
Article:
Ahmed, H. (2026) Blockchain and quantum technologies for securing the global Nuclear supply chain: synergies, applications, technical challenges and opportunities. Journal of Critical Infrastructure Policy, 7 (1). e70021. ISSN: 2693-3101

https://doi.org/10.1002/jci3.70021

Journal of Critical Infrastructure Policy

WILEY

RECENT ADVANCES OPEN ACCESS

Blockchain and Quantum Technologies for Securing the Global Nuclear Supply Chain: Synergies, Applications, Technical Challenges and Opportunities

Hafiz Ahmed[1,2]

[1]Autonex Systems Limited, London, UK | [2]School of Electrical and Electronic Engineering, The University of Sheffield, Sheffield, UK

Correspondence: Hafiz Ahmed (hafiz.h.ahmed@ieee.org; hafiz.ahmed@sheffield.ac.uk)

Received: 21 August 2025 | **Revised:** 6 January 2026 | **Accepted:** 3 February 2026

Funding: CHIST-ERA, Grant/Award Number: CHIST-ERA-22-SPiDDS-07; Engineering and Physical Sciences Research Council, Grant/Award Number: EP/Y036344/1

Keywords: blockchain | critical infrastructure | nuclear energy | quantum technology | supply chain

ABSTRACT

The infiltration of counterfeit, fraudulent, and suspect items into civil nuclear supply chains, notably within power generation and medical isotope production, poses severe safety and security threats. The ever-increasing growth in nuclear installations (70 power plants are under construction and another 100 are in the planning stage) and the associated supply chain will further expand this threat, leading to compromised system integrity and a heightened risk of operational failures. This perspective article explores the technological synergies between emerging blockchain and quantum technologies to mitigate these vulnerabilities. Specifically, the paper examines how permissioned and hybrid blockchain models, combined with quantum key distribution, quantum random number generators, and post-quantum cryptography, can enhance traceability, provenance verification, data integrity, and secure communications across the supply chain. Drawing upon theoretical frameworks, practical implementation strategies, and emerging real-world case studies, including those from analogous critical sectors, the article analytically examines the technological potential and specific applications of these advanced technologies. A forward-looking roadmap outlines essential technical steps and addresses the inherent technical challenges and opportunities necessary for effective integration of these solutions, ultimately proposing a robust, transparent, and quantum-resilient nuclear supply chain for the future.

1 | Introduction

The urgent global need for decarbonization and energy security has sparked a renewed interest in nuclear energy. According to the World Nuclear Association, around 70 nuclear power plants (NPPs) under construction and another 100 are in the planning stage. Each NPP is a large infrastructure project containing millions of components. As this expansion accelerates, the industry faces growing exposure to counterfeit, fraudulent, and suspect items (CFSI) entering its supply chains. These compromised parts threaten both safety and security. A stark example of the potential consequences of fraudulent parts is the September 2024 pager and walkie-talkie explosions in Lebanon, as detailed in [1], serving as a critical reminder of the dangers when supply chains are compromised. The aerospace sector provides a useful parallel: it operates under strict regulation yet still contends with counterfeit parts, which account for as much as 10% of the legal aircraft parts market, as mentioned in [2]. The rapid growth of nuclear installations could reproduce this same vulnerability as global manufacturing scales up, increasing the likelihood of counterfeit components entering safety-critical systems.

A special inquiry by the U.S. Nuclear Regulatory Commission's Inspector General [3] confirmed the presence of CFSI in operating US reactors. A King's College London report [4] cited seven notable cases worldwide, including a counterfeit emergency

diesel generator piston pin in Mexico, a fraudulent operational amplifier in Canada, counterfeit circuit breakers in the United States, falsified quality assurance certificates in South Korea, record inconsistencies in reactor pressure vessel manufacturing in France, nuclear fuel data falsification in the United Kingdom, and a counterfeit vibration sensor in Russia. None have yet led to a major accident, but the risk is clear: a substandard component failing under stress or a sabotaged one bypassing safety systems could have catastrophic results. Despite such evidence, ref [5]. notes that the nuclear sector long underestimated the counterfeiting risks. Many operators focused on the most safety-critical systems, assuming the broader supply chain was secure. Combined with poor reporting, this complacency has obscured the true scale of the problem. Publicly available data show that the threat is global. Beyond safety, such scandals damage trust, erode public confidence, and can stall nuclear progress altogether.

The industry has begun to respond. Over the past decade, forums such as the Convention on Nuclear Safety and the International Atomic Energy Agency (IAEA) General Conference have recognized the counterfeit threat and called for tighter supply chain oversight. The IAEA issued guidance on managing CFSI in 2019 [6], followed in 2023 by a coordinated research project (CRP) on the subject (https://www.iaea.org/projects/crp/j02019). Yet progress remains uneven. Countries and organizations take divergent approaches, and significant gaps persist in detection, reporting, and prevention.

Emerging technologies, particularly blockchain and quantum systems, offer new ways to close these gaps. Blockchain can record every transaction and movement of a part on a tamper-proof digital ledger, making it nearly impossible for counterfeit items to go undetected. Quantum technology, especially quantum encryption involving quantum random number generator (QRNG) and quantum key distribution (QKD), can secure communications and data links against interception or tampering, even by future quantum computers. Together, they can make the supply chain transparent, resilient and verifiable end-to-end. Quantum technology provider, D-Wave, has already proposed a quantum blockchain architecture [7] that demonstrates this potential.

In essence, the integration of these technologies creates a tiered defense-in-depth for data integrity. QRNG provides the foundation by producing truly unpredictable entropy, ensuring that the cryptographic keys securing the supply chain are immune to pattern-based hacking. QKD then provides a secure delivery mechanism, using the laws of physics to detect any attempt at eavesdropping during key exchange. Finally, Blockchain acts as the immutable ledger where this quantum-secured data is recorded. Together, they shift the supply chain from a model of "presumed trust" in human actors to a model of "mathematical certainty," where the history of a nuclear component is physically protected and computationally permanent.

A small but growing body of research now explores how these technologies could secure the nuclear supply chain. Blockchain has been proposed for numerous application cases in the nuclear sector, such as nuclear waste management [8], nuclear material tracking [9], secure inspection of nuclear steam generators [10], and NPP operation [11]. Quantum technologies are also entering the nuclear field as well. For example, ref [12]. presents a quantum-secure communication method for nuclear applications.

However, the literature still lacks a system-level view of how blockchain and quantum technologies can operate together across the entire nuclear supply chain, as well as practical roadmaps for deployment. This article addresses that gap by examining both technologies jointly, identifying challenges to their adoption, and outlining a path toward deployment. Unlike earlier studies focusing solely on blockchain [8–11], this work incorporates quantum technologies to present an integrated security architecture capable of achieving what neither technology can alone.

