PNNL-26229

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

Exploratory study on potential safeguards applications for shared ledger technology

February 2017

SL Frazar
KD Jarman
CA Joslyn
SJ Kreyling
AM Sayre
MJ Schanfein
CL West
ST Winters

U.S. DEPARTMENT OF
ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <http://www.ntis.gov/about/form.aspx>
Online ordering: http://www.ntis.gov

This document was printed on recycled paper.
(8/2010)

PNNL-26229

Exploratory study on potential safeguards applications for shared ledger technology

SL Frazar
KD Jarman
CA Joslyn
SJ Kreyling
AM Sayre
MJ Schanfein
CL West
ST Winters

February 2017

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Summary

The International Atomic Energy Agency (IAEA) is responsible for providing credible assurance that countries are meeting their obligations not to divert or misuse nuclear materials and facilities for non-peaceful purposes. To this end, the IAEA integrates information about States' nuclear material inventories and transactions with other types of data to draw its safeguards conclusions. As the amount and variety of data and information has increased, the IAEA's data acquisition, management, and analysis processes have greatly benefited from advancements in computer science, data management, and cybersecurity during the last 20 years. Despite these advancements, inconsistent use of advanced computer technologies as well as political concerns among certain IAEA Member States centered on trust, transparency, and IAEA authorities limit the overall effectiveness and efficiency of IAEA safeguards. As a result, there is an ongoing need to strengthen the effectiveness and efficiency of IAEA safeguards while improving Member State cooperation and trust in the safeguards system. These chronic safeguards needs could be met with some emerging technologies, specifically those associated with the digital currency bitcoin.

In 2009, bitcoin was released as a digital currency with the intent to disrupt the traditional paradigm of trust in financial systems. Meaning, bitcoin users would place their trust in computer algorithms and electronic ledgers, rather than banks, to monitor and record their financial transactions. As bitcoin's popularity grew, and experts became more familiar with bitcoin's underlying technology, the blockchain, some began to consider the blockchain as having "even greater potential to change how we make transactions online."[1]

Soon, research expanded into an exploration of a broader set of shared ledgers that are enabled by blockchain technology. Such shared ledger technology (SLT) marries existing state-of-the-art cryptographic techniques, modern information technology tools, and electronic distributed ledgers to maintain a history of transactions.[2] SLT, most simply, offers a way for parties that may or may not trust each other to maintain a history of financial and other types of exchanges, including exchanges of physical goods and information. This research eventually involved an exploration of how "smart contracts" might layer in legal agreements in the SLT to solve more complex problems.

This gradual transition away from using blockchain and other SLTs strictly for decentralized peer-to-peer financial transactions has raised the question whether such technologies might benefit other types of systems involving multiple parties, such as the international safeguards system. Specifically, could SLT improve the effectiveness or efficiency of certain activities or by promoting cooperation and trust in the safeguards system?

Accordingly, the Office of International Nuclear Safeguards at the National Nuclear Security Administration (NNSA) commissioned the Pacific Northwest National Laboratory to explore the potential

[1] Naomi LaChance, "Not Just Bitcoin: Why the Blockchain Is a Seductive Technology to Many Industries," *NPR* (2016), Accessed May 17, 2016 at http://www.npr.org/sections/alltechconsidered/2016/05/04/476597296/not-just-bitcoin-why-blockchain-is-a-seductive-technology-to-many-industries?utm_source=facebook.com&utm_medium=social&utm_campaign=npr&utm_term=nprnews&utm_content=20160507.

[2] https://gendal.me/2015/04/27/how-to-explain-the-value-of-replicated-shared-ledgers-from-first-principles/

implications of these rapidly evolving technologies on safeguards. The salient finding from this work is that SLT offers a spectrum of benefits to the safeguards system. SLT can be used to promote efficient, effective and timely reporting, but SLTs are not unique in offering this solution. Modern databases and information technology solutions may be just as, if not more effective, to advance these objectives. However, SLT solutions are unique in their ability to increase transparency in the safeguards system without sacrificing confidentiality of safeguards data. This increased transparency and involvement of Member States in safeguards activities involving digital transactions could lead to increased trust and cooperation among States, which generates a number of benefits that are described in this study.

