blockchains

MDPI

Article

Towards Achieving Transparent and Secure Nuclear Fuel Transportation: A Technical Framework Integrating Consortium Blockchain and IoT

Yuxiang Xu [1,2], Wenjuan Yu [3], Yuqian Wan [4] and Zhongming Zhang [1,*]

[1] School of Engineering, Lancaster University, Bailrigg, Lancaster LA1 4YW, UK
[2] Lancaster University College, Beijing Jiaotong University, Weihai 264401, China
[3] School of Computing and Communications, InfoLab21, Lancaster University, Bailrigg, Lancaster LA1 4YW, UK; w.yu8@lancaster.ac.uk
[4] Management School, Lancaster University, Bailrigg, Lancaster LA1 4YW, UK
* Correspondence: zhongming.zhang@lancaster.ac.uk

Abstract

This study addresses critical challenges in managing the transportation of spent nuclear fuel, including inadequate data transparency, stringent confidentiality requirements, and a lack of trust among collaborating parties—issues prevalent in traditional centralized management systems. Given the high risks involved, balancing data confidentiality with regulatory transparency is imperative. To overcome these limitations, a technical framework integrating blockchain technology and the Internet of Things (IoT) is proposed, featuring a multi-tiered consortium chain architecture. This system utilizes IoT sensors for real-time data collection, which is immutably recorded on the blockchain, while a hierarchical data structure (operational, supervisory, and public layers) manages access for diverse stakeholders. This approach significantly enhances data immutability, enables real-time multi-sensor data integration, improves decentralized transparency, and increases resilience compared to traditional systems. It should be noted that the proposed framework is a theoretical study and has not yet been implemented or empirically validated, with practical deployment reserved for future work. Ultimately, this blockchain-IoT framework improves the safety, transparency, and efficiency of spent fuel transportation, effectively resolving the conflict between confidentiality and transparency in nuclear data management and offering significant practical implications.

Keywords: blockchain; spent nuclear fuel; consortium chain; internet of things

Academic Editor: Keke Gai

Received: 25 July 2025
Revised: 6 October 2025
Accepted: 9 October 2025
Published: 15 October 2025

Citation: Xu, Y.; Yu, W.; Wan, Y.; Zhang, Z. Towards Achieving Transparent and Secure Nuclear Fuel Transportation: A Technical Framework Integrating Consortium Blockchain and IoT. *Blockchains* **2025**, *3*, 13. https://doi.org/10.3390/blockchains3040013

1. Introduction

Spent nuclear fuel (SNF), also referred to as spent fuel, is the nuclear fuel that has been irradiated in and discharged from a nuclear reactor after its useful lifetime in power generation. It contains significant quantities of highly radioactive isotopes and requires careful management and secure transportation. Globally, thousands of shipments of radioactive materials, including both waste products and spent nuclear fuel, are transported daily [1].

The International Atomic Energy Agency (IAEA) issued the Regulations for the Safe Transport of Radioactive Material as early as 2012. IAEA member states are required to transport radioactive materials, including spent nuclear fuel, in compliance with these regulations. However, the transportation of radioactive materials continues to be one of the most vulnerable aspects of nuclear safety. According to the IAEA Incident and Trafficking

Database (ITDB) [2], spent nuclear fuel has been involved in numerous incidents, including theft, unauthorized disposal, and loss. Between 1993 and 2024, a total of 353 incidents were recorded involving the trafficking or malicious use of nuclear materials. Of these, approximately 86% were related to trafficking activities, around 13% involved fraud, and less than 2% pertained to malicious use. Nuclear waste contains precious extractable metals, such as platinum and palladium, which are very expensive on the black market. In addition, certain radioactive materials, such as plutonium and uranium, can be utilized in the production of radiological weapons. If mishandled or leaked, these materials could lead to significant public concern and panic [3]. The reasons for these vulnerabilities can be attributed to the following factors. First, nuclear waste is susceptible to loss or theft during transport in barrels to storage facilities because of inadequate protection measures. Second, there are significant management lapses in abandoned facilities. Third, insufficient international collaboration and weak regulatory systems in some countries hinder the effective tracking of radioactive sources throughout their entire lifecycle. Consequently, developing a comprehensive, secure, and stringent tracking and handling system for spent nuclear fuel has become an urgent priority for all nations.

This article aims to explore potential solutions for nuclear waste fuel accidents from the perspective of transportation tracking, utilizing distributed ledger technology (blockchain) to overcome the limitations of traditional data interaction methods. Additionally, it proposes a multi-layer data on-chain mechanism based on consortium chains to address the tension between the confidentiality of nuclear industry data (e.g., radiation dose and container location) and regulatory transparency (i.e., the disclosure by regulatory authorities to the public regarding regulatory activities, enforcement, and compliance of regulated entities) [4]. For instance, the Nuclear and Industrial Safety Agency (NISA) and the Japan Nuclear Energy Safety Organization (JNES) examined the challenge of balancing confidentiality and transparency in nuclear data during the "Transparency of Nuclear Regulatory Activities" symposium, held in Tokyo and Tokai-Mura, Japan, from 22 to 24 May 2007 [5]. The symposium established a common understanding of transparency and the expectations of key stakeholders, encouraging increased public engagement, and establishing a robust trust framework. However, this method faces challenges such as complex information categorization, delayed updates, vulnerability to tampering, difficulty in trust establishment, inefficient data sharing, weak traceability, restricted public involvement, and limited international cooperation. These challenges align precisely with the strengths of consortium chains.

This paper makes four major contributions. First, it proposes a consortium blockchain–IoT framework specifically tailored for the secure and transparent transportation of spent nuclear fuel. Second, it designs a hierarchical data governance structure that addresses the tension between strict confidentiality requirements and the need for regulatory transparency. Third, it enables the immutable storage and traceability of heterogeneous multi-sensor data streams—such as radiation levels, GPS trajectories, and container status—through blockchain anchoring combined with edge-level preprocessing. Finally, it outlines a reproducible experimental evaluation plan and comparative analysis with existing prototypes, thereby providing a practical roadmap for future empirical studies and subsequent real-world validation.

The rest of this paper is structured as follows. Section 2 elaborates on the characteristics of spent nuclear fuel, the limitations of current transportation management approaches, and the conflict between data confidentiality and regulatory transparency. Section 3 introduces blockchain's features, classification, its applications in supply chains and existing nuclear-related research, and the feasibility of blockchain-based multi-layer architectures. Section 4 details IoT sensor selection, a comparison with traditional tracking methods, the five-layer IoT-blockchain architecture, solutions to IoT device limitations, a consortium chain-based

multi-layer architecture for balancing confidentiality and transparency, and quantitative assessment indicators. Section 5 compares the proposed framework with existing systems (SLAFKA, Sellafield DLT Field Lab, TRANSCOM) and verifies its effectiveness through two real time cases.

2. Background

This section provides the necessary background on spent nuclear fuel and its management. It first outlines the characteristics and risks of spent fuel, then reviews current transportation management practices and their limitations, and, finally, discusses the critical conflict between confidentiality and regulatory transparency that motivates the proposed solution.

2.1. Characteristics of Spent Nuclear Fuel

As previously noted, spent fuel contains significant quantities of radioactive elements and requires appropriate management. During the cooling phase, spent nuclear fuel continuously emits decay heat due to the radioactive decay of nuclides. Excessive heat decay may compromise the functionality of the cooling systems in transportation equipment (e.g., dry storage casks), thereby increasing the risk of overheating. Consequently, continuous monitoring of temperature data for transportation equipment is essential during transit. Additionally, these nuclides exhibit high radioactivity levels. While radioactivity diminishes over extended cooling periods, certain long-lived radioactive nuclides in spent fuel, such as 238Pu, 241Am, and 137Cs, necessitate cooling durations exceeding a century [6].

As shown in Figure 1, there are two primary approaches to the management of spent fuel. One involves recycling the spent fuel by extracting reusable nuclear materials and repurposing them. Using chemical separation techniques, such as the PUREX process, uranium and plutonium can be recovered from spent fuel to produce mixed oxide (MOX) fuel, effectively reducing the volume of radioactive waste [7]. The other option is the underground storage of spent fuel. After being unloaded from the reactor, spent fuel is cooled first, then packaged and transported, and then directly buried underground as waste. Whether through spent fuel recycling and utilization or underground storage, its transportation must be based on the principle of safety.

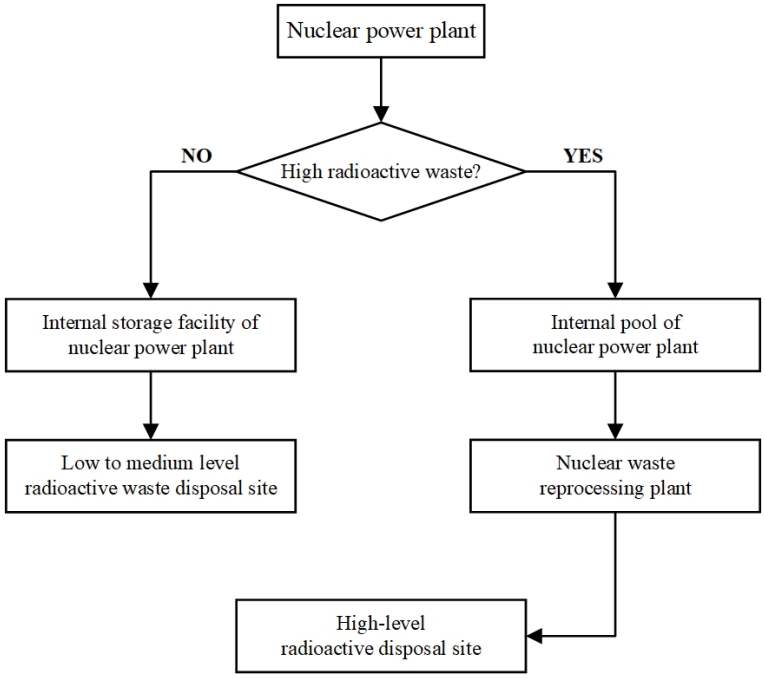

Figure 1. The process of spent nuclear fuel treatment.

