THE PROSPECT OF BLOCKCHAIN FOR STRENGTHENING NUCLEAR SECURITY
Navigating the Technological Frontier

M. L. UMAYAM
Stimson Center
Washington, DC, USA
Email: lumayam@stimson.org

C. VESTERGAARD
Stimson Center
Washington, DC, USA
Email: cvestergaard@stimson.org

Abstract

In the last few years, distributed ledger technology (widely recognized in the form of blockchain) has demonstrated practical benefits beyond the development and exchange of cryptocurrencies. Blockchain solutions are being implemented in the fields of international development, healthcare, and education, predominantly as an information-sharing platform that enables parties to interact in a trusted environment. The strength of blockchain stems from its cryptographically-secure properties: when data is recorded onto the blockchain by any user, it is automatically copied onto other connected nodes (or participants) on the chain, as opposed to storing it directly into a centralized database. Consequently, the information has "no single point of failure" in a blockchain; any changes to the information – an attempt to extract or manipulate sensitive data, for instance – will be logged. Thus, blockchain's ability to preserve the integrity of data could potentially help enhance security measures across businesses, including the nuclear sector. For instance, blockchain technology could make it difficult for a malevolent actor to reconfigure files or install code that could linger in a computer network undetected, among other applications. This paper outlines the exploratory research the Stimson Center conducted in the Fall of 2019 – including expert interviews with blockchain developers and nuclear facility operators – to better understand the possible applications for nuclear security. The paper examines use cases that could potentially prevent or mitigate security vulnerabilities in nuclear facilities that could be exploited by cyber and insider threats. Moreover, the paper discusses potential difficulties in applying blockchain for nuclear security, and the ways in which the use of this technology could alter security considerations -- for better or worse – at the national and operational level.

1. INTRODUCTION

The rapid pace of tech innovation today has opened an uncharted technological frontier. Governments and businesses must navigate this exciting yet challenging landscape, requiring an open mind towards 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 [1, 2]. The appeal of DLT is rooted in its ability to establish immutable digital record-keeping without reliance on a centralized system, thereby enhancing data transparency and assurance among all parties involved. As tech expert Bettina Warburg explained, DLT platforms create a "shared reality across non-trusting parties" in such a way that lowers uncertainty and builds confidence [3]. 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 [4–6]. 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 that DLT holds an unprecedented potential to strengthen data integrity. As public and private organizations amass large quantities of personal and/or sensitive information, cyber-adversaries – from unstructured hackers to organized groups with resources – have grown more sophisticated in their ability to steal or sabotage this data [7]. In 2018 alone, an estimate of 6,515 organizations publicly reported data breaches[8]. DLT proponents encourage governments and businesses to examine the ways in which DLT can be used as a tamper-resistant accountability system that prevents adversaries from posing as legitimate users to steal or corrupt data [9].

As various sectors generate research around the role and value of DLT for security, there are certain elements that could be applicable to protecting chemical, biological, radiological and nuclear material, including sensitive information regarding facilities and personnel. It has already piqued the interest of stakeholders within the chemical and nuclear fields [10].[1] Growing attention within the WMD nonproliferation community begs the need for a comprehensive and impartial analysis of where new technologies such as DLT may fit or not.

The 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 the first set of interviews with DLT and nuclear security experts conducted as part of a year-long study on the topic.[2] These ideas are by no means exhaustive or conclusive. Rather, the paper is the first to be presented in a series of discussions that will culminate in a final paper that will be published in June 2020.

2. 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 (i.e., Bitcoin). The technology underpinning 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"[11].

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 transactions are kept in "nodes," which in turn are added into the ledger as cryptographically linked "blocks." Any changes to the records of transactions will also be added to the chain, which allows for unparalleled transparency among all stakeholders involved without having to go through a middleman – such as a bank – to verify the authenticity and accuracy of data. Since blockchain used in cryptocurrencies operate in *open* systems, it is often assumed that all DLT are public in nature, thus allowing anyone to contribute to the maintenance and integrity of the ledger. This is only true for certain types of DLT; there are other DLT platforms that are *private* or *permissioned* that restrict who can access certain records and can carry out specific actions. While blockchain for cryptocurrencies are widely recognized and discussed in the media, it is the private and permissioned DLT platforms that are attracting the attention from governments and businesses, albeit more quietly. DLT in this regard is already being used (or currently tested) for a wide range of public and private services, including tracking the provenance of high-value minerals; safe-keeping health records for an entire country; and fortifying supply chains that deliver food items and other goods around the world [12, 13].

