STIMSON

TECHNOLOGY & TRADE

POLICY PAPER

Complementing the Padlock: The prospect of blockchain for strengthening nuclear security

Cindy Vestergaard, Co-Author
Maria Lovely Umayam, Co-Author

EXECUTIVE SUMMARY

In the last few years, distributed ledger technology (DLT, widely recognized as blockchain) has demonstrated practical benefits beyond the development and exchange of cryptocurrencies. DLT solutions, especially when only specific stakeholders are permissioned to gain access to certain information (also referred to as private DLT), are now being tested and implemented in the fields of international development, healthcare, and education. These use cases are showing early signs of promise, especially the ability to better streamline various data flows in a single, immutable platform that allows different types of stakeholders to interact in a trusted environment. These DLT platforms also demonstrate a unique security component that renders data embedded on the chain extremely difficult to manipulate; any attempt to change the information would be logged as part of the ledger and flagged for users that need to know that a change has occurred. Thus, DLT's ability to preserve the integrity of data could potentially help enhance security measures across businesses, including the nuclear sector. This policy paper outlines the exploratory research the Stimson Center's Blockchain in Practice team conducted beginning the fall of 2019 to better understand the possible applications for securing nuclear materials, technologies, and facilities. The paper examines three use cases – improving nuclear material accounting; facilitating insider threat mitigation; and enhancing data tracking and material tracking during nuclear transport – and discusses the opportunities and challenges to implementation.

***Note*:** *This is an updated version of a working paper initially published and presented as part of the IAEA International Conference on Nuclear Security, held February 2020.*

DLT and International Security Regimes Project

Blockchain in Practice Program

June 2020

Contents

Introduction

The rapid pace of tech innovation has opened an uncharted technological frontier. Governments and businesses must navigate this exciting yet challenging landscape, which requires having an open mind toward new technologies that promise improved quality of work and life while also approaching them with a healthy dose of caution. *Distributed ledger technology* (DLT) — more commonly known as *blockchain* — is one such innovation that has received mixed reception, touted as a revolutionary digital interface on the one hand and suspected as an overhyped idea on the other.[i] The appeal of DLT is rooted in its ability to establish immutable digital recordkeeping without reliance on a centralized system, thereby enhancing transaction transparency and assurance while providing data privacy among all parties involved. As tech expert Bettina Warburg explained, DLT platforms create a "shared reality across non-trusting entities" in a way that lowers uncertainty and builds confidence.[ii] Despite predictions that DLT will not achieve mainstream adoption until 2028, there are hundreds of DLT-based projects worldwide, 140 of which are related to the energy sector.[iii] Moreover, DLT has attracted major players in the financial, health, and logistics sectors eager to experiment and better understand its potential.

In addition to its principal benefit of bringing transparency and assurance into transactions and workflows, experts suggest DLT holds an unprecedented potential to strengthen data integrity. As public and private organizations amass large quantities of sensitive data, cyber-adversaries — from unstructured hackers to organized groups with resources — have grown more sophisticated in their ability to steal or sabotage these data.[iv] In 2018 alone, 6,515 reported "data compromise events," exposing millions of records.[v] DLT proponents encourage governments and businesses to examine the ways in which DLT can be used as a tamper-resistant accountability system to prevent adversaries from posing as legitimate users in order to gain access.[vi]

As various sectors generate research around the role and value of DLT for security, certain elements could be applicable to protecting CBRN[vii] material, including sensitive information regarding facilities and personnel. DLT has already piqued the interest of stakeholders within the chemical and nuclear fields, which in turn encourage additional research and the development of prototypes to demonstrate applicability.[viii] Growing attention within the WMD nonproliferation community calls for a comprehensive and impartial analysis of where new technologies such as DLT may fit — or not.

This paper presents a preliminary survey of DLT in the context of *nuclear security* — the ways in which the advantages of DLT can be harnessed to better protect nuclear materials, technologies, and facilities to prevent theft, sabotage, and unauthorized use. The paper outlines possible use cases based on interviews and roundtable discussions with DLT and nuclear security experts conducted as part of a year-long investigation.[1] These ideas are by no means exhaustive or conclusive. Rather, they explore how blockchain could possibly benefit security by offering integrity and traceability to enhance *governance* — an additional layer of protection to complement the nuclear security "padlock."

