Stanley Center
FOR PEACE AND SECURITY

ANALYSIS & NEW INSIGHTS

Better Than a Floppy

The Potential of Distributed Ledger Technology for Nuclear Safeguards Information Management

Cindy Vestergaard, Ph.D.

Blockchain is transitioning away from the hype and gaining legitimacy as the next-wave technological solution to distribute data and build a network of trust among parties. The technology, which is the distributed ledger technology (DLT) underpinning cryptocurrencies such as bitcoin, is a combination of already-existing technologies (such as cryptography) interlinked in an innovative way to provide a network ability to securely manage and easily audit large volumes of data. It is moving beyond financial systems to a growing list of applications by other industries, whether providing digital identification for refugees, tracing diamonds, or streamlining global trade.[1] Even the United Nations and other international organizations are considering the potential. According to one report, seven UN agencies are exploring and/or using blockchain technologies to support their operations and programs.[2]

The International Atomic Energy Agency (IAEA) has also identified the need to "monitor the potential utility of block chain [*sic*] technology for safeguards applications (e.g. nuclear material accounting)."[3] To this end, the agency is including a panel session on blockchain for the first time at its Symposium on International Safeguards in November 2018. The symposium's theme, "Building Future Safeguards Capabilities," looks to the potential for emerging technologies and innovative approaches "for strengthening and streamlining the implementation of safeguards."[4] This is in keeping with the agency's long-term goal of investing in modern information technologies to more efficiently meet rising demands on its Department of Safeguards under fairly static budgets.[5]

This Analysis and New Insights provides an overview of DLT and explores its utility for safeguards information management. It considers the ecosystem of safeguards information management, specifically the landscape of factors determining how safeguards data is inputted, processed, and accessed. The findings and recommendations suggest where adding a DLT layer could be applied to provide greater efficiency, data reconciliation, accuracy, and trust in information management at the international, national, and facility levels.

Distributed Ledger Technology

The word *blockchain* refers to the public transaction ledger designed for bitcoin as invented by Satoshi Nakamoto. Although the term is not explicitly used in Nakamoto's 2008 Bitcoin white paper, the paper outlined how the technology and its supporting network can provide an open, peer-to-peer system to authenticate transactions or a "chain of blocks" instead of intermediaries or banks.[6] The blockchain is a subset of distributed ledger technology (DLT), which is a type of decentralized database spread across multiple sites, regions, or participants.[7] According to Michael Rauchs et al., DLT is:

> "A system of electronic records that (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."[8]

Although blockchain has become the catchall term for all forms of DLT, not all DLTs make use of blockchain. The disruption of the bitcoin blockchain is disintermediation—by removing middlemen and allowing anyone with an Internet connection to participate—whereas closed (private) DLT platforms have evolved to restrict participation to known and identified participants across multiple organizations or internally within one. These permissioned platforms do not necessarily disrupt centralization, but they are transforming business operations and the way organizations interact.

DLT systems can be categorized as permissionless or permissioned based on the system's degrees of openness.[9]

- In a permissionless (open) system, as with bitcoin, the platform is open to participation without users having to request access. Data in these ledgers are generally public, as the systems tend to allow anyone to inspect and contribute data.

- In a permissioned (private or closed) system, gatekeepers can restrict access rights to specific participants. This includes restrictions on who can access the network, what functions and tasks a participant can perform, who can read data, and how data is diffused among participants.[10]

DLT systems can therefore be designed to meet specific organizational and operational needs. The banking sector mostly uses closed consortium DLT systems to make use of the technology's innovation for securing and streamlining large volumes of transactions across integrated cross-border databases.[11] IBM and Maersk are also jointly developing TradeLens, a "blockchain-enabled shipping solution" to innovate and secure the global supply chain, which today has more than 90 organizations participating.[12] Private DLT platforms can also be applied at the national and municipal levels. Estonia has been using the technology since 2012 for its national e-Health Record and e-Land Registry systems (to name a few).[13] Dubai is planning to become a fully fledged Blockchain City by 2020 as part of its ongoing Smart Dubai initiative.[14]

Whether permissioned or open, every transaction on a DLT system is "hashed" with its own digital fingerprint, or cryptographic signature, which is time-stamped and mathematically linked to previous transactions to provide a traceable history of all information stored on the database. This makes DLT systems highly tamper resistant. They also provide auditability, given DLT is typically append-only and creates a history of all information on the ledger. This auditability makes it easy to detect any successful tampering. It also further enhances data reconciliation given all participants work from the same shared data.