Owing to the unique characteristics and high risks associated with spent nuclear fuel, its information management approach differs significantly from that of other materials. The information management strategy for spent nuclear fuel exhibits distinct features, necessitating transportation design specifically adapted to these attributes. Most importantly, continuous monitoring of radioactive containers during spent nuclear fuel transportation is critical to ensure their safety over extended periods (spanning years or even decades). Throughout its lifecycle, spent nuclear fuel is typically transported across long distances between various facilities, requiring continuous detection and analysis of its safety levels based on sensor data during transit. Any unforeseen incidents must be promptly reported. Additionally, the management of spent nuclear fuel transportation must establish mechanisms for providing appropriate access control for audits, thereby ensuring regulatory transparency [8].

2.2. Current Management Approach and Its Limitations

Globally, the management approaches for the transportation of spent nuclear fuel are largely consistent. Taking China as an example, the country enforces a stringent application process for spent fuel transportation. Prior to transportation, the consignor is required to submit an application for a spent fuel transportation permit to the national nuclear safety regulatory authority, accompanied by detailed transportation plans, radiation monitoring reports, and other relevant data [9]. Transportation can only commence upon approval. During transit, real-time data regarding the spent fuel's location, temperature, and radiation levels are transmitted to the consignor, carrier, and regulatory authorities via IoT-enabled devices installed on transportation vehicles or vessels, such as GPS positioning systems and Geiger counters. This facilitates continuous monitoring of the transportation process. In the event of any anomalies during transportation—such as excessive radiation levels or damage to the transportation container—the onboard emergency communication systems will immediately alert relevant emergency response agencies and simultaneously transmit real-time data from the accident site (e.g., video footage and images) to the emergency command center, enabling prompt emergency actions. Upon completion of the transportation, the consignor, carrier, and consignee must consolidate and archive all data collected during the transportation process and report relevant information to the national nuclear safety regulatory authority [8].

However, despite the relatively stringent process of China's management approach for spent nuclear fuel transportation, it is fundamentally based on a client–server architecture. This traditional client–server architecture exhibits limitations in processing and storing large volumes of real-time data, resulting in inefficiencies in data sharing and management. Specifically, data are stored locally and accessed only when necessary, precluding real-time interaction across the system. Given the numerous stakeholders involved in the transportation process, ensuring safe and accurate transportation requires strict reliance on point-to-point approvals and precise system-wide data interaction. Within this framework, authority is centralized among a few entities (primarily regulators), granting them primary control over the entire system. Similar deficiencies are evident in nuclear spent fuel transportation management systems in other countries, including issues such as insufficient real-time data accuracy, lack of transparency, and erosion of public trust. For example, the 2014 accident at the Waste Isolation Pilot Plant (WIPP) in Carlsbad, New Mexico, United States, which was caused by incorrect container labeling and improper chemical filling, resulted in a chemical explosion that incurred substantial economic losses [10].

2.3. Problem of the Conflict Between Confidentiality and Transparency

Throughout the entire lifecycle of spent nuclear fuel—encompassing generation, transportation, storage, and final disposal—this material presents considerable risks that necessitate rigorous confidentiality protocols. The transportation of nuclear waste entails the handling of highly sensitive information, including the precise locations of containers, radiation dose levels, detailed transport routes, and security measures. Unauthorized disclosure of such information could result in significant security threats, including theft, sabotage, or potential terrorist activities. To address these risks, nations implement stringent access controls to critical information. For example, the Office for Nuclear Regulation (ONR) in Bootle, Merseyside, United Kingdom, requires carriers to submit detailed Transport Security Statements and ensures that only individuals who have undergone thorough security vetting are permitted access to sensitive nuclear data. Similarly, the United States Nuclear Regulatory Commission (NRC) enforces strict protective measures for confidential information, safeguards Information, and Sensitive Unclassified Non-Safeguards Information [11].

Concurrently, there has been a notable demand for transparency in nuclear waste management practices, particularly in the context of transportation, from both the public and regulatory authorities. The historical culture of secrecy within the nuclear sector, combined with concerns regarding environmental contamination, has significantly undermined public trust. In order to restore and maintain this trust, regulatory agencies are required to provide comprehensive disclosures regarding their oversight activities, the outcomes of compliance verifications, and the adherence of regulated entities to established regulatory standards. For instance, the U.S. Department of Energy (DOE) has faced criticism for its lack of transparency in the management of certain low-level waste disposal strategies, primarily due to its failure to effectively communicate the rationale behind its decisions. Enhancing transparency is deemed crucial for improving the decision-making process and cultivating trust among various stakeholders, including local communities, state regulatory bodies, and tribal nations [5]. Nevertheless, an inherent and difficult-to-reconcile tension exists between the imperative for regulatory transparency and the necessity to ensure the security and confidentiality of sensitive transportation data. Over-disclosure could compromise transportation safety, whereas over-securing such information might exacerbate public skepticism and erode trust.

3. Applying Blockchain to Nuclear Waste Tracking

This section introduces blockchain technology and examines its relevance to nuclear waste tracking. It begins by reviewing blockchain's characteristics and types, followed by its applications in supply chains and existing nuclear-related research projects such as SLAFKA and Sellafield DLT. Finally, it explains the feasibility of adopting a multi-layer blockchain architecture to address confidentiality-transparency conflicts.

3.1. Blockchain Characteristics

In 2008, Satoshi Nakamoto published "Bitcoin: A Peer-to-Peer Electronic Cash System," marking the inception of Bitcoin [12]. The underlying technology of Bitcoin, blockchain, has garnered significant attention due to its immutability, openness, and other distinctive features. At its core, blockchain is a distributed ledger system. Unlike traditional centralized ledgers (characterized by centralized transactions), blockchain does not rely on a single centralized storage entity. In a blockchain network, each participant (node) maintains a complete copy of the ledger. Blockchain consists of a series of blocks, where each block contains a specific number of transaction records. These records may include currency transfers (such as Bitcoin transactions), smart contract execution logs, and various other types of data. Blocks are interconnected through cryptographic techniques, primarily hash

algorithms. Each new block incorporates the hash value of the preceding block, forming a chain-like structure that ensures the immutability of the entire blockchain.

In addition to its immutability, blockchain also exhibits openness. Owing to this characteristic, various industries have shown keen interest in adopting blockchain technology, particularly consortium chains. However, in practical applications, organizations must balance data sharing with the protection of internal data while ensuring compliance with regulatory requirements. This necessitates addressing the challenge of enabling specific user groups within different organizations to access data at varying sensitivity levels appropriately. Failure to do so may result in the risk of data privacy breaches [13].

Blockchain can be categorized into three primary types: public chain, consortium chain, and private chain. Among these, the public chain enables anyone to participate in both the maintenance and reading of blockchain data, operates without control by any single institution, and ensures open and transparent data. However, it is characterized by relatively low transaction performance and a slower overall development pace, as exemplified by Bitcoin. The consortium chain, leveraging its specific organizational structure and consensus mechanism, enhances system performance and security while maintaining a certain degree of decentralization. Notable examples include Hyperledger Fabric and Openchain. The private chain offers a high level of data privacy protection but exhibits relatively limited openness. Table 1 provides a summary of the distinctions among public chain, consortium chain, and private chain across various dimensions, including access permissions, number of nodes, consensus mechanisms, and data privacy.

Table 1. Blockchain comparison.

Feature	Public Blockchain	Consortium Blockchain	Private Blockchain
Access Permissions	Open	Requires permission	Private
Nodes Number	Many	Fewer	Very few
Consensus Mechanism	PoW, PoS, etc.	PBFT, Raft, etc.	Customized
Data Privacy	Transparent	Semi-transparent	Private
Regulation	Unregulated	Regulatory Compliance *	Regulatory Compliance

[*] In the framework proposed in this article, Regulatory Compliance refers to the ability of the framework to operate under the nuclear safety and safeguards regulations, ensuring that the competent authorities can verify the monitoring.

3.2. Blockchain Application

3.2.1. Application of Blockchain in the Supply Chain

The unique attributes and advantages of blockchain technology can substantially enhance supply chain management. By increasing the transparency of tracking goods movement across the entire supply chain, blockchain is expected to significantly improve supply chain operations. This enhancement will lead to higher data accuracy and immutability, thereby reducing instances of fraud and minimizing errors. Furthermore, the automation of certain processes and the reduction in reliance on intermediaries will boost overall supply chain efficiency. Additionally, the unidirectional flow of information, which automatically encrypts all communications, enhances security when sensitive information is shared among parties [14]. Since blockchain transaction records are more accessible for querying, they exhibit enhanced auditability and transparency. In contrast to multi-layered approval processes, blockchain systems are more efficient and easier to manage.

Blockchain demonstrates greater applicability in the supply chain management of high-value and hazardous materials. Its decentralized and transparent nature plays a critical role in preventing theft, counterfeiting, and ensuring the authenticity of goods. Recently, Yi Dai et al. introduced a blockchain-based access control system tailored for

the dangerous goods supply chain [15]. By leveraging blockchain technology and smart contracts, this system offers a secure, efficient, and transparent access control solution for the supply chain of hazardous materials, thereby significantly enhancing the efficiency and security of supply chain operations. A substantial body of research supports the adoption of blockchain in high-value and hazardous material supply chains, thereby establishing a robust foundation for its application in the specific context of nuclear waste tracking. The key advantages often highlighted in scholarly literature—enhanced security, transparency, and traceability—are intrinsically aligned with the stringent requirements associated with nuclear waste management.