Demystifying Distributed Ledger Technology

There is a significant barrier to understanding DLT because of its association and often conflation with the term "blockchain," which gained a contentious reputation over the years as the underpinning technology of cryptocurrency (e.g., Bitcoin). Bitcoin represents the world's first and largest open blockchain, a platform that allows anyone with an Internet connection to participate in a system of digital payments. Bitcoin became linked with blockchain in popular culture; but in fact, blockchain should be understood as a *subset* of DLT. By definition, DLT is the catch-all category for decentralized digital databases that can include a wide range of participants from multiple locations. A database is considered as DLT when it

(i) enables a network of independent participants to establish a consensus around (ii) the authoritative ordering of cryptographically validated ("signed") transactions. These records are made (iii) persistent by replicating the data across multiple nodes, and (iv) tamper evident by linking them by cryptographic hashes. (v) The shared result of the reconciliation/consensus process — the "ledger" — serves as the authoritative version for these records.[ix]

In other words, blockchain falls under the category of DLT, but not all DLT implement blockchain technology. Blockchain initially gained prominence for its decentralized design whereby a ledger of transactions is not stored in a central location. Rather, copies of

[1] The Stimson Center, with support from the U.S. Department of Energy – National Nuclear Security Administration, is conducting a year-long study on the application of DLT to address nuclear security challenges related to information management and insider threat mitigation. This paper is the first draft summarizing initial interviews — facilitated in Tallinn, Estonia; London, United Kingdom; Vienna, Austria; and Paris, France — at the onset of this study.

transactions are kept in "nodes," which in turn are added into the ledger as cryptographically linked "blocks." Since blockchain used in cryptocurrencies operates mostly in *open* systems, it is often assumed that all DLTs are public in nature, allowing anyone to contribute to the maintenance and integrity of the ledger. But this is true only for certain types of DLTs; other DLT platforms are *private* or *permissioned,* restricting who can access certain records and who can carry out specific actions. Permissioned DLT platforms are already being used (or currently tested) for a wide range of government and private services, including tracking the provenance of high-value minerals, safekeeping health records for an entire country, and fortifying supply chains that deliver food items and other goods around the world.[x]

Whether private or permissioned, DLT offers novel security features that are not readily available in existing recordkeeping platforms, leading some technology experts to consider it tamper-resistant. DLT systems employ a special cryptographic function called *hashing*, a process in which transactions are given an encrypted fixed-length value that acts as its unique identifier. This encrypted hashing makes it incredibly challenging to alter or reverse-engineer transactions, as it is linked to the other transactions on the ledger. Any attempt to alter a transaction is rejected; it becomes incompatible with the rest of the chain and alerts participants.[xi] Furthermore, any changes to transactions — editing amounts or ownership of a given set of information, for example — would be logged as part of the chain, so all activity is preserved.

DLT also employs shared protocols among stakeholders — also known as consensus mechanisms — to ensure that the ledger remains consistent across all stakeholders who have access, which acts as a bridge of trust among the network. DLT combines computing concepts of cryptographic hashing, peer-to-peer protocols, and distributed consensus algorithms to allow a network of participants to share and validate data across the ledger. Thus, DLT platforms are less likely to experience a single point of failure, given that data are linked and replicated among participants that in turn must meet certain conditions that uphold the ledger. This structure suggests a different approach toward the concept of *governance*. Instead of relying on external systems to protect transaction data, blockchain offers a novel way to embed protective properties into data collection by tracking and validating the integrity of the transactions. For example, in the use case of DLT platforms used for medical recordkeeping, the platform does not store personal health-related data directly on the blockchain ledger, but instead stores the *signature* or *metadata* of the data. The appropriate stakeholders (either doctor or patient) are simultaneously notified whenever activity about health records is accessed; any modifications — points of access, sharing, or edits — would be logged. In this example, the "locus of control" is shifted from the healthcare system to empower other players, especially patients, to manage and trust that their data are current and unaltered.[xii]

More broadly, trust is no longer facilitated through a singular, centralized system (medical institutions), but by the data themselves, and accessed by designated actors who need to know.

