BLOCKCHAIN AND SAFEGUARDS INFORMATION MANAGEMENT
The Potential for Distributed Ledger Technology

Cindy Vestergaard
Stimson Center
Washington, D.C., United States of America
Email: cvestergaard@stimson.org

Abstract

The ability of blockchain technology to manage large volumes of data in a distributed, secure and transparent manner has potentially far-reaching value for the way safeguards information is collected, processed and analysed. The Stimson Center, in partnership with the Stanley Foundation, held a series of workshops in 2018 from Vienna to Silicon Valley to discuss this potential. The findings and recommendations in the paper consider the ecosystem of safeguards information management, specifically the landscape of factors determining how safeguards data is inputted, processed and accessed. It suggests how distributed ledger technology (DLT) could be applied, if at all, to provide greater efficiency, data reconciliation, accuracy and trust in information management. The paper also touches upon the potential for DLT to be applied to export controls and supply chain auditing.

1. INTRODUCTION

Over the past few years, the excitement surrounding blockchain has been intensifying. The technology, which is the distributed ledger technology underlying cryptocurrencies such as bitcoin, is considered revolutionary, not just in its potential to alter the world economy, but for all industries, whether providing digital identification for refugees [1], cybersecurity for British nuclear power plants [2] or streamlining the global shipping industry [3]. In 2018, the Stimson Center and the Stanley Foundation partnered on a project “Blockchain and Nuclear Safeguards” to bring together experts and stakeholders at a series of roundtables to consider the application of distributed ledger technology (DLT) to the management of safeguards information. The results suggest there is space for further exploration, including potential cases for testing a proof of concept. At this stage, DLT is not considered a replacement of current information management systems but as an additional layer to provide access permissions, inputting and processing of information exchange.

2. DLT BY DESIGN

Although still in its infancy, the potential of distributed ledger technology is in its ability to record, store and replicate transactions across different participants and locations in ways that are highly tamper resistant. It is a combination of already-existing technologies (such as cryptography) interlinked in a unique way to provide a network ability to securely manage and easily audit large volumes of data. The name blockchain refers to “blocks” added to transaction records which are recorded across, and therefore transparent to, all nodes in a system. It is one form of DLT, but not all DLTs use blockchain.

Common features across DLT platforms are secure hashing and consensus techniques to allow for information integrity. Each piece of data is hashed with a digital fingerprint, or cryptographic representation (versus a secret key), which is timestamped and mathematically linked to previous data. A set of distributed algorithms form the consensus mechanism to triangulate the correctness of data, thereby verifying valid information and rejecting invalid data from being added to the database. The types of consensus mechanisms vary across DLT networks, from “proof of work” [4] associated with Bitcoin to consensus ledgers whereby only the balance of member accounts is updated after each validation round (instead of grouping and chaining transactions). Hyperledger, for example, uses “endorsement policies” to guide which network users must endorse certain transactions against a set of policy criteria [5]. The combined effect of hashing and consensus make a DLT network difficult to compromise while providing for a verifiable, immutable history of information stored in the database.

Depending on the consensus mechanism, the architecture of a DLT system can be public (open) or restricted to a specified group (private), allowing only parties involved in a transaction or data exchange to have a copy of it. In both types, each member in the network may have access to the entire ledger or only a part of it and, in all cases, can contribute with data [6]. Permissioned (private) databases can also plug in others such as a regulator, or another party as needed (and permitted). Given a strict confidentiality commitment by the International Atomic Energy Agency (IAEA) to its member states, only the State's representatives and relevant IAEA staff have access to that State's declaration. Accordingly, any DLT option for the IAEA would have to be private and maintain the role of the Agency as primary sponsor. It would require an immutable transaction history flexible enough to allow for a back-and-forth of clarifications and corrections between the State and the IAEA, and from inspectors in the field. It must be multilingual, operating seamlessly within the IAEA's six official languages (Arabic, Chinese, English, French, Russian and Spanish).

3. POTENTIAL TEST CASES

Safeguards information management 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 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). Initially paper-based in both SSACs and the IAEA, the management of safeguards information has been evolving to digital-based systems. With a variety of actors involved in the generating, processing and analysis of safeguards information, DLT systems can be constructed to meet the needs of a specific facility, SSAC and regional and international organizations. Obstacles to adopting DLT technology reside mainly in national policies on transmitting information and the long lag times in adapting legislation to emerging technologies.