3.2.2. Current Research Progress

SLAFKA, officially launched in Helsinki, Finland on 10 March 2020, represents the world's first blockchain prototype explicitly tailored for nuclear safeguards. It was collaboratively developed by the Finnish Radiation and Nuclear Safety Authority (STUK, based in Helsinki), the Stimson Center (Washington, DC, USA) and the University of New South Wales (UNSW, Sydney, Australia) [16]. This system leverages distributed ledger technology (DLT) to streamline the reporting and inspection processes of nuclear materials, addressing challenges related to data integrity, cyber threats, and inefficiencies inherent in traditional reporting systems. By establishing a shared, immutable ledger, SLAFKA facilitates secure and transparent communication of safeguard data between operators and regulatory authorities. The prototype's design adheres to the requirements of Finland's current State System for Accounting and Control of Nuclear Material (SSAC) and aligns with the regulations set forth by the European Commission. Technically, SLAFKA is constructed on the Hyperledger Fabric platform, functioning as a private, permissioned blockchain. This architecture inherently satisfies the stringent demands for data confidentiality and access control in nuclear safeguards information management. Within SLAFKA's simulation environment, it encompasses three nuclear facility operators—two nuclear power plants and one deep geological repository—and three tiers of regulatory authorities representing national, regional, and international levels. The system abstracts actual nuclear material batches into digital assets with unique identifiers ("batches") for management and circulation within the distributed ledger. Functionally, SLAFKA successfully enables the input, storage, display, and output of nuclear material accounting information, fulfilling the reporting requirements of institutions such as IAEA and the European Atomic Energy Community (Euratom), including formats like ICR, PIL, and MBR. SLAFKA supports a comprehensive range of key nuclear material management transactions, encompassing material production, domestic and international transportation and receipt, nuclear conversion and loss, as well as changes in attributes or location and re-batching. These transactions meticulously document detailed batch attributes, including material balance areas (MBAs), key measurement points (KMPs), material form, container type, weight, and isotopic composition, among other critical parameters [16].

Despite its significant achievements, it is crucial to acknowledge that SLAFKA remains a proof-of-concept prototype at present. It relies on fictional data and has not been fully security-hardened for production environments. Additionally, it does not yet leverage all the advanced capabilities offered by Hyperledger Fabric, such as channels, private data collections, and endorsement policies. Its current scope primarily centers on fundamental nuclear material accounting and does not yet encompass the specific requirements of Additional Protocol (AP) reporting or the complex provisions of multinational nuclear cooperation agreements (NCAs).

A few years ago, the Sellafield DLT Field Lab in the UK collaborated with RKVST to investigate the potential of DLT for digitizing the tracking of nuclear waste data, leading to the establishment of the Sellafield DLT Field Lab project. As the largest nuclear decommissioning organization in the UK, Sellafield faced significant challenges in nuclear waste management and worker qualification management, necessitating improvements in productivity and cost reduction through digital transformation. The project was executed in two phases: the first phase identified two critical areas—nuclear waste tracking and worker qualification management—and engaged technical partners; the second phase involved RKVST and Condatis in developing prototype solutions. The project successfully enabled transparent tracking of nuclear waste, rapid verification of worker qualifications, minimized manual processes, and strengthened data security and audit capabilities [17].

These studies still offer opportunities for improvement in critical areas such as data integrity and network threats and have yet to fully address the specific requirements of complex cross-border nuclear cooperation. Building on the aforementioned research advancements, this paper aims to further investigate the potential applications of blockchain technology in tracking the transportation of spent nuclear fuel.

3.3. Multi-Layer Architecture in Blockchain Applications

Blockchain-based multi-layer architecture refers to a technical framework that divides data into different layers according to sensitivity, access permissions, and stakeholder needs, with each layer maintaining independent ledger logic but relying on cryptographic techniques (such as hash anchoring) for cross-layer verification. This architecture is distinct from the hierarchical architecture in IoT systems: the latter is a technology-oriented stratification based on functional modules (e.g., perception layer for data collection, network layer for transmission, as introduced in Section 4.1.3), while blockchain multi-layer architecture is a data-oriented stratification centered on "confidentiality-transparency balance". Existing studies have demonstrated the feasibility of multi-layer architectures in blockchain applications. For instance, in supply chain management, researchers proposed tiered data storage where core transaction data are stored in private layers accessible only to participants, while compliance data are shared in semi-public layers for regulators [15]. In nuclear-related fields, the SLAFKA prototype, though focused on material accounting, hinted at the potential of layered data management by separating operator data from regulatory data [16]. The Sellafield DLT Field Lab project also explored stratified access control for waste tracking data, distinguishing between operational logs and public statistics. These practices confirm that multi-layer architectures can effectively resolve conflicts between data privacy and shared needs, laying a foundation for their application in spent nuclear fuel transportation tracking.

4. Integrated System of Consortium Blockchain and IoT

This section presents the proposed integrated system that combines IoT sensors with consortium blockchain for secure and transparent nuclear fuel tracking. It details the selection of IoT sensors, compares blockchain-enabled tracking with traditional systems, explains the system's five-layer architecture, and addresses IoT device limitations. It further proposes a multi-layer consortium blockchain design for balancing confidentiality and transparency and introduces quantitative assessment indicators.

4.1. Integrated System of Blockchain and IoT

Designing a secure spent nuclear fuel tracking system requires the implementation of robust data collection technology. The IoT is particularly well-suited for integration into such systems due to its ability to facilitate real-time data collection. Unlike traditional computers, IoT devices are characterized by their extensive coverage despite having lim-

ited computational power. Numerous studies have explored the application of blockchain technology within the IoT ecosystem. A comprehensive review has examined the applications, challenges, and solutions associated with integrating blockchain technology into IoT systems, highlighting key issues such as resource constraints, data processing limitations, and privacy concerns, while also proposing viable approaches to address these challenges [18]. These studies provide a solid foundation for the integration of IoT with blockchain technology.

4.1.1. Selection of IoT Sensors

The type of IoT sensors selected determines the breadth and quality of data that can be collected. When monitoring the transportation of dangerous or sensitive materials, it is essential to select a diverse set of IoT sensors to ensure the effective collection of real-time data for integration into the blockchain. Below are the types of sensors that may be applicable:

- GPS trackers: Provide real-time geographical location data of transportation vehicles. For instance, the U.S. Department of Energy's Transportation Tracking and Communication System (TRANSCOM) uses satellite tracking to frequently provide location updates, once per minute [19].
- Radiation detectors: Ensure the integrity of spent nuclear fuel, monitor external radiation dose rates, and detect violations. For instance, by surrounding spent fuel barrels with SiLiF and SciFi sensor arrays, the status of spent fuel can be detected in real time [20].
- Temperature sensor: Monitors the environmental conditions and the thermal state of the packaging during transportation.
- Shock/vibration sensor: Detect physical impacts and drops during transportation.
- Anti-tampering sealed sensor: Prevents unauthorized damage and disassembly of spent fuel packaging.
- RFID tags: Radio Frequency Identification tags, which can be used for automatic identification and tracking of sensor data. They can enhance security, safety and service (3S) while providing real-time status and environmental data.

4.1.2. Comparative Analysis: IoT-Blockchain vs. Traditional Tracking Methods

Compared to traditional client–server tracking methods, which typically depend on centralized databases, manual reporting, and less precise monitoring, the integration of IoT and blockchain provides a shared distributed ledger. This ledger serves as a single source of truth and enables near real-time access for all authorized stakeholders, such as regulators, shippers, consignees, and emergency responders. As a result, spent fuel becomes fully transparent to regulators throughout its entire transportation lifecycle, effectively breaking down the information silos prevalent in traditional systems where data are often fragmented across multiple platforms [21]. The integration of the IoT and blockchain offers substantial advantages in auditability and traceability. Each transaction or data entry recorded on the blockchain is timestamped and cryptographically linked, creating a permanent, verifiable, and auditable event tracking record. This capability supports regulatory compliance checks and accident investigations while enabling end-to-end traceability of nuclear waste packaging from origin to final disposal. It effectively addresses limitations of traditional methods, such as manual logs, decentralized databases, or records susceptible to tampering or loss. In terms of efficiency and cost, this system automates data recording and verification (potentially through smart contracts), reduces dependency on intermediaries, and streamlines reporting processes. Moreover, real-time data availability enhances decision-making speed and quality. Studies on general supply chains [14] demonstrate that blockchain technology can significantly lower management costs.

Take the TRANSCOM Communication Center of the U.S. Department of Energy (DOE) as an example. TRANSCOM is an unclassified tracking and communication web application of the DOE, used to monitor the progress of special nuclear materials (domestic), foreign nuclear materials, transuranic waste, and any other authorized goods. Authorized TRANSCOM users (such as DOE shippers, carriers, state and local governments, and various federal agencies) can access the web application from their computers or any mobile devices. TRANSCOM is the traditional tracking system based on client–server mentioned above. Table 2 provides a comparison of key functions between the hypothetical integrated IoT-Blockchain system and the traditional tracking system TRANSCOM:

Table 2. TRANSCOM vs. IoT-Blockchain system.

Feature	TRANSCOM	IoT-Blockchain System
Data Immutability	Rely on conventional database security, access controls, audit logs.	Cryptographically enforced via hashing and consensus; tamper evident.
Real-time Multi-Sensor Data	Primarily GPS location and messaging; sensor integration via add-ons.	Designed for native integration of diverse real-time sensor data streams.
Decentralization	Typically centralized architecture.	Distributed ledger replicated across multiple authorized nodes.
Stakeholder Transparency	Access controlled by central authority.	Shared ledger accessible by all permissioned stakeholders; configurable transparency.
Audit Trail Verifiability	Relies on database logs; potentially alterable by administrators.	Permanent, time-stamped, cryptographically verifiable transaction history.
Long-term Integrity Assurance	Dependent on database longevity, backups, institutional continuity.	Enhanced resilience via distribution and cryptographic linking.
Resistance to Single Point Failure	Central server/database represents a potential single point of failure.	Distributed nature eliminates single points of failure for data records.
Trust Mechanism	Trust in the central authority (DOE) managing the system.	Through shared, immutable data and consensus protocols.

