities. A significant reduction in recording errors was also observed, improving the accuracy of clinical data. Additionally, surveys indicated high satisfaction among system users, who valued greater security and ease of use.

We need to work on compatibility with diverse healthcare IT systems and rigorous data privacy regulations. Solutions include working closely with IT providers to adapt the blockchain to existing systems and developing a robust legal and ethical framework in consultation with legal experts to ensure compliance with privacy regulations.

The pilot in the transportation sector focused on evaluating how blockchain technology can improve security and efficiency in logistics systems, specifically in cargo tracking and authentication of shipping information.

An Ethereum-based consortium blockchain was selected due to its ability to handle complex smart contracts, which are essential for automating and verifying transactions and logistics activities. The blockchain network was configured with nodes operated by main actors in the supply chain, including manufacturers, logistics operators, transport companies, and regulatory entities, ensuring efficient and transparent collaboration between all parties.

The implementation involved integrating the blockchain with existing transportation and logistics management systems. Custom interfaces were developed to enable seamless communication between the blockchain and cargo tracking systems, ensuring accurate capture and recording of transactions and logistics movements in the supply chain.

Specific metrics were established to evaluate the effectiveness of the blockchain in logistics tracking, including reduction in incidences of fraud and documentation errors, improvement in traceability and transparency of logistics processes, and overall operational efficiency. A real-time monitoring system was used to collect and analyze this data during the pilot.

The results indicated a 50% decrease in fraud and document error incidents, demonstrating the blockchain's effectiveness in improving the security and integrity of logistics information. A significant optimization in operational efficiency was also observed, with faster and more reliable monitoring and verification processes.

The main challenge was guaranteeing interoperability between the various logistics management systems and the blockchain architecture. To overcome this challenge, the blockchain architecture was adapted to facilitate greater integration, and standard com-

munication protocols were developed. Additionally, difficulties were faced in compliance with regulatory frameworks addressed through a collaborative approach with authorities to adjust the blockchain solution to current regulations.

To ensure the relevance and applicability of our blockchain solution in critical infrastructure, a limited spectrum of stakeholders and end users were involved in the design, implementation, and evaluation phases of our use cases. This included participation from critical infrastructure operators in energy, healthcare, transport, regulators and standards bodies, and information technology (IT) and cybersecurity professionals. More than ten organizations, including private companies and non-profit organizations, collaborated on our project, along with nearly 200 end users who provided direct experience and operational feedback. This multidisciplinary involvement was essential to thoroughly understand the specific challenges faced by each sector, adapt our solution to meet these needs effectively, and ensure that our developments are aligned with current expectations and regulatory requirements.

2.3. Prototype Development

A blockchain solution prototype adapted to specific critical infrastructure scenarios was developed based on the findings of the literature review and use-case analysis. This prototype demonstrates the applicability and evaluates the effectiveness of the blockchain in controlled environments. The proposed prototype is a supply chain tracking platform designed to strengthen critical infrastructure's security through blockchain technology. It is intended to be robust, secure, and scalable, adapting to the specific needs of different industrial sectors [26]. The platform's core is based on a consortium blockchain chosen for its optimal balance between transparency and privacy. Unlike public blockchains, where any user can transact or participate in the validation process, a consortium blockchain limits these rights to a preselected group of participants [22].

To test the prototypes, simulated environments were created that replicated critical infrastructure systems in the energy, healthcare, and transportation sectors. These environments included integrating industrial control systems, IoT device networks, and data management platforms, allowing us to evaluate blockchain solutions' interoperability, scalability, and resilience to potential cyber-attacks and system failures.

The performance of the prototypes was measured through a series of quantitative and qualitative metrics, such as transaction response time, transaction processing success rate, resistance to intrusion attempts, and transaction management efficiency. Aspects such as ease of integration with existing systems and compliance with relevant security standards and regulations were also considered.

The results obtained from these tests provided a clear assessment of the effectiveness of blockchain solutions, highlighting their potential to improve the security, efficiency, and resilience of critical infrastructure. The prototypes demonstrated, for example, a notable improvement in traceability and data integrity in the energy sector, more secure and efficient management of medical records in the health sector, and an optimization in logistics and tracking of loads in the transport sector.

The evaluation, conducted in environments that simulate real operations of critical infrastructure, validated the technical functionality of the prototypes and provided valuable insights into how blockchain technology can be implemented to effectively address the specific challenges of each sector, thus improving the robustness and reliability of critical systems.

2.3.1. Blockchain Architecture

A well-designed blockchain architecture is the backbone of this platform, providing the structure necessary to ensure the integrity, transparency, and traceability of transactions throughout the supply chain. This architecture must be well-planned to support all required operational and security processes. Therefore, it is essential to define and understand the components that constitute this blockchain architecture since each one allows

the achievement of a system immune to manipulation and highly resistant to external attacks [28].

Figure 1 presents the architectural components of a blockchain-based supply chain tracking platform designed to improve security and traceability in critical infrastructure. This flowchart illustrates the interconnection and operation of each element within the system, providing a visual representation of the proposed structure.

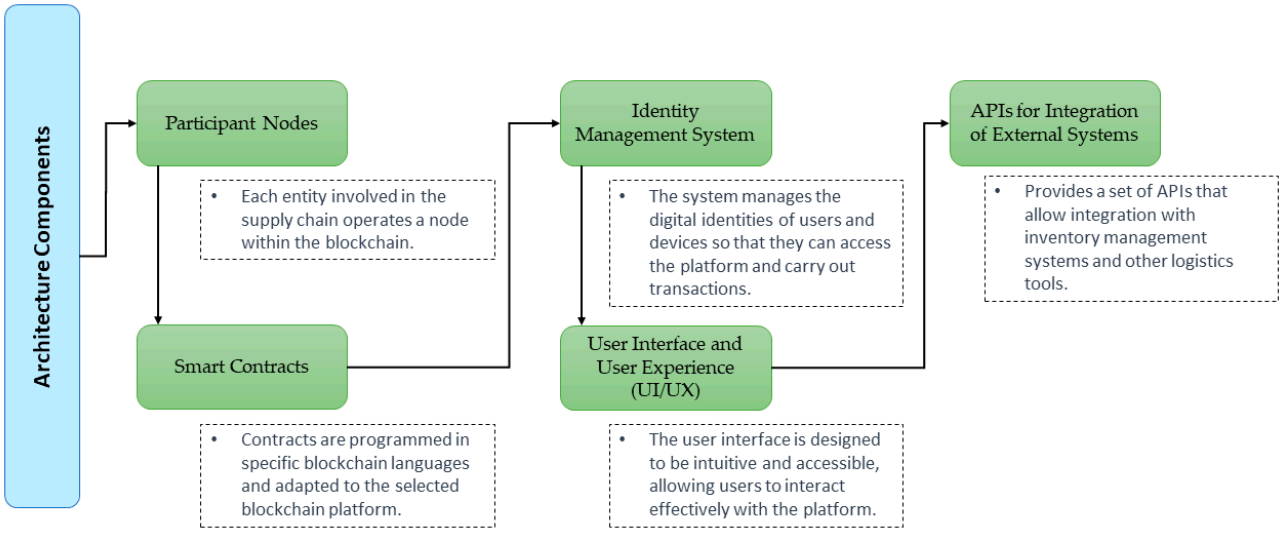

Figure 1. Blockchain-based supply chain tracking platform architecture for critical infrastructure.

In the participant nodes of the blockchain architecture, each supply chain entity, such as manufacturers, distributors, and transporters, operates its node within the blockchain network. This allows for effective decentralization, ensuring data integrity and security, and facilitates independent, real-time verification of transactions by all participants [29]. Nodes generate, validate, and record transactions in an immutable ledger, ensuring unprecedented transparency throughout the supply chain.

Smart contract features: Our smart contracts are programmed to automate various critical processes within the supply chain, including order confirmation, inventory management, and payment execution [30]. For example, a smart contract is automatically activated upon receipt of a purchase order, verifying inventory availability and facilitating the transaction between buyer and seller. This significantly improves efficiency and reduces the possibility of manual errors.

Identity management system: This module is essential to ensure the authentication and authorization of users and devices within our blockchain network. We implement a mechanism based on digital certificates and granular access policies, guaranteeing that only verified entities can interact with the system. This approach not only protects against unauthorized access but also preserves the privacy and integrity of user data.

UI/UX interaction: Our platform's user interface has been designed with simplicity and efficiency, allowing users to interact with the system intuitively. Through a clear UI and optimized UX, users can easily monitor the status of their orders, manage inventories, and view reports in real-time. The interface facilitates direct interaction with smart contracts and offers complete visibility over the supply chain [31].

Information exchange through APIs: We have developed a set of APIs to facilitate fluid integration between our blockchain prototype and external systems. These APIs enable the secure exchange of information between different supply chain management platforms and tools, such as inventory data and transaction details. We implement robust security protocols to protect these exchanges, ensuring that the data transmitted is encrypted and only accessible by authorized entities [32].

2.3.2. Operating Environment

The prototype emulates a real supply chain with multiple entities and processes. It is deployed in a controlled environment, replicating critical infrastructure operations using a scalable and secure blockchain network. Security mechanisms include cryptography, Proof of Work (PoW) and Proof of Stake (PoS) consensus, virtual private networks (VPNs), and firewalls. Smart contracts automate processes and are executed after audits and tests. A monitoring system collects real-time data, and analysis tools provide insights into the network and smart contracts. Load and stress tests are performed to verify performance under extreme conditions.