DLT systems also vary by what consensus mechanisms they use. These are the sets of rules and algorithms that a distributed ledger uses to authenticate and validate transactions. Common mechanisms include "Proof of Work" (PoW) used by bitcoin, which requires participants to expend significant computing power (an action known as "mining") before adding a block to the chain and earning some reward for the effort (usually in cryptocurrency). During the cryptocurrency boom, this led to the establishment and concentration of large mining operations (collaborations of individual indexing services) to the point where validation can be accomplished by only a few who have the hardware to process large amounts of data and the financial resources to pay high energy bills.[15] In other words, while the blockchain supporting bitcoin removed intermediaries from transactions, the PoW consensus mechanism has led to the emergence of new forms of centralization.[16] "Proof of Stake" (PoS) is a common alternative that does not involve mining but instead rewards transaction fees to validators who are stakeholders in the system's cryptocurrency.[17]

Consensus mechanisms are one of the most rapidly advancing aspects of the technology. As more consortiums continue to test proofs, DLT scientists are applying the technology to meet various scalability and compliance needs within different business enterprises and their global operations. Hyperledger Fabric, for example, uses "endorsement policies" whereby a set of policy criteria guide which network users must approve certain transactions.[18] Such mechanisms are faster and more energy efficient than those associated with PoW and PoS.

It is the combined effect of consensus and hashing that make a DLT network highly tamper resistant, offering better protection from some forms of cyberattacks and improved resiliency to the impact of cybersecurity incidents. DLT avoids the risk of single points of failure that could disable the network and makes recovery easier given data is replicated throughout the system.[19] It also provides immediate notification of security breaches, which offers significant benefits given it can take an average of six months for organizations to discover a breach with other

systems.[20] For these reasons, DLT may provide greater efficiencies and security to the management of safeguards information.

The Ecosystem of Safeguards Information Management

Safeguards are a set of technical measures applied on nuclear material and activities to verify that nuclear facilities are not misused nor materials diverted for nuclear weapons purposes. The 1957 Statute of the IAEA provides the fundamental basis for the establishment of safeguards, which today are grounded within the 1970 Treaty on the Non-Proliferation of Nuclear Weapons (NPT) alongside regional nuclear-weapon-free zones and in multilateral trading guidelines such as the Nuclear Suppliers Group (NSG). As such, the global safeguards ecosystem is made up of states; facility operators; international, regional, and bilateral treaties; regimes and institutions; and their corresponding national legislation, rules, and regulations.

The management of safeguards information begins with the state, first at the facility level, with operators submitting nuclear material accounts to national regulatory authorities, which are responsible for establishing and maintaining a State System of Accounting for and Control of Nuclear Material (SSAC). The SSAC in turn submits declarations to the IAEA (via Euratom for European members or the Brazilian–Argentine Agency for Accounting and Control of Nuclear Materials for Argentina and Brazil). The amount and variety of information submitted to the IAEA has grown exponentially over the decades as the safeguards system has evolved and more states have adopted comprehensive safeguards agreements (CSAs), small quantity protocols (SQPs) and Additional Protocols. In 1983, the IAEA received 16,500 incoming reports.[21] Today, it receives around one million reports annually.[22]

All state declarations are held in a single internal IAEA database for nuclear material accounting (NMA), Additional Protocol, voluntary reporting and requests for termination, exemption, and reapplication of safeguards. The IAEA is also able to draw on trade data, commercial satellite imagery, environmental sampling and its surveillance cameras, complementary access visits, and open-sourced, third-party information. This combination of measures provides for information-driven safeguards and enables the agency to triangulate data in order to verify that states are honoring their obligations and for the IAEA to respond to any violations.

At the state level, national electronic (and paper-based) databases maintain a register of permit holders and set material-accountancy and (usually) physical-protection requirements to track nuclear material domestically and overseas. National databases include material measurements, record keeping, and preparation of submission of reports from facility operators to the SSAC. Material is grouped according to safeguards agreements, including a category for "foreign-obligated" material, that is, imported nuclear material that requires reporting to the IAEA and to the exporting state.