DLT also offers novel security features that are not readily available in existing record-keeping platforms, leading some technology experts to consider it as 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 signature is incredibly challenging to alter or reverse-engineer as it is linked to the other transactions on the ledger. Any attempt to alter this signature would be rejected as it would be incompatible with the rest of the chain, and will alert participants [14, 15]. Furthermore, any changes to

[1] There are ongoing studies investigating DLT as a supply chain management platform to ensure that chemical products, particularly those considered sensitive or of high-value, reach their final destinations. There also is ongoing research into the use of DLT in streamlining nuclear safeguards.

[2] 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– 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.

And as mentioned above, shared protocols among stakeholders – also known as consensus mechanisms – also ensure that trust is maintained, and that the ledger remains consistent [14, 15]. In short, DLT combines computing concepts of hashing along with cryptography, 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 data is linked and replicated among participants that in turn must meet certain conditions that uphold the ledger.

3. POTENTIAL PATHWAYS FOR NUCLEAR SECURITY

Securing nuclear materials, technologies, and facilities from non-state adversaries remain 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 are essential in preventing any adversary from believing that an attempt to commit a malicious act would be successful (i.e., deterrence by denial) [16]. Moreover, countries are increasingly vigilant towards the shadowy borders of the new technological frontier, particularly the ways it can 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 [17]. 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 [18]. 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 [19]. Many security experts attribute information mismanagement and data breaches to human error, with some claiming numbers as high as 90% [20, 21]. As such, the 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 [22]. As it is the State's sole responsibility to define nuclear security in accordance to 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 include: Principle F (Security Culture); Principle I (Defense in Depth); Principle J (Quality Assurance); and Principle L (Confidentiality) [23].

DLT's unique properties 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 a cursory look at DLT's relevance to the nuclear security challenges described above. These ideas are compiled from interviews with DLT experts and nuclear security practitioners (i.e., 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?). Irrespective of whether DLT has a role to play, these kinds of thought-exercises about breakthrough technologies should be embedded in conversations and reflections towards the future of nuclear security, if the international community earnestly desires to continuously improve.

3.1. For nuclear material accounting and control

DLT's primary function as a secure and shared information management platform naturally prompts interest in the ways in which it can enhance nuclear material accounting and control (NMAC) systems. NMAC in facilities are designed primarily for effective safeguards implementation by providing operators and competent authorities accurate, complete, and reliable information of nuclear material. But a strong NMAC also has direct benefits to security since a strong accounting system plays a critical role in 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 [24]. While physical protection is responsible for implementing the "guns, guards, and gates" for immediate detection and deterrence against nuclear security incidents, NMAC acts as the reliable source of data helpful during an investigation (i.e., if an emergency inventory must be performed).

However, not all regulators or facilities have an effective NMAC – either some elements of record-keeping are still done via hardcopy; or there are significant challenges in reconciling data amidst the multiple streams of information coming from different actors; or worse, a 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 manpower and other resources. If NMAC systems are layered with DLT (or as one DLT expert put it, "blockchain-backed"), it could potentially streamline and secure accounting information as material move through material balancing areas, as well as 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 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 try and subvert the system. In fact, one of the most promising features of DLT platforms is a customizable interface showcasing the "where / what / when" of a product in a moment in time. Such interfaces already exist to track the routes of minerals and foods; it could possibly exist for nuclear materials (viewed as a timeline or for a given item) in the future. If applied in the nuclear sector, this could potentially provide state authorities instantaneous information of where nuclear materials are in facilities and in transit. Overall, evaluating the utility of DLT for NMAC necessitates a conversation between security and safeguards practitioners since there could be promising overlapping benefits, shared lessons, or if not careful, overstepping of boundaries in adopting this technology.