It also considers how these smart technologies can contribute to a more robust security architecture that keeps CFSI out of nuclear systems, strengthening safety and security, and protecting public trust. It also provides a deployment roadmap to guide researchers and industry practitioners toward achieving a technology readiness level (TRL) 9. Furthermore, lessons from other safety-critical sectors, such as aerospace and pharmaceuticals (where blockchain is already in practice), are discussed to inform future applications in the nuclear domain.

While the current analysis focuses primarily on the technical architecture of trust, such as verifiable data exchange and cryptographic integrity, it acknowledges that these tools are part of a broader sociotechnical system. Here, we emphasize the "central" technical requirements while inviting further discourse on the "peripheral" regulatory and cultural shifts needed to support them.

This article is intended for a technology-focused audience interested in how blockchain and quantum technologies can work together to secure the nuclear supply chain. Readers are assumed to have at least a high-level understanding of these technologies. Those less familiar with the underlying concepts may wish to begin with introductory material on conventional cryptography, such as F. Piper's "*Cryptography: A Very Short Introduction.*" For a concise overview of blockchain, J.H. Witte's "*The Blockchain: A Gentle Four Page Introduction"* provides useful context. A non-technical introduction to quantum key distribution can be found in A. Frigyik's "*Quantum Cryptography: Quantum Key Distribution, a Non-technical Approach.*"

The rest of this article is organized as follows: First, a brief introduction to blockchain and quantum technologies is given in Section 2. Then, the synergies of these emerging technologies are discussed in Section 3. High-potential applications and the challenges to implementing them are discussed in Sections 4 and 5, respectively. Subsequently, the development roadmap for these technologies in the context of the nuclear supply chain is provided in Section 6. Cross-sector lessons from other safety-critical and regulated industries are given in Section 7. Finally, concluding remarks and future perspectives are given in Section 8.

2 | Overview of Blockchain and Quantum Technology

2.1 | Blockchain Technology

Blockchain is a decentralized, distributed ledger that records transactions or data in cryptographically linked blocks. Unlike traditional databases managed by a single authority, blockchain networks are maintained by multiple independent nodes that validate each new block through consensus algorithms [13].

TABLE 1 | Qualitative comparison between conventional versus distributed ledgers.

Feature	Conventional ledger	Distributed ledger
Control	Centralized. A single entity (e.g., individual, corporation, government) has full control.	Decentralized. All participants in the network collectively manage the ledger.
Security	Susceptible to a single point of failure and hacking. The data can be altered by the central authority.	Highly secure and resistant to tampering. Uses cryptography and consensus mechanisms.
Transparency	Limited. Only the central authority and a few authorized individuals can see the full record.	Transparent. All participants can view the full, immutable record of transactions.
Trust	Requires trust in the central authority to maintain the ledger honestly and securely.	Trust is established through the network's consensus mechanisms and cryptography, not a single party.
Record Alteration	Records can be changed, edited, or deleted by the central authority.	Records are immutable; once a transaction is added, it cannot be altered.
Efficiency	Can be faster for simple transactions as it doesn't require network consensus.	Transactions may be slower as they require verification by the entire network, but they eliminate the need for intermediaries.

Once recorded, data in a block cannot be changed without re-writing all subsequent blocks and gaining approval from most of the network, making tempering highly detectable.

Table 1 (next page) compares conventional and distributed ledger technologies, highlighting blockchain's advantages in transparency, data integrity, and resilience against single points of failure. Public-key cryptography (using digital signatures and hash functions) further secures transactions by verifying senders and preventing unauthorized modifications.

In safety-critical domains such as the nuclear supply chain, these properties make blockchain a promising foundation for secure information management [14]. It provides a verifiable history of actions and decisions, ensuring accountability across complex networks of suppliers, regulators, and operators.

2.2 | Quantum Technologies

Quantum technology covers a range of innovations that draw on the principles of quantum physics. In certain areas, these approaches can outperform their classical counterparts. For securing the nuclear supply chain, three areas are particularly relevant.

2.2.1 | *Quantum Cryptography*

As discussed in Section 2.1, blockchain relies on cryptography secure data exchange but keys generated by traditional systems are inherently vulnerable to classical attacks. Quantum key distribution (QKD) overcomes this by generating a shared encryption key whose security is guaranteed by the laws of physics. QKD transmits the key using photons, which are particles of light. The core principle is that any attempt to measure these particles changes their quantum state. This change immediately signals an eavesdropper's presence. By comparing a small sample of the exchanged bit, the legitimate parties can spot intrusions and discard compromised keys. The result is a key that no outsider has touched, enabling highly secure communications. This isn't theoretical: QKD was successfully tested at a research reactor, encrypting and decrypting thousands of signals in real-time over 135 km of optical fiber, as detailed in [15].

2.2.2 | *Post-Quantum Cryptography*

Beyond QKD dedicated quantum hardware requirement, post-quantum cryptography (PQC) offers an approach to strengthen classical systems against future quantum attacks. Quantum computers, leveraging qubits, will eventually use algorithms like Shor's to break widely used encryption systems (RSA and elliptic-curve cryptography). This creates the risk of "harvest now, decrypt later" attacks, where adversaries store encrypted data today, waiting for sufficiently powerful quantum hardware to crack it (consult [16] for related vulnerabilities in industrial control systems). PQC addresses this risk by developing new algorithms (e.g., lattice-based or hash-based schemes) and ref [17]. can be consulted for a survey of these algorithms. Unlike QKD, PQC runs on ordinary hardware, offering a practical upgrade path for many existing systems. With PQC standardization nearing completion by 2025, industries, including nuclear, have the opportunity to adopt quantum-resistant security well before large quantum computers become a reality.

2.2.3 | *Quantum Sensors and Unclonable Tags*

For complete nuclear supply chain traceability, quantum-based sensors and physical authentication tags are essential. Certain quantum and nanoscale materials possess unique, naturally occurring, and nearly impossible-to-duplicate signatures. For example, quantum dots, which are a nanometer-scale semiconductor particle, can be embedded in a polymer to form a physically unclonable marker. Because their distinct optical patterns arise from inherently random quantum processes, no two markers are alike, and none can be copied. Similarly, optical physical unclonable functions use light scattering through microscopic imperfections to generate a unique "fingerprint" for each item. These techniques link a physical object's identity to an unforgeable quantum property, providing a crucial physical layer that complements digital security

measures. Ref [18]. can be consulted to understand the security implications of these sensors.

3 | Technological Synergies of Blockchain and Quantum Technologies in Securing the Nuclear Supply Chain

With over a million components and a vast network of contractors, subcontractors, and suppliers operating under a constant schedule, the nuclear supply chain is vulnerable to CFSI slipping into the system. Documented weak points include poor traceability across multi-tier supplier networks, reliance on paper records vulnerable to falsification, siloed information flows that limit industry-wide visibility, and insufficient verification of component authenticity before installation. For a deeper dive into this topic, consult references [19–21].