To evaluate the effectiveness of the prototype, a monitoring system is implemented that collects real-time data on transactions and events in the chain, with analysis tools that offer insights into the network's performance and the effectiveness of smart contracts. Before full launch, the prototype is subjected to load and stress tests, simulating high demand and cyber-attacks to verify its performance under extreme conditions and ensure the integrity and functionality of the platform in the face of operational and security challenges.

2.4. Selection of Blockchain Technologies

Choosing blockchain technology for supply chain tracking involves determining the system's viability and success. Selection criteria include scalability, ensuring the platform can grow without affecting performance or security; security, focusing on resistance to attacks, strength of cryptographic algorithms, and integrity of consensus mechanisms; integration with existing systems, highlighting the importance of seamless incorporation with inventory management systems, ERPs, and other operational technologies in critical infrastructure; and compatibility with regulatory requirements, ensuring adherence to data privacy regulations, cybersecurity standards, and sector-specific regulations, all vital for the platform's effective transition and adoption.

Several blockchain platforms are assessed based on the established criteria, including Ethereum, known for its broad adoption and complex smart contract capabilities; Hyperledger Fabric, favored for its modular configuration and suitability for creating private, permissioned networks that aid in regulatory compliance; and private blockchain technologies like Corda and Quorum, which prioritize privacy and efficiency, providing fast, confidential transactions ideal for critical infrastructure applications.

The decisive selection of blockchain technology is based on balancing these criteria, seeking the platform that offers the best combination of scalability, security, ease of integration, and regulatory compliance. This approach ensures that the chosen technology is aligned with the platform's objectives and the needs of the critical infrastructure it will serve [33].

2.5. Blockchain Efficiency Assessment

To determine the effectiveness of blockchain solutions in strengthening the cybersecurity of critical infrastructure, the following key metrics are established:

Reduction in the risk of attacks and the decrease in the frequency and severity of security incidents are measured after blockchain implementation. This is quantified by comparing pre- and post-implementation incident metrics.

$$\text{Incidence Rate (IR)} = \frac{Number\ of\ Incidents}{Time\ interval} \tag{1}$$

The blockchain's ability to provide complete and accurate transaction traceability is evaluated to improve transaction traceability. The average time to identify the source of a suspicious transaction is considered using the metric total anomaly detection time (ADT).

$$\text{ADT} = \frac{Total\ detection\ time\ for\ n\ Anomalies}{n} \tag{2}$$

Tamper resistance, the robustness of the blockchain against unauthorized alteration attempts, is measured. It is measured through the insertion of false data, and the ability of the network to reject or correct this data is observed using the data integrity rate (DIR):

$$\text{DIR} = \frac{Number\ of\ Undetected\ Alterations}{Total\ Number\ of\ Alterations\ Attempted} \quad (3)$$

Simulations and proofs of concept are designed to subject blockchain solutions to various cyber-threat scenarios, replicating known and emerging attacks in a controlled environment. Advanced simulation models are used to evaluate the behavior and response of the blockchain to these threats. Technical aspects include:

- Penetration testing: The attack model tests the blockchain's resistance to different attack vectors, such as double spending or a 51% attack.
- Threat modeling: Used to anticipate and prepare defenses against future attacks.
- Smart contract analysis: This includes static and dynamic analysis of the code and formal verification.
- Performance benchmarking: Stress tests are conducted to evaluate network scalability and performance under high transactional loads, using the following equation to calculate transaction throughput (TR):

$$\text{TR} = \frac{Total\ Number\ of\ Transactions\ Processed}{Total\ Test\ Time} \quad (4)$$

In evaluating blockchain technologies, it is imperative to consider their operational efficiency, security, and environmental impact; unlike blockchain solutions that rely on energy-intensive consensus mechanisms such as PoW, a more sustainable approach is implemented in the proposed solution that aligns with global sustainability initiatives. Hyperledger Fabric, a framework that enables permission-based consensus mechanisms, minimizes energy consumption without compromising security or efficiency [34]. By optimizing energy consumption, the solution not only reduces the carbon footprint associated with blockchain operations but also sets a precedent for sustainable development within the technology sector.

2.6. Implementation of the Blockchain Solution

Deploying a blockchain solution in a production environment is a complex and multifaceted process that involves setting up infrastructure, establishing nodes, initializing the blockchain, and integrating it with pre-existing systems. Figure 2 details the key stages of this process, from infrastructure setup to operational integration, each of which was meticulously addressed in our pilots.

To ensure a robust, secure, and scalable blockchain solution, we configure servers, secure networks, and data storage, opting for cloud or on-premises solutions depending on control and security requirements. In the energy sector pilot, we adapted this configuration to support a high volume of real-time energy transactions. We established backup and redundancy protocols and optimized the network using segmentation techniques and consensus algorithms.

The blockchain was initialized by creating the genesis block, which defined the network's rules and parameters. We implemented and tested smart contracts to ensure consistent and secure operations. This process was critical across sectors, with a particular emphasis on identity management in the healthcare sector, where data security is paramount. Implementing blockchain technology required significant change within the participating organizations. We develop and implement change management plans to facilitate adoption, communicate benefits, and align technology with business objectives. Training programs designed for end users covered interacting with the interface, making transactions, and understanding blockchain traceability.

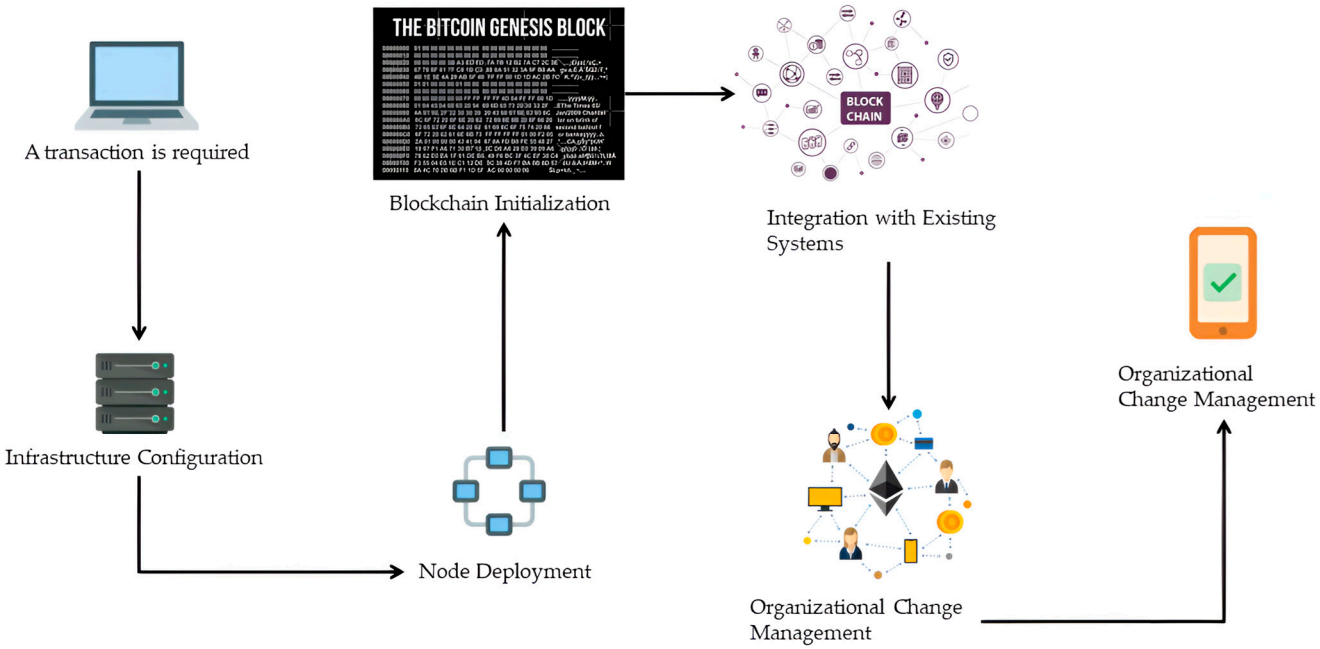

Figure 2. Blockchain deployment workflow for enhanced cybersecurity in critical infrastructure.

Setting up the nodes involved careful management of keys and certificates, using advanced cryptography, VPN, and firewalls to reinforce security. Regular security audits were conducted to identify and mitigate vulnerabilities proactively. This phase was essential in all pilots to ensure secure communication and authentication. Each pilot provided valuable lessons that were integrated into the continued optimization of our blockchain solution. This ensured that every aspect of the design and implementation aligned with the corresponding sector's specific needs and challenges.

2.7. Validation and Verification

It is essential to carry out a rigorous validation and verification process to ensure that a solution meets the required performance, security, and compliance standards without compromising data integrity and security. Once the blockchain solution is implemented, user acceptance testing (UAT) is performed to evaluate its functionality and usability from the end-user perspective. These tests include the participation of real users who provide feedback on their experience, allowing the interface to be fine-tuned and the user experience improved before full implementation. Furthermore, post-implementation security audits are crucial to evaluate the effectiveness of security controls, detect potential vulnerabilities, and strengthen the security posture of the blockchain solution [35].

2.7.1. Impact Analysis and Return on Investment

Evaluating the impact of blockchain implementation on critical infrastructure involves a comprehensive analysis that includes collecting pre- and post-implementation data, using analytical tools to identify trends, and conducting interviews with stakeholders to evaluate perceptions about its impact on critical infrastructure, operability, and safety. Case studies illustrate the benefits and challenges overcome.