Adding a DLT Layer

The actors involved in the global safeguards information ecosystem are unmistakably centralized in their organization. They are also disparate in club memberships and highly untrusting of others. Sensitive information is shared within and among national, regional, and international institutions that operate under a variety of international, multilateral, and bilateral treaties and regimes that in turn have been evolving and expanding as obligations for sharing safeguards information have grown. With the variety of actors involved in generating, processing, and analyzing safeguards information, DLT systems may offer unique solutions for prioritizing confidentiality and information integrity while optimizing the reconciliation process and reducing time and costs.

Several design recommendations for a DLT system for safeguards information include:

- **A layer, not a substitute.** At this stage, DLT is not considered a replacement for current information management systems but an additional layer to provide access permissions, inputting, and processing of information exchange.
- **Permissioned.** Any DLT system for safeguards information would have to be permissioned, with the agency, state, regional authority, or facility serving as central authority. In the ecosystem of nuclear safeguards, actors must follow rules regarding the way classified information is stored, accessed, and submitted. The IAEA, for example, maintains a strict confidentiality commitment to its member states whereby only a state's representatives and relevant IAEA staff have access to that state's declaration. Similar rules apply to facility operators and national authorities. A permissioned system is the best way to meet those confidentiality requirements and can be constructed to meet participants' specific needs.
- **Energy efficiency.** The consensus mechanism developed should be energy efficient, avoiding the absurd energy usage associated with Bitcoin and its PoW model. A number of alternative mechanisms are being designed to be more efficient, particularly for permissioned systems.
- **Cost and integration.** Additional costs of hardware requirements for a DLT system should not be onerous, given the limited resources, tight budgets, and/or thin margins for possible participants. Similarly, a system would need to fit with participants' IT strategies and integrate or interface with current systems.
- **Language.** It must be multilingual, operating seamlessly within the IAEA's six official languages (Arabic, Chinese, English, French, Russian, and Spanish).

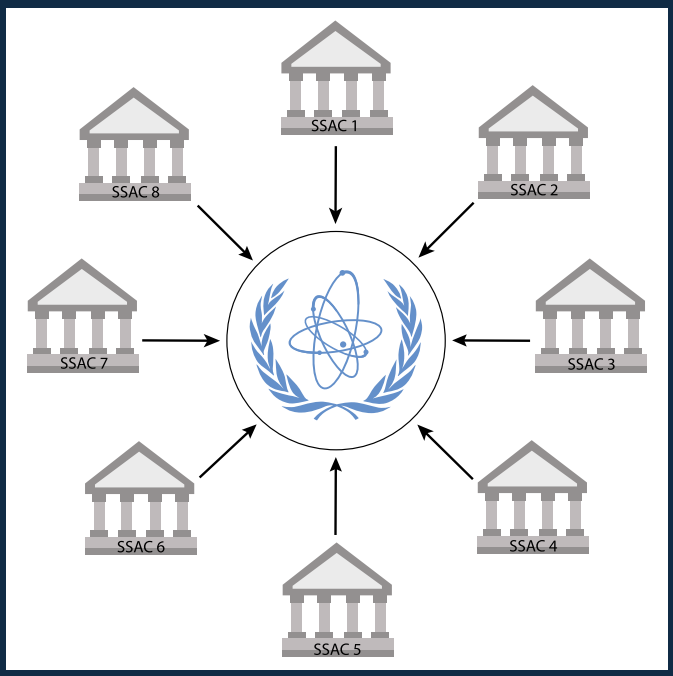


Figure 1. Potential Design of Nodes Within an IAEA DLT System

Potential for Proof of Concept

The research on the potential for DLT for safeguards, alongside closed discussions with safeguards and DLT experts, has identified a number of areas at the international, national, and facility levels where a DLT layer could provide advantages for efficiency and security in safeguards information management. The question for actors moving forward is whether DLT systems can offer strong enough benefits on efficiency, security, and integrity to remove the desire to rely on legacy practices. The main obstacles to adopting DLT technology reside in national policies on transmitting information and the long lag times in adapting legislation to emerging technologies.

At the International Level

Over the past ten years, the IAEA has been moving to a digital-based system for safeguards information management. Encrypted e-mail was introduced in 2005, with a two-computer encryption system (with public key infrastructure) used internally since 2007. In 2017, the agency launched the Safeguards Declarations Portal (SDP) as part of the Modernization of Safeguards Information Technology (MOSAIC) project, allowing SSACs and regional authorities to directly upload reports to the portal. This new system provides a layered approach to security, including key login, two-factor authentication, and end-to-end encryption. By the end of July 2018, approximately 25 states had begun to use the portal, with more signing up each week.[23]

The updated system provides a much-needed tune-up for the agency's information management system, but it is still challenged by a legacy of practice whereby a fair number of states still prefer hand-delivered hard-copy, CD, or thumb-drive submissions to the IAEA. The practice of using floppy disks was finally discontinued only five to six years ago.[24] The advantages of adding a DLT layer to the SDP would be to provide extra measures of cybersecurity and greater assurance that safeguards data has not been tampered with.