3.1. Adding a DLT Layer to the IAEA

At the international level, all declarations are held in a single, internal IAEA database for all States for nuclear material accounting (NMA), Additional Protocol, voluntary reporting and requests for termination, exemption and re-application of safeguards. The Agency 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 [7]. As the number of States with Comprehensive Safeguards Agreements (CSAs), Small Quantity Protocols (SQPs) and Additional Protocols has grown, the amount and variety of information submitted to the IAEA has also grown. In 1983, the IAEA received 16,500 incoming reports [8]. Today, around one million reports are received annually [9].

Over the past ten years, the IAEA has been moving to a digital-based system for safeguards information management. The Agency introduced encrypted email in 2005, using a two-computer encryption system (with PKI encryption) 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 [10]. By the end of July 2018, approximately 25 States had begun to use the portal and more signing up each week [9].

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 hardcopy, CD or thumb drive submissions to the IAEA (the practice of using floppy disks was finally discontinued 5-6 years ago) [9] [10].

An added DLT layer would still operate unidirectionally as the portal system, with data flowing from the State to the IAEA, but 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 [10]. 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. The question for States carrying forward practice legacies is whether DLT and the design of the consensus mechanism can offer strong enough security guarantees regarding encryption and authentication to remove the intermediary.

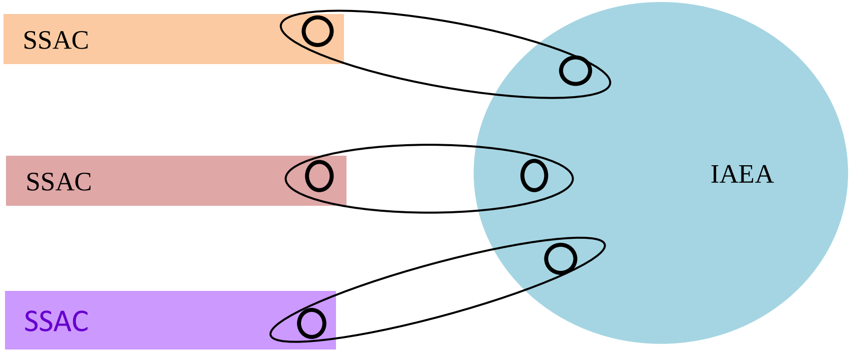

FIG. 1. Potential Design of Nodes within IAEA DLT system

DLT platforms can theoretically address the data challenges associated with transit matching of inventory change reports (ICRs), i.e. the matching of domestic and international shipments and receipts in and out of material balance areas (MBAs), which in turn are connected to the information in the IAEA's database. Transit matching illustrates a constant tension between standardization and flexibility within safeguards implementation in which 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) [9] [11]. Currently, the Agency machine-matches approximately 95% of domestic transfers and only 25% of foreign transfers with the rest manually processed by hand [11]. In 2014, there were approximately 3,000 - 4,000 records unmatched in each quarter [11].

The IAEA and member states are also expanding the network of remote sensors used for safeguards, capitalizing on advances in other technologies, such as in electronics and the Internet-of -Things (IoT) [12]. Along with concerns about connectivity and data security, technological advances in sensors and IoT also generate additional and varied data sets that can overrun existing databases. Work is being done on consensus mechanisms linked to IoT devices in a network without requiring the hefty computing power needed for proof-of-work. In April 2018, for example, IBM applied to patent a method for connected devices to execute blockchain-based smart contracts [13].

Overall, DLT offers 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 towards integrated safeguards and focusing on a State's nuclear activities as a whole.

3.2 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. These national databases maintain a register of permit-holders and track nuclear material domestically and overseas. The number of safeguards 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 the country's 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 bilateral trade of nuclear material and technology by a number of States which go beyond IAEA safeguards requirements, essentially attaching 'flags' or obligations to material as it moves globally through the different stages of the nuclear supply chain. The practice of "flag swaps" under NCAs is one area where DLT solutions and their "smart contracts" (essentially the representation of data on a ledger) could make book transfers of material more efficient. A proof of concept for an SSAC would therefore need to consider the various physical and legal characteristics of swaps that require national guidance, a system of reporting and procedures for prior approval [10]. DLT could be a solution for creating greater efficiencies in registering and processing swaps which in turn would further improve transit matching by the IAEA by permitting information related to specific transfers to be securely shared not just with another SSAC but also with the IAEA as depicted in Figure 2 [10].