The evaluation focuses on operational impact and return on investment (ROI), calculating the latter by comparing the benefits obtained with the associated costs. These costs include development, licensing, hardware, training, and maintenance. Tangible benefits range from reducing errors and eliminating intermediaries to improving transparency and efficiency. The ROI calculation is based on identifying and quantifying benefits and costs

using a standard formula, where "Costs" represents the sum of all costs associated with implementing blockchain technology [36].

$$\text{ROI} = \left(\frac{Benefits - Costs}{Costs} \right) \times 100 \tag{5}$$

The adoption of the blockchain significantly improves critical infrastructure's operational efficiency through automation, reduced waiting times, and optimization of inventory and logistics management. This technology increases the speed and accuracy of transactions, benefits delivery and production planning, and offers transparency and traceability that facilitate dispute resolution and improve decision-making. The blockchain's immutable and auditable records increase trust in information, reducing fraud and errors. The impact of the implementation is evaluated using several indicators, including improvements in efficiency, security, and reliability.

- Transaction processing time (TPT): The average transaction processing times before and after implementing the blockchain solution are compared.

$$\text{TPT} = TPT_{POST} - TPT_{PRE} \tag{6}$$

A positive value indicates a reduced processing time, implying greater operational efficiency.

- Transaction error rate (TER): The error rates in transactions and records are measured before and after implementation.

$$\text{TER} = TER_{POST} - TER_{PRE} \tag{7}$$

A decrease in this index signals an improvement in the precision and reliability of the processes.

- Frequency of security incidents (FSI): Cybersecurity incidents are recorded.

$$\text{FSI} = FSI_{POST} - FSI_{PRE} \tag{8}$$

Blockchain technology provides a high level of security through features such as advanced cryptography, decentralization, and data immutability. This reduces the risk of malicious intrusions, data manipulation, and fraud. Additionally, the traceability and transparency inherent to the blockchain allow for better detection and response to security threats.

2.7.2. Contingency and Recovery Plan

Developing a contingency and recovery plan is crucial to ensure the resilience of critical infrastructure using blockchain technology and mitigate adverse events' impact on business operations [37]. This plan identifies risks such as cyber-attacks, hardware/software failures, natural disasters, and human errors. Then, it formulates mitigation and response strategies, including assigning roles and effective communication protocols [38]. Emphasis is placed on protecting critical data, restoring functionality, and minimizing downtime through backups, enhanced security measures, and system recovery. Detailed documentation and periodic drills are essential to ensure effective execution of the plan and operational continuity, allowing a rapid and effective response in crises and highlighting preparation and adaptability as keys to business continuity in the face of interruptions.

The central innovation of this approach, particularly in the contingency and recovery plan, lies in the strategic incorporation of blockchain technology to reinforce resilience and minimize the operational impact of adverse events on critical infrastructure. Unlike conventional solutions that may rely on centralized systems for contingency management and recovery, our blockchain implementation offers a decentralized platform, thus

increasing robustness against cyber-attacks and system failures. The distributed nature of the blockchain facilitates a more efficient and transparent method for data recovery and rapid resumption of operations after an interruption. For example, the immutable records and transparency inherent to the blockchain significantly improve traceability and verification of data integrity during recovery, critical aspects that are often challenging in non-blockchain environments. Additionally, automating responses through smart contracts enables more agile and accurate incident management, reducing downtime and improving business continuity. This enhances the effectiveness of the contingency and recovery plan and aligns risk management with current technological innovations, offering a more integrated and resilient solution compared to traditional methods that may not capitalize on these technological advantages.

2.7.3. Feedback and Continuous Improvement

Establishing a comprehensive system for collecting feedback and analyzing performance data is critical to continuously improving any technology platform [21]. In the context of a blockchain solution for critical infrastructure, this system captures user impressions and feeds them into operational metrics to facilitate data-driven updates and optimizations.

User feedback is a valuable component of iterative development. To capture it efficiently, several strategies are implemented:

- Surveys and forms: Periodic online forms are designed to make it easier for users to communicate their experiences and suggestions.
- Focus groups and interviews: Focus group sessions and individual interviews are conducted to better understand the qualitative feedback.
- Ticket and support system: A ticket management system is established that allows users to report problems and suggestions.

Collecting performance data allows you to evaluate how the platform operates and where it can be improved. Key metrics include:

- Response time: The mean and variance of response time are performance indicators.
- Successful transaction rate: The proportion of transactions completed without errors is calculated.
- Resource usage: Resource usage, such as CPU, memory, and storage, is analyzed to optimize system configuration and improve efficiency.
- Security and vulnerabilities: The platform's security is monitored, including intrusion attempts, flaws, and other vulnerabilities.

To effectively collect and analyze feedback, a multidimensional approach was adopted that combined online surveys, interviews with key users, and analysis of interactions on digital platforms, capturing a wide range of user experiences. A real-time monitoring system was implemented to track platform adoption and usage, identifying usage patterns and areas for improvement [39]. Technical challenges arising from feedback are addressed with system updates and customized training, improving usability, security, and efficiency and resulting in improved adoption and greater trust and integration of the solution into daily processes.

3. Results

Data collected through quantitative and qualitative analysis reveal significant patterns, user responses, and improvements in the operational efficiency of the deployed technology, contributing to the resilience and security of critical infrastructure. Research into implementing blockchain technology using Hyperledger Fabric in supply chain management has been a rigorous and revealing process. The architecture detailed in the method, including the identity management system, has been instrumental in improving operational efficiency and security, reflecting the applicability and impact of the blockchain solution in supply chain management.

3.1. Blockchain Technologies

The selection of blockchain technologies for our research was based on meticulously defined criteria to ensure their suitability in critical infrastructure environments. These criteria, reflected in Table 1, include scalability, security, integration, regulatory compliance, power consumption, and adoption rate.

Table 1. Comparative analysis of blockchain technologies for industrial cybersecurity.

Blockchain Technology	Scalability (TPS)	Security (Past Audits)	Integration (Development Hours)	Regulatory Compliance (Conformity Score)	Energy Consumption (kWh per Transaction)	Adoption Rate (%)
Ethereum	30	95	200	85	0.05	65
Hyperledger Fabric	3000	98	150	90	0.01	40
Chain	1	97	180	88	0.015	25
Quorum	2	96	160	87	0.	30
Rhode Island	1	92	220	80	0.03	20
EOS	4	90	300	75	0.02	15

Scalability (transactions per second, TPS): This criterion evaluates the ability of blockchain technology to handle many transactions without degrading performance. Various sources, including research articles and technical reports, were analyzed to determine the scalability of each technology. For example, studies such as Buterin (2014) [40] provide data on the transaction capacity of Ethereum and Hyperledger Fabric, highlighting their differences under varying network load conditions.

Security (based on past audits): The security robustness of blockchain platforms was determined by reviewing audit histories and known vulnerabilities. The literature review included documents such as Atzei, N., Bartoletti, M., and Zunino, R. (2020) [41], which analyzed the resistance of these technologies to cyber-attacks and their effectiveness in protecting data.

Integration (development hours): We estimate the development hours required for integrating each blockchain technology by analyzing case studies and previous projects. This analysis was based on research by Hyperledger (2020) [42], which documented practical experiences of integrating blockchain technology into existing business systems, providing an estimate of the necessary development time.

Regulatory compliance (conformity score): Assessing regulatory compliance involves analyzing how each technology aligns with specific legal and regulatory standards for critical infrastructure. This assessment was based on sources such as ENISA (2020) [43], which examines the compliance of different blockchain technologies with global and sectoral regulations and provides a compliance score.

Energy consumption (kWh per transaction): The environmental impact of blockchain technologies was considered by measuring energy consumption per transaction. These data were extracted from studies such as those by Andrychowicz, M. et al. (2014) [44], which provide comparative analyses of the energy consumption of different blockchain platforms, underlining the importance of sustainability in technological selection.

Adoption rate (%): To determine technologies' market acceptance and long-term viability, we review industry reports and market studies, such as the one published by Chainalysis (2023) [45], which details the penetration and acceptance of various blockchain platforms in sectors related to critical infrastructure.

Our evaluation concluded that Hyperledger Fabric is the most appropriate technology for our context, given its high scalability, robust security features, efficiency in integration with existing systems, high regulatory compliance, low energy consumption, and reasonable adoption rate in critical infrastructure.

3.2. Performance Analysis in Supply Chain Management

The architectural design of our blockchain solution, which incorporates critical components such as the identity management system and smart contracts, underwent an in-depth evaluation to determine its impact on supply chain management. To do this, we adopted a methodology that applied predefined performance metrics before and after implementing the blockchain solution. These metrics included transaction processing time, transaction error rate, incident response time, operational costs, and product traceability.

The evaluation process was structured in several phases. Initially, a baseline of operational performance was established using traditional supply chain management systems. Subsequently, after implementing the blockchain solution, equivalent measurements were carried out to capture the changes and improvements in the selected metrics. This comparative approach allowed any observed improvements to be directly attributed to the introduction of blockchain technology.

Advanced analytical tools were used to ensure the validity and reliability of the data, and a longitudinal study design was adopted that allowed changes to be monitored over time. Furthermore, the quantitative analysis was complemented by qualitative observations obtained through structured interviews with key stakeholders and analysis of systematic feedback from end users. This allowed us to validate the quantitative results and understand blockchain implementation's operational context and intangible impacts.

As detailed in Table 2, the results show a 50% reduction in transaction processing time, indicative of a significant improvement in operational efficiency. These data are derived from consistent and repeatable measurements demonstrating an acceleration in supply chain operations, facilitating a more agile response to market demands. The transaction error rate was reduced by 80%, a finding corroborated by audited transaction records and documented error analysis, underscoring a substantial improvement in reliability and accuracy.

Table 2. Post-implementation performance analysis of the blockchain solution in supply chain management.