4.1.3. The Architecture of the IoT-Blockchain System

Figure 2 illustrates a nuclear spent fuel tracking system that integrates blockchain technology with the Internet of Things (IoT), enhancing the transparency and security of nuclear spent fuel management through dynamic monitoring and data sharing. The system's foundation is a blockchain-based smart contract platform, such as Ethereum or Hyperledger Fabric, which collaborates with IoT devices (e.g., RFID tags) to ensure comprehensive oversight throughout the entire lifecycle of nuclear spent fuel. Within this framework, IoT devices (as indicated by the RFID box in the figure) serve a critical function. These devices are strategically placed at key locations, including nuclear power plants, transportation hubs, reprocessing facilities, and geological storage sites, to continuously monitor the status of nuclear spent fuel containers. This includes core parameters such as temperature, humidity, radiation levels, and GPS location. Communication between IoT devices occurs via low-power wide-area networks, such as LoRa/LoRaWAN or LTE [22]. The collected data are uploaded to the blockchain system, ensuring their real-time availability and accuracy. IoT devices not only enable dynamic monitoring but also enhance the transparency of multi-party collaboration. For example, during transportation, IoT sensors continuously gather container status data and synchronize it in real time to the blockchain. This allows transportation companies, regulatory authorities, and destination facilities to simultaneously access the latest status information. Such an

information sharing mechanism ensures that all relevant parties maintain real-time awareness of the spent nuclear fuel's status, thereby strengthening the transparency and trustworthiness of the management process [8]. Once the data collected by IoT sensors are uploaded to the blockchain, they become permanently recorded and tamper-proof. This permanence ensures the authenticity and integrity of the information while providing verifiable public records for regulatory agencies and the public. For instance, when a geological storage node receives spent nuclear fuel, IoT devices verify whether the container status complies with safety standards and record the results on the blockchain, making them accessible for review by all relevant parties.

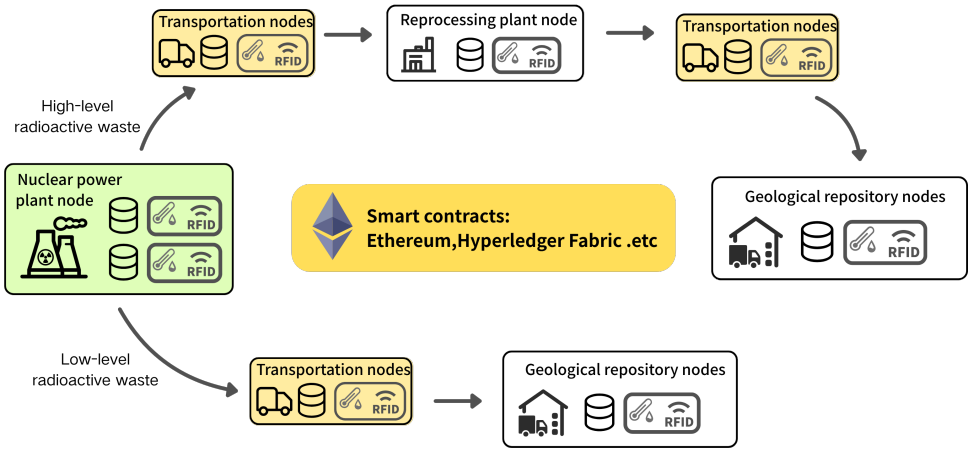

Figure 2. The nuclear spent fuel transportation process integrating blockchain and IoT.

To effectively manage the system's complexity and ensure its modularity and scalability, this architectural design employs a layered architecture pattern. This pattern is widely utilized in the development of IoT systems, with its primary advantage being the clear delineation of each component's functional scope and the facilitation of standardized interaction interfaces between layers, based on the general IoT architecture model [23]. As shown in Figure 3, the architecture of this system is divided into five layers. To more clearly demonstrate the technical features of the system, Figure 3 illustrates by explicitly showing the direction and type of data flow. The other parts of this article have provided a detailed explanation of the data flow.

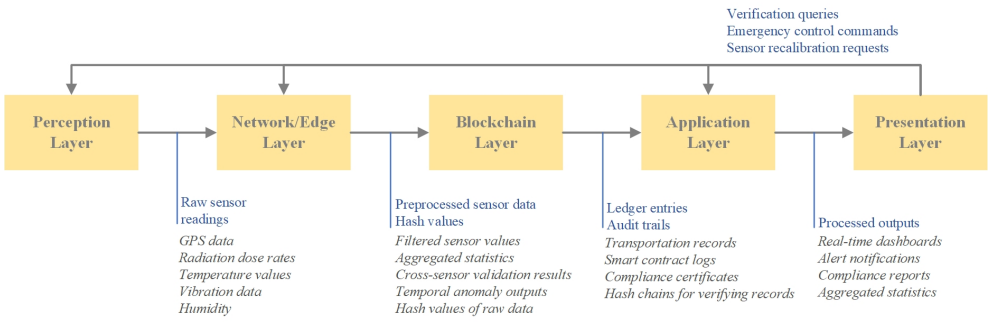

Figure 3. System hierarchical architecture and data flow.

1. Perception Layer: This layer consists of various IoT physical sensors (e.g., temperature, radiation, RFID, etc.) installed on nuclear waste transport containers or vehicles. These sensors are capable of collecting raw data in real time related to the container's location, environmental conditions, physical status, and identification information.
2. Network/Edge Layer: This layer is responsible for securely and reliably transmitting the data collected by the perception layer to the subsequent processing layers. It sup-

ports a wide range of communication protocols (both short-range and long-range) and network technologies (e.g., cellular networks, satellite communications). Additionally, it incorporates edge computing, a paradigm that performs computation at the network edge. By preprocessing, filtering, and aggregating data on gateway devices near the data source, edge computing reduces the volume of transmitted data, minimizes latency, and improves system responsiveness [24].

3. Blockchain Layer: This layer acts as the system's core trust layer, leveraging distributed ledger technology (specifically Hyperledger Fabric) to securely and immutably record verified transportation data. Moreover, smart contracts are deployed in this layer to execute predefined business logic, including data validation, status updates, access control enforcement, and alert triggering mechanisms.
4. Application Layer: Serving as an intermediate layer, this layer connects the blockchain layer with the presentation layer. It retrieves data from the blockchain ledger and processes it into formats that are accessible to users or external systems. Additionally, it provides API interfaces to enable seamless integration with external systems, including regulatory reporting systems and emergency response systems.
5. Presentation Layer: This layer serves as the interface through which users interact with the system. It delivers customized dashboards and advanced visualization tools tailored to the specific needs of different user roles, including shippers, carriers, regulatory agencies, and emergency response personnel. Examples of these tools include sensor data charts, historical audit trails, and real-time alert notifications.

4.1.4. Limitations of IoT Devices and Solutions

In the blockchain system based on the IoT, the stability of IoT sensors is of utmost importance. Sensors are prone to sensor drift during long-term operation, and their measured values will gradually deviate from the true values as environmental conditions or device aging occur. If erroneous data are written into the blockchain, due to its immutability, it will inevitably lead to cumulative risks. Our solution is to introduce two verification mechanisms:

- Multi-sensor cross-validation mechanism: Firstly, various types of heterogeneous sensors were deployed in the same transportation link, such as Global positioning systems, accelerometers, and radiation detectors. Tomer Golomb et al. once proposed a lightweight distributed anomaly detection framework called CIoTA, which enables multiple IoT devices to collaboratively update the trusted anomaly detection model through blockchain [25]. This model can be referred to, and consistency verification can be carried out through the correlation of different physical quantities. For instance, when the Global Positioning System data indicate that the transport container is at rest, if the accelerometer continuously records the vibration, it can be determined that at least one group of sensors is abnormal. For instance, cross-validation of radiation dose issues using micro radiation detectors can prevent problems such as numerical jumps and drifts of individual detectors.
- Temporal correlation verification mechanism: According to the literature review work on IoT time series anomaly detection solutions made by Arnaldo Sgueglia et al. [26], it is feasible to conduct time-dependent verification mechanisms for the IoT. The system conducts trend analysis on the historical data of the same sensor. If its output undergoes sudden changes that do not conform to physical laws or long-term drift within a short period of time, an abnormal alarm will be triggered and a secondary confirmation will be carried out at the edge node layer.

The system completes the computing and comparison work (Edge computing technology) in the Edge Layer mentioned in the text, and submits the hash value of the "comparison data" or "verification result" to the blockchain. This can not only ensure that the off-chain result is trustworthy and immutable, but also reduce the burden on the chain.

4.2. Consortium Chain: Balancing Confidentiality and Regulatory Transparency with Multi-Layer Architecture

4.2.1. Demand for Data Management

In order to effectively establish a robust tracking system for the transportation of nuclear waste, it is imperative to undertake a comprehensive examination of the unique and frequently conflicting data management requirements associated with this field. These requirements include the implementation of rigorous confidentiality protocols for highly sensitive information, alongside the need for regulatory compliance and transparency.

The following bullet points describe the highly sensitive information involved in the nuclear waste transportation process, which is governed by the confidentiality protocols of the system.

1. Real-time container location: Provide precise GPS coordinate data to prevent potential interception or attacks during transportation.
2. Radiation measurement: Monitor real-time or historical radiation levels outside and outside the container, which may indicate material properties or container integrity.
3. Transportation route and schedule: It is essential to provide comprehensive details regarding planned routes, alternative routes, departure times, and estimated arrival times. This information is vital for security planning purposes, and any unauthorized dissemination of such data could substantially elevate associated risks.
4. Security details: Specify security systems, procedures, personnel deployment, and emergency response plans outlined in the Transport Security Statement (TSS).
5. Personnel information: Include identities, security clearance levels, and specific responsibilities of individuals involved in transportation operations.
6. National security information: This may include classified information, restricted data, protective measures, or sensitive yet unclassified information that is intricately associated with the physical security of nuclear materials or facilities.
7. Handover points and procedures: Sensitive operational details such as specific handover locations, times, and confirmation protocols for transferring responsibility.