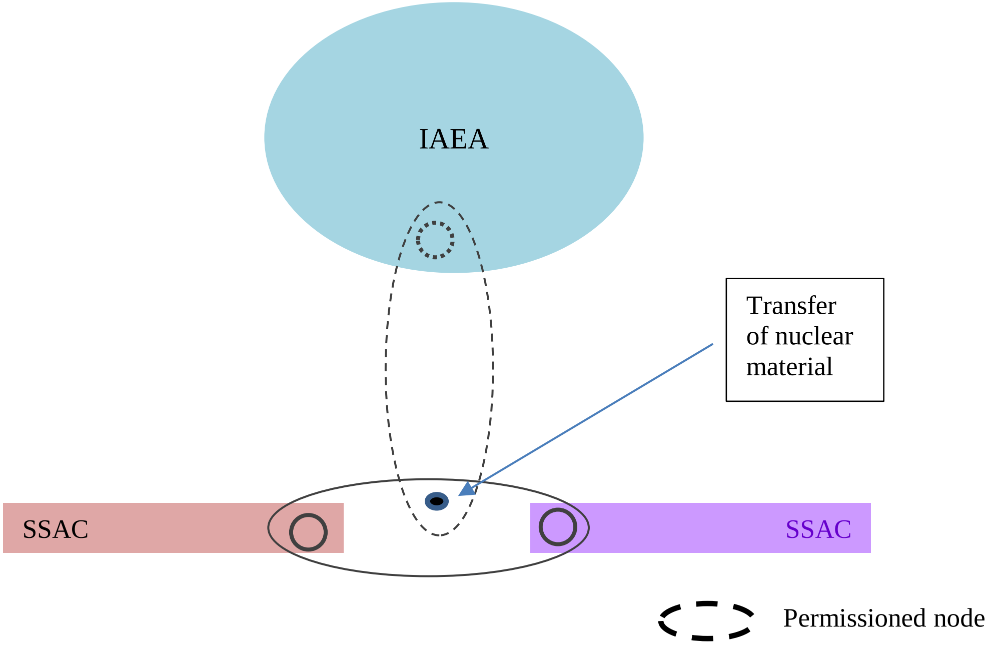

FIG. 2. Potential DLT Design of Bilateral SSAC and Permissioned IAEA Node

DLT could also better streamline export controls for nuclear (and other) materials and technologies and provide for greater assurances in the integrity of the nuclear supply chain. Competing platforms by carriers (including TradeLens by IBM and Maersk [3]) 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 Nuclear Suppliers Group, which also use digital platforms in exchanging information related to denied transfers and proliferation trends. Although the technology is still maturing, the results so far suggest one example may not fit all, but there is promise in using DLT among disparate actors in an environment of mistrust.

3.3 Deep Geological Repository

As the global nuclear fuel cycle becomes increasingly a back-end fuel cycle, 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, the design process for DGRs can fully integrate safety, physical security and safeguards considerations alongside the incorporation of emerging technologies, whether for verification purposes and/or long-term information management. In 2017, Finland became the first country to issue a construction license for a DGR. 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 [14].

As a central site for a State's used fuel, coupled with its multigenerational lifecycle stretching tens or even hundreds of thousands of years, DGRs will 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 [10]. Long-term data integrity will be a priority for all stakeholders. The IAEA notes that "information and knowledge preservation and transfer" for DGRs "are activities which need to be carefully defined and implemented over time. However, there is no practical experience available at this stage" [15].

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. Instrumentation is still to be developed and involves the consideration of technologies such as 3-D laser scanning and advances in geophysical exploration for remote monitoring [16]. As the "Internet of Nuclear Things" [17] expands, DGRs are primed for digital integration and to be the first facilities to test a proof of concept in applying DLT to safeguards information management.

4.0 CONCLUSION

Although the term "disruption" is not generally a welcomed one in nuclear field, the innovation of distributed ledger technology has potentially far-reaching value for the way safeguards information is collected, processed and analysed. One of the biggest hurdles to the adoption of DLT will be acceptance by States, each with different policies for information and technology practices as well as a range of ideas for how to create greater efficiencies. International organizations lag farther behind, taking upwards of five to ten, even fifteen years to adopt technological advancements.