3.2 For insider threat mitigation

A nuclear operator's 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 provided information that could have been used to tailor the attack for maximum damage [25]. 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. And only when necessary, this information can be shared with state authorities (i.e., during a security incident). Several companies are piloting projects that pair DLT with "Internet of Things" (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 how long [26, 27]. Under this DLT overlay, personnel *activity* is logged onto the chain, not the actual sensitive information itself [28]. 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 a specific piece of data deviated from its original or agreed "truth." This is better understood in the context of video or audio editing; the new technological frontier is rife with altered digital content, some of which spread 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 when a file could have been doctored [29–31]. If this DLT use-case is proven effective, this could have broader implications in protecting source material, including source code. This could be particularly useful in critical infrastructures like nuclear facilities that must maintain mechanical integrity, i.e., that sensitive equipment cannot be sabotaged or manipulated by external parties by secretly adding malware or malicious code [32].

3.3 For incident reporting

DLT's growing reputation as a confidence builder, or "trust machine" among disparate, untrusting parties holds the potential to strengthen incident reporting by protecting the identity of participants who are otherwise cautious about the integrity of a reporting system. Preserving anonymity and providing assurance that incident reports won't be mishandled or leaked can incentivize reporting, which in turn leads to more and better data acquisition to discern patterns in attack vectors and improve overall incident analysis. Within the nuclear community, the most recognized international reporting mechanism for security incidents is the IAEA Incident and Trafficking Database (ITDB), which tracks nuclear material found outside of regulatory control. Using the database, IAEA Information Management Section also conducts additional open-source information to substantiate incident reports, as well as performs a needs assessment as a response to the reporting party [33]. Aside from providing a reporting platform, the IAEA also holds meetings throughout the year on the ITDB; in 2018, 102 states participated in at least one of these events.[34] Most recently, there were 117 incidents between July 2018 and June 2019 that were reported by Member States to the ITDB.[35] While the ITDB is considered an effective long-standing resource, reporting security incidents remain an occasional practice because states are not obligated to report.

Legally-binding instruments for nuclear security – UNSCR 1540 ; ICSANT; and the CPPNM-A – have different provisions related to reporting, with some encouraging bilateral knowledge transfers for the purpose of threat coordination, but not transparency or post-incident analysis [36]. Due to the sensitive nature of the topic including proprietary information, reporting could be perceived as a hindrance rather than a benefit. A case study on an internal incident reporting system for a nuclear facility found that only 14% of employees actively used the reporting platform since it was perceived to be "blame"-oriented [37]. Although sharing errors, consequences, and lessons learned is universally lauded as best practice, these actions require acknowledging vulnerability in ways that can be difficult for companies and organizations to do. Integrating permissioned DLT into reporting databases could ease the process by separating incident data from confidential or proprietary business information, such that the former can be shared more freely among other participants, while the latter information is viewable and controlled only by the company or organization. A similar DLT model is being studied for protecting personal information online, whereby users hold the authority to share or restrict elements of their information found online [38].

Data collected from incident reporting is an invaluable source of information, potentially allowing businesses to sketch a better portrait of their risk. The InsurWave platform, jointly developed by A.P Moller – Maersk; accounting firm EY; DLT developer Guardtime; and other industry stakeholders, presents an intriguing test case of what rigorous data collection through DLT could possibly offer. The InsurWave platform connects shippers, brokers, and insurers together to facilitate common transactions including tracking assets, negotiating premiums, and paying claims. By overlaying specific data elements gathered overtime, InsurWave can help identify risk exposure for shippers and insurers, i.e., choosing a certain shipping route already known for turbulent waters / piracy can increase the likelihood of risk compared to an established safer route. With this information readily available, industry hopes that it can make informed business decisions in real-time [39, 40]. Ultimately, the goal is to create a transparent space for all these actors involved to conduct business and share information with the collective goal of minimizing business disruption. While nuclear operators observe special liability principles, the InsurWave model is nonetheless a thought-provoking project to strengthen industry-to-industry transparency for the sake of operational efficiency and data security.

4. CONCLUSION – THE ROAD AHEAD

From the various use-cases mentioned above, DLT is finding a footing in a variety of sectors, positioning it as one of the innovations that will dominate and shape our new technological frontier. But all technologies inevitably face a series of trials before mainstream adoption. Due to the hype public DLTs in the form of blockchain cryptocurrency have stirred over the years and the explosive rise of blockchain start-ups for all types of applications, it is easy to label DLT as 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 [41]. These prototypes are not only putting the technology to the test, but they are also gauging savings and costs – with respect to installation fees, computational efficiencies, maintenance, and workforce – compared to existing data management systems and security methods [42]. 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. Moreover, many technologists are quick to remind that DLT is only as good as the information stored in it; users must ensure that initial data is correct since the chain's primary task is to manage and protect this input, not rectify it. In sum, the DLT system design must fit neatly within the ecosystem of activities, 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.