In the domain of nuclear waste management, there exists a considerable necessity for regulatory transparency. Attaining this transparency is crucial for cultivating and maintaining public trust, in addition to ensuring accountability. On 7 December 1993, the U.S. Department of Energy (DoE) introduced its "Openness Initiative," which aimed to bolster public confidence by augmenting transparency and disseminating extensive information regarding all departmental activities [27]. This initiative set a benchmark for the disclosure of nuclear-related data and information, thereby incorporating the public as active stakeholders in the regulatory process. Regulatory authorities are expected to disclose specific types of information to the public, local communities, state governments, tribal nations and other stakeholders. This typically includes regulatory activities and processes, compliance status, regulatory enforcement actions, anonymous data, etc. According to the latest publication of the International Atomic Energy Agency on the safety of the transport of nuclear and other radioactive materials (2024) [28], Table 3 assesses the requirements for confidentiality and transparency in the transportation of nuclear waste.

The analysis of these conflict points highlights a critical insight: the solution cannot simply be "fully open" or "fully closed." The system design must be capable of distinguishing among different types of data, varying time dimensions (real-time versus historical/aggregate data), and diverse audiences (operators, regulators, and the public).

This nuanced differentiation serves as the cornerstone of a multi-layered architecture design. Furthermore, merely granting data access rights is inadequate; in light of trust deficits, the system must also provide mechanisms to verify the integrity and authenticity of disclosed information, such as through tamper-proof records and cryptographic proofs—capabilities that represent the core strengths of blockchain technology.

Table 3. Requirements for confidentiality and transparency.

Data Category	Confidentiality	Transparency	Conflict Points
Physical Location/Path	High	Low	Balance security monitoring with tracking needs.
Radiation dosage	High	Low	Prove compliance without revealing sensitive data patterns.
Security Programs	High	Low	Show security plan approval without revealing vulnerabilities.
Personnel Identity	High	Low	Verify personnel qualifications without exposing private info.
Interaction Records	Medium	Low	Prove handover occurred without revealing sensitive operational details.
Compliance Audit Reports	Medium	High	Issue credible audits while protecting sensitive operational data within them.
Regulatory Decision	Low	High	Disclose decisions/processes while protecting confidential info/trade secrets.
Aggregated Operational Statistics	Low	High	Ensure aggregated data are reliable and free of sensitive details.
Environmental Impact Statements	Low	High	Ensure disclosed EIS is complete, accurate, and decisions are justified.

4.2.2. Multi-Layer Architecture Based on Consortium Blockchain

As elaborated in Section 3.3, blockchain multi-layer architecture enables data-oriented stratification, which is uniquely suited to address the confidentiality-transparency conflict in nuclear waste transportation. Unlike the IoT hierarchical architecture (focused on technical functional division), this multi-layer architecture in consortium blockchain is designed to classify data by sensitivity and stakeholder roles, achieving precise control over information visibility. A consortium chain is a type of blockchain that lies between public and private chains, jointly managed and maintained by a pre-selected group of organizations. It combines the controllability of private chains with some decentralized features of public chains, making it suitable for scenarios where multiple parties collaborate but require controlled data sharing [29]. Its core features include permissioned access, identity management via MSPs and PKI, controlled transparency, and efficient consensus

mechanisms (e.g., PBFT, Raft), which align with the needs of nuclear waste transportation tracking (well-defined participants, strict access control, and multi-party trust). By integrating the consortium chain with multi-layer architecture, the system achieves hierarchical data management as follows:

- Operational Layer: The most strictly permission-controlled tier, recording real-time sensitive operational data (e.g., precise GPS location, radiation dose, detailed routes, security logs). Access is restricted to authorized personnel under the "need-to-know" principle. Using Hyperledger Fabric's Private Data Collections (PDCs), sensitive data are transmitted point-to-point among authorized nodes, with only data hashes anchored on the main ledger for verification.
- Supervisory Layer: A bridge between confidentiality and transparency, storing verified compliance information (e.g., regulatory approval records, audit logs). Regulatory authorities access this layer via privacy-enhancing technologies like Zero-Knowledge Proofs (ZKPs), which demonstrate compliance without exposing underlying operational details.
- Controlled Transparency: Designed for public transparency, containing aggregated, anonymized data (e.g., transportation statistics, regulatory document links) and hash values of supervisory layer data for authentication. Access is public and read-only, ensuring verifiability while protecting sensitivity.

As shown in Table 4, through this layered design, the system achieves precise management of information visibility and access rights based on the nature of the data and its intended audience, effectively balancing the high confidentiality required for secure nuclear material transportation with the regulatory transparency needed to build public trust.

Table 4. Specific layering of the blockchain layer.

Layer Level	Purpose	Key Data Types	Access Restrictions
Operation Layer	Record real-time sensitive operation data to ensure transportation safety and efficiency	Raw sensor data, detailed routes, security logs, etc.	High degree of restriction, based on tasks and permissions, need "need to know"
Supervision Layer	Store verification of compliance information, supervision activity records, etc.	Compliance certificates, supervision approval records, etc.	Permissioned access, based on roles and policies
Public Layer	Provide publicly verifiable information to meet transparency and establish trust	Aggregated statistical data, anonymized compliance summaries, regulatory data layer hash	Wide read access, strict control over write permissions

4.3. Quantitative Assessment

To objectively assess the effectiveness of the proposed multi-layer data chain system based on consortium blockchain for nuclear waste transportation tracking, a comprehensive evaluation framework must be established. Subsequently, blockchain benchmarking tools such as Blockbench and Hyperledger Caliper can be employed to conduct a thorough performance evaluation of the blockchain [30].

The evaluation framework should not only focus on the functional realization of the system but also quantify its performance in balancing confidentiality and transparency, a core objective. Additionally, it must comprehensively measure the system's performance, resource consumption, and security. The primary dimension of the evaluation is the effectiveness of data access control. Given the extreme sensitivity of nuclear material transportation data, the system must rigorously enforce predefined access policies. Evaluation indicators should include the rejection rate of unauthorized access attempts (target: 100%) and the success rate of granting authorized access (target: 100%), which can be assessed through log analysis and simulated penetration testing. Ensuring that only entities with appropriate permissions and adhering to the "need-to-know" principle can access specific data layers, particularly the operational layer, constitutes the cornerstone of system security.

The assessment framework must measure the transparency and verifiability of regulatory information, which are critical to building public trust. Key indicators include the timeliness of public layer information release (e.g., the time delay from the completion of a regulatory event to public disclosure, with target values defined by service level agreements) and the success rate of verifying public data. The latter involves simulating an audit process to confirm whether public statements, such as aggregated reports, can be reliably traced back to the records in the regulatory layer using their hash values or proof references, aiming for a verification success rate approaching 100%.

System performance is a critical factor in assessing its practical usability. Key performance indicators include transaction throughput (TPS) and transaction latency. Throughput quantifies the system's capacity to process critical transactions, such as sensor data recording and compliance proof verification, within a given time frame. Latency measures the duration from transaction submission to its final confirmation. These metrics should be evaluated under simulated real-world network conditions and workloads using benchmarking tools like Hyperledger Caliper, and compared against expected load requirements and baseline systems. For example, the target may involve handling the aggregate rate of all sensor data during peak hours, while ensuring that latency satisfies near real-time monitoring needs.

Additionally, system overhead must be taken into account, including data storage overhead (e.g., ledger size growth rate) and computational overhead (e.g., CPU and memory usage). Monitoring these resource consumption metrics ensures the system's sustainable operation and prevents resource bottlenecks, particularly when processing high volumes of transactions or executing complex computations. Table 5 lists the key evaluation indicators.

Table 5. Key evaluation indicators.

Evaluation Dimension	Index	Description	Emphasis
Access Control Effectiveness	Unautorized Access Attempt Rejection Rate	System's ability to block unauthorized access	Strictness of security policy enforcement
Transparency and Verifiability	Public Data Verifiability Success Rate	Success rate of traceable verification for public information	Credibility of regulatory information and audit support
System Performance	Transaction Throughput (TPS)	Number of critical transactions successfully processed per unit time	Processing capability and efficiency
	Transaction Latency	Time from transaction submission to confirmation	Responsiveness and real-time performance

Table 5. *Cont.*

Evaluation Dimension	Index	Description	Emphasis
System Overhead	Computational Overhead (CPU/Memory Usage Rate)	Computational resources required to run system components	Resource efficiency and scalability
Security and Resilience	Tamper Attempt Detection Rate	Proportion of detected tamper attempts on submitted data	Data integrity assurance
	ZKP Soundness Failure Rate (if applicable)	Proportion of invalid ZKPs rejected by verifiers	Reliability of cryptographic proofs
	System Availability (under DoS/Failure)	Ability to maintain service during attacks or failures	System robustness and reliability

4.4. Core Algorithmic Workflow

At the implementation level, the core process of the proposed blockchain–IoT framework involves the collection, preprocessing, validation, and recording of nuclear fuel transportation data across multiple layers. This subsection details the algorithmic logic governing the edge layer, blockchain layer, and application layer to ensure data integrity, privacy, and traceability throughout the lifecycle of spent fuel tracking.