An anonymous survey as presented in [5] found that some organizations source parts through independent distributors or brokers, bypassing the original manufacturer and official channels. In some cases, electronic components were bought from the open market, often accompanied by questionable authentication certificates. This "weakest link" effect, where one uncertified supplier can compromise an entire chain, is amplified by the scale and global reach of nuclear procurements.

Counterfeiters also exploit misplaced trust in documentation. Substandard parts have been delivered with forged safety certificates and test reports, deceiving operators until failures occurred. Even established vendors have engaged in fraud, such as the Japanese fire equipment supplier cited in [4], showing that conventional quality assurance alone is insufficient.

The ways blockchain and quantum technologies could address these systemic vulnerabilities are described below.

3.1 | Blockchain's Role: End-to-End Traceability and Trust

Applied to the nuclear supply chain, blockchain enables full traceability and accountability for every component from origin to installation, as noted in [22]. Every custody transfer, inspection, and certifications are recorded on a distributed ledger, time-stamped, and cryptographically signed by the responsible party. Authorized participants can view the complete chain of custody for a reactor-grade part, which includes covering manufacturing, testing, transport, and receipt. They can access this information without needing on paper records or isolated databases.

This visibility makes counterfeiting and record manipulation significantly harder. A falsified part, for example, would lack the cryptographic trail of legitimate production and testing, triggering alerts or halting acceptance, as detailed in [23]. Certification and testing integrity also benefit: instead of paper certificates or emailed PDFs, accredited entities log inspection data and results directly onto the blockchain, as discussed in [24, 25]. Supporting evidence such as sensor readings, photos, or videos can be attached to these digital records, creating an auditable, temper-evident certification process.

Past scandals, such as the falsification of reactor part certifications in South Korea as detailed in [4], show how critical such measures are. Blockchain mitigates these risks by recording exactly who supplied what, when, and under what conditions. Smart contracts (cf. ref [26] for an overview of this concept) can enforce compliance automatically: deliveries are accepted only if approved entities and inspection criteria are verified, while nonconforming components are flagged before installation. In effect, blockchain embeds verification and accountability into the supply chain itself rather than relying on after-the-fact audits.

3.2 | Quantum Technology's Role: Securing Communications and Authenticating Hardware

Quantum technologies complement blockchain by securing the channels and devices through which supply chain data flows. Cyber intrusions, such as hacking procurement systems, intercepting documents, or spoofing supplier identities, can enable the insertion of fraudulent components, as noted in [27]. QKD provides intrusion-sensitive encryption and authentication, ensuring that orders, design specifications, and inventory data cannot be covertly altered, as highlighted in [28]. Any eavesdropping attempt is immediately detectable, protecting sensitive information ranging from engineering drawings to nuclear material compositions. This capability is especially relevant for next-generation reactors that rely on remote monitoring. Experiments, such as Purdue University's quantum-secured reactor control data demonstrate the feasibility of building QKD links between manufacturing sites, transport vehicles, and plants.

PQC addresses future risks posed by quantum computers, which could eventually break current blockchain signatures and encryption. Integrating PQC algorithms into blockchain platforms and communication protocols (cf. ref [29] for a case-study) helps ensure that the nuclear supply chain remains secure against "harvest now, decrypt later" threats. Migrating sensitive databases and communication channels to quantum-resistant encryption is therefore a prudent near-term step. For a detailed comparison of QKD and PQC across use cases, see [30].

Quantum technologies also enable physical authentication of components and materials, as shown in [31]. Quantum-based tags, such as quantum dots, act as unclonable physical certificates for high-value parts like control boards or reactor components. Inspectors can scan these tags and verify them against the record stored on the blockchain. This process ensures that even if the blockchain were to be compromised, the quantum "fingerprint" associated with the tags cannot be duplicated.

For nuclear materials, quantum sensors such as magnetometers or gravimeters can detect tampering or substitution during transport. These sensors can identify even small changes in sealed containers, triggering alerts in cases of diversion or smuggling. Although still developing, integrating quantum sensors into supply chain monitoring could add a powerful layer of security for nuclear material integrity.

4 | High-Potential Applications of Blockchain and Quantum Technologies in Securing the Nuclear Supply Chain

The synergies of blockchain and quantum technologies reveal promising applications for the nuclear supply chain. The most relevant applications are detailed below, demonstrating their

TABLE 2 | High-potential applications of blockchain and quantum solutions in nuclear supply chain.

High-potential applications	Mitigated risks
Comprehensive nuclear material tracking	Material diversion/smuggling
Authenticating components & spare parts	Counterfeit/substandard parts
Real-time monitoring & automated auditing	Tampering during transport or storage
Secure procurement & vendor validation	Rogue suppliers or fake companies
Quantum-protected remote operations and maintenance	Cyberattacks on control systems and updates

potential to strengthen traceability, authentication, auditing, and threat detection. A summary of these solutions is provided in Table 2.

4.1 | Comprehensive Nuclear Material Tracking

Blockchain can maintain a continuous, tamper-proof record of nuclear materials throughout the entire fuel cycle, from uranium mining to waste disposal (*cf*. ref [32] for a case study). At every stage, records are logged on a shared ledger accessible to suppliers, operators, regulators, and international authorities. Entries link material to its source, processing facility, and inspection results, enabling full life-cycle visibility. This continuous tracking makes diversion or substitution difficult to achieve undetected and could complement IAEA safeguards by providing real-time, encrypted, and transparent data. For example, a shipment discrepancy (e.g., leaving one facility but not arriving at the next) would quickly trigger alerts. QKD could further secure this data transmission, preventing interception or falsification.

4.2 | Authenticating Components and Spare Parts

Blockchain can prevent counterfeit or substandard parts from entering nuclear plants by creating a digital passport for each component, which records manufacturing details, test results, and custody changes. Upon arrival, the part's identity is verified against the ledger, immediately revealing any tampering or substitution. To enhance verification and develop a trustworthy inspection framework, inspection data (such as X-rays or material analyses) can be attached to the record. Ref [33]. can be consulted for more details about such a framework. Quantum physical unclonable tags (Q-PUTs) enhance this system by embedding a unique, unclonable code directly into each part, verifiable with a handheld scanner. By leveraging the complementary strengths of blockchain records and Q-PUTs, it is possible to make incidents like South Korea's counterfeit parts scandal far less likely while simultaneously streamlining quality assurance.

4.3 | Real-Time Monitoring and Automated Auditing With IoT Integration

Integrating internet of things (IoT) sensors with blockchain can significantly improve the security of transported and stored nuclear materials. Sensors on waste drums, for instance, could continuously log temperature, radiation levels, seal integrity, and location to an immutable ledger. An example of such a monitoring system is given in [34]. Any tampering, such as opening a container, would be instantly recorded, with smart contracts triggering alarms or halting shipments. For sensitive equipment, shock and vibration sensors could document handling quality. With QKD-secured data channels, these logs become tamper-proof audit trails, enabling rapid detection and response to sabotage or mishandling.