It is important to add that most of the SLT ideas explored in this study are centered on the use of cryptography. If the idea of using cryptography, in particular if sharing encrypted data with other Member States is unacceptable, then there may be limited to no utility in using this technology for safeguards. That said, many Member States already rely on encryption when they send their sensitive reports to the IAEA. SLT is capable of using the same level of encryption to protect sensitive transactions. Additional cryptographic techniques are applied, making SLT effectively impossible to hack. The perceptions about the security of this emerging technology will only be addressed through further testing and validation, which may demonstrate that SLTs are as secure, if not more secure, than current practices.

Ultimately, further testing of different SLT environments specifically addressing safeguards problems is needed to validate projections about how the technology will grow. To that end, a variety of actions can be taken to explore the collective benefits and contributions to safeguards:

- Identify opportunities to engage companies experimenting with SLT to address non-financial problems. Such engagement will be critical to track advancements in the field and monitor opportunities to validate or refute the ideas presented in this study.
- Engage the Office of Research and Development to fund S&T research related to SLT (e.g., consortium consensus mechanisms, homomorphic encryption, etc.). Such research might involve design and development of a pilot SLT that is specifically designed around a set of safeguards requirements selected by NNSA and IAEA.
- Socialize the concept of SLT with the IAEA and selected Member States and document the feasibility and desirability of implementing SLT for safeguards purposes.

Acronyms and Abbreviations

DAO	Decentralized Autonomous Organization
GPS	Global Positioning System
IAEA	International Atomic Energy Agency
ICR	inventory change report
IT	information technology
NNSA	National Nuclear Security Administration
PNNL	Pacific Northwest National Laboratory
SLC	State Level Concept
SLT	shared ledger technology
UMS	Unattended and Surveillance Monitoring System

Contents

Figures

Tables

1.0 Introduction

The International Atomic Energy Agency (IAEA) is responsible for providing credible assurances that countries are meeting their obligations not to divert or misuse nuclear materials and facilities for non-peaceful purposes. To this end, the IAEA integrates information about States' nuclear material inventories and transactions with other types of data[3] to draw its safeguards conclusions. As the amount and variety of data and information has increased, the effectiveness and efficiency of the IAEA's data acquisition, management, and analysis processes have greatly benefited from advancements in computer science, data management, and cybersecurity during the last 20 years. However, the IAEA and its Member States have yet to take full advantage of recent technological developments that could strengthen the security, effectiveness, and efficiency of safeguards activities.

Meanwhile, political challenges centered on trust, transparency, and Agency authorities persist, creating a number of thorny strategic issues for the IAEA. For example, the IAEA is developing and applying in a limited context the State Level Concept (SLC), which is a comprehensive approach to implementing safeguards that uses all relevant information about a State's nuclear program to draw safeguards conclusions. Key principles underlying the SLC are that implementation should be "non-discriminatory," "independent," and "objective."[4] Despite significant investments in IAEA infrastructure and operations to support a transition to the SLC in ways that are aligned with these principles, some States continue to voice "suspicions that the approach is discriminatory and allows for the use of political, rather than objective technical factors to guide safeguards implementation. The use of intelligence information provided by Member States has also played into this concern."[5] In short, despite significant efforts to demonstrate a commitment to objectivity and nondiscrimination, the IAEA is still confronted with mistrust by some States. This environment creates a compelling rationale to examine new technologies that could contribute to more trusting relationships.

This study focuses on the emerging area of shared ledger technology (SLT), which has the potential to both increase the trust and transparency in some of the many regulatory processes executed by the IAEA and also serve as an efficient and modern information technology (IT) solution. SLT, most simply, offers a way for parties that may or may not trust each other to maintain a consistent, immutable transaction history (of exchanges of physical goods, money, information, etc.).

The first mainstream example of SLT was bitcoin, a digital "cryptocurrency" introduced in 2009. As interest in bitcoin grew, technologists began to explore other uses of its underlying ledger technology, the blockchain. Researchers recognized that the blockchain facilitating bitcoin transactions was designed for a very specific set of functional requirements. If a different set of functional requirements existed, they would likely require a different type of ledger. Meaning, the core "services" of the blockchain remained desirable regardless of the ledger design. Over time, the marriage of existing state-of-the-art