Figure 4 depicts the intricate algorithmic workflow of the proposed IoT–Blockchain system for spent nuclear fuel transportation. This figure obviously showcases the direction of data flow among modules, thereby complementing the pseudocode presented in this section. The workflow commences at the perception layer, where heterogeneous IoT sensors continuously generate raw data. These data encompass GPS trajectories, radiation dose rates, container temperature, vibration status, and RFID-based package identification. These raw data streams are then transmitted to the edge node, which undertakes preprocessing tasks such as noise filtering, cross-sensor consistency checks, and temporal correlation validation. Based on the outcomes of anomaly detection, the edge node determines the subsequent data flow. In the event that an anomaly is detected, the original sensor data are encrypted and uploaded to off-chain storage, with only the corresponding hash being anchored on the blockchain. In all scenarios, the edge node generates a transaction that includes the filtered summary, metadata, timestamp, anomaly score, and the data hash. This transaction is subsequently submitted to the blockchain layer. Within the blockchain layer, smart contracts validate and immutably record the incoming data. When regulators request compliance verification, the system utilizes the ZKP module. This module generates a ZKP based on the private dataset, demonstrating compliance with regulatory requirements without disclosing sensitive operational data. The verification results are then broadcast as blockchain events. The application layer subscribes to blockchain events and updates dashboards with alerts, audit logs, and compliance records. These outputs are tailored for different stakeholders: operators receive anomaly notifications, regulators verify compliance proofs, and the public accesses anonymized summaries. Ultimately, the application layer might send out downlink feedback commands, such as modifying transport parameters or initiating emergency protocols. These commands are signed, transmitted via MQTT, and validated by the edge nodes before execution. The results of the executed actions are written back to the blockchain, closing the operational loop.

This integrated workflow ensures that every step—from data collection and anomaly detection to compliance proof and control feedback—is both tamper-proof and verifiable, effectively balancing confidentiality and transparency in spent nuclear fuel transportation.

4.4.1. Edge-Level Preprocessing and Validation Pseudocode

To clarify the workflow at the edge level, Algorithm 1 presents the procedure executed by edge nodes for sensor data preprocessing, anomaly detection, and blockchain submission. It demonstrates how raw IoT data are filtered, verified, and anchored to the blockchain through hash computation, ensuring data integrity and traceability at the very first stage of the system.

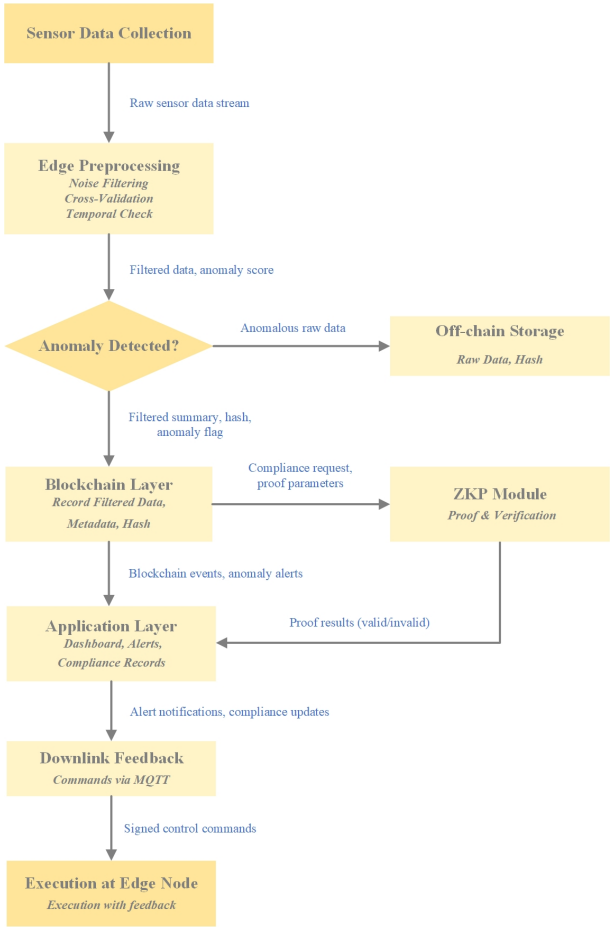

Figure 4. Detailed algorithmic workflow of the system.

Algorithm 1: Edge Node Data Processing and Blockchain Recording.

Input: Sensor readings $S = \{GPS, Radiation, Temp, Accel, RFID\}$
Output: Blockchain transaction tx
while *system running* **do**
  $raw \leftarrow$ CollectSensorData(S);
  $filtered \leftarrow$ NoiseFilter(raw);
  $anomaly \leftarrow$ AnomalyDetection($filtered$);
  $hash \leftarrow$ SHA256(raw);
  $tx \leftarrow \{filtered, hash, anomaly, timestamp\}$;
  if $anomaly = TRUE$ **then**
    $cid \leftarrow$ IPFS_Upload(Encrypt(raw));
    AddToPrivateData(cid);
  Fabric_Submit(tx);
  if $anomaly = TRUE$ **then**
    TriggerAlert(tx);

4.4.2. Chaincode Pseudocode

After the edge-level data are transmitted to the blockchain, the core smart contract logic governs data storage and validation. As shown in Algorithm 2, the chaincode functions handle public and private data transactions, compliance proof verification, and control command issuance. This algorithm encapsulates the essential on-chain mechanisms that guarantee secure, automated, and auditable interactions among network participants.

Algorithm 2: Core Chaincode Functions for Sensor Data Management.

Input: Transaction request *req* from edge/application nodes
Output: Blockchain state update or event emission
Function `submitSummary`(*tx_public*)**:**
  key ← "summary:" + tx_public.edge_id + ":" + tx_public.timestamp;
  PutState(key, tx_public);
  EmitEvent("SummaryRecorded", {*key*, *anomaly* : *tx_public.anomaly*});
  return OK;
Function `submitPrivatePayload`(*collection*, *pdc_payload*)**:**
  PutPrivateData(collection, "pdc:" + pdc_payload.cid, pdc_payload);
  EmitEvent("PrivateDataStored", {*cid_hash* : *SHA*256(*pdc_payload.cid*)});
  return OK;
Function `verifyComplianceProof`(*proof*, *public_inputs*)**:**
  ok ← VerifyZKP(proof, public_inputs);
  record ← {proof_status: ok, verifier: clientID, ts: Now()};
  PutState("zkp:" + Hash(public_inputs), record);
  EmitEvent("ZKPVerified", {*hash* : *Hash*(*public_inputs*), *ok*});
  return ok;
Function `submitControlCommand`(*target_id*, *cmd*)**:**
  if *not Authorized(clientID)* **then**
    return Error("unauthorized");
  PutState("cmd:" + target_id + ":" + Now(), {*payload* : *cmd*, *issuer* : *clientID*});
  EmitEvent("ControlCommand", {*target_id*, *issuer* : *clientID*});
  return OK;

4.4.3. Zkp Proof and Verification Pseudocode

To preserve confidentiality while enabling verifiable compliance, the proposed framework integrates a ZKP mechanism. Algorithm 3 outlines the process of generating and verifying ZKPs, which allows regulators to confirm compliance without accessing sensitive operational data. This algorithm enhances privacy protection while maintaining full auditability across layers of the system.

4.4.4. Application and Feedback

The final component of the workflow concerns real-time communication and feedback between the application and edge layers. Algorithm 4 illustrates how blockchain events are processed at the application layer to update dashboards, issue control commands, and synchronize downstream actions. This algorithm ensures closed-loop responsiveness, enabling timely alerts and coordinated control during nuclear fuel transportation.

Algorithm 3: ZKP Generation and Verification.

Input: Private sensor dataset D, public statement P
Output: Boolean result of proof verification
Function `GenerateComplianceProof(`D, P`)`**:**
  witness ← ComputeWitness(D, P);
  proof ← ZK_Prove(witness, proving_key);
  Fabric_Submit(chaincode="sensorCC", func="verifyComplianceProof",
   args={proof, P});
  return proof;
Function `VerifyZKP(`$proof, P$`)`**:**
  ok ← ZK_Verify(proof, verification_key, P);
  PutState("zkp:" + Hash(P), {status: ok, ts: Now()});
  EmitEvent("ZKPVerified", {hash: Hash(P), ok});
  return ok;

Algorithm 4: Application Layer Event Handling and Downstream Feedback.

Input: Blockchain events E, control command *cmd*
Output: Alerts to dashboard or feedback to edge nodes
while *true* **do**
  event ← WaitForEvent(E);
  if *event.type == "SummaryRecorded"* ***and*** *event.anomaly == TRUE* **then**
    NotifyDashboard(event);
  if *event.type == "ZKPVerified"* **then**
    UpdateComplianceRecord(event);
  if *event.type == "ControlCommand"* **then**
    cmd ← GetState(event.key);
    signed_cmd ← Sign(AppPrivKey, cmd);
    MQTT_Publish("edge/" + event.target_id, {*cmd*, *signed_cmd*});
Function `EdgeHandleCommand(`msg`)`**:**
  if *VerifySignature(msg.signed_cmd, AppPubKey)* **then**
    ExecuteCommand(msg.cmd);
    Ack ← {cmd_id, status: "executed", ts: Now()};
    Fabric_Submit("sensorCC", "submitExecutionAck", Ack);
  else
    Log("Invalid command signature");

4.5. Reproducible Experimental Configuration

To facilitate subsequent experimental verification and reproduction, this study provides a detailed and reproducible experimental configuration and procedure here. Please ensure that all experiments are conducted in an isolated local area network environment, and the data and commands are simulation or non-sensitive samples from the laboratory.

4.5.1. Experimental Hierarchical Architecture Planning

- Perception layer (analog/physical sensors): 100 sensor terminals (expandable to over 1000) are distributed and installed in a simulated or real manner on the container model.
- Edge nodes: One edge gateway (Raspberry Pi 4 or NVIDIA Jetson Nano) is equipped for every 10 to 50 sensors to perform preprocessing and local validation.