4.4 | Secure Procurement and Vendor Validation Network

A blockchain-based supplier network could verify that every vendor, manufacturer, and contractor is authorized, recording their credentials and digitally signing all transactions. A demonstration of such a supplier network is given in [35]. This blocks rogue actors from posing as legitimate suppliers and ensures a verified lineage for all delivered parts. Federated auditing across multiple utilities and regulators creates a shared intelligence system. For example, a counterfeit detected in one country could instantly alert others to check for the same issue. Over time, machine learning could flag recurring risks. Quantum-secure communication would protect sensitive procurement data, such as specifications for reactor or security equipment, from interception or tampering.

4.5 | Quantum-Protected Remote Operations and Maintenance

As nuclear facilities adopt more digital and remote capabilities, quantum technologies can secure these operations. QKD-secured communication could enable safe remote software updates or maintenance on reactor systems (*cf*. the demonstration in [15]). Concurrently, blockchain would log the update details such as firmware hashes, timestamps, and approvals, for future auditing. This integrated process ensures only authorized personnel can issue commands, protecting against hackers or fraudulent updates. Furthermore, quantum-resistant authentication would safeguard control actions, addressing emerging threats at the intersection of cybersecurity and supply chain security.

From a technical standpoint, the integration of quantum technologies and blockchain into the nuclear supply chain presents numerous application areas, as highlighted in this section, with the potential to mitigate the introduction of CFSI items. However, the effectiveness of this solution is inherently linked to organizational adherence and standardization policies. Although these issues fall outside the scope of the current manuscript, they must be considered in any potential deployment scenarios.

5 | Technical Challenges of Applying Blockchain and Quantum Technologies in Securing the Nuclear Supply Chain

Implementing the high-potential applications of blockchain and quantum technologies in the nuclear supply chain presents significant challenges. These barriers span technology maturity, regulatory hurdles, workforce readiness, scalability, security, cost, and global coordination. Understanding these is essential before any deployment, and they are addressed in detail below.

5.1 | Technological Maturity and Integration

Blockchain and quantum tools are still developing (*cf.* ref [36] for a TRL assessment of some blockchain use cases). Many nuclear facilities rely on decades-old software or analog systems for procurement and inventory, as noted in [37]. Connecting these legacy systems to modern blockchain platforms requires custom interfaces and major IT upgrades. Safety culture adds a barrier where only proven, certified tools are acceptable. Following events like the Fukushima disaster in Japan further complicated the safety culture (*cf.* ref [38] for a critical evaluation of nuclear safety thinking), any new blockchain must be exhaustively tested to ensure it introduces no vulnerabilities or operational halts upon network failure. Quantum systems face distinct hurdles. QKD requires specialized hardware and has distance limitations. For example, fiber networks can only extend for a few hundred kilometers without the use of trusted relays or satellites. Thus, global QKD coverage is a long-term effort, making near-term deployment likely regional. PQC avoids hardware needs but is still being standardized, leading to industry hesitation in committing to algorithms that may later change.

5.2 | Expertise and Cultural Adoption

Workforce readiness in the nuclear sector is a significant challenge due to the general workforce's lack of core blockchain skills, as noted in [39]. Engineers and quality staff must learn distributed consensus, smart contracts, and key management, concepts outside of their traditional scope. Every actor, from reactor operators to subcontractors, would need training to use the system correctly, which suggests the need to align nuclear pedagogy. In this context, the ideas presented in [40] could be useful. Cultural adoption presents another major barrier. Some organizations distrust opaque technologies or fear losing control over proprietary data, requiring permissioned ledgers to carefully balance transparency with confidentiality. Historically, parts of the industry denied that counterfeit risks existed. Changing this mindset requires strong leadership and building trust in new systems. Additionally, it necessitates a cultural change within the organization. Furthermore, if smaller suppliers opt out due to cost or complexity, they remain weak links where counterfeits can still enter the supply chain.

5.3 | Scalability and Performance

Scaling of the solution is a major challenge, given that the nuclear supply chain involves millions of parts from hundreds of suppliers. Recording every test, movement, and transfer could create massive transaction volumes. While enterprise blockchains handle heavy loads, bottlenecks may emerge, if smart contracts are complex or if PQC adds computational overhead. This could increase both latency and cost. Careful architecture selection is necessary, such as using a permissioned consortium chain together with off-chain storage for bulky data. QKD also presents scaling challenges, as current systems generate keys at limited rates. If thousands of links require fresh quantum keys, the infrastructure must expand through multiplexing or higher-rate QKD technologies, which is an active engineering challenge that also contributes to increased cost.

5.4 | Data Privacy and Security Considerations

Blockchain's transparency fundamentally clashes with nuclear secrecy. Sensitive data such as fuel compositions, design details, or sourcing, cannot be freely shared. This necessitates permissioned ledgers using encryption and selective disclosure techniques, such as zero-knowledge proofs to verify legitimacy without revealing sensitive details. However, adding these cryptographic layers increases complexity. Furthermore, nations may resist sharing supply chain data on international ledgers, fearing adversaries could infer vulnerabilities (*cf* [41] for blockchain privacy issues). Laws on export controls and data privacy further constrain what can be recorded or shared, particularly on cross-border blockchains spanning diverse alliances (e.g., NATO and non-NATO members). Finally, smart contracts themselves pose risks, as highlighted in [42]. Poor coding could allow exploits that falsify records. Therefore, strong cybersecurity discipline must be maintained, as these tools enhance security but do not eliminate implementation flaws.

5.5 | Energy and Environmental Concerns

Sustainability is a key challenge. Public blockchains using Proof-of-Work (PoW) consume massive energy (although quantum PoW may reduce that, as claimed in [7]). While nuclear applications would avoid this by using Proof-of-Authority or Byzantine Fault Tolerance (*cf.* ref [43] for a review of consensus mechanisms), running nodes and cryptographic operations still consume power. Additionally, QKD equipment requires stable energy and cooling. Given nuclear power's constant scrutiny on sustainability, any added systems must minimize environmental impact. Cost is an equally major barrier. Blockchain infrastructure, quantum devices, and operational upkeep represent substantial expenses. This high cost could prevent adoption by smaller suppliers or resource-constrained countries, creating uneven security across the global chain. This imbalance could be exploited, with attackers targeting weaker participants. Shared funding or international support might be needed to prevent such gaps.