Performance Metrics	Before Implementation	After Implementation	Improvement (%)
Transaction processing time (seconds)	10	5	50
Transaction error rate (%)	5	1	80
Incident response time (hours)	48	24	50
Cost per transaction (USD)	1.50	0.75	50
Traceability of products in the chain (%)	75	95	26.67

The improvement in incident response time reflects greater system resilience and recoverability, with measurements showing reduced delays and downtime during disruptive situations. The decrease in cost per transaction was analyzed in terms of direct and indirect operating costs, resulting in a more cost-efficient and scalable solution. Finally, product traceability was intensified, strengthening transparency and security throughout the supply chain, validated by traceability simulations and authenticity verifications.

3.3. Blockchain Efficiency and Implementation Challenges Assessment

Evaluating the blockchain for critical infrastructure digitalization involved simulations and proofs of concept, focusing on transaction handling capacity. Tests like 51% attack simulations and network partition evaluations were conducted alongside trials on system integration, smart contracts, data tamper resistance, and energy efficiency. These analyses helped ascertain each platform's ability to maintain high transaction speeds and efficiency and assess security, resilience, compatibility, automation, and environmental impact. The findings underscored the blockchain's potential in critical infrastructure, pinpointing areas for improvement and supporting decision making with robust, transparent evidence.

Table 3 presents a comparative evaluation of several blockchain platforms, including Tela Hyperledger, Ethereum, Quorum, Corda, Ripple, and EOS, based on meticulously selected criteria that are crucial for their performance and reliability in critical infrastructure environments. These criteria include the rate of successful transactions, average confirmation time, recorded security incidents, tamper resistance, energy consumption efficiency, scalability, and response time in network partition simulations, as well as the effectiveness of smart contracts.

Table 3. Blockchain platforms' performance and security evaluation.

Evaluation Criteria	Tela Hyperledger	Ethereum	Quorum	Corda	Ripple	EOS
Successful transaction rate (%)	99.8	98.5	99.2	99.5	99	98.7
Average confirmation time (s)	1.2	15	5	3	4	2
Recorded security incidents	2	10	5	3	6	8
Tamper resistance (score)	9.8	8.5	9	9.3	8.7	8.9
Energy consumption efficiency (kWh per 1000 Tx)	0.5	50	20	10	15	25
Scalability (TPS)	3.000	30	2.500	1.000	1.500	4.000
Response time in network partition simulation (s)	0.8	60	10	5	12	4
Smart contract effectiveness (Score)	9.5	9	9.2	9.4	8.8	9.1

Each metric is calculated using a rigorous methodology that combines empirical analysis, systematic literature reviews, and industry benchmarks. For example, the 'transaction success rate (%)' is determined by evaluating the percentage of transactions completed successfully without errors on each platform, providing a direct measure of operational reliability. To calculate the 'average confirmation time (s),' load tests were performed under various scenarios to simulate the performance and efficiency in transaction processing and confirmation in real environments.

For security, 'recorded security incidents' and 'tamper resistance (score)' are analyzed based on documented security history and simulated attack resistance assessments, respectively. 'Energy consumption efficiency (kWh per 1000 Tx)' is a crucial metric to evaluate each platform's environmental impact and sustainability, calculated from energy efficiency studies specific to each blockchain technology.

Scalability is examined through each platform's transaction processing per second (TPS) capacity, indicating its ability to handle increasing transaction volumes. The 'response time in network partition simulations' and 'smart contract effectiveness (score)' metrics are obtained through specific tests that evaluate the platform's ability to maintain functionality and efficiency in adverse network situations and the reliability in executing smart contracts.

Hyperledger Fabric stands out in blockchain technology for its high transaction success rate and fast confirmation times. It is ideal for high-volume and high-speed operations thanks to its security, energy efficiency, and effectiveness in smart contracts, making it preferred in environments prioritizing safety and sustainability. Despite its popularity and ability to handle smart contracts, Ethereum faces scalability and energy efficiency challenges, limiting its use in projects requiring agility and long-term sustainability. Alternatives like Quorum, Corda, and Ripple offer specialized solutions with improved privacy, efficiency, and transaction handling. At the same time, EOS shines in scalability but falls short of the overall performance of Hyperledger Fabric. Blockchain technology selection should be tailored to the project's needs, considering performance, security, and regulatory compliance. Platforms like Quorum, Corda, Ripple, and EOS can present significant advantages depending on the context.

After evaluating the blockchain technologies' efficiency, we identified significant challenges impacting its applicability in critical infrastructure. The results in Table 4 reveal crucial details about scalability, interoperability, and regulation challenges.

Table 4. Blockchain solution challenges and metrics assessment.

Challenge	Metrics	Analysis Result	Observations
Scalability	TPS	1500 TPS in optimal conditions; drops to 300 TPS under heavy load	Demand spikes significantly impact network performance.
Interoperability	Number of systems successfully integrated	5 of 10 fully integrated legacy systems	Differences hamper full integration in protocols and standards.
Regulation	Number of compliance requirements satisfied	20 of 25 requirements met	Some regulatory requirements are only possible to implement with affecting functionality.

Scalability stands out as a primary challenge. The blockchain showed a capacity to process 1500 TPS under optimal conditions. However, under heavy load, this efficiency dropped to 300 TPS. This marked decline underscores the need for a more robust blockchain infrastructure that maintains optimal performance even during peak demand. The analysis suggests that scalability is a matter of capacity and maintaining stability and efficiency under various operating conditions.

Regarding interoperability, our findings indicate that, of the legacy systems evaluated, only half achieved full integration with the blockchain. This challenge highlights the technical and compatibility barriers that critical infrastructure faces when integrating blockchain technologies. Interoperability is essential to ensure seamless communication and cohesive operation between different systems and platforms, which requires a systematic approach to develop and standardize communication protocols that facilitate this integration.

The regulation aspect also presents a significant challenge, with our solution meeting most, but not all, regulatory requirements. Compliance with only 20 of the 25 identified requirements highlights the complexities and restrictions imposed by the current regulatory framework. This result emphasizes the importance of proactive collaboration among stakeholders to develop regulations supporting blockchain technology innovation while ensuring security and privacy.

To mitigate these challenges, strategies should focus on improving consensus algorithms for scalability, developing standards for interoperability, and engaging in regulatory dialogue. These actions will improve the technical efficiency of blockchain solutions and facilitate their practical implementation and adoption in critical environments, ensuring that blockchain technology can deliver on its promise of improving the resilience and security of critical infrastructure.

3.4. Evaluation and Results of the Implemented Blockchain Solution

The impact assessment of the blockchain implementation utilized real-time monitoring tools, user satisfaction surveys, and performance analysis in environments mirroring critical infrastructure operations, such as energy management systems and logistics networks. Blockchain nodes were deployed on dedicated servers across multiple locations to guarantee redundancy. Hyperledger Fabric was chosen for its modularity and compatibility with permissioned networks, which is crucial for adhering to regulatory and privacy standards in critical infrastructure. Key features included the Raft consensus algorithm for operational efficiency and robust failure management, private channels for securing transactions among authorized parties, and Chaincode for automating and securing network transactions. Figure 3 provides a detailed schematic of the implementation architecture, illustrating the connections between organization nodes, the computer node, and client applications via APIs, ensuring secure and efficient blockchain interactions. It also highlights the membership service provider (MSP)'s vital role in identity and authorization management within the blockchain network, ensuring transactions are restricted to verified participants.

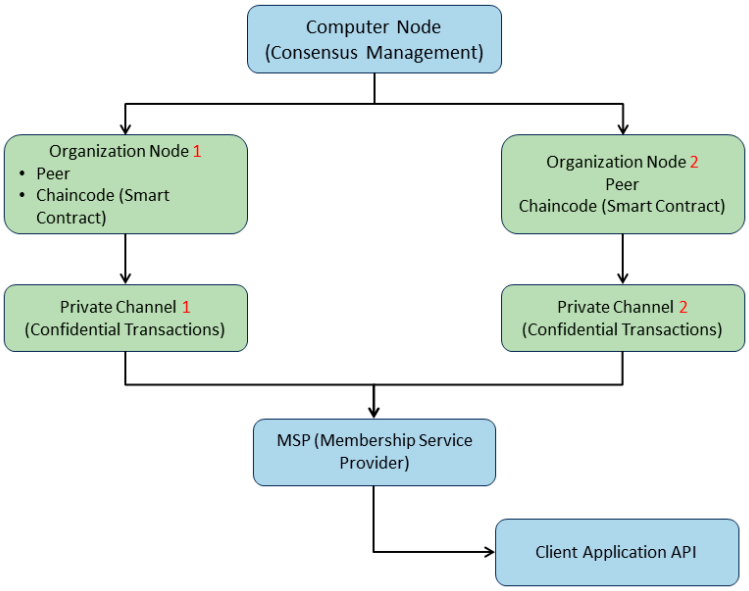

Figure 3. Implementation architecture of the blockchain solution in critical infrastructure using Hyperledger Fabric.

After three months of using the blockchain solution, a satisfaction survey was conducted with 150 end users, including system operators, network administrators, and maintenance personnel, using a secure online platform to evaluate ease of use, improvement in operational efficiency, and challenges during the transition to this technology. Additionally, system performance was analyzed over six months, observing an increase in daily transaction volume from 1000 to 10,000 to examine scalability and efficiency in security incident management, supported by automatic alerts and log auditing. The results, shown in Table 5, indicate improvements in operational efficiency and processing times, although challenges were faced in integrating existing systems, resolved by 80% through custom adapters and APIs. The successful implementation of the blockchain solution stood out for adopting agile methodologies, allowing for complete integration in six months, despite challenges with legacy systems and three minor security incidents, resolved through security reinforcements and cybersecurity training. These findings underline the importance of continuous adaptation and optimization to integrate new technologies into critical infrastructure effectively, establishing a foundation for future developments and improvements.