[3] Such data sources include State inventory declarations, inspections at facilities and other locations, unattended monitoring systems installed in selected facilities, open source information, third party information, documents detailing material shipments between facilities, and process monitoring systems.
[4] International Atomic Energy Agency. "The Conceptualization and Development of Safeguards Implementation at the State Level." GOV/2013/38. 12 August 2013.
[5] Fact Sheet #3: Information Relevant to the IAEA General Conference. "Topic: Safeguards Resolution." Vienna, September 2014. Available here: http://www.nonproliferation.org/wp-content/uploads/2014/09/2014_IAEA_GC_QA_Safeguards.pdf

cryptographic techniques with modern IT tools and distributed ledger technology like blockchain began to be referred to as shared ledger technologies. Different shared ledger designs could be considered when solving a wide variety of problems. [6],[7]

SLT has a number of features and possible uses that could benefit certain safeguards functions, particularly functions involving digital communications. The goal of this study is to explore conceptually whether these features have the potential to make positive contributions to the international safeguards system. As part of this study, the Pacific Northwest National Laboratory (PNNL) considered several questions and scenarios to determine whether, and to what extent, SLT might improve the effectiveness, efficiency, security, transparency, or State confidence in specific safeguards functions.

This study begins with a description of the methodology used to conduct the analysis. Section 3.0 describes IAEA objectives and key functional requirements for new technologies. Section 4.0 provides an overview and history of SLT. Sections 5.0-6.0 propose an analytical framework for evaluating whether different SLT models are likely to achieve safeguards objectives or functional requirements. Finally, the study turns to specific safeguards use cases to help demonstrate the potential applicability of different SLT models. The paper concludes with findings and recommendations.

Findings and recommendations from this study benefit the National Nuclear Security Administration's (NNSA) Office of International Nuclear Safeguards' Concepts and Approaches Program, which sponsors National Laboratories to explore the implications and impact of advanced technologies on the international safeguards system.

2.0 Methodology

The project team comprised safeguards and SLT subject matter experts. The teams worked on a variety of tasks in parallel to establish a useful foundation for discussion. The safeguards experts performed a literature review of relevant safeguards publications, including model safeguards agreements,[8] IAEA guidance documents on safeguards implementation practices[9], and the IAEA's long-term R&D plan[10] to define the safeguards context in which SLT could potentially be applied. The team identified and evaluated several use cases involving safeguards activities with digital safeguards elements, including information reporting, transit matching, nuclear material shipment tracking, and unattended remote monitoring systems. For sake of completeness, the team also considered export control

[6] https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/

[7] https://gendal.me/2015/06/08/towards-a-unified-model-for-replicated-shared-ledgers/

[8] IAEA - International Atomic Energy Agency. 1972. The Structure and Content of Agreements Between the Agency and States Required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons. INFCIRC/153, International Atomic Energy Agency, Vienna, Austria. Available at https://www.iaea.org/publications/documents/infcircs/structure-and-content-agreements-between-agency-and-states-required

[9] IAEA - International Atomic Energy Agency. 2014. *Guidance for States Implementing Comprehensive Safeguards Agreements and Additional Protocols.* Service Series 21, International Atomic Energy Agency, Vienna, Austria. Available at http://www-pub.iaea.org/MTCD/Publications/PDF/SVS-21_web.pdf.

[10] IAEA, "IAEA Department of Safeguards Long-Term R&D Plan, 2012-2023 " (Vienna, Austria: IAEA, 2013). Accessed May 12, 2016 at https://www.iaea.org/safeguards/symposium/2014/images/pdfs/STR_375_--_IAEA_Department_of_Safeguards_Long-Term_R%26D_Plan_2012-2023.pdf.

information and multi-lateral fuel bank exchanges, activities that are not part of a State's obligations to the IAEA but but have digital elements as part of their implementation process or involve multiple party interactions that require third party involvement to ensure activities are completed.

In parallel, the SLT experts completed a review of peer reviewed articles, blogs, and news articles about current SLT advancements, private companies using SLT for various purposes, and the future direction of SLT. Based on their review of the current literature on both domains, the SLT and safeguards teams prepared an analytical framework to underpin future research on this topic. The framework enabled the evaluation of several conceptual models against a set of strategic objectives documented in the IAEA's long-term R&D plan. The team then envisioned a use case to illustrate the potential benefits of SLT for the IAEA. The team concluded with a set of findings and recommendations for future research.