5.6 | Standards and Interoperability

The lack of universal standards poses a significant hurdle. While general blockchain standards exist (e.g., https://blockchain.ieee.org/standards), none yet address the specific needs of the nuclear supply chain. Without common protocols

for data formats, security, and governance, systems will not interoperate, forcing suppliers to deal with multiple platforms and complicating implementation. Achieving this coordination requires consensus among many stakeholders through slow-moving bodies like the IAEA or ISO. Quantum technologies face similar issues. QKD protocols, including synchronization, error correction, and integration with conventional networks, are still evolving as highlighted in [44]. Until these standards mature, early adopters face the risk of vendor lock-in or bespoke integrations.

Legal recognition also lags. Blockchain records and smart contracts may not hold official weight in regulatory or court settings. The crucial question of whether a blockchain entry will suffice as proof of compliance remains unanswered until legal frameworks catch up. For recent legal developments, readers may consult [45] and the references therein.

6 | Development Roadmap for Securing the Nuclear Supply Chain With Blockchain and Quantum Technologies

The deployment of blockchain and quantum security within the nuclear supply chain requires a phased, strategic roadmap focused on overcoming significant technical and regulatory integration challenges. This path involves initial proof-of-concept testing, parallel standards development, and careful, incremental scaling within a heavily regulated environment. A potential deployment path forward is described in detail in this section.

6.1 | Pilot Projects and Testbeds (Years 1–3)

The initial phase must focus on technical feasibility testing in controlled environments to identify integration hurdles with legacy nuclear infrastructure.

Blockchain Pilot: A permissioned distributed ledger should track a limited segment of the supply chain, preferably involving non-safety-related items. The core technical challenge is demonstrating successful integration with existing enterprise resource planning systems and identifying potential latency or usability issues under nuclear operational constraints. A secondary pilot could combine IoT sensors with the blockchain to monitor nuclear waste storage drums, logging their status in real time to assess the reliability of the data-logging mechanism within shielded environments (e.g., Sellafield). The primary goal is to validate operational integrity.

Quantum Pilot (Communication Security): QRNGs present a logical entry point due to their commercial maturity. Testing should focus on applying QRNGs to strengthen encryption within a facility's supervisory control and data acquisition (SCADA) network, measuring performance impact and integration complexity. Further pilots, building on existing research (e.g., Purdue University), could test QKD links between a reactor site and a remote emergency center, challenging the stability and distance limitations of the QKD transmission over fiber or satellite. Refer to [46] for different strategies to increase the QKD key rate. These early efforts must involve regulators to ensure early familiarity with the technical implementation and operational artifacts. The target is clear evidence of technical reliability and utility by year three.

6.2 | Standards Development and Policy Framework (Years 2–5)

Pilot documentation must inform the concurrent and critical phase of developing technical and interoperability standards. This is necessary to move beyond proprietary testbeds.

Technical Consensus: Building on existing standards, organizations like IAEA and ISO/IEC must draft rigorous protocols. Technical outputs should include:

[A] Detailed specifications for distributed ledger applications, defining data schema, access control mechanisms, and required software quality verification for nuclear use.

[B] Guidance on quantum-safe encryption migration and the required cryptographic agility for systems with decades-long lifecycles, drawing from national migration timeline (e.g., the UK government timeline of full migration by 2035).

Regulatory Modernization: Regulators must adapt accepted practices to recognize the technical validity of these new systems. This includes the challenge of recognizing blockchain logs as legitimate, tamper-evident compliance evidence and defining when digital provenance records can replace paper-based documentation.

Governance Architecture: This phase requires establishing an international working group to tackle the architectural design of a global nuclear supply chain consortium blockchain. Key design challenges include defining: node distribution, mechanisms for confidentiality in a shared ledger environment, and the vulnerability assessment and vetting process for participants. Global, decentralized involvement is essential to mitigate the technical risk of control by a single geopolitical actor.

6.3 | Incremental Deployment and Capacity Building (Years 5–10)

Standards enable the transition to incremental and interoperable deployment, prioritizing new builds and high-risk existing systems.

Phased Deployment: New nuclear projects, particularly small modular reactors, should be designed as blockchain-native supply chains to avoid the significant technical debt of later retrofits. Existing reactors should upgrade gradually, beginning with tracking safety-critical components where counterfeit risks are highest. Regulators face the challenge of mandating proof-of-provenance for critical components and ensuring consistent, auditable logging of counterfeit incidents.

Post-Quantum Migration: Organizations must proactively address the challenge of cryptographic compromise by quantum computers. This involves inventorying current cryptographic systems, migrating long-term data to PQC algorithms, and rigorous interoperability testing. The deployment of QKD links should target key communication points, such as between plants and headquarters, or between plants and emergency responders, by leveraging into emerging national quantum networks. A technical challenge is the scaling of QKD infrastructure for cross-border links via satellite.

Skill Gap Mitigation: Deployment is technically impossible without skilled personnel. Training programs must be developed to close the talent gap in specialized areas like blockchain

engineering and quantum-proof systems integration, ensuring that nuclear supply chain managers and engineers can practically manage these tools.

6.4 | Global Integration and Adaptative Defense (Years 10+)

The long-term vision is a globally integrated, quantum-secured network. Focus shifts to continuous defense against evolving threats and system resilience.

Automated Compliance: A core technical objective is to integrate regulatory treaty rules directly into the ledger via smart contracts. This automates compliance checks, for example, a shipment remaining "pending" until the IAEA logs receipt, embedding safeguards within supply logistics rather than layered atop them.

Quantum-Resistant Resilience: Continuous migration to quantum-resistant algorithms is essential to avoid catastrophic security gaps upon the advent of practical quantum computers. Furthermore, exploring the use of technologies like quantum sensors to instantly log cargo scans for illicit materials onto the immutable ledger presents a significant integration challenge between advanced physics and distributed systems.

Continuous Threat Modeling: The technology and threat landscape mandate continuous adaptation. International committees must run regular adversarial exercises and hackathons to test system resilience against data spoofing or infiltration attempts, with findings feeding directly into protocol updates. This adaptive governance structure, where a central body sets baseline rules and regional subnetworks handle localized implementation challenges, is critical for system longevity.

7 | Cross-Sector Lessons for Securing the Nuclear Supply Chain

While the nuclear sector has unique regulatory and security requirements, it shares many vulnerabilities with other safety-critical and regulated industries that depend on complex, globally distributed supply chains. Lessons from sectors such as aerospace (cf [46]) and pharmaceuticals (cf [47]), both early adopters of digital trust and traceability frameworks, offer valuable guidance for applying blockchain and quantum technologies to nuclear systems. Interested readers.

7.1 | Aerospace: Multi-Tier Traceability and Secure Certification

The aerospace industry has faced persistent challenges with counterfeit and unapproved parts entering the supply chain. It is highlighted in [2] that as much as 10% of the legal market are counterfeits. To address this, manufacturers and regulators have adopted digital part tracking systems such as the Airworthiness Certification process [48] and AS5553 standards [49]. These frameworks emphasize component-level traceability, authenticated documentation, and continuous oversight of suppliers.