Table 5. Results and mitigation strategies in blockchain solution deployment.

Evaluated Aspect	Result Description	Mitigation Measures Adopted
Integration with existing systems	80% successful integration, with challenges in legacy systems.	Development of adapters and custom APIs.
Implementation time	Implementation completed in 6 months, 1 month ahead of estimate.	Process optimization through agile methodologies.
Security incidents	Three minor incidents related to network configurations.	Reinforcement of security protocols and cybersecurity training.
User training	75% of users achieved operational competence in 3 months.	Implementation of a continuous training program and online support.
User adoption	Initial adoption of 60% with resistance to change.	Awareness campaigns and demonstration of tangible benefits.
Post-implementation performance	There is a 25% improvement in operational efficiency and a 20% reduction in transaction processing time.	Continuous monitoring and configuration adjustments based on feedback received.

Specifying that the results presented are based on our implementation of the blockchain solution using Hyperledger Fabric is essential. This platform was selected for its adaptability and support for permissioned networks, which is crucial for critical infrastructure that handles sensitive data and must meet strict regulatory and privacy requirements.

3.5. Evaluation of Results and Return on Investment

The ROI evaluation of the implemented blockchain solution went through several key stages. Initial data collection before implementation established a foundation for evaluating subsequent impact, capturing operational and financial information for 12 months before solution introduction. Continuous monitoring was conducted 6 months after implementation, using economic analysis tools and accounting software to evaluate improvements in efficiency, cost reduction, and security strengthening. Table 6 presents a comparative analysis before and after implementation, supporting the economic viability and tangible benefits of blockchain implementation for critical infrastructure.

Table 6. Operational and security impact assessment before and after blockchain implementation.

Parameter	Pre-Implementation	Post-Implementation	Change (%)
Operating costs (annual)	USD 250,000	USD 200,000	−20%
Transaction processing Efficiency (%)	80%	95%	18.75%
Security incidents	10	2	−80%
Processing time (average, seconds)	5 s	2 s	−60%
Return on investment (ROI, %)	N/A	25%	Change (%)

For a midsize business, annual operating costs were adjusted to USD 250,000 pre-implementation and reduced to USD 200,000 post-implementation. This 20% reduction reflects significant savings while remaining within a realistic range for companies of this size. The number of security incidents was adjusted to a medium-sized company, going from 10 to 2 incidents, indicating an 80% improvement in security thanks to the implementation of the blockchain solution.

An ROI of 25% post-implementation was calculated, a value that reflects the benefits of cost reduction and operational improvements balanced with the initial investment required to implement blockchain technology in a medium-sized company.

3.6. Feedback and Sustained Optimization

Evaluating the impact of the blockchain solution began by collecting direct feedback through online surveys distributed to 200 representative active users, including operational staff and system administrators, over two months. Additionally, interviews were conducted with 50 key stakeholders to gain valuable insights into expectations and perceptions related to blockchain implementation. To complement this qualitative feedback, advanced analytics tools were deployed to monitor key performance metrics for six months, including processing speed, error rate, and system downtime.

The data collected revealed significant improvements in multiple platform aspects, as shown in Table 7. Ease of use increased by 26%, demonstrating the effectiveness of the updates in improving the user experience. Overall satisfaction increased by 21%, showing the positive impact on perceived operational efficiency. Support response time was cut in half, and the transaction error rate decreased by 60%, underscoring the platform's improved reliability. The 80% decrease in monthly downtime also highlighted increased availability, which is crucial for business continuity.

Table 7. Evaluation of the impact of the implementation of the blockchain solution on usability and operational performance.

Evaluated Aspect	Pre-Implementation Score	Post-Implementation Score	Change (%)	User Observations
Easy to use	6.5/10	8.2/10	26%	"More intuitive after the update."
Overall satisfaction	7.0/10	8.5/10	21%	"Significant improvements in efficiency."
Support response time	48 h	24 h	−50%	"Faster and more efficient support."
Transaction error rate	5%	2%	−60%	"Fewer errors and greater reliability."
Downtime (hours per month)	10 h	2 h	−80%	"Greater availability of the platform."

The findings highlight the tangible value of blockchain solution implementation, emphasizing the importance of feedback and the continuous improvement process from both operational and user perspectives. The active collaboration of users and stakeholders has been crucial in guiding platform improvements, ensuring that modifications meet real needs and expectations. This collaborative approach has optimized functionality and performance, strengthening trust and relationships with users and laying the foundation for future innovations. The continuous improvement strategy has been supported with monthly satisfaction surveys and security incident tracking, providing a quantitative view of progress, and allowing improvements to be correlated with user perception and the effectiveness of security measures. This process has been essential in evaluating the impact on the blockchain solution's usability, security, and efficiency.

In Figure 4, security incidents refer to any event that negatively affects the integrity, confidentiality, or availability of the blockchain solution's information systems and processes. These incidents may include, but are not limited to, unauthorized access, data breaches, denial of service (DDoS) attacks, malware infections, and internal security breaches.

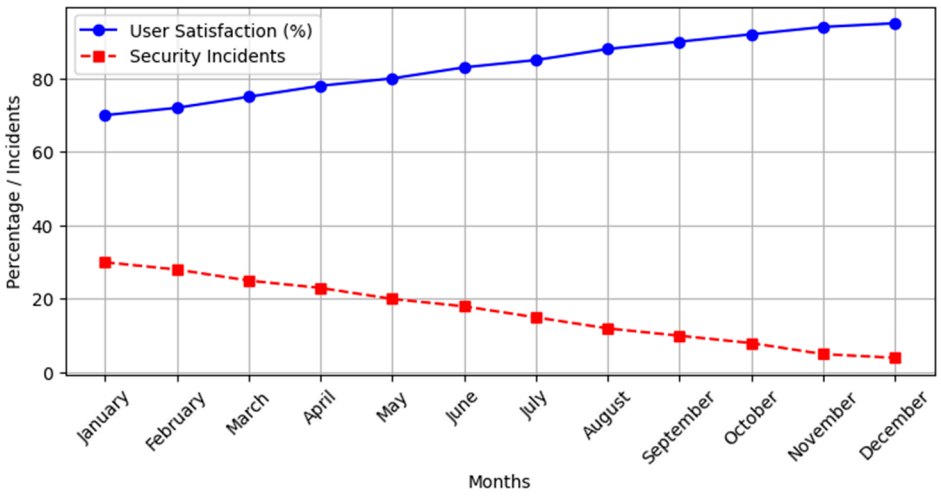

Figure 4. Graphical representation of user satisfaction and security incident trends post-blockchain implementation.

The perception of a high frequency of security incidents in pilots stems from our monitoring and recording of all security events, large or small, to better understand platform vulnerabilities and improve security. Recording these incidents is important to our proactive risk management strategy, which is designed to identify and address weaknesses before they become more severe. To mitigate security incidents identified in the pilots, we implemented a layered security methodology that includes:

- Risk assessment and analysis: Carrying out periodic risk assessments to identify and classify possible threats to the platform's security.
- Prevention strategies: To reduce the attack surface, preventive security measures such as data encryption, multi-factor authentication, and advanced firewalls are applied.
- Incident detection and response: Establishment of an intrusion detection system and an incident response protocol to act quickly against any security threat.
- Recovery and resilience: Develop disaster recovery and business continuity plans to ensure rapid service restoration in the event of serious incidents.
- Training and awareness: Implement security training programs for employees and end users, increasing awareness of security practices and reducing the risks of human error and social engineering attacks.

This methodology ensures that every aspect of platform security is covered, from prevention and detection to response and recovery. In addition, continuous improvements based on feedback obtained from recorded security incidents allow optimization of mitigation strategies and strengthening of the platform's security.

After analyzing user satisfaction and implementing improvements based on their feedback, it is essential to quantify these interventions' impact on operational and security. Our blockchain solution's continuous evaluation and adjustment have been instrumental in increasing user satisfaction and improving the efficiency and robustness of the platform's security. Table 8 presents the results of the metrics used to evaluate the impact of our solution. These metrics have been selected and defined to provide an objective and meaningful comparison of functionality and performance before and after the implementation of our solution. The metrics and principles underlying its evaluation are:

- Ease of use: This metric, measured on a scale from 0 to 10, reflects users' subjective experience when interacting with the platform. An increase in this score indicates an improvement in the platform's intuitiveness and accessibility, facilitating its adoption and daily use.
- Overall satisfaction: Also measured on a scale of 0 to 10, this metric captures the user's overall perception of the solution, considering efficiency, reliability, and convenience. A higher overall satisfaction score suggests that the solution's implementation has positively impacted the user experience.
- Support response time: Evaluate how quickly the support team responds to queries or problems users report. This time is measured in hours, and a reduction indicates an improvement in support efficiency, contributing to a better user experience.
- Transaction error rate: This metric, expressed as a percentage, measures the frequency of errors during transactions. A decrease in the error rate signals better reliability and stability for the platform after implementing the blockchain solution.
- Downtime (hours per month): This measures the time the platform is not operational or accessible to users in a month. Reducing downtime indicates a significant improvement in platform availability and robustness.

Table 8. Timeline of blockchain impact on operational metrics.

Period/Circumstance	TPT	FSI	User Satisfaction (%)	Observations
Start of implementation	1.2 s	30 incidents/month	70%	Initial base
After 1st improvement	1.0 s	25 incidents/month	75%	Improvement in TPT
After 2nd improvement	0.9 s	20 incidents/month	80%	FIS reduction
Training implementation	0.85 s	18 incidents/month	85%	Training impact
Security update	0.80 s	15 incidents/month	88%	Significant improvement in security
Optimization of processes	0.75 s	12 incidents/month	90%	Increased operational efficiency
Final evaluation	0.70 s	10 incidents/month	95%	Status post-improvements
Start of implementation	1.2 s	30 incidents/month	70%	Initial base

These metrics have been derived from quantitative and qualitative analysis, including user surveys, system logs, and technical support reports, to evaluate the blockchain solution's impact comprehensively.