- Blockchain network: Built with Hyperledger Fabric 2.x (permissioned), it includes three organizations (Operator, Regulator, and Transit Country), each with two peers. The Orderer uses the Raft consensus mechanism (with three orderer instances). To support the private data layer, Fabric Private Data Collections (PDCs) are utilized.
- Off-chain storage: Use IPFS or CouchDB to store the original large files/timeseries data, and the blockchain only writes the summary hash and metadata.
- Application and perception Layer: One or more servers run the backend (Node/Go), and the frontend Dashboard (React) displays data and alerts.

4.5.2. Hardware and Software List

Table 6 shows the hardware list.

Table 6. Experimental sensor configuration (model and parameters).

Sensor Type	Model	Key Parameters
GPS	u-blox NEO-M8N	Update rate 1–5 Hz; Accuracy < 2.5 m CEP; UART/I^2C/USB interface
Radiation Detector	LND 712 Geiger tube	Range: 0.01–1000 μSv/h; Sample rate 0.5–1 Hz (spectrum window 1–10 s)
Temperature	DS18B20	Range -55 to $+125$ °C; Accuracy ± 0.5 °C; Resolution 9–12 bit; 0.5–1 Hz
Accelerometer	ADXL345	Range ± 16 g; Resolution 13-bit; Sample rate 50–200 Hz; I^2C/SPI interface
RFID Seal	NXP UCODE DNA	UHF 860–960 MHz; Tamper-evident; Trigger event "seal-broken"

The following is the software list.

- Edge node: Raspberry Pi 4 (4GB) or Jetson Nano (4GB), operating system Linux (Ubuntu 20.04 LTS).
- Gateway communication: MQTT Broker (Eclipse Mosquitto), TLS encryption.
- Blockchain platform: Hyperledger Fabric 2.x, Fabric CA. Chaincode is written in Go or Node.
- ZKP prototype (if needed): ZoKrates (for generating and verifying simple ZKP prototypes) or other zkSNARK toolchains.
- Performance testing tools: Hyperledger Caliper (for testing TPS, latency, etc.), Blockbench (optional).
- Logging/Monitoring: Prometheus + Grafana, cAdvisor (for monitoring CPU/Memory).

4.5.3. Brief Steps for Experiment Replication

1. Deploy the Fabric network (3 orgs × 2 peers, 3 orderers Raft), configure the channel and PDC.
2. Deploy chaincode (sensor summary, compliance proof, alert).
3. Start the MQTT Broker and the edge node data collection simulator (or real sensors), and the edge node will perform preprocessing logic and invoke the blockchain SDK to upload to the chain (or submit the hash).
4. Run the scenario script with Caliper to collect TPS/latency/resource logs.
5. Check the on-chain logs, ZKP verification results, and Dashboard alerts for injected abnormal events.

4.5.4. Performance Testing Scenarios and Steps

1. Scenario A (Functional Validation): 100 sensors, with the edge device uploading a summary transaction every 5 s; inject five anomalies (radiation threshold exceeded or

tamper-evident event), and verify the following: if the smart contract triggers an alert, if a verifiable log is produced on-chain, and validate the ZKP process.
2. Scenario B (Baseline Performance): 100 virtual sensors, 1 Hz, where each record is packaged as 1 tx (or merged into a batch tx). Measure TPS, Tx latency (submission to block height), CPU/Memory, and ledger growth rate.
3. Scenario C (Stress Test) 1000 virtual sensors with a peak burst (bursting 10,000 writes). Evaluate the system's throughput, latency, and availability under high concurrency.

Execution Tool: Write scripts using Hyperledger Caliper to define the transaction types (sensor summary, compliance proof, alert), and run each scenario three times to take the average.

4.5.5. Evaluation Metrics and Judgment Criteria

1. Functional Correctness: 100% of anomaly events are detected by the edge device and generate corresponding records on-chain; regulators can verify compliance using ZKP without accessing raw data (Proof success rate $\geq$ 99%).
2. Access Control: Simulating unauthorized subjects attempting to access private data, the rejection rate should be 100%.
3. Performance: In the baseline scenario (100 sensors in 1Hz), the target TPS should be maintained at $\geq$100 TPS, and the average confirmation latency (submission to block) should be $<$2 s (can be relaxed based on actual network/hardware).
4. Resource Consumption: Single peer CPU utilization should be $<$70%, and the daily ledger growth rate must be controllable (e.g., $<$5 GB/day, depending on the upload strategy).
5. Robustness: In the event of a single peer failure, the system should remain available, providing service through other peers and complete data consistency verification after the failed peer is restored.

5. Performance Evaluation and Security Analysis

This section evaluates the proposed framework by comparing it against existing systems in terms of performance and security. It also provides two real-world case studies to demonstrate how the framework can improve cross-border regulatory collaboration and rebuild public trust in spent fuel transportation.

5.1. Comparison with SLAFKA

SLAFKA employs a Hyperledger Fabric prototype to prioritize regulatory data sharing but exhibits limitations in scalability (due to unoptimized chain loads) and lacks support for real-time IoT sensor integration. In contrast, the proposed framework introduces edge computing at the edge layer, offloading computational overhead from the blockchain and improving end-to-end system throughput. From a security standpoint, the framework implements a hierarchical data structure (operational layer, supervision layer, public layer) coupled with smart contract-driven access control. This design enables fine-grained permission management for transporters, regulators, and public stakeholders, resolving the inherent trade-off between sensitive nuclear data confidentiality and transparency more robustly than SLAFKA's rudimentary access mechanisms.

5.2. Comparison with Sellafield DLT Field Lab

The Sellafield DLT Field Lab leans towards proof of concept, mainly testing the feasibility of putting material transportation data on the chain, without a systematic security analysis. The framework integrated consortium blockchain and IoT extends this work by the following:

- Performance Innovation: Adopt a consortium blockchain that complies with regulatory requirements, and at the same time deeply integrate IoT sensors with the blockchain. This ensures real-time, tamper-proof data ingestion, going beyond the laboratory's static data-centric approach.
- Security Maturity: The framework constructed in this study has achieved a deep integration of IoT sensors and blockchain technology, ensuring that transportation data are uploaded to the chain in real time in an immutable manner. This design ensures the authenticity and integrity of information from the data source. At the same time, it introduces multiple verification mechanisms in the IoT to prevent sudden failures in the IoT.

5.3. Comparison with TRANSCOM

TRANSCOM is a centralized system for monitoring nuclear transport; however, it is inherently susceptible to single-point failures, vulnerable to data tampering, and constrained by limited capabilities for transparent and auditable operations.

- Performance Evolution: Replacing centralization with a consortium blockchain + multi-party consensus architecture, enabling real-time cross-organization verification and auditability. This distributed model maintains high throughput while eliminating TRANSCOM's latency and scalability bottlenecks.
- Security Upgrade: By leveraging distributed ledger technology to replicate data among authorized nodes, the reliance on a single central authority is reduced. The consensus mechanism dynamically builds trust, reducing the inherent tampering risk of the TRANSCOM monolithic architecture.

5.4. Two Real-Time Cases

5.4.1. A Case of Multi-Subject Regulatory Collaboration

Consider a scenario where European nuclear energy operators are required to transport spent nuclear fuel generated by Finnish nuclear power plants to reprocessing facilities located in France. This transportation process must adhere to the Euratom nuclear safeguards regulations, the international standards set by the IAEA [31], as well as the national sovereignty and security requirements imposed by transit countries such as Sweden and Germany. As a result, the regulatory framework governing this activity constitutes a complex, cross-regional system characterized by multiple legal regimes and the involvement of numerous stakeholders.

This study proposes an architecture scheme based on the IoT and the consortium blockchain. Radiation detectors and high-precision GPS sensors are deployed on the transportation vehicles. After being verified through edge computing, the data are pushed in real time to the entry layer of the consortium blockchain, achieving the transformation from the traditional "offline reporting" to "online dynamic monitoring".

The application of the consortium blockchain can solve the problem of regulatory conflicts and has established a three-level architecture consisting of the Operation Layer, Supervision Layer and Public Layer. In this framework, the operator stores all sensitive data in the Operation Layer and generates compliance certificates to Euratom, IAEA and transit country nodes through ZKP technology. The regulatory authorities only need to verify the validity of this certificate to complete the audit, without accessing the original data.

5.4.2. A Case of Rebuilding Public Trust

A retired nuclear power plant in Japan needs to transfer spent fuel storage containers to an intermediate storage facility. The "Fukushima nuclear accident" occurred in 2011, and two of the significant causes of the accident were the lack of safety culture and the absence

of supervision [32]. Therefore, the local community in this case suffered an "institutional trust trauma" regarding the safety of the transportation. The public strongly demanded "secure evidence that can be independently verified" and formed a demand for "regulatory transparency".

The traditional approach has primarily involved the public relying on centralized statements issued by operators or regulatory agencies. However, the absence of independent verification mechanisms may give rise to public skepticism regarding the potential concealment of risks by these entities. Secondly, the verification threshold is high. Even if the monitoring data are made public, the interpretation of the original sensing data (such as radiation waveforms, GPS trajectories) is very difficult. Some scholars in South Korea, through analyzing public inquiries and public opinions, found that the public has difficulty in interpreting nuclear radiation [33]. This indicates that, even if the data are made public, ordinary residents find it difficult to effectively judge the safety situation.

This architecture employs the entire process perception and closed-loop technology of the IoT. Transport vehicles are equipped with multiple sensors to achieve a closed-loop mechanism of "IoT sampling - edge computing - on-chain evidence storage". Once the monitoring data exceeds the safety threshold (for example, the radiation dose rate exceeds 10 μSv/h), the smart contract will automatically trigger on-chain alerts and emergency response measures, thereby enhancing data transparency and public trust.

The trust-down mechanism of the consortium blockchain cryptography is based on ZKP technology, generating "non-interactive secure proofs", such as "the entire transportation process did not enter the restricted area" and "the radiation dose rate was always compliant" and other security statements. This proof only contains "verification conclusion" and "cryptographic evidence", completely hiding the sensitive original data. At the same time, the public can call the smart contract on the chain through the client function and verify the authenticity of the proof without requiring knowledge of cryptography, achieving the goal of converting "institutional endorsement" into "mathematical credibility".