Proof of concepts will be the first step to understanding the plausibility of DLT for safeguards information management, particularly in demonstrating that risks related to cryptography can be mitigated. The research suggests applicability to various aspects of safeguards implementation, from the facility to the SSAC and IAEA. The technology is still maturing, but there is promise in its use among actors that mistrust another.

ACKNOWLEDGEMENTS

This research is made possible by the generous financial and logistical support of the Stanley Foundation in bringing experts and stakeholders together to discuss the potential of distributed ledger technology for the management of safeguards information. The author is especially grateful to Benjamin Loehrke, Policy Program Officer, Nuclear Policy at the Stanley Foundation for his wit, humour, patience and dedicated efforts as the project has progressed. To him, and to the experts from the DLT community, IAEA, national regulators and labs that have participated in the various roundtables, I raise the glass with a resounding Blockchain!

REFERENCES

[1] Such as the Rohingya Project (http://www.rohingyaproject.com/about/) and the Building Blocks Project for displaced Syrians (https://www.huffingtonpost.com.au/2017/11/05/how-blockchain-technology-is-helping-syrian-refugees_a_23267543/). Both accessed 20 July 2018.

[2] COINFOX, Guardtime: Blockchain to guard nuclear power plants, http://www.coinfox.info/news/4316-guardtime-using-blockchain-to-guard-industries, (2016).

[3] MAERSK, Maersk and IBM Introduce TradeLens Blockchain Shipping Solution, (2018), https://www.maersk.com/news/2018/06/29/maersk-and-ibm-introduce-tradelens-blockchain-shipping-solution.

[4] PORAT, A., PRATAP, A., SHAH, P., ADKHAR, V., Blockchain Consensus: An analysis of Proof-of-Work and its applications, http://www.scs.stanford.edu/17au-cs244b/labs/projects/porat_pratap_shah_adkar.pdf, Stanford. Accessed 24 August 2018.

[5] HYPERLEDGER Hyperledger Fabric Model, (2018), https://hyperledger-fabric.readthedocs.io/en/release-1.2/fabric_model.html#consensus.

[6] EUROPEAN CENTRAL BANK, "Distributed Ledger Technology," In Focus, Issue 1, (2016) 2.

[7] IAEA, IAEA Safeguards: Staying Ahead of the Game, (2007), 16.

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

[9] DISCUSSIONS DURING STIMSON-STANLEY FOUNDATION ROUNDTABLES ON DLT, 2018.

[10] VESTERGAARD, C., "Better than Floppy: The potential of distributed ledger technology for nuclear safeguards information management," Stanley Foundation, (in preparation).

[11] FRAZAR, SL., SCHANFEIN, MJ., JARMAN, KD., WEST, CL., JOSLYN, CA., WINTERS, ST., KREYLING, SJ., and SAYRE, AM., Exploratory study on potential safeguards applications for shared ledger technology, Pacific Northwest National Laboratory, (2017) 27.

[12] GALDOZ, E., CALZETTA, O., FERNANDEZ MORENO, S., LLACER, C., "Remote Monitoring in Safeguards: Security of Information and Enhanced Cooperation," Paper presented at the INMM 52nd Annual Meeting, Palm Desert, (2011).

[13] US PATENT & TRADEMARK OFFICE, Proof-of-Work for Smart Contracts on a Blockchain, (2018), http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20180115425.PGNR.&OS=dn/20180115425&RS=DN/20180115425.

[14] NUCLEAR WASTE MANAGEMENT ORGANIZATION, What Other Countries Are Doing, (2018), .https://www.nwmo.ca/en/Canadas-Plan/What-Other-Countries-Are-Doing.

[15] IAEA, The Management System for the Development of Disposal Facilities for Radioactive Waste, IAEA Nuclear Energy Series, No. NW-T-1.2, (2011) 17.

[16] WANG, J., LIANG, C., SU, R., ZHAO, X., The Beishan underground research laboratory for geological disposal of high-level radioactive waste in China: Planning, site selection, site characterization and in situ tests, Journal of Rock Mechanics and Geotechnical Engineering, (2018).

[17] HOFFMAN, W., VOLPE, T.A., An Internet of Nuclear Things: Emerging Technology and the Future of Supply Chain Security, Policy Analysis Brief, Stanley Foundation, (2018).