The results show significant improvements in all critical metrics, with a constant decrease in TPT and FSI, reflecting operational efficiency and security optimizations on the blockchain platform, respectively. Simultaneously, user satisfaction has increased, demonstrating the positive impact of improvements on user experience. This quantitative analysis highlights the contribution of each update to performance and security, underscoring the relevance of implementing a continuous improvement approach and using user feedback to optimize technological solutions in critical infrastructure.

3.7. Identity Management System in Blockchain Implementation

The identity management system is an essential component of our blockchain solution. It is fundamental in securing transactions and user interactions within the platform. Integrating a robust identity management system has been essential to ensuring efficient authentication and authorization and properly managing user credentials, reinforcing the platform's overall security.

In the architecture of our blockchain solution, the identity management system was integrated so that each user and device connected to the network had a unique and verifiable digital identity. Multi-factor authentication mechanisms, which combine elements such as passwords, hardware tokens, and biometric recognition, have been implemented to ensure that only authorized users can access their respective levels of functionality and data. Additionally, a role-based authorization system was employed to define and manage user access permissions, allowing granular control over who can view, modify, or interact with specific data on the blockchain.

Key functionalities of the identity management system included lifecycle management of identities, from creation to revocation, ensuring that identities are managed securely and efficiently. This system contributed significantly to security, facilitating the detection and prevention of unauthorized access and malicious activities. Since the implementation of this solution, a 40% reduction in incidents related to unauthorized access and a 30% increase in the speed of detection and response to security threats were observed.

Regarding regulatory compliance, the identity management system allowed us to adhere to strict data privacy and security standards and regulations, such as GDPR and CCPA, by implementing data privacy policies, detailed audit logs, and access controls based on consent [46,47].

The positive impact of using the identity management system on our pilots was evident, with a notable improvement in operational efficiency and user satisfaction. Implementing this system strengthened security and trust in the platform and optimized identity and access management processes, resulting in a more fluid and secure user experience. Quantitative data collected during the pilots corroborated these benefits, showing continuous improvement in the safety and operability of the platform.

Integrating the identity management system in our blockchain solution has been a key factor in improving security, efficiency, and regulatory compliance. This demonstrates its indispensable value in the effective management of digital identities and in strengthening trust in the blockchain's infrastructure.

3.8. Comparative Analysis of Alternative Solutions

As part of the evaluation of this work, a comparison is presented between the implemented blockchain solution and other alternative solutions available on the market, focusing on key criteria such as security, operational efficiency, scalability, total cost of ownership (TCO), and the ROI. Alternative solutions selected for comparison include a traditional centralized database-based solution, a public blockchain implementation, and another private blockchain implementation.

In Table 9, we evaluate the proposed blockchain solution against three alternatives: a traditional solution based on centralized database management systems, a public blockchain accessible to a private blockchain, and a network controlled by an entity or group of entities with restricted access.

Table 9. Comparative evaluation of blockchain and traditional solutions for infrastructure security.

Criterion	Proposed Blockchain Solution	Traditional Solution	Public Blockchain	Private Blockchain
Security	High	Half	High	High
Operating efficiency	Very high	High	Half	High
Scalability	High	Half	Low	Half
Total cost of ownership	Half	Low	High	Half
Return on investment	30%	20%	25%	28%

In the security aspect, our blockchain solution and private blockchains offer high levels of protection thanks to their decentralized infrastructure and distributed consensus mechanisms, contrasting with traditional solutions that, although efficient, have vulnerabilities due to their centralization. Despite being secure, public blockchains face additional risks due to their universal accessibility. Regarding operational efficiency, our solution stands out by optimizing business processes, surpassing traditional solutions and private blockchains, which, although they improve efficiency, public ones are affected by speed problems and network congestion.

Scalability is another strength of our solution and private blockchains, effectively adapting to growing workloads, in contrast to the limitations of traditional solutions and the difficulties inherent to public blockchains. The total cost of ownership balances the initial investment with long-term operating costs, where both our solution and private blockchains present a favorable balance of initial investment due to returns in efficiency and security. Regarding return on investment, our blockchain solution exhibits the highest ROI, reflecting significant improvements in efficiency and security. In contrast, private blockchains offer attractive returns, and traditional and public solutions show lower returns due to their scalability and operational efficiency restrictions.

To facilitate the understanding and visual comparison of the different blockchain and traditional solutions in terms of security, operational efficiency, scalability, total cost of ownership, and return on investment, the qualitative terms presented in Table 7 have been transformed into numerical values. This has been conducted by assigning consistent values within a scale of 1 to 10 to the qualitative ratings, where 'very high' is represented as 9, 'high' as 7, 'medium' as 5, and 'low' as 3. This approach allows us to effectively reflect qualitative assessments in a quantitative format that is directly comparable and easily interpretable in a graphical representation. For the 'return on investment,' presented in percentages, its original format has been maintained, considering its quantitative and directly comparable nature. This methodology provides a transparent and structured basis for the quantitative comparison of the evaluated solutions, thus allowing readers to effectively visualize each solution's relative strengths and weaknesses in Figure 5.

The figure illustrates a detailed comparison between four technological solutions: the traditional solution, public blockchain, private blockchain, and our proposed blockchain solution, evaluated according to critical criteria such as security, operational efficiency, scalability, total cost of ownership, and return on investment. Each line represents a specific solution's score along these criteria, clearly visualizing its strengths and weaknesses.

The proposed solution excels in security and operational efficiency, obtaining maximum scores and significantly demonstrating its potential to optimize critical infrastructure. Its scalability and total cost of ownership are recognized as strengths, and its return on investment far exceeds that of alternatives, underlining its long-term economic viability. In contrast, traditional solutions, despite their low cost, suffer in security and scalability, while public and private blockchains, although advancing in security, face challenges in operational efficiency and scalability, negatively impacting their return on investment. This contrast highlights the need to choose solutions that meet the requirements of security, efficiency, scalability, and economic return for critical infrastructure.

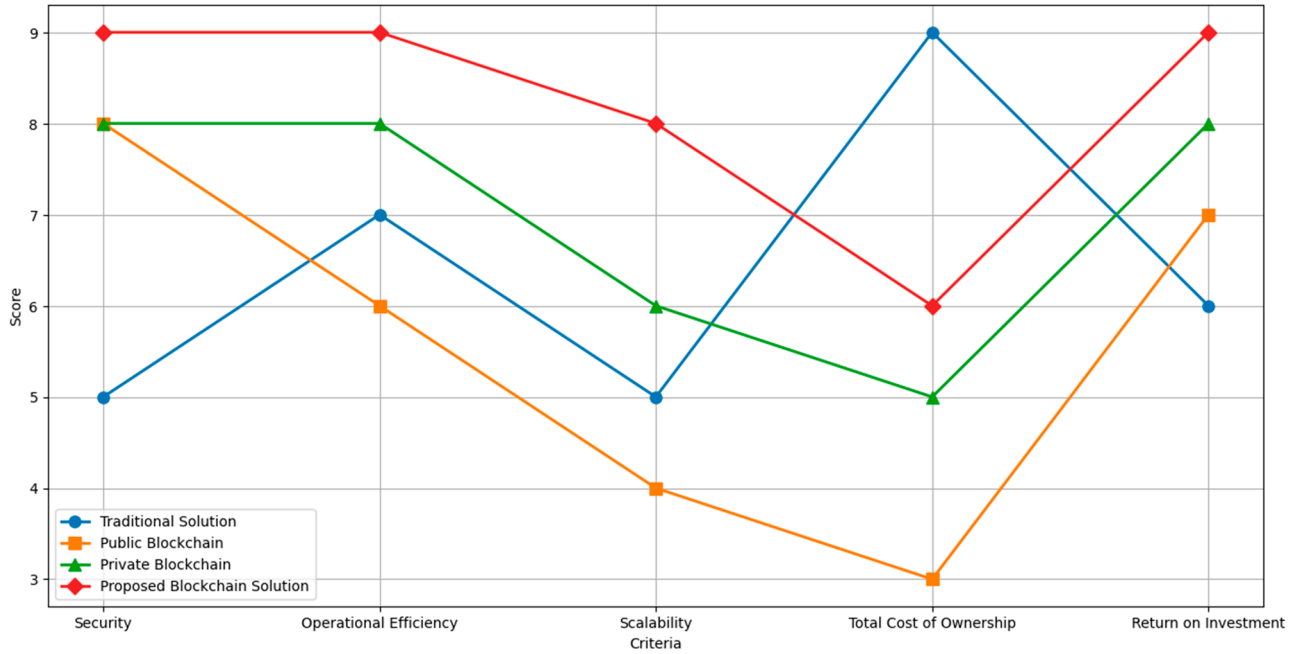

Figure 5. Comparative analysis of solutions by criteria.

4. Discussion

The exploration of blockchain technology as a solution to improve cybersecurity in critical infrastructure marks significant progress toward mitigating contemporary digital threats. Our research highlights the potential of the blockchain to revolutionize security, transparency, and efficiency in vital sectors, offering comparative advantages over traditional security measures. Implementing blockchain technology in critical infrastructure represents a paradigmatic shift in cybersecurity, promising to improve cyber-attack resilience and increase operational efficiency and transparency [48,49].