This concept of "truth in data" could fundamentally shift perceptions of what strong security entails. The nuclear security community relies on the traditional foundations of *physical protection* and *computer security*, which are predominantly a *perimeter-centric* interpretation of security: building defenses/air gaps to ensure that the assets (here, nuclear materials, technologies, or facilities) are guarded against outside attacks. DLT encourages an alternative, if not complementary, perimeterless approach, which builds integrity and cultivates security in a self-interrogating environment to ensure that there are no anomalies that could trigger unsafe or insecure conditions. Pioneering efforts to combine breakthrough technologies — artificial intelligence, Internet of Everything (IoE), and blockchain — present a preliminary picture of how these technologies can pave the way for perimeterless thinking for security.[xiii] For instance, some researchers are studying the pairing of smart devices (a subset of the IoE known as the "Internet of Things" or IoT) with blockchain to protect the stream of information transmitted and analyzed through the IoT device (e.g., the sensor in a smart home device).[xiv]

Potential Pathways for Nuclear Security

Securing nuclear materials, technologies, and facilities from non-state adversaries remains an important facet of national security for countries that possess civil nuclear programs. While theft and sabotage are low-probability events, maintaining strong and redundant security measures is essential in preventing any adversary from believing that an attempt to commit a malicious act would be successful (e.g., deterrence by denial).[xv] Moreover, countries are increasingly vigilant toward the shadowy borders of the new technological frontier, particularly the ways to invent creative outlets for nefarious activities to exploit vulnerabilities in security culture and cyber resilience.

For the past few years, top law enforcement agencies including the U.S. Department of Homeland Security and INTERPOL have cautioned the international community about hybrid security incidents that combine physical and cyberattack vectors.[xvi] Critical infrastructures including the nuclear sector have fallen victim to increasingly complicated cyber breaches: In 2018, several nuclear power plants in the United States were targeted by hackers who hid their trail effectively to obscure the nature and level of damage.[xvii] The problem is not purely a technological construct; for most organizations, part of the challenge stems from the lack of security culture around sensitive information, leading to miscommunication and other mistakes.[xviii] Many security experts attribute information mismanagement and data breaches to human error, with some claiming numbers as high as 90%.[xix,xx] As a result, the International Atomic Energy Agency (IAEA) Nuclear Security Plan for 2018–2021 notes that, while Member States recognize physical protection as the bedrock of nuclear security, information and computer security are growing priorities.[xxi] As it is the State's sole responsibility to define nuclear security in accordance with respective circumstances and threat profiles, countries are encouraged (and obligated, if party to the Amended Convention of the Physical Protection of Nuclear Material) to establish nuclear security regimes that align with the twelve Fundamental Principles. The principles that are particularly relevant to information security are Principle F (Security Culture), Principle I (Defense in Depth), Principle J (Quality Assurance), and Principle L (Confidentiality).[xxii]

The unique properties of DLT that enhance access controls and anti-tampering have proven useful in protecting proprietary and sensitive personal data in other sectors. As this technology is better understood, refined, and accepted in the near term, it may also hold untapped value for nuclear security. The following sections present an overview at the relevancy of DLT to the nuclear security challenges described above. These ideas are compiled from interviews and roundtables with DLT experts and nuclear security practitioners (e.g., select IAEA representatives, competent authorities, and industry representatives) who are in the early stages of exploring DLT as a tool. Hence, the use cases discussed should not be considered definitive. Instead, these should be treated as initial impressions that could be further investigated for desirability (are nuclear security stakeholders interested?), feasibility (does it meet technical criteria to solve security problems in the field?), and viability (can it be sustained?). Ultimately, the goal of this research is to pinpoint the main drivers behind pursuing DLT for nuclear security: *What would DLT offer to substantially improve the protection of nuclear materials and facilities that existing approaches and traditional measures cannot readily offer?*

Irrespective of whether DLT has a role to play, if the international community earnestly desires to continuously improve, these kinds of thought exercises about breakthrough technologies should be embedded in conversations about and reflections on the future of nuclear security. Dialogue on DLT could serve as a forum to consider the ways in which breakthrough technologies can help articulate the relationship between the "3S" — safety, security, and safeguards — when appropriate. For instance, what types of nuclear material data could improve management and security on all three fronts? Or how might a DLT platform help reduce risks from all three areas? Moreover, thinking about DLT applications can prompt conversation about innovative ways of storing data, especially as the IAEA, regulators, and operators are tasked to manage increasing volumes of information. Given that transactional data are replicated and shared, private DLT platforms consolidate information across authorized stakeholders, consequently empowering them to trust the data — in effect *spreading* confidence and responsibility in enforcing governance.