6. Conclusions

This paper proposes a multi-layer architecture integrating blockchain and the IoT, designed to enable comprehensive tracking and management throughout the entire lifecycle of spent nuclear fuel transportation. By leveraging the immutability and distributed nature of blockchain, the automation provided by smart contracts, and the real-time data acquisition capabilities of IoT, the system effectively tackles key challenges in current spent nuclear fuel transportation management, including insufficient data transparency, stringent confidentiality requirements, and the lack of trust among collaborating parties. The hierarchical architecture in the system design successfully balances the conflicting demands of data confidentiality and regulatory transparency during transportation while fulfilling stringent security requirements. Furthermore, this paper establishes evaluation criteria for critical aspects such as data access control, transparency verification, transaction throughput, and latency. Overall, this research introduces an innovative technical framework for spent nuclear fuel transportation management, significantly improving the safety, transparency, and efficiency of the process.

Author Contributions: Conceptualization, Z.Z.; methodology, Y.X. and Z.Z.; validation, Z.Z., W.Y. and Y.W.; investigation, Y.X. and Z.Z.; resources, Z.Z.; data curation, Y.X. and Z.Z.; writing—original draft preparation, Y.X. ; writing—review and editing, Z.Z., W.Y. and Y.W.; visualization, Y.X.; supervision, Z.Z.; project administration, Z.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Please contact the corresponding author for the data.

Acknowledgments: The authors would like to acknowledge the support of the undergraduate final year project programme at Lancaster University College, Beijing Jiaotong University.

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

References

1. Esser, M.; Borremans, A.; Dubgorn, A.; Shaban, A. Nuclear Waste Transportation: Quality Assurance and Control. *Transp. Res. Procedia* **2021**, *54*, 871–882. [CrossRef]
2. International Atomic Energy Agency. Incident and Trafficking Database (ITDB), 2019. Available online: https://www.iaea.org/resources/databases/itdb. (accessed on 12 October 2025)
3. Hunt, O.; Mladineo, S.V. Deterring Nuclear and Radiological Material Theft, Sabotage, or Illicit Trafficking; Pacific Northwest National Laboratory: Washington, D.C., USA, and Vienna, Austria, 23 May 2023. Available online: https://resources.inmm.org/sites/default/files/2023-07/finalpaper_321_0502125504.pdf (accessed on 12 October 2025).
4. Du, J.; Zhu, X.. Regulatory Transparency and Citizen Support for Government Decisions: Evidence from Nuclear Power Acceptance in China. *J. Environ. Policy Plan.* **2023**, *25*, 766–780. [CrossRef]
5. OECD; Nuclear Energy Agency. *Transparency of Nuclear Regulatory Activities. Technical Report. Nuclear Regulation. Workshop Proceedings, Tokyo and Tokai-Mura, Japan, 22–24 May 2007*; Organisation for Economic Co-operation and Development and Nuclear Energy Agency: Paris, France, 2007. [CrossRef]
6. Čalič, D.; Kromar, M. Spent Fuel Characterization Analysis Using Various Nuclear Data Libraries. *Nucl. Eng. Technol.* **2022**, *54*, 3260–3271. [CrossRef]
7. Natarajan, R. Reprocessing of Spent Nuclear Fuel in India: Present Challenges and Future Programme. *Prog. Nucl. Energy* **2017**, *101*, 118–132. [CrossRef]
8. Yessenbayev, O.; Nguyen, D.C.D.; Jeong, T.; Kang, K.J.; Kim, H.R.; Ko, J.; Park, J.Y.; Roh, M.S.; Comuzzi, M. Combining blockchain and IoT for safe and transparent nuclear waste management: A prototype implementation. *J. Ind. Inf. Integr.* **2024**, *39*, 100596. [CrossRef]
9. Jiu, L. Research on the Management System of Spent Nuclear Fuel in China and Suggestions for Improvement. *China's Nuclear Industry* **2024**, 30–32. Available online: https://www.cnki.com.cn/Article/CJFDTotal-ZHGY202407015.htm (accessed on 25 July 2025).
10. Keffer, S. *Accident Investigation Report. Technical Report;* U.S. Department of Energy Office of Environmental Management: Washington, DC, USA, 2014.
11. Information Security. Available online: https://www.nrc.gov/security/info-security.html (accessed on 10 April 2025)
12. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. *SSRN* **2008**, *3440802*. Available online: https://ssrn.com/abstract=3440802 (accessed on 12 October 2025).
13. Yao, Z.; Ge, J. A Review of the Principles and Applications of Blockchain Technology. *Inf. Technol. Appl. Sci. Res.* **2017**, *8*, 3–17.
14. Sharabati, A.A.A.; Jreisat, E.R. Blockchain Technology Implementation in Supply Chain Management: A Literature Review. *Sustainability* **2024**, *16*, 2823. [CrossRef]
15. Dai, Y.; Lu, G.; Huang, Y. A Blockchain-Based Access Control System for Secure and Efficient Hazardous Material Supply Chains. *Mathematics* **2024**, *12*, 2702. [CrossRef]
16. Vestergaard, C.; Obbard, E.; Yu, E.; Dharma Putra, G.; Green, G. *SLAFKA: Demonstrating the Potential for Distributed Ledger Technology for Nuclear Safeguards Information Management. Technical Report*; Stimson: Washington, DC, USA, 2020.
17. Digital Catapult. *Harnessing the Power of Distributed Ledger Technology: How Digital Catapult's Field Lab Methodology Can Transform Your Business. Sellafield DLT Field Lab Report*; Digital Catapult and Sellafield Ltd.: London, UK, 2022.
18. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions. *Blockchain Res. Appl.* **2021**, *2*, 100006. [CrossRef]
19. Craig, B.; Lee, J.; Tsai, H.; Liu, Y.; Shuler, J. ARG-US RFID for Monitoring and Tracking Nuclear Materials—The Operating Experience. In Proceedings of the 17th International Symposium on the Packaging and Transportation of Radioactive Materials, PATRAM 2013, San Francisco, CA, USA, 18–23 August 2013.
20. Cosentino, L.; Ducasse, Q.; Giuffrida, M.; Lo Meo, S.; Longhitano, F.; Marchetta, C.; Massara, A.; Pappalardo, A.; Passaro, G.; Russo, S.; et al. SiLiF Neutron Counters to Monitor Nuclear Materials in the MICADO Project. *Sensors* **2021**, *21*, 2630. [CrossRef] [PubMed]
21. Ecemis, I.N.; Ekinci, F.; Acici, K.; Guzel, M.S.; Medeni, I.T.; Asuroglu, T. Exploring Blockchain for Nuclear Material Tracking: A Scoping Review and Innovative Model Proposal. *Energies* **2024**, *17*, 3028. [CrossRef]

22. Khutsoane, O.; Isong, B.; Abu-Mahfouz, A.M. IoT Devices and Applications Based on LoRa/LoRaWAN. In Proceedings of the IECON 2017—43rd Annual Conference of the IEEE Industrial Electronics Society, Beijing, China, 29 October–1 November 2017; pp. 6107–6112. [CrossRef]
23. Oktian, Y.E.; Lee, S.G.; Lee, H.J. Hierarchical Multi-Blockchain Architecture for Scalable Internet of Things Environment. *Electronics* **2020**, *9*, 1050. [CrossRef]
24. Cao, K.; Liu, Y.; Meng, G.; Sun, Q. An Overview on Edge Computing Research. *IEEE Access* **2020**, *8*, 85714–85728. [CrossRef]
25. Golomb, T.; Mirsky, Y.; Elovici, Y. CIoTA: Collaborative IoT Anomaly Detection via Blockchain. *arXiv* **2018**, arXiv:1803.03807. [CrossRef]
26. Sgueglia, A.; Di Sorbo, A.; Visaggio, C.A.; Canfora, G. A Systematic Literature Review of IoT Time Series Anomaly Detection Solutions. *Future Gener. Comput. Syst.* **2022**, *134*, 170–186. [CrossRef]
27. Schaper, A. *Looking for a Demarcation between Nuclear Transparency and Nuclear Secrecy*; Number no. 68 in PRIF Reports; Peace Research Institute: Frankfurt am Main, Germany, 2004.
28. International Atomic Energy Agency. *Security of Nuclear and Other Radioactive Material in Transport*; IAEA Nuclear Security Series; International Atomic Energy Agency (IAEA) and Vienna International Centre: Vienna, Austria, 2024. [CrossRef]
29. Chen, X.; He, S.; Sun, L.; Zheng, Y.; Wu, C.Q. A Survey of Consortium Blockchain and Its Applications. *Cryptography* **2024**, *8*, 12. [CrossRef]
30. Fan, C.; Ghaemi, S.; Khazaei, H.; Musilek, P. Performance Evaluation of Blockchain Systems: A Systematic Survey. *IEEE Access* **2020**, *8*, 126927–126950. [CrossRef]
31. International Atomic Energy Agency. *Safeguards Implementation Practices Guide on Provision of Information to the IAEA*; IAEA Services Series No. 33; IAEA: Vienna, Austria, 2016. Available online: https://www.iaea.org/publications/11083/safeguards-implementation-practices-guide-on-provision-of-information-to-the-iaea (accessed on 29 August 2025).
32. International Atomic Energy Agency (IAEA). *A Decade of Progress after the Fukushima Daiichi NPP Accident*, 1st ed.; International Atomic Energy Agency: Vienna, Austria, 2023.
33. Jeong, S.Y.; Kim, J.W.; Joo, H.Y.; Kim, Y.S.; Moon, J.H. Identification of Public Concerns about Radiation through a Big Data Analysis of Questions Posted on a Portal Site in Korea. *Nucl. Eng. Technol.* **2021**, *53*, 2046–2055. [CrossRef]