3.0 Evaluating New Technologies for Safeguards

To develop an evaluation methodology for SLT, the safeguards team consulted the *IAEA Department of Safeguards Long-Term R&D Plan, 2012-2023*[11]*, and the IAEA Department of Safeguards Long-Term Strategic Plan, 2012-2023*[12] to understand IAEA Department of Safeguards' technical and strategic objectives and goals when evaluating a new technology for a safeguards application. The *Long-Term R&D and Strategic Plans* discussthree strategic objectives:

1) Deter the proliferation of nuclear weapons by detecting early the misuse of nuclear material or technology, and by providing credible assurances that States are honoring their safeguards obligations.
2) Contribute to nuclear arms control and disarmament, by responding to requests for verification and other technical assistance associated with related agreements and arrangements.
3) Continually improve and optimize departmental operations and capabilities to effectively implement the IAEA's verification mission.

For the purposes of this study, the team considered the first and third objectives as part of its analysis but ultimately focused on SLT's impact on the first objective. The second objective was deemed to be outside the scope of this study, while the third objective is likely to be met with both SLT and existing technologies and approaches. The team's focus on the first objective was based on the hypothesis that the unique value proposition of SLT lies in the trust and transparency it is able to offer; promoting trust and transparency will help provide credible assurances that States are honoring their safeguards obligations and might also lead to early detection of misuse of nuclear materials or technology.

The intention of Table 1 is to provide a set of safeguards goals aligned with the first strategic objective against which SLT systems could be assessed. The goals are informative, but they do not

[11] IAEA, "IAEA Department of Safeguards Long-Term R&D Plan, 2012-2023." (Vienna, Austria: IAEA, 2013). Accessed May 12, 2016 at https://www.iaea.org/safeguards/symposium/2014/images/pdfs/STR_375_--_IAEA_Department_of_Safeguards_Long-Term_R%26D_Plan_2012-2023.pdf.

[12] IAEA, "IAEA Department of Safeguards Long-Term Strategic Plan, 2012-2023." (Vienna, Austria: IAEA, 2013). Accessed January 31, 2017 at https://www.iaea.org/safeguards/symposium/2014/images/pdfs/LongTerm_Strategic_Plan_(20122023)-Summary.pdf.

represent the more rigorous process employed by the IAEA to approve technologies for safeguards use. They offer qualitative assessment criteria to explore whether the conceptual models warrant further research. The evaluation of SLT systems against these goals will be performed in Sections 5.0 and 6.0. The next section will provide an overview of the current SLT landscape.

Table 1. IAEA Strategic Objectives in the Context of Emerging Technologies

IAEA Strategic Objectives	A New Technology Should…
Deter the proliferation of nuclear weapons, by **early detection of** the misuse of nuclear material or technology, and by providing **credible assurances** that States are honoring their safeguards obligations.	Improve/Contribute to Timely Detection Build Confidence/Trust in Member State nuclear programs Build Confidence/Trust in the IAEA (Increase transparency)

4.0 SLT Overview

The concept of SLT first emerged in public discussions in 2009 with the implementation of bitcoin, a digital currency and payment software system. Bitcoin, which generally refers to the currency itself, was built on top of a replicated, electronic ledger called the blockchain. The blockchain was the first mainstream example of a shared ledger. The intent of bitcoin was to disrupt the traditional paradigm of trust in financial systems, which relies on a presumption of trust in central authority to regulate transactions and maintain the transaction history. Instead, parties to the blockchain underlying bitcoin placed their trust in computer algorithms and relied on decentralized consensus to monitor and record transactions. Simply put, rather than a single entity maintaining a global ledger to manage transactions, all parties in the bitcoin network maintain an independent ledger to manage the transactions.

For example, if Party A wants to send money to Party B, the proposed transaction is broadcast to the network with a digital signature that authenticates Party A as the sender. Once a transaction is proposed, it is posted to a block, where computer algorithms then determine the funds are available (valid) and no double-spending taking place (unique). Once the transaction is confirmed to be valid and unique, a network node (computer) propagates the confirmation to other nodes to which it is currently connected.[13] If the transaction is determined to be invalid, the node will reject it and synchronously return a rejection message to the originator. The ledger, once updated, is functionally immutable as a result of the cryptographic hash functions[14] used in the software.[15] Meaning, the ledger cannot be altered.

[13] This is a major simplification. There are plenty of great resources that explain the full process of bitcoin, such as *Mastering Bitcoin: Unlocking Digital Currencies*, by Andreas Antonopoulos. Antonopoulos, Andreas. “Mastering Bitcoin: Unlocking Digital Currencies.” O’Reilly Media, Inc. Sebastopol, CA. 2015.