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 present 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 proof-of-concept. Overall, the study hopes to present a thoughtful process of 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 (NNSA) 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 and Stimson Nonresident Fellow Diego Cándano Laris for their assistance in developing this paper.

REFERENCES

[1] RYERSON, J., Is Blockchain Technology Overhyped?, New York Times (15 Feb. 2019).

[2] SEEBACHER, S., SCHÜRITZ, R., Blockchain Technology of Service Systems: A Structured Literature Review, Exploring Services Science: 8the International Conference (ZA, S., DRĂGOICEA, M., CAVALLARI, M., Eds), Springer, Rome (2017) 12–23.

[3] 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.

[4] MUNSTER, B., DECRYPT, Advisory Firm Gartner Puts Blockchain Tech in the "Trough of Disillusionment", Yahoo Financ. (9 Oct. 2019).

[5] Gartner 2019 Hype Cycle Shows Most Blockchain Technologies Are Still Five to 10 Years Away From Transformational Impact, Gartner (8 Oct. 2019).

[6] EU Blockchain Initiative Map, EU Blockchain Observatory and Forum, https://www.eublockchainforum.eu/initiative-map.

[7] PARKER, T., SACHS, M., MILLER, T., DEVOST, M.G., Cyber Adversary Characterization, Black Hat.

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

[9] 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.

[10] VESTERGAARD, C., Better Than a Floppy The Potential of Distributed Ledger Technology for Nuclear Safeguards Information Management, (2018).

[11] RAUCHS, M. et al., Distributed Ledger Technology Systems, (2018).

[12] WIGGERS, K., Everledger Raises $20 Million to Track Assets with Blockchain Tech, VentureBeat (24 Sep. 2019).

[13] Learning from the Estonian e-Health System, Heal. Eur. (11 Jan. 2019).

[14] 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.

[15] Data Immutability in Private Channels, Blockchain Backyard (16 Feb. 2018).

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

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

[18] PERLOTH, N., SANGER, D.E., Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says, New York Times (15 Mar. 2018).

[19] Corporate Governance Arrangements for Nuclear Security, (2018).

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

[21] NOBLES, C., Shifting the Human Factors Paradigm in Cybersecurity, (2018).

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

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

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

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

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

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

[28] SHARMA, S., GUPTA, R., SRIVASTAVA, S.S., SHUKLA, S.K., Detecting Insider Attacks on Databases Using Blockchains, Kanpur.

[29] GARCIA MARTÍNEZ, A., The Blockchain Solution to Our Deepfake Problems, https://www.wired.com/story/the-blockchain-solution-to-our-deepfake-problems/.

[30] ORCUTT, M., The New York Times Thinks a Blockchain Could Help Stamp Out Fake News, MIT Technol. Rev. (Jul.).

[31] 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).

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

[33] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Illicit Trafficking Database (ITDB), International Atomic Energy Agency, Vienna (2008).

[34] IAEA, IAEA INCIDENT AND TRAFFICKING DATABASE (ITDB), (2019).

[35] GENERAL, I.A.D., Nuclear Security Report 2019, (2019).

[36] MUTI, A., Information-Sharing in Nuclear Security, (2018).

[37] ROSSIGNOL, N., OUDHEUSDEN, M. van, Learning from Incidents and Incident Reporting: Safety Governance at a Belgian Nuclear Research Center, Sci. Technol. Hum. Values **42** 4 (2017) 679.

[38] IEEE, DLT Model.

[39] Insurwave, Insurwave, https://insurwave.com/.

[40] GUARDTIME, EY, INSURWAVE, New Real-Time, Blockchain-Enabled Platform to Secure and Streamline Key Insurance Processes, Guardtime and EY.

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

[42] IBM, Emerging Technology Projection: The Total Economic Impact^{TM} Of IBM Blockchain, (2018).