For nuclear material accounting and control

DLT's primary function as a secure and shared information management platform naturally stimulates interest in the ways in which it can enhance nuclear material accounting and control (NMAC) systems. NMAC in facilities is designed primarily for effective safeguards implementation by providing operators and competent authorities with accurate, complete, and reliable information on nuclear material. But NMAC also has direct benefits to security, since a strong accounting system plays a critical role for inventory controls and determining discrepancies from unauthorized removal. As noted in the IAEA Nuclear Security Series 25-G, NMAC complements physical protection by providing precise knowledge of the quantities, types, and locations of nuclear material.[xxiii] While physical protection is responsible for implementing the "guns, guards, and gates" for immediate detection and deterrence against nuclear security incidents, NMAC acts as a reliable source of data that is helpful during an investigation (e.g., if an emergency inventory must be performed).

However, not all regulators or facilities have an effective NMAC system. Either some elements of recordkeeping are still done via hardcopy, there are significant challenges in reconciling data amid the multiple streams of information coming from different actors, or — even worse — an NMAC system does not exist at all. Several nuclear security practitioners have noted that matching operator and regulator records can be incredibly cumbersome, causing delays in detecting irregularities as well as wasted labor and other resources. SLAFKA, the world's first DLT prototype for nuclear material accountancy for safeguards, demonstrates how DLT platforms create network ledgers based on operator data.[xxiv] If NMAC systems were layered with DLT (or, as one DLT expert put it, "blockchain-backed"), it could potentially streamline and secure accounting information as materials move through material balancing areas and facilitate better knowledge-sharing across appropriate stakeholders.

With DLT, information or activity about the flow of nuclear material within a facility or across facilities can be protected in such a way that if an insider threat attempts to manipulate records, the adversary would also have to change the rest of the chain and risk detection. In a permissioned DLT, selected stakeholders can be provided specific access rights — information about material flows from operator to regulator, for example — which allows for easy and secure segregation of data to those with a need to know. A DLT layer in this regard could also apply to material in transport whereby carriers, shippers, and relevant national authorities share the status of shipments to ensure continuity of knowledge during transit, i.e., traceability of shipping documents. Transparency among actors (those granted access for permissioned

DLTs) could also allow for earlier detection of suspicious activity, since all participants would have an identical set of information about the ledger. In theory, any actor along the chain would have the means to spot abnormalities in the transaction history, making it difficult for anyone to subvert the system. In fact, one of the most promising features of DLT platforms is a customizable interface showcasing the "where, what, and when" of a product in a moment in time. Such interfaces already exist to track the routes of minerals and foods; applied in the nuclear sector, they could potentially provide state authorities with instantaneous information on the location of nuclear materials in facilities and in transit. Overall, evaluating the utility of DLT for NMAC necessitates a conversation between security and safeguards practitioners; there could be promising overlapping benefits, shared lessons, or (if not careful) overstepping of boundaries in technological adoption.

For insider threat mitigation

The inability to detect an insider threat can become an Achilles heel; one recent security breach in a nuclear power facility caused by a well-tailored malware suggests that an insider was provided information that could have been used to modify the attack for maximum damage.[xxv] Insider threats are a universal challenge for all sectors, and some companies are exploring DLT applications to support human reliability programs. For instance, a DLT layer could assist in monitoring activities related to personnel and other sensitive operations such as blueprints, equipment, and computer patches internal to the facility. When necessary, this information could be shared with state authorities (e.g., during a security incident). Several companies are piloting projects that pair DLT with IoT, such as biometric devices to implement facial recognition security for employees, especially those handling highly sensitive and valuable information. While this concept is still in its nascent stages and must overcome technical and political hurdles, the goal is to create digital identities for high-level personnel to authenticate their credentials and track the data they share with whom, when, and for how long.[xxvi,xxvii] Under this DLT overlay, personnel *activity* is logged onto the chain, not the actual sensitive information itself.[xxviii] Thus, DLT would operate orthogonally to existing information security measures, which follows the principles of defense in depth for nuclear facilities.