An added DLT layer to IAEA systems would still operate unidirectionally as the portal system, with data flowing from the state to the IAEA. It would allow both parties to see the transaction history and be assured that data is not corrupted or accessed by anyone other than the SSAC and the IAEA. Information shared by the SSAC cannot be shared across other SSACs (unless explicitly permitted to do so by the SSAC) as outlined in Figure 1. Moreover, by tracking when data is uploaded, viewed, and modified, all changes are permanently stored in the blockchain, and users would be notified immediately if there is an intrusion.

Exploratory research by Pacific Northwest National Laboratories highlighted the data challenges associated with transit matching that DLT platforms could theoretically address. Transit matching of inventory change reports (ICRs) involves the IAEA matching domestic and international shipments and receipts in and out of material balance areas (MBAs). This is connected to the information in the IAEA's database, where there is a need for both standardization and flexibility. Standardized codes for NMA are required to process large volumes of data within a system that is flexible enough to accommodate high numbers of data corrections and clarifications continually being added to the database (approximately 130,000 of the one million submissions processed annually are data corrections). Currently, the IAEA machine matches approximately 95 percent of domestic transfers and only 25 percent of foreign transfers, with the rest processed by hand. In 2014, approximately 3,000 to 4,000 records were unmatched in each quarter.[25]

Varied and delayed processing times also complicate transit-matching efforts. For example, nonnuclear weapon states are required to submit an ICR within 30 days of the end of the month when the transaction occurred (60 days for regional authorities), whereas nuclear weapon states are required to submit as soon as possible. Often one state may record one shipment in one month while the other logs the receipt a few months later. The receiving state might also parse out a shipment into four smaller batches/receipts. Moreover, some states voluntarily report to the IAEA changes related to "flag swaps," which decouples the original match (discussed below), requiring the IAEA to make a correction and rematch the transfer. DLT systems have the advantage of allowing for reconciliation of transit matching and consequently for more-efficient data analytics of transfers.

The IAEA and member states are also expanding the network of remote sensors used for safeguards, capitalizing on improvements in sensor capabilities, size, and cost along with other advances in the Internet of Things.[26] The IAEA currently has 1,250 surveillance

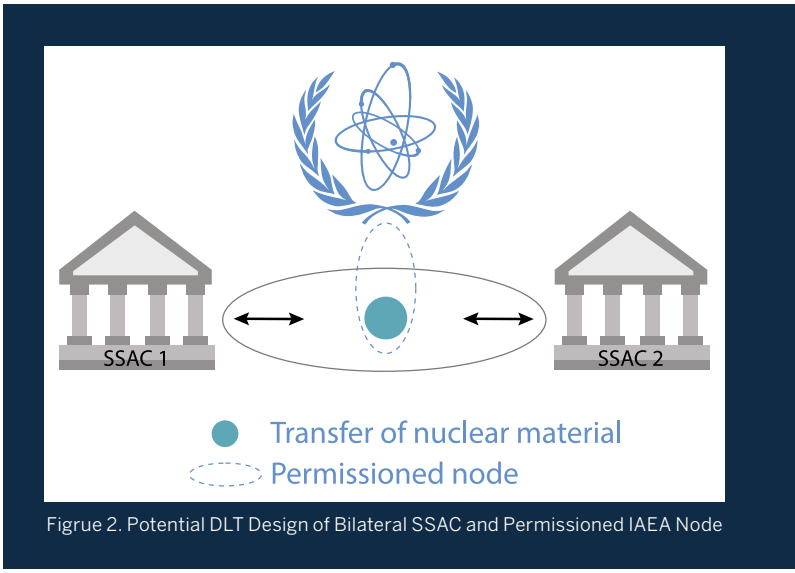
cameras installed in 250 facilities in 33 countries to remotely monitor the flow of materials alongside a variety of sensors (including radiation, pressure, temperature, flow, vibration, and electromagnetic sensors) to collect qualitative and quantitative data.[27] The system is computer based for data retrieval by the IAEA either on- or off-site. Not all states allow for remote electronic transmission of safeguards data across international borders. There is potential, however, for DLT to "black box" sensitive information while transmitting State of Health (SoH) to the IAEA, such as performance, connectivity, and operation of a camera.