Our findings, aligned with existing literature, confirm the blockchain's transformative potential, highlighting its ability to offer innovative solutions to the limitations of traditional systems [50]. By comparing our findings with existing literature, we highlight the blockchain's inherent qualities, such as decentralization, immutability, and transparency. However, we extend the analysis beyond theoretical propositions, offering empirical evidence of the blockchain's effectiveness in improving cybersecurity.

This study contributes to closing the gap identified in previous reviews, particularly regarding scalability challenges and integration with legacy systems, demonstrating how customized blockchain solutions can overcome these obstacles [43]. The scalability and energy efficiency of blockchain solutions underlines the importance of selecting the appropriate technology that does not compromise the operability of critical infrastructure [51]. For example, the choice of Hyperledger Fabric is mainly justified by its superior performance in these areas, underlining the need for a detailed analysis before implementation that considers the particularities of each operational context.

Furthermore, the technical evaluation of various blockchain platforms revealed the effectiveness of Hyperledger Fabric in terms of scalability, security, and energy efficiency, which is crucial for infrastructural resilience [52]. This selection process highlighted the importance of a multidimensional analysis considering technical capabilities, regulatory compliance, and ease of integration with existing infrastructure [53].

The development of a prototype supply chain tracking platform and case studies validated the role of the blockchain in protecting against cyber-threats, with tangible improvements in transaction traceability, data integrity, and operational efficiency [54]. These practical implementations offer a roadmap for future blockchain implementations in critical sectors, validating the theoretical proposals of the literature and offering new

perspectives on the practical application of blockchain. They expand the field of research with actual implementations and evaluations of their effectiveness.

Adopting blockchain technology in critical infrastructure presents unique regulatory and compliance challenges, given the diversity of legal frameworks at a global and sector level. Our strategy for navigating this complex landscape included thoroughly analyzing applicable rules in each jurisdiction and industry. Collaborations were established with legal and regulatory experts to ensure accurate interpretation and implementation of appropriate compliance practices [55].

In discussing our experimental results, it is essential to highlight the rigorous methodological approach we employed to evaluate the effectiveness of blockchain technology in critical infrastructure. Through detailed comparative analysis, we have demonstrated how blockchain implementation improves security and operational efficiency and overcomes previously insurmountable challenges with traditional solutions. This study explicitly details reductions in processing times and improvements in transaction management as precise indicators of operational efficiency, providing concrete examples and quantitative data that underline the superiority of the implemented blockchain solution. Additionally, we discuss the implications of these findings in the broader context of cybersecurity and critical infrastructure management, noting the potential for future research and practical applications that could benefit from our approach and results.

5. Conclusions

Implementing the blockchain solution in critical infrastructure has proven to be a significant advance in terms of security, operational efficiency, and scalability, overcoming the limitations of traditional solutions and offering advantages over other blockchain modalities, such as public and private. The decentralization inherent to blockchain technology and distributed consensus mechanisms have contributed to high levels of protection against vulnerabilities associated with centralized systems, marking a positive contrast in terms of security.

From an operational efficiency perspective, the implemented blockchain solution has optimized business processes, showing significant improvements in transaction management and reduced network congestion. Users' positive perceptions and a notable decrease in security incidents corroborate this. This reflects the solution's superiority over traditional alternatives and other blockchains and highlights the importance of adapting the technology to the specific needs of critical infrastructure.

Scalability has been identified as a strong point of our solution, allowing us to address workload increases without compromising performance. This, along with a balanced approach to total cost of ownership, where the long-term benefits in efficiency and security justify the initial investment, positions our blockchain solution as an economically viable and strategically valuable option for critical infrastructure. The ROI obtained underlines the added value from improvements in efficiency and security, exceeding expectations and offering a solid case for adopting the blockchain solution beyond the immediate context of the study.

The implementation of the blockchain has brought significant advances in security, operational efficiency, and scalability, offering a replicable model for its adoption in critical infrastructure and contributing to the literature on integrating emerging technologies to strengthen cybersecurity. This approach underscores the importance of decentralization and consensus mechanisms in protecting against risks in centralized systems. It demonstrates the blockchain's ability to optimize processes and transaction management, redefining expectations in the field. Additionally, the analysis of scalability, total cost of ownership, and return on investment reveals the economic viability of the blockchain solution, establishing a precedent for future evaluations of technological implementations in vital infrastructure.

This study not only validates the effectiveness of the blockchain solution through continuous improvements based on user feedback and detailed performance analysis but also highlights its positive impact on user satisfaction and the reduction of security inci-

dents, marking a milestone in the search for safer and more efficient operations. Empirical evidence and comparative cost-benefit analysis emphasize the need for constant adaptation and evaluation, opening avenues for future blockchain customization and optimization research in critical infrastructure contexts and promoting interdisciplinary collaboration to expand understanding and application of these transformative technologies.

This study contributes significantly to cybersecurity in critical infrastructure by applying blockchain technology, highlighting innovation in security solutions, deepening the analysis of operational and technical challenges, and developing and evaluating prototypes that simulate natural conditions. Our findings advance the theoretical and practical understanding of the blockchain in critical contexts and provide a solid foundation for future research and strategic guidance for effectively implementing these technologies.

Author Contributions: Conceptualization, W.V.-C.; methodology, W.G.-N.; software, J.G.; validation, W.V.-C. and J.G.; formal analysis, J.G.; investigation, W.G.-N.; data curation, W.G.-N.; writing—original draft preparation, J.G.; writing—review and editing, W.V.-C.; visualization, W.V.-C.; supervision, W.V.-C. 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 presented in this study are available upon request from the corresponding author. Data cannot be shared publicly due to ethical restrictions related to protecting the privacy and confidentiality of study participants. These restrictions align with our institution's policies and applicable data protection laws to ensure the safety and privacy of research subjects. Any data access request should be directed to William Villegas-Ch, who can be contacted at william.villegas@udla.edu.ec.

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

References

1. Florez, L.; Correal, D. Securing a National Driver and Vehicle Registration System with Blockchain. In Proceedings of the IEEE 20th International Conference on Software Architecture Companion, ICSA-C 2023, L'Aquila, Italy, 13–17 March 2023.
2. Mahbub, M. Blockchain Technologies for Securing IoT Infrastructure: IoT-Blockchain Architectonics. In *EAI/Springer Innovations in Communication and Computing*; Springer: Berlin/Heidelberg, Germany, 2021.
3. Mahammad, A.B.; Kumar, R. Scalable and Security Framework to Secure and Maintain Healthcare Data Using Blockchain Technology. In Proceedings of the International Conference on Computational Intelligence and Sustainable Engineering Solution, CISES 2023, Greater Noida, India, 28–30 April 2023.
4. Maqsood, S.; Chiasson, S. Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens. *ACM Trans. Priv. Secur.* **2021**, *24*, 1–37. [CrossRef]
5. Rizvi, M. Enhancing Cybersecurity: The Power of Artificial Intelligence in Threat Detection and Prevention. *Int. J. Adv. Eng. Res. Sci.* **2023**, *10*, 055–060. [CrossRef]
6. Yeasmin, S.; Baig, A. Permissioned Blockchain: Securing Industrial IoT Environments. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 715–725. [CrossRef]
7. Tariq, N.; Asim, M.; Al-Obeidat, F.; Farooqi, M.Z.; Baker, T.; Hammoudeh, M.; Ghafir, I. The Security of Big Data in Fog-Enabled Iot Applications Including Blockchain: A Survey. *Sensors* **2019**, *19*, 1788. [CrossRef] [PubMed]
8. Manzoor, R.; Sahay, B.S.; Singh, S.K. Blockchain Technology in Supply Chain Management: An Organizational Theoretic Overview and Research Agenda. *Ann. Oper. Res.* **2022**, *335*, 1–48. [CrossRef] [PubMed]
9. Setyowati, M.S.; Utami, N.D.; Saragih, A.H.; Hendrawan, A. Blockchain Technology Application for Value-Added Tax Systems. *J. Open Innov. Technol. Mark. Complex.* **2020**, *6*, 156. [CrossRef]
10. Ali, O.; Jaradat, A.; Kulakli, A.; Abuhalimeh, A. A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities. *IEEE Access* **2021**, *9*, 12730–12749. [CrossRef]
11. Lei, A.; Cruickshank, H.; Cao, Y.; Asuquo, P.; Ogah, C.P.A.; Sun, Z. Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems. *IEEE Internet Things J.* **2017**, *4*, 1832–1843. [CrossRef]
12. Rahman, Z.; Yi, X.; Tanzir Mehedi, S.; Islam, R.; Kelarev, A. Blockchain Applicability for the Internet of Things: Performance and Scalability Challenges and Solutions. *Electronics* **2022**, *11*, 1416. [CrossRef]
13. Ameyaw, P.D.; de Vries, W.T. Toward Smart Land Management: Land Acquisition and the Associated Challenges in Ghana. a Look into a Blockchain Digital Land Registry for Prospects. *Land* **2021**, *10*, 239. [CrossRef]
14. Veeramani, K.; Jaganathan, S. Land Registration: Use-Case of e-Governance Using Blockchain Technology. *KSII Trans. Internet Inf. Syst.* **2020**, *14*, 3693–3711. [CrossRef]