There are also emergent studies around the use of DLT for validating data provenance — a way to ascertain whether specific data deviated from their original or agreed "truth." This concept is better understood in the context of video or audio editing; the new technological frontier is rife with altered digital content, some of which spreads misleading or inaccurate information (also known as "deepfakes"). Organizations including law enforcement and news outlets are already considering how to leverage DLT's immutable time-stamping features to corroborate the authenticity of photographs or videos, keeping record of any changes to the original copies *by the pixel* to glean a timeline of when a file could have been doctored.[xxix] If this DLT use case is proven effective, it could have broader implications in protecting source material, including source code. Those implications could be particularly useful in critical infrastructures like nuclear facilities that must maintain mechanical integrity, i.e., the impossibility of sensitive equipment being sabotaged or manipulated by external parties by secretly adding malware or malicious code.[xxx]

For transport security

Nuclear material is especially vulnerable when in transit, given that sensitive materials are taken out of tightly controlled environments (i.e., beyond the perimeter) and into the outside world where conditions are harder to anticipate and manage. According to a recent analysis of incidents reported to the IAEA, more than half of incidents categorized as theft of radioactive material between 1993 and 2019 occurred while the material was in transport.[xxxi] It is also important to remember the global magnitude and reach of nuclear transport activities: An estimated 20 million shipments are regularly transported within countries and across borders every year via air, road, or rail. A major incident during transport is likely to inflict adverse knock-on effects to the greater community, as it could harm people along the path (especially unwitting citizens that encounter stolen material taken out of containers) or restrict the movement of other goods if traffic is severely disrupted.[xxxii] Regional relationships could also be compromised should a security incident occur amid cross-border transit. In such an event, rapid response and information sharing would be desirable, but it is unclear to what extent such communication channels are readily available among neighbouring states.[xxxiii]

DLT could potentially contribute an organized tracking system to complement existing security measures for transport. Currently, the web of information facilitating transport of nuclear materials comprises hardcopy (e.g., faxed paperwork or coded communication) and digital information being passed around to different actors with varying levels of “need to know” — supplier, regulator, shipper, receiver, port personnel, etc. Moreover, the type of security for a given shipment will have different requirements depending on the type of nuclear material, i.e., category of material attractiveness. Transporters must be mindful of the risks associated with these materials and the ways in which these varying risks impact the development of a robust transport security plan. Data about these shipments are highly sensitive and must be conveyed to the right person at the right time. For example, information about the quantity of material should only be made privy to certain actors (e.g., operators, regulators), whereas routes and shipping times may have a different classification that can be accessed by a broader array of stakeholders (e.g., drivers, port personnel). The complexity of this ecosystem may be compounded by safety guidelines that are mostly electronically distributed, while security information is more likely to be transmitted via hardcopy to deter the likelihood of being shared easily. Most importantly, transport involves synchronized movement of information (documentation) *and* material (the asset in transit). While paperwork is passed around, stakeholders must have assurance that the physical material is where it should be throughout transport. For example, shippers rely on GPS technology to monitor truck locations, but this does not necessarily guarantee that nuclear material casks and packages are still loaded on the truck. Although nuclear transport has not experienced a major security incident to date, continuous evaluation and improvement is a core value in nuclear operations, which includes a critical look at the efficiency and efficacy of existing security measures and procedures.

A private DLT platform could offer an added layer of assurance on the flows of sensitive data related to transport by logging information onto the chain as nuclear material travels from origin to destination. With smart contracts, these data — such as personnel credentials or authentication of necessary documents — could be monitored and accessed by specific personnel depending on their need-to-know requirements proportionate to the risk (i.e., maintain a *graded approach* to information).[xxxiv] And combined with other breakthrough technologies such as an IoT "smart" device, this platform could present a new way of linking the digital information with the physical material by *translating* the actual movement of a given shipment into signals that act as a digital signature, which is stored on the blockchain and cross-referenced with other relevant data such as documents exchanged and validated among shippers, operators, and regulators. Put another way, these raw sensor data collected through IoT are placed into a blockchain in order to create cryptographic "evidence" verifying the integrity of the process, e.g., assurance that the material is supposed to be where it is with the right set of people in any point in time during its physical move. Overall, there are interesting areas in which DLT can help facilitate digital "gatekeeping" between nuclear material transfers by creating a provenance trail that would hold all participating stakeholders accountable, thereby improving security governance of material.