Overall, DLT offers the agency the potential to streamline systems and optimize the reconciliation process, reducing time and costs, by providing an auditable, linked history of data—even if corrections are made years after the initial transaction is recorded. It also rejects changes that do not meet the consensus criteria, providing more trust in the traceability of submissions. In turn, DLT enables data analytics to identify patterns—an important function as the agency moves toward integrated safeguards and focusing on a state's nuclear activities as a whole.

State System of Accounting and Control

At the state level, SSACs have also been modernizing to integrated electronic databases with industry reporting digitally (with encryption) to SSACs. The number of submissions to the SSAC will vary depending on the breadth of a state's nuclear activities, the number of participants (operators and regulators) involved, and national and international rules and regulations. Similar to a DLT design for the IAEA, DLT options for SSACs would likely be unidirectional from operator to regulator, with information shared as needed among stakeholders, including bilateral information-sharing measures under nuclear cooperation agreements (NCAs). The latter are treaty-level requirements for the bilateral trade of nuclear material and technology by a number of states. NCAs go beyond IAEA safeguards requirements, essentially attaching "flags," or obligations, to material as it moves through the different stages of the nuclear supply chain globally. NCAs therefore tack on additional reporting requirements between states.

The practice of flag swaps under NCAs is one area where DLT solutions and "smart contracts" could make book transfers of material more efficient. These book transfers are used when a physical transfer would be allowed, but the actual physical transfer can be avoided by swapping materials at facilities. This allows operators with uranium originating from one supplier to relabel the material under the nationality of another to minimize transport costs, ensure timeliness of product availability at contract-specified quantities, meet unexpected demand requirements, and optimize inventories. Swaps of nuclear material can be complicated by the various physical and legal characteristics of the nuclear fuel, including the isotopic composition, location, mining and customs origins, safeguards obligations, and ownership. All require national guidance, a system of reporting, and procedures for prior approval.[28]



Figrue 2. Potential DLT Design of Bilateral SSAC and Permissioned IAEA Node

and across national authorities. Competing platforms by carriers (including TradeLens by IBM and Maersk) are dedicating efforts to use blockchain technology in the global shipping industry to reduce reliance on traditional paper-based transactions to streamline processes across borders and jurisdictions. To this end, DLT could also assist multilateral export control regimes, such as the NSG, which also use digital platforms in exchanging information related to denied transfers and proliferation trends. Although the technology is still maturing, and the results so far suggest one example may not fit all, there is promise in using DLT among disparate actors in an environment of mistrust.

Deep Geological Repository

The deep geological repository (DGR) is widely considered the best, safest option for long-term isolation and containment of spent nuclear fuel without future maintenance. As a newcomer to the nuclear fuel cycle, DGRs can fully integrate into the design process their safety, physical security, and safeguards considerations alongside the incorporation of emerging technologies, for verification purposes and/or long-term information management. Finland became the first country to issue a construction license for a DGR in 2015. Sweden and France are next in line. A handful of others are committed to national DGRs and are at varying stages in consent-based site selection.[30]

The lifetime of DGRs is multigenerational, stretching tens or even hundreds of thousands of years. DGRs will therefore generate, process, store, and submit large amounts of data related to the facility's construction, operation, environmental impact, physical security, safety, and nuclear material accountancy. To this end, long-term data integrity will be a priority for all stakeholders. Moreover, with physical verification not feasible after closure, there will be a reliance on continuous containment and surveillance (C/S) safeguards measures, such as sensors, satellite imagery, and surveying techniques. As remote sensor data expands and information and knowledge preservation are defined for DGRs, these next-generation facilities are primed for digital

integration and to be the first nuclear facilities to test a proof of concept in applying DLT to safeguards information management. DGRs could benefit from the full sweep of advantages that DLT systems can offer on integrity, cybersecurity, and efficiency for the management of safeguards information.

Conclusion

Proof of concepts will be the first step to understanding the plausibility of DLT for safeguards information management. It would not be difficult to configure a permissioned DLT to meet specifications of the organizations involved, whether national, bilateral, multilateral, or within the IAEA. The bigger hurdles to adoption will be acceptance by member states, with each having its own policies for information exchange and technology practices, as well as different ideas on how to create greater resource efficiencies within the IAEA and different lead times in adoption of emerging technologies.