[14] A cryptographic hash function consists of an algorithm that can be run on a piece of data to generate a hash value or checksum. A hash value is used to determine the authenticity of the data. “Two files can be assured to be identical only if the checksums generated from each file, using the same cryptographic hash function, are identical.” For more information, see About Tech. “Cryptographic hash function.” Available at: http://pcsupport.about.com/od/termsc/g/cryptographic-hash-function.htm.

[15] Ch 8, Mastering Bitcoin, Andreas Antonopolous

Bitcoin parties act pseudonymously, which adds a layer of privacy, but all parties have a copy of the ledger, which increases the transparency in the regulation and history of transactions. Since its first release in 2009, bitcoin has been wildly popular; as of July 26, 2016, bitcoin had a market cap of $10,276,486,312[16] and averaged 184,132 transactions a day.[17] Due to its enormous growth, bitcoin has garnered significant attention from the media, industry and governments globally as a technology that could revolutionize finance by providing a global, decentralized currency.

As global interest in bitcoin grew, so did the attention given to the blockchain, which experts believed could be applied to a much broader set of problems than the decentralization of peer-to-peer bitcoin (cryptocurrency) transactions. Media reports and bloggers began claiming that blockchain "has even greater potential to change how we make transactions online."[18] In fact, many researchers, technology developers, and executives in both technology and financial sectors have heralded blockchain technology as the wave of the future and a "game changer" for international transactions.[19],[20] For example, major banks around the globe are interested in applying blockchain to traditional currency to help them manage and secure their accounts.[21] There also is speculation that blockchain could be applied to non-financial applications including: voting systems, vehicle registration, gun background checks, academic records, ownership transfers, stock market transactions, "smart contracts"[22] and clinical trials.[23]

A variety of organizations are starting to explore the feasibility and challenges associated with using blockchain algorithms in such non-traditional applications, for example SWIFT and the Depository Trust & Clearing Corporation (DTCC) for large-scale financial clearing,[24] Cisco and IBM in the context of the Internet of Things[25], and Seimens for microgrid technologies[26]

[16] https://coinmarketcap.com

[17] https://blockchain.info/charts/n-transactions# calculated from 7/28/15 to 7/25/16

[18] Naomi LaChance, "Not Just Bitcoin: Why the Blockchain Is a Seductive Technology to Many Industries," *NPR* (2016), Accessed May 17, 2016 at http://www.npr.org/sections/alltechconsidered/2016/05/04/476597296/not-just-bitcoin-why-blockchain-is-a-seductive-technology-to-many-industries?utm_source=facebook.com&utm_medium=social&utm_campaign=npr&utm_term=nprnews&utm_content=20160507.

[19] Portia Crowe, "There Is a 'Game Changer' Technology on Wall Street and People Keep Confusing It with Bitcoin," *Business Insider* (2016), Accessed May 17, 2016 at http://www.businessinsider.com/what-is-blockchain-2016-3.

[20] Oscar Williams-Grut, "Goldman Sachs: 'The Blockchain Can Change... Well Everything'," *Business Insider* (2015), Accessed May 17, 2016 at http://www.businessinsider.com/goldman-sachs-the-blockchain-can-change-well-everything-2015-12?r=UK&IR=T.

[21] Ibid.

[22] Ibid.

[23] "Better with Bitcoin," *Economist* (2016), Accessed June 6, 2016 at http://www.economist.com/news/science-and-technology/21699099-blockchain-technology-could-improve-reliability-medical-trials-better.

[24] "SWIFT, The DTCC and How Blockchain Will Go Mainstream", Coindesk.com, accessed February 1, 2017 at http://www.coindesk.com/dtcc-swift-blockchain-future-2017-announcements/

[25] "Cisco fosters Blockchain protocol development, IBM shows why technology could relieve security anxiety", NetworkWorld, accessed February 1, 2017, at http://www.networkworld.com/article/3163044/cisco-subnet/cisco-fosters-blockchain-protocol-development-ibm-shows-why-technology-could-relieve-security-anxie.html?google_editors_picks=true

[26] "Tech Giant Siemens is Now Working on Blockchain Microgrids", Coindesk.com, accessed February 1, 2017 at http://www.coindesk.com/siemens-blockchain-microgrid-lo3-ethereum/

Ethereum is a decentralized platform that runs applications, governed by "smart contracts," that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference. [27] Smart contracts are computer protocols that record agreements between parties, rather than just shared facts or transactions. When incorporated into an SLT system