DATA IN MOTION

Envisioning A DLT Prototype For Nuclear Transport

Stakeholders in the nuclear sector are interested in the ways in which private DLT platforms compare with existing systems and procedures that secure and streamline the information and material flows during transport. While the transport industry has a good track record of keeping nuclear materials secure, a number of incidents over time in several countries serve as a reminder that security approaches must be continuously evaluated and improved. This exercise is especially critical in a post-COVID-19 environment where personnel (guards) may not be readily available to help track material as a result of physical distancing constraints, or where operators are compelled to turn to "no-touch" systems. The political, economic, and social fallout of COVID-19 is undeniably a stress test on current systems and raises questions about how our reliance on technology will change, for better or worse, as our global security landscape shifts over time. The purpose of the prototype would be to identify the benefits — whether they be improved information security, efficiency gains, or cost savings — in utilizing a DLT platform to manage and validate a subset of information related to nuclear materials transport.

To begin, a prototype would include "dummy" data to ascertain whether flow of information and real-time notification among different need-to-know stakeholders would be efficient and secure. **If successful, this framework would not only provide an immutable record of checkpoints for a given shipment in real time, but also monitor the activities of individuals handling the materials directly (detection of any activities that could indicate insider threat).**

Some questions to consider while developing a prototype:

- What does the current ecosystem of information management and tracking look like, and where are areas that could use improvement?
- What types of data/metadata would stakeholders be willing to manage and track through this platform, especially in an environment of mistrust (not necessarily toward one another, but due to an enduring culture of limiting information sharing for the sake of strong security)?
- What are some of the barriers related to new technologies and their applications that need to be addressed in order to achieve acceptability?
- How would a DLT platform distinguish between types of material that carry different risk profiles (Category I, II, and III material) and take into consideration additional transport security requirements when material crosses state/country borders (different locales may require extra measures)?

Conclusion: The Road Ahead

DLT is finding a footing in a variety of sectors, positioning itself as one of the innovations that will dominate and shape our new technological frontier. The hype that open, public DLT platforms in the form of cryptocurrencies have stirred over the years has led to an explosive rise in start-ups for all types of applications, which gives the impression that DLT is a solution blindly seeking an answer. While DLT has shown transformative gains in healthcare and supply chain markets, many projects are still in the testbed phase such that positive results have yet to demonstrate sustainability.[xxxv] These prototypes are not only putting the technology to the test, but are also gauging savings and costs — with respect to installation fees, computationalefficiencies, maintenance, and workforce — compared to existing data management systems and security methods.[xxxvi] For high-cost industries such as the nuclear sector, achieving top security should not come at the expense of maintaining a cost-effective business. Thus, applications for nuclear security must demonstrate that the system can be harmonized with rest of the enterprise with little to no added costs. For example, studies conducted by safety engineers have shown that added safety measures in certain circumstances can make complex systems less safe.[xxxvii] It may also be true for security: the use of DLT must serve to improve and streamline, and not confuse security systems in nuclear facilities.

Many technologists are quick to remind us that DLT is only as good as the information stored in it; users must ensure that initial data are correct, since the chain's primary task is to manage and protect this input, not rectify it. Thus, some form of physical verification would still be necessary. The DLT system design must fit neatly within the ecosystem of activities and governance, which in turn dictates the conditions and types of information shared in the ledger. The success of the technology is dependent on whether its role is clearly defined and how it will seamlessly interact or intersect with other technologies already being used. It will also be critical to achieve corporate acceptability, which will require a detailed articulation of how DLT will tangibly reduce security risks while maintaining reasonable security costs that will not impact other aspects of business. As with any new technology, there are also barriers to learning and eventually accepting the concept of DLT as a legitimate technological system or service. Nuclear stakeholders will need to understand that DLT itself is not going to be a direct solution to improved security, but rather presents a new way of working and sharing information that could yield greater efficiencies, streamlined processes, and a stronger security practice.

At this stage, it cannot be definitively stated that a DLT-backed platform can enhance nuclear security. But witnessing the promising pursuit of DLT applications for other sectors to secure data management that have parallel circumstances for nuclear security presents a question on whether lessons can be learned and eventually transferred into the nuclear field. With any technological breakthrough, finding the answer requires rigorous questioning, research, and experimentation. As the new technological frontier becomes the norm, it will be incumbent on governments, industries, and organizations to keep pace. Ultimately, this research aims to assist the nuclear community in sifting through the opportunities and pitfalls of DLT for nuclear security, leading any positive discussion and concrete interests into an appropriate prototype, and ultimately a proof of concept. Overall, the study hopes to present a thoughtful process for navigating the technological frontier, identifying what can make nuclear security stronger along the way.