The application of DLT to nuclear safeguards information management will not displace the essential role of the IAEA as a central authority nor diminish the importance of its work. Instead, it could add layers of security and traceability to better control and streamline data that in turn can facilitate more-effective safeguards implementation. The technology therefore will not radically transform the safeguards information ecosystem, but it will allow operations to be refined and adapted to an evolving safeguards system. The technology is still maturing, but there is promise in its use among actors that mistrust one another. It may not solve every problem, but it is much better than the floppy.

Endnotes

1 Skot Thayer and Alex Hern, "Rohingya Turn to Blockchain to Solve Identity Crisis," *Guardian*, August 20, 2018, https://www.theguardian.com/world/2018/aug/21/rohingya-turn-to-blockchain-to-solve-identity-crisis; Siobhan Kenna, "How Blockchain Technology Is Helping Syrian Refugees," HuffPost, November 28, 2017, https://www.huffingtonpost.com.au/2017/11/05/how-blockchain-technology-is-helping-syrian-refugees_a_23267543/; Everledger, "Do You Know Your Diamond?," *https://diamonds.everledger.io/*; Maersk, "Maersk and IBM Introduce TradeLens Blockchain Shipping Solution," August 9, 2018, https://www.maersk.com/news/2018/06/29/maersk-and-ibm-introduce-tradelens-blockchain-shipping-solution.

2 International Development Research Centre, "Blockchain: Unpacking the Disruptive Potential of Blockchain Technology for Human Development," white paper, August 2017, p. 38; see also United Nations System, Secretariat of the Chief Executives Board for Coordination, "Compendium of Responses to the CEB Survey on Frontier Issues," October 27, 2017, p. 474, https://www.unsceb.org/CEBPublicFiles/CEB_Survey_Compendium.pdf.

3 IAEA, "Research and Development Plan Enhancing Capabilities for Nuclear Verification," STR-385 January 2018, p. 15.

4 IAEA, Symposium on International Safeguards, "Building Future Safeguards Capabilities," https://www.iaea.org/events/symposium-on-international-safeguards-2018.

5 See Florin Abazi, John Coyne, Scott Partee, Alex Sunshine, and Adem Mutluer, "MOSAIC—The Modernization of Safeguards Information Technology," Institute of Nuclear Materials Management (INMM) Annual Meeting Proceedings, July 2018, https://www.inmm.org/Events/Annual-Meeting/International-Safeguards-Abstracts#Abstract%20#409; IAEA, "The Modernization of Safeguards Information Technology: Completing the Picture," January 24, 2017, https://www.iaea.org/sites/default/files/17/01/mosaic.pdf.

6 Satoshi Nakomoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008, p. 1, https://bitcoin.org/bitcoin.pdf.

7 For a more technical explanation of DLT and blockchain, see Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone, "Blockchain Technology Overview," National Institute of Standards and Technology, January 2018, https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf.

8 Michael Rauchs et al., "Distributed Ledger Technology Systems: A Conceptual Framework," Cambridge Centre for Alternative Finance, August 2018, p. 24, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-08-20-conceptualising-dlt-systems.pdf.

9 "Blockchain and Distributed Ledger Technologies," *BlockchainHub*, accessed September 15, 2018, https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/.

10 Rauchs et al., "Distributed Ledger Technology Systems," pp. 58-60.

11 KlickEx, for example, is a blockchain payment solution for central banks in 12 currency corridors across the Pacific Islands, Australia, New Zealand, and the United Kingdom.

It delivers regional micropayment facilities connected to mobile banking services that enable real-time person-to-person payments internationally. Presentation by IBM to Stimson, September 13, 2018. See also "KlickEx," KlickEx, https://www.klickex.co/. In Japan, a blockchain consortium of financial institutions, led by the Japan Exchange Group, is testing DLT for capital market infrastructure. See "Proof of Concept Testing for Utilization of Blockchain/DLT in Capital Market Infrastructure," Japan Exchange Group, https://www.jpx.co.jp/english/corporate/research-study/dlt/index.html.

[12]

[13] Estonia is the first to fully install an e-government, using blockchain technology to protect national data, e-services, and smart devices. See "Estonian Blockchain Technology," e-Estonia, accessed Feb 26, 2018, https://e-estonia.com/wp-content/uploads/faq-a4-v02-blockchain.pdf.