Blockchain extends these principles by creating a tamper-evident ledger for part provenance and certification. For instance, aerospace consortia made of Thales and Accenture[1] have piloted distributed ledgers to record every maintenance and inspection event for aircraft components. This ensures that a turbine blade or avionics module can be traced through every stage of its lifecycle, even across multiple maintenance organizations. The nuclear sector could adapt this approach to critical components like control system hardware or reactor-grade materials, where verifying origin and maintenance records is equally vital. Integrating blockchain with existing regulatory documentation systems could provide a unified, auditable record accessible to both operators and oversight bodies.

7.2 | Pharmaceuticals: Authenticity, Compliance, and Real-Time Monitoring

Pharmaceutical supply chains face parallel risks: counterfeit drugs, falsified test data, and fragmented oversight across global manufacturers. Regulations such as the U.S. Drug Supply Chain Security Act and the EU Falsified Medicines Directive have driven adoption of serialization and blockchain-based traceability systems as described in [50]. Each batch of medication is assigned a unique identifier, logged through production, distribution, and dispensing, creating an end-to-end verification trail.

The nuclear domain could apply similar serialization principles to critical items: assigning unique, blockchain-verified identifiers to each part, material batch, or digital component. Moreover, the pharmaceutical industry's integration of real-time sensor and IoT data for storage condition monitoring provides a model for embedding quantum-safe communication and verification tools into nuclear logistics. Combining cryptographically secure data sharing with quantum-resistant encryption can ensure both authenticity and confidentiality across national and institutional boundaries.

7.3 | Integrating Cross-Sector Lessons in the Nuclear Supply Chain

The key insight from these safety-critical and regulated sectors is that trust is engineered through transparency, standardization, and verifiable data exchange. Aerospace demonstrates how distributed traceability can strengthen certification and maintenance oversight. Pharmaceuticals show how blockchain and digital identity systems can eliminate counterfeit risks through serialization and real-time validation. Synthesizing these sectoral successes, frameworks such as the ISO/IEC 27000 series and the NIST Cybersecurity Framework [51, 52]—specifically SP 800-53, 800-82, and 800-161—provide the architectural guidelines necessary to scale these practices. By leveraging these established standards, organizations can establish a rigorous security foundation for the emerging integration of blockchain and quantum technologies within global supply chains.

For the nuclear supply chain, combining these approaches would enable a unified trust architecture, where every actor, from component manufacturer to reactor operator, interacts through a verifiable, quantum-secure digital framework. This cross-sector synthesis highlights a path forward: adapting proven digital assurance mechanisms from other critical infrastructures while addressing the heightened security, regulatory, and confidentiality demands of the nuclear context.

8 | Conclusion and Future Perspectives

Counterfeit and fraudulent items remain an immediate and serious threat to the nuclear supply chain. These items jeopardize the safety and security of nuclear installations and, by extension, public safety worldwide. History has shown that a single substandard component can compromise critical systems, yet for years, the issue was under-reported and underestimated. Emerging technologies such as blockchain and quantum cryptography now offer a path toward prevention rather than reaction. Immutable ledgers and quantum-secured communication could create a transparent, verifiable chain of custody where every part, test, and transfer are authenticated and tamper-evident. That vision, however, must be grounded in realism. Some advances can be achieved in the near term. However, others will take years of research, standardization, and infrastructure change.

Near-term priorities are clear. Blockchain-based supplier authentication, certification tracking, and tamper-evident documentation can already be piloted within existing nuclear procurement frameworks. Several industries, including aerospace and pharmaceuticals, have proven that distributed ledgers can improve traceability and reduce fraud without overhauling legacy systems. Likewise, preparing for PQC adoption is both urgent and feasible. Cryptographic migration plans, hybrid encryption schemes, and quantum-resistant digital signatures should be developed now, well before the "year-to-quantum" (Y2Q) moment when current algorithms become vulnerable. These are practical steps regulators and operators can take within the next 5 years.

Longer-term developments, such as widespread quantum sensor deployment, quantum-secure networks across borders, and AI-driven predictive risk analysis using blockchain data, remain aspirational. These technologies show enormous promise for high-fidelity monitoring and automated anomaly detection, but their integration into nuclear facilities will require not only technical maturity but also international governance, interoperability standards, and public investment.

Even as these innovations advance, technology alone wouldn't offer a foolproof solution. Blockchain and quantum systems must complement strong procurement policies, rigorous supplier vetting, inspections, and above all, a culture of integrity. Technology amplifies human judgment and bias; it doesn't replace it. Addressing the counterfeit threat requires a comprehensive approach, and the integration of blockchain and quantum solutions must be aligned with existing policy and regulatory evolution.

Protecting the nuclear supply chain ultimately protects the public and the environment, as nuclear energy provides a feasible path to net zero alongside renewable energy. The path forward is a phased one: deploy what is ready today, prepare for what's coming tomorrow, and align technological adoption with policy and regulatory evolution. With coordinated action now by relevant stakeholders such as governments, industry leaders, and international bodies, the vision of a counterfeit-resistant, digitally trusted nuclear supply chain can move from concept to reality.

Acknowledgments

We would like to thank the anonymous reviewers for their careful reading of our manuscript and their many insightful comments and suggestions. This work is supported by the CHIST-ERA funded TROCI Project (CHIST-ERA-22-SPiDDS-07) through the Engineering and Physical Sciences Research Council (EPSRC) under Grant EP/Y036344/1.

Ethics Statement

The author has nothing to report.

Consent

The author has nothing to report.

Conflicts of Interest

The author declares no conflicts of interest.

Declaration of Generative AI and AI-Assisted Technologies in the Writing Process

During the preparation of this work, the author used ChatGPT to improve grammar, enhance readability, and refine the language of the manuscript. After using ChatGPT, the author reviewed and edited the content as needed and takes full responsibility for the content of the publication.

Data Availability Statement

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Endnotes

[1] https://www.ledgerinsights.com/thales-accenture-aerospace-blockchain.

References

1. T. B. Back, "Weaponising 'Apparently Harmless Portable Objects': Emerging Categorisations of Trust and Risk in Post 'Pager Attacks' Lebanon," *Small Wars & Insurgencies* 36, no. 6 (2025): 1025–1048, https://doi.org/10.1080/09592318.2025.2507223.

2. J. Kotzé and G. A. Antonopoulos, "Con Air: Exploring the Trade in Counterfeit and Unapproved Aircraft Parts," *British Journal of Criminology* 63, no. 5 (2022): 1293–1308, https://doi.org/10.1093/bjc/azac089.

3. US Nuclear Regulatory Commission, Audit of the Nuclear Regulatory Commission's Oversight of Counterfeit, Fraudulent, and Suspect Items at Nuclear Power Reactors; 2022, https://www.nrc.gov/docs/ML2204/ML22040A111.pdf.