Acknowledgements

The authors are grateful to the Office of International Nuclear Security of the U.S. National Nuclear Security Administration for their generous support in funding this research. Additionally, the authors give their sincerest thanks to the various organizations — from the nuclear security and DLT community — who entertained the authors' challenge of thinking about DLT technology in the context of nuclear security. Their open-mindedness, as well as thoughtful critique, provided this paper a strong foundation of research. The authors also would like to acknowledge Stimson Research Associate Gabrielle Green, as well as Stimson Nonresident Fellows Diego Cándano Laris and Kim Anderson, for their assistance in developing this paper.

[i] RYERSON, J., Is Blockchain Technology Overhyped?, New York Times (15 Feb. 2019).; SEEBACHER, S., SCHÜRITZ, R., Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review, Exploring Services Science: 8th International Conference (ZA, S., DRĂGOICEA, M., CAVALLARI, M., Eds.), Springer, Rome (2017) 12–23.

[ii] WARBURG, B., How the Blockchain Will Radically Transform the Economy, TED, https://www.ted.com/talks/bettina_warburg_how_the_blockchain_will_radically_transform_the_economy.

[iii] MUNSTER, B., Advisory Firm Gartner Puts Blockchain Tech in the "Trough of Disillusionment," Yahoo Finance. (9 Oct. 2019); Gartner 2019 Hype Cycle Shows Most Blockchain Technologies Are Still Five to 10 Years Away From Transformational Impact, Gartner (8 Oct. 2019).; EU Blockchain Initiative Map, EU Blockchain Observatory and Forum, https://www.eublockchainforum.eu/initiative-map; ANDONI, M et al., Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities, Renewable and Sustainable Energy Reviews (2019) http://www.sciencedirect.com/science/article/pii/S1364032118307184.

[iv] THE COUNCIL OF ECONOMIC ADVISERS, The Cost of Malicious Cyber Activity to the U.S. Economy, (2018) 1–58 pp.; THE WHITE HOUSE, National Cyber Strategy of the United States of America, (2018).

[v] RBS, Over 6,500 Data Breaches and More Than 5 Billion Records Exposed in 2018, Risk Based Secur. (13 Feb. 2019).

[vi] ZYSKIND, G., NATHAN, O., PENTLAND, A., Decentralizing Privacy: Using Blockchain to Protect Personal Data, 2015 IEEE Security and Privacy Workshops, IEEE, San Jose (2015) 180–184.

[vii] Chemical, biological, radiological and nuclear.

[viii] There are ongoing studies investigating DLT as a supply chain management platform. See "Take Advantage of Blockchains: Decentralized Digital Networks Offer Chemical Makers a Variety of Opportunities," Chemical Processing (12 July 2019). Additionally, there are nascent explorations to use DLT in streamlining nuclear safeguards (a Stimson Center project). See VESTERGAARD, C., Better Than a Floppy: The Potential of Distributed Ledger Technology for Nuclear Safeguards Information Management (2018).

[ix] RAUCHS, M. et al., Distributed Ledger Technology Systems, Cambridge Center for Alternative Finance, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-10-26-conceptualising-dlt-systems.pdf.

[x] WIGGERS, K., Everledger Raises $20 Million to Track Assets with Blockchain Tech, VentureBeat (24 Sep. 2019).; Learning from the Estonian e-Health System, Heal. Eur. (11 Jan. 2019).

[xi] ZHENG, Z., XIE, S., DAI, H.-N., CHEN, X., WANG, H., Blockchain Challenges and Opportunities: A Survey, Int. J. Web Grid Serv. **14** 4 (2018) 352-375.; Data Immutability in Private Channels, Blockchain Backyard (16 Feb. 2018).

[xii] HALAMKA, J.D., LIPPMAN, A., EKBLAW, A., The Potential for Blockchain to Transform Electronic Health Records, Harv. Bus. Rev. (3 Mar. 2017).

[xiii] This paper makes a distinction between "emerging" and "breakthrough." Emerging technologies are still trying to gain attention and penetrate markets, while breakthrough technologies are further into development and are beginning to identify commercial application.