[14] "Dubai Blockchain Strategy," Smart Dubai, accessed Feb 28, 2018, https://smartdubai.ae/en/Initiatives/Pages/DubaiBlockchainStrategy.aspx.

[15] It is estimated that both Bitcoin and Ethereum burn over $1 million USD of electricity and hardware costs per day as part of their respective transaction verification mechanisms. See "AERO: Enabling the Drone Superhighway Using the Blockchain," *Hacker Noon*, September 24, 2017.

[16] A few nodes now control a large share of the mining market. The top five companies control over 50 percent. See International Development Research Centre, "Blockchain: Unpacking the Disruptive Potential," p. 29.

[17] Andre Boaventura, "Demystifying Blockchain and Consensus Mechanisms—Everything You Wanted to Know but Were Never Told," Oracle Developers, April 12, 2018, https://medium.com/oracledevs/demystifying-blockchain-and-consensus-mechanisms-everything-you-wanted-to-know-but-were-never-aabe62145128; Blockchain Hub, "Consensus Mechanisms," July 4, 2018, https://blockchainhub.net/blog/blog/consensus-mechanisms-2/.

[18] Elli Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," April 17, 2018, https://arxiv.org/abs/1801.10228v1.

[19] Erin English, Amy Davine Kim, and Michael Nonaka, "Advancing Blockchain Cybersecurity," Microsoft, 2018, https://www.microsoft.com/en-us/cybersecurity/content-hub/advancing-blockchain-cybersecurity.

[20] Ponemon Institute, "2017 Cost of Data Breach Study: Global Overview," June 2017, p. 6, https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf.

[21] IAEA, IAEA Safeguards Information System (ISIS), IAEA-TECDOC-316, (1984), p. 17.

[22] Discussions during Stimson-Stanley Center for Peace and Security roundtables on DLT, 2018.

[23] Ibid.

[24] Ibid.

[25] S.L. Frazar, M.J. Schanfein, K.D. Jarman, C.L. West, C.A. Joslyn, S.T. Winters, S.J. Kreyling, and A.M. Sayre, "Exploratory Study on Potential Safeguards Applications for Shared Ledger Technology," Pacific Northwest National Laboratory, February 2017, p. 27.

[26] E. Galdoz, O. Calzetta, S. Fernancez Moreno, and C. Llacer, "Remote Monitoring in Safeguards: Security of Information and Enhanced Cooperation," paper presented at the INMM 52nd Annual Meeting, Palm Desert, California, 2011.

[27] Frazar et al., "Exploratory Study," p. 28.

[28] Cindy Vestergaard, "Governing Uranium Globally," Danish Institute for International Studies report, pp. 96-101.

[29] See "Smart Contracts," BlockchainHub, https://blockchainhub.net/smart-contracts/.

[30] "What Other Countries Are Doing," Nuclear Waste Management Organization, 2018, https://www.nwmo.ca/en/Canadas-Plan/What-Other-Countries-Are-Doing.

About the Author

Cindy Vestergaard, Ph.D. is the director of the Nuclear Safeguards Program at the Stimson Center. Her current research focuses on the impact of evolving international safeguards obligations on states and facility operators. Her portfolio also includes chemical weapons disarmament, biosecurity, and import/export controls. Previous to Stimson, Dr. Vestergaard was a senior researcher at the Danish Institute for International Studies in Copenhagen, Denmark. Before that she worked on nonproliferation, arms control, and disarmament policy and programming at Canada's Department of Foreign Affairs and International Trade.

Analysis and New Insights are thought-provoking contributions to the public debate over peace and security issues. The views expressed in this brief are those of the author. The author's affiliation is listed for identification purposes only.

About Us

The Stanley Center for Peace and Security partners with people, organizations, and the greater global community to drive policy progress in three issue areas—mitigating climate change, avoiding the use of nuclear weapons, and preventing mass violence and atrocities. The center was created in 1956 and maintains its independence while developing forums for diverse perspectives and ideas. To learn more about our recent publications and upcoming events, please visit stanleycenter.org.

This paper contains 100 percent post-consumer fiber, is manufactured using renewable energy—Biogas—and processed chlorine free. It is FSC®, Rainforest Alliance™, and Ancient Forest Friendly™ certified.

BIOGAS ENERGY PERMANENT TCF

10/18