4. C. Hobbs, Z. Naser, D. Salisbury, and S. Tzinieris, *Securing the Supply Chain: A Handbook of Case Studies of the Nuclear Security Implications of Counterfeit, Fraudulent, and Suspect Items* (King's College London, 2024), https://doi.org/10.18742/PUB01-164.

5. C. Hobbs, Z. Naser, and S. Tzinieris, "Securing the Nuclear Supply Chain: Addressing the Issue of Counterfeiting," *International Journal of Critical Infrastructure Protection* 50 (2025): 100767, https://doi.org/10.1016/j.ijcip.2025.100767.

6. I. A. E. A. Managing, *Counterfeit and Fraudulent Items in the Nuclear Industry. No. NP-T-3.26 in Nuclear Energy Series* (Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2019).

7. M. H. Amin, J. Raymond, D. Kinn, et al. (2025). Blockchain With Proof of Quantum Work (Version 2). arXiv, https://doi.org/10.48550/ARXIV.2503.14462.

8. O. Yessenbayev, D. C. D. Nguyen, T. Jeong, et al., "Combining Blockchain and IoT for Safe and Transparent Nuclear Waste

Management: A Prototype Implementation," *Journal of Industrial Information Integration* 39 (2024): 100596, https://doi.org/10.1016/j.jii.2024.100596.

9. I. N. Ecemis, F. Ekinci, K. Acici, M. S. Guzel, I. T. Medeni, and T. Asuroglu, "Exploring Blockchain for Nuclear Material Tracking: A Scoping Review and Innovative Model Proposal," *Energies* 17, no. 12 (2024): 3028, https://doi.org/10.3390/en17123028.

10. M. Diaz, E. Soler, L. Llopis, and J. Trillo, "Integrating Blockchain in Safety-Critical Systems: An Application to the Nuclear Industry," *IEEE Access* 8 (2020): 190605–190619, https://doi.org/10.1109/access.2020.3032322.

11. C. Chang, "Blockchain for Integrated Nuclear Power Plants Management System," *Information* 11, no. 6 (2020): 282, https://doi.org/10.3390/info11060282.

12. K. Gkouliaras, V. Theos, and S. Chatzidakis, "Exploring the Feasibility of Quantum-Based Secure Communications for Nuclear Applications," *Nuclear Technology* 211, no. 5 (2024): 994–1013, https://doi.org/10.1080/00295450.2024.2368977.

13. C. Komalavalli, D. Saxena, and C. Laroiya, "Overview of Blockchain Technology Concepts." *Handbook of Research on Blockchain Technology* (Elsevier, 2020), 349–371, https://doi.org/10.1016/b978-0-12-819816-2.00014-9.

14. A. Arora, V. Wright, and C. Garman, "Strengthening the Security of Operational Technology: Understanding Contemporary Bill of Materials," *Journal of Critical Infrastructure Policy* 3, no. 1 (2022): 111–135, https://doi.org/10.18278/jcip.3.1.8.

15. K. Gkouliaras, V. Theos, T. Miller, et al. (2025). Demonstration of Quantum-Secure Communications in a Nuclear Reactor (Version 2). arXiv, https://doi.org/10.48550/ARXIV.2505.17502.

16. M. J. D. Vermeer, C. Heitzenrater, E. Parker, A. Moon, D. Lumpkin, and J. Awan, "Evaluating Cryptographic Vulnerabilities Created by Quantum Computing in Industrial Control Systems," *Journal of Critical Infrastructure Policy* 5, no. 2 (2024): 88–110, https://doi.org/10.1002/jci3.12024.

17. A. Joshi, P. Bhalgat, P. Chavan, T. Chaudhari, and S. Patil, "Guarding Against Quantum Threats: A Survey of Post-Quantum Cryptography Standardization, Techniques, and Current Implementations." *Communications in Computer and Information Science* (Springer Nature Singapore, 2024), 33–46, https://doi.org/10.1007/978-981-97-9743-1_3.

18. A. Brooksby, A. Smith, A. Hickam, M. Manda, A. Rogers, and M. LaDuke, "A Conceptual Framework for Describing the Future Impacts of Quantum Sensors to National Security," *Academia Quantum* 2, no. 1 (2025), https://doi.org/10.20935/acadquant7590.

19. S. Eggers, "A Novel Approach for Analyzing the Nuclear Supply Chain Cyber-Attack Surface," *Nuclear Engineering and Technology* 53, no. 3 (2021): 879–887, https://doi.org/10.1016/j.net.2020.08.021.

20. A. Finan, A. Foss, M. Goff, C. King, and C. Lohse, *Nuclear Energy: Supply Chain Deep Dive Assessment* (USDOE Office of Policy (PO), 2022).

21. O. Martin, and M. Abbt, *Current challenges of the European Nuclear Supply Chain* (Publications Office of the European Union, 2020).

22. R. Azzi, R. K. Chamoun, and M. Sokhn, "The Power of a Blockchain-Based Supply Chain," *Computers & Industrial Engineering* 135 (2019): 582–592, https://doi.org/10.1016/j.cie.2019.06.042.

23. M. Mhatre, H. Kashid, T. Jain, and P. Chavan, "BCPIS: Blockchain-Based Counterfeit Product Identification System," *Journal of Applied Security Research* 18, no. 4 (2023): 740–765, https://doi.org/10.1080/19361610.2022.2086784.

24. S. Kocadag, M. Pohl, and A. Schreiber, "Trusted Provenance with Blockchain Technology: A Systematic Literature Review." *Lecture Notes in Business Information Processing* (Springer Nature Switzerland, 2025), 93–105, https://doi.org/10.1007/978-3-031-89277-6_6.

25. M. Alsadi, J. Arshad, J. Ali, A. Prince, and S. Shishank, "TruCert: Blockchain-Based Trustworthy Product Certification Within Autonomous Automotive Supply Chains," *Computers and Electrical Engineering* 109 (2023): 108738, https://doi.org/10.1016/j.compeleceng.2023.108738.

26. G. Prause, "Smart Contracts for Smart Supply Chains," *IFAC-PapersOnLine* 52, no. 13 (2019): 2501–2506, https://doi.org/10.1016/j.ifacol.2019.11.582.

27. A. Boiko, V. Shendryk, and O. Boiko, "Information Systems for Supply Chain Management: Uncertainties, Risks and Cyber Security," *Procedia Computer Science* 149 (2019): 65–70, https://doi.org/10.1016/j.procs.2019.01.108.

28. R. Mohanty, K. Anusha, N. Manikandan, M. Braveen, and M. A. Jerlin (2024). "Secure Logistics Using Blockchain and Quantum Techniques." in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. IEEE. 1–13, https://doi.org/10.1109/icccnt61001.2024.10724489.