[xiv] SALAH, K., IoT Security: Review, Blockchain Solutions, and Open Challenges, Futur. Gener. Comput. Syst. (2017).

[xv] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventative Measures for Nuclear and Other Radioactive Material Out of Regulatory Control, Vienna (2019).

[xvi] BANKS, W.C., SAMUEL, K., Hybrid Threats, Terrorism, and Resilience Planning, Int. Cent. Counter-Terrorism-Hague (17 Sep. 2019).

[xvii] DEPARTMENT OF HOMELAND SECURITY AND FEDERAL BUREAU OF INVESTIGATION JOINT TECHNICAL ALERT, Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors (15 Mar. 2018). https://www.us-cert.gov/ncas/alerts/TA18-074A

[xviii] WORLD INSTITUTE FOR NUCLEAR SECURITY, Corporate Governance Arrangements for Nuclear Security (2018). https://wins.org/document/corporate-governance-arrangements-for-nuclear-security/

[xix] WILLIAMS, S., More Than Half of Personal Data Breaches Caused by Human Error, Secur. Br. (21 Aug. 2019).

[xx] NOBLES, C., Shifting the Human Factors Paradigm in Cybersecurity, NIST Cyber Security Resource Center, https://csrc.nist.gov/CSRC/media/Events/Federal-Information-Systems-Security-Educators-As/documents/17.pdf.

[xxi] IAEA DIRECTOR GENERAL, Nuclear Security Plan 2018-2021, General Conference (61)/24, International Atomic Energy Agency, Vienna (2017).

[xxii] INTERNATIONAL ATOMIC ENERGY AGENCY, INFCIRC/274/Rev.1/Mod.1, International Atomic Energy Agency, Vienna (2016).

[xxiii] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities, Vienna (2015).

[xxiv] VESTERGAARD, C., SLAFKA Prototype: DLT for Nuclear Material Accounting and Control, Stimson Center (2020). https://www.stimson.org/project/slafka-prototype/

[xxv] DAS, D., An Indian Nuclear Power Plant Suffered a Cyberattack. Here's What You Need to Know, Washington Post (4 Nov. 2019).

[xxvi] Blockchain for Digital Identity, Accenture, https://www.accenture.com/us-en/services/blockchain/digital-identity (2020).

[xxvii] GARCIA, P., Biometrics on the Blockchain, Biometric Technol. Today, 5 (2018).

[xxviii] RMA, S., GUPTA, R., SRIVASTAVA, S.S., SHUKLA, S.K., Detecting Insider Attacks on Databases Using Blockchains, Workshop on Blockchain Technologies and Its Applications, Indian Institute of Technology Bombay, Mumbai (2017).

[xxix] GARCIA MARTÍNEZ, A., The Blockchain Solution to Our Deepfake Problems, Wired (26 Mar. 2018).; ORCUTT, M., The New York Times Thinks a Blockchain Could Help Stamp Out Fake News, MIT Technol. Rev.

(Jul.).; NEISSE, R., STERI, G., NAI-FOVINO, I., A Blockchain-Based Approach for Data Accountability and Provenance Tracking, ARES '17 Proceedings of the 12th International Conference on Availability, Reliability and Security, ACM, Reggio Calabria (2017).

[xxx] ROBERTSON, J., RILEY, M., The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies, Bloom. Businessweek (4 Oct. 2018).

[xxxi] PLETUKHINA, I., A Moving Target: Nuclear Security During Transport, IAEA Bull. (24 Jan. 2020).

[xxxii] CHAPPELL, B., Stolen Radioactive Material Found in Mexico, The Two-Way, NPR (4 Dec. 2013).

[xxxiii] INTERNATIONAL ATOMIC ENERGY AGENCY, International Conference on the Security of Radioactive Material: The Way Forward for Prevention and Detection, Vienna (2018).

[xxxiv] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Material in Transport: Implementing Guide, Vienna (2015).

[xxxv] SHIN, L., Industries, Looking for Efficiency, Turn to Blockchain, New York Times (27 Jun. 2018).

[xxxvi] IBM, Emerging Technology Projection: The Total Economic Impact™ of IBM Blockchain, (2018).

[xxxvii] DOWELL, A.M., HENDERSOT, D.C., No Good Deed Goes Unpunished: Case Studies of Incidents and Potential Incidents Caused by Protective Systems. Proc. Safety Prog., 16 (2004) 132-139.