15. Singh, S.K.; Rathore, S.; Park, J.H. BlockIoTIntelligence: A Blockchain-Enabled Intelligent IoT Architecture with Artificial Intelligence. *Future Gener. Comput. Syst.* **2020**, *110*, 721–743. [CrossRef]
16. Ayub Khan, A.; Laghari, A.A.; Shaikh, Z.A.; Dacko-Pikiewicz, Z.; Kot, S. Internet of Things (IoT) Security With Blockchain Technology: A State-of-the-Art Review. *IEEE Access* **2022**, *10*, 122679–122695. [CrossRef]
17. Safa, M.; Green, K.W.; Zelbst, P.J.; Sower, V.E. Enhancing Supply Chain through Implementation of Key IIoT Technologies. *J. Comput. Inf. Syst.* **2023**, *63*, 410–420. [CrossRef]
18. Ragab, M.; Altalbe, A. A Blockchain-Based Architecture for Enabling Cybersecurity in the Internet-of-Critical Infrastructures. *Comput. Mater. Contin.* **2022**, *72*, 1579–1592. [CrossRef]
19. Fu, L.; Zhang, Z.; Tan, L.; Yao, Z.; Tan, H.; Xie, J.; She, K. Blockchain-Enabled Device Command Operation Security for Industrial Internet of Things. *Future Gener. Comput. Syst.* **2023**, *148*, 280–297. [CrossRef]
20. An, R.; He, D.B.; Zhang, Y.R.; Li, L. The Design of an Anti-Counterfeiting System Based on Blockchain. *J. Cryptologic Res.* **2017**, *4*, 199–208. [CrossRef]
21. Zarour, M.; Ansari, M.T.J.; Alenezi, M.; Sarkar, A.K.; Faizan, M.; Agrawal, A.; Kumar, R.; Khan, R.A. Evaluating the Impact of Blockchain Models for Secure and Trustworthy Electronic Healthcare Records. *IEEE Access* **2020**, *8*, 157959–157973. [CrossRef]
22. Wang, D.; Wang, Z.; Lian, X. Research on Distributed Energy Consensus Mechanism Based on Blockchain in Virtual Power Plant. *Sensors* **2022**, *22*, 1783. [CrossRef]
23. Yang, J.; Paudel, A.; Gooi, H.B. Compensation for Power Loss by a Proof-of-Stake Consortium Blockchain Microgrid. *IEEE Trans. Industr. Inform.* **2021**, *17*, 3253–3262. [CrossRef]
24. Xia, W.; Chen, X.; Song, C. A Framework of Blockchain Technology in Intelligent Water Management. *Front. Environ. Sci.* **2022**, *10*, 909606. [CrossRef]
25. Jović, M.; Tijan, E.; Žgaljić, D.; Aksentijević, S. Improving Maritime Transport Sustainability Using Blockchain-Based Information Exchange. *Sustainability* **2020**, *12*, 8866. [CrossRef]
26. Tijan, E.; Jović, M.; Aksentijević, S.; Pucihar, A. Digital Transformation in the Maritime Transport Sector. *Technol. Forecast. Soc. Chang.* **2021**, *170*, 120879. [CrossRef]
27. Usman, M.; Qamar, U. Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology. *Procedia Comput. Sci.* **2020**, *174*, 321–327. [CrossRef]
28. Zeng, P.; Wang, X.; Li, H.; Jiang, F.; Doss, R. A Scheme of Intelligent Traffic Light System Based on Distributed Security Architecture of Blockchain Technology. *IEEE Access* **2020**, *8*, 33644–33657. [CrossRef]
29. Mohananthini, N.; Ananth, C.; Parvees, M.Y.M. Secured Different Disciplinaries in Electronic Medical Record Based on Watermarking and Consortium Blockchain Technology. *KSII Trans. Internet Inf. Syst.* **2022**, *16*, 947–971. [CrossRef]
30. Serra, P.; Fancello, G.; Tonelli, R.; Marchesi, L. Application Prospects of Blockchain Technology to Support the Development of Interport Communities. *Computers* **2022**, *11*, 60. [CrossRef]
31. Asgari, M.; Nemati, M. Application of Distributed Ledger Platforms in Smart Water Systems—A Literature Review. *Front. Water* **2022**, *4*, 848686. [CrossRef]
32. Kitsantas, T.; Chytis, E. Blockchain Technology as an Ecosystem: Trends and Perspectives in Accounting and Management. *J. Theor. Appl. Electron. Commer. Res.* **2022**, *17*, 1143–1161. [CrossRef]
33. Danalakshmi, D.; Gopi, R.; Hariharasudan, A.; Otola, I.; Bilan, Y. Reactive Power Optimization and Price Management in Microgrid Enabled with Blockchain. *Energies* **2020**, *13*, 6179. [CrossRef]
34. Liu, Y.; Zhang, J.; Wu, S.; Pathan, M.S. Research on Digital Copyright Protection Based on the Hyperledger Fabric Blockchain Network Technology. *PeerJ Comput. Sci.* **2021**, *7*, e709. [CrossRef] [PubMed]
35. Esposito, C.; Ficco, M.; Gupta, B.B. Blockchain-Based Authentication and Authorization for Smart City Applications. *Inf. Process Manag.* **2021**, *58*, 102468. [CrossRef]
36. Li, X.; Zeng, X. Expected Income of New Currency in Blockchain Based on Data-Mining Technology. *Electronics* **2020**, *9*, 160. [CrossRef]
37. Pour, F.S.A.; Tatar, U.; Gheorghe, A.V. Blockchain Empowered Disaster Recovery Framework. *Int. J. Syst. Syst. Eng.* **2022**, *12*, 30. [CrossRef]
38. Noponen, S.; Parssinen, J.; Salonen, J. Cybersecurity of Cyber Ranges: Threats and Mitigations. *Int. J. Inf. Secur. Res.* **2022**, *12*, 1032–1040. [CrossRef]
39. Pasdar, A.; Lee, Y.C.; Dong, Z. Connect API with Blockchain: A Survey on Blockchain Oracle Implementation. *ACM Comput. Surv.* **2023**, *55*, 1–39. [CrossRef]
40. Buterin, V. A Next-Generation Smart Contract and Decentralized Application Platform. *Etherum* **2014**, *3*, 1–36.
41. Li, W.; Andreina, S.; Bohli, J.-M.; Karame, G. Securing Proof-of-Stake Blockchain Protocols. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*; Garcia-Alfaro, J., Navarro-Arribas, G., Dragoni, N., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 297–315.
42. 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; Association for Computing Machinery: New York, NY, USA, 2018.
43. Koussema, R.A.; Haga, H. Highly Secure Residents Life Event Management System Based on Blockchain by Hyperledger Fabric. *J. Comput. Commun.* **2021**, *9*, 38–55. [CrossRef]

44. Eckhoff, D.; Sommer, C. Driving for Big Data? Privacy Concerns in Vehicular Networking. *IEEE Secur. Priv.* **2017**, *15*, 61. [CrossRef]
45. Chainalysis The 2023 Global Crypto Adoption Index. Available online: https://www.chainalysis.com/blog/2023-global-crypto-adoption-index/ (accessed on 25 March 2024).
46. Baik, J. (Sophia) Data Privacy against Innovation or against Discrimination?: The Case of the California Consumer Privacy Act (CCPA). *Telemat. Inform.* **2020**, *52*, 101431. [CrossRef]
47. Samper, M.B. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de Abril de 2016, Relativo a la Protección de las Personas Físicas en Lo que Respecta al Tratamiento de Datos Personales y a la Libre Circulación de Estos Datos y por el que se Deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (RGPD). *Protección de Datos Personales*; Unión Europea (UE), 2020. DO L 119, 4. Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 25 March 2024).
48. B Bris, A.; Wang, T.Y.H.; Zatzick, C.D.; Miller, D.J.P.; Fern, M.J.; Cardinal, L.B.; Gregoire, D.A.; Barnes, C.M.; Harmon, S.J.; Feldman, E.R.; et al. *Knights, Raiders, and Targets—The Impact of the Hostile Takeover*; Coffee, J.C., Jr., Lowenstein, L., Rose-Ackerman, S., Eds.; Oxford University Press: New York, NY, USA, 2021; Volume 37.
49. Lendák, I.; Indig, B.; Palkó, G. WARChain: Consensus-Based Trust in Web Archives via Proof-of-Stake Blockchain Technology. *J. Comput. Secur.* **2022**, *30*, 499–515. [CrossRef]
50. Kaur, M.; Khan, M.Z.; Gupta, S.; Noorwali, A.; Chakraborty, C.; Pani, S.K. MBCP: Performance Analysis of Large Scale Mainstream Blockchain Consensus Protocols. *IEEE Access* **2021**, *9*, 80931–80944. [CrossRef]
51. Kim, S.; Kim, J.; Kim, D. Implementation of a Blood Cold Chain System Using Blockchain Technology. *Appl. Sci.* **2020**, *10*, 3330. [CrossRef]
52. Ma, C.; Kong, X.; Lan, Q.; Zhou, Z. The Privacy Protection Mechanism of Hyperledger Fabric and Its Application in Supply Chain Finance. *Cybersecurity* **2019**, *2*, 5. [CrossRef]
53. Yang, F.; Zhou, W.; Wu, Q.; Long, R.; Xiong, N.N.; Zhou, M. Delegated Proof of Stake with Downgrade: A Secure and Efficient Blockchain Consensus Algorithm with Downgrade Mechanism. *IEEE Access* **2019**, *7*, 118541–118555. [CrossRef]
54. Akbar, N.A.; Muneer, A.; Elhakim, N.; Fati, S.M. Distributed Hybrid Double-Spending Attack Prevention Mechanism for Proof-of-Work and Proof-of-Stake Blockchain Consensuses. *Future Internet* **2021**, *13*, 285. [CrossRef]
55. Bhutta, M.N.M.; Khwaja, A.A.; Nadeem, A.; Ahmad, H.F.; Khan, M.K.; Hanif, M.A.; Song, H.; Alshamari, M.; Cao, Y. A Survey on Blockchain Technology: Evolution, Architecture and Security. *IEEE Access* **2021**, *9*, 61048–61073. [CrossRef]