29. D. Marchsreiter, "Towards Quantum-Safe Blockchain: Exploration of PQC and Public-Key Recovery on Embedded Systems," *IET Blockchain* 5, no. 1 (2025), https://doi.org/10.1049/blc2.12094.

30. N. Aquina, B. Cimoli, S. Das, et al., "A Critical Analysis of Deployed Use Cases for Quantum Key Distribution and Comparison With Post-Quantum Cryptography," *EPJ Quantum Technology* 12, no. 1 (2025): 51, https://doi.org/10.1140/epjqt/s40507-025-00350-5.

31. B. P. Williams, K. A. Britt, and T. S. Humble, "Tamper-Indicating Quantum Seal," *Physical Review Applied* 5, no. 1 (2016): 014001, https://doi.org/10.1103/physrevapplied.5.014001.

32. M. Siddig, A. Alhawsawi, and E. Abdelraheem, *Blockchain Model for Enhancing Safety & Security of Nuclear Materials at Trade Points* (Cambridge University Press (CUP), 2024), https://doi.org/10.33774/coe-2024-5n2w0.

33. W. Zhang, G. Sun, L. Xu, et al., "A Trustworthy Safety Inspection Framework Using Performance-Security Balanced Blockchain," *IEEE Internet of Things Journal* 9, no. 11 (2022): 8178–8190, https://doi.org/10.1109/jiot.2021.3121512.

34. J.-W. Lee, T.-J. Kim, and H.-K. Lee, "Design of an IoT-Based Indoor Tracking and Condition Monitoring System for the Safe and Transparent Management of Drums Storing Low- and Intermediate-Level Radioactive Waste," *Journal of the Air & Waste Management Association (1995)* 73, no. 2 (2023): 133–145, https://doi.org/10.1080/10962247.2022.2149636.

35. T. K. Agrawal, J. Angelis, W. A. Khilji, R. Kalaiarasan, and M. Wiktorsson, "Demonstration of a Blockchain-Based Framework Using Smart Contracts for Supply Chain Collaboration," *International Journal of Production Research* 61, no. 5 (2022): 1497–1516, https://doi.org/10.1080/00207543.2022.2039413.

36. K. Holm and R. C. Goduscheit (2020). "Assessing the Technology Readiness Level of Current Blockchain Use Cases." in *2020 IEEE Technology & Engineering Management Conference (TEMSCON)*. IEEE. 1–6, https://doi.org/10.1109/temscon47658.2020.9140147.

37. A. M. Saley, J. Marchand, A. Sekhari, V. Cheutet, and J.-B. Danielou, "State-of-Art and Maturity Overview of the Nuclear Industry on Predictive Maintenance." *IFIP Advances in Information and Communication Technology* (Springer Nature Switzerland, 2023), 337–346, https://doi.org/10.1007/978-3-031-25182-5_33.

38. M. Ylönen and T. Litmanen, "Signaled and Silenced Aspects of Nuclear Safety: A Critical Evaluation of International Nuclear Safety Thinking," *Risk, Hazards & Crisis in Public Policy* 6, no. 1 (2015): 22–43, https://doi.org/10.1002/rhc3.12072.

39. F. Prager, J. Martinez, and C. Cagle, "Blockchain and Regional Workforce Development: Identifying Opportunities and Training Needs." *Public Administration and Information Technology* (Springer International Publishing, 2021), 47–72, https://doi.org/10.1007/978-3-030-55746-1_3.

40. B. Costelloe-Kuehn, D. A. González-Rueda, I. Kim, E. Liu, and J. Olson, "A Systems Thinking Approach to Nuclear Pedagogy and Workforce Development," *Journal of Critical Infrastructure Policy* 6, no. 2 (2025): e12040, https://doi.org/10.1002/jci3.12040.

41. R. Henry, A. Herzberg, and A. Kate, "Blockchain Access Privacy: Challenges and Directions," *IEEE Security & Privacy* 16, no. 4 (2018): 38–45, https://doi.org/10.1109/msp.2018.3111245.

42. S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, "Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract," *IEEE Access* 10 (2022): 6605–6621, https://doi.org/10.1109/access.2021.3140091.

43. A. O. Bada, A. Damianou, C. M. Angelopoulos, and V. Katos (2021). "Towards a Green Blockchain: A Review of Consensus Mechanisms and Their Energy Consumption." in *2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE. 503–511, https://doi.org/10.1109/dcoss52077.2021.00083.

44. J. M. Sáez, A. P. Perales, R. C. Palancar, et al. (2024). "Current Status, Gaps, and Future Directions in Quantum Key Distribution Standards: Implications for Industry." in *2024 International Conference on Quantum Communications, Networking, and Computing (QCNC)*. IEEE. 341–345, https://doi.org/10.1109/qcnc62729.2024.00059.

45. M. Kiskis, "Private Law Framework for Blockchain," *Frontiers in Blockchain* 7 (2024), https://doi.org/10.3389/fbloc.2024.1205461.

46. J. K. Yadav, D. C. Verma, S. Jangirala, S. K. Srivastava, and M. N. Aman, "Blockchain for Aviation Industry: Applications and Used Cases." *Lecture Notes in Networks and Systems* (Springer Nature Singapore, 2022), 475–486, https://doi.org/10.1007/978-981-16-5655-2_46.

47. W. Chien, J. De Jesus, B. Taylor, et al., "The Last Mile: DSCSA Solution Through Blockchain Technology: Drug Tracking, Tracing, and Verification at the Last Mile of the Pharmaceutical Supply Chain With BRUINchain," *Blockchain in Healthcare Today* (2020), https://doi.org/10.30953/bhty.v3.134.

48. T. Raoofi and S. Yasar, "Analysis of Frontier Digital Technologies in Continuing Airworthiness Management Frameworks and Applications," *Aircraft Engineering and Aerospace Technology* 95, no. 10 (2023): 1669–1677, https://doi.org/10.1108/aeat-06-2022-0166.

49. SAE International Technical Standard. Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition, SAE Standard AS5553, Issued April 2009, https://doi.org/10.4271/AS5553.

50. G. Smith, J. Smith, and D. Brindley, "The Falsified Medicines Directive: How to Secure Your Supply Chain," *Journal of Generic Medicines: The Business Journal for the Generic Medicines Sector* 11, no. 3–4 (2014): 169–172, https://doi.org/10.1177/1741134315588986.

51. J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook, and M. Fallon (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-161r1-upd1, https://doi.org/10.6028/NIST.SP.800-161r1-upd1.

52. N. Mexis, B. Lill, Y. Doleh, and S. Katzenbeisser, "Exposing the Gaps: The State of Supply Chain Coverage in Current Security Standards." in *Information Security Education. Empowering People Through Information Security Education. WISE 2025. IFIP Advances in Information and Communication Technology*, eds. L. Drevin, W. S. Leung, and S. von Solms (Springer, 2026) 742, https://doi.org/10.1007/978-3-031-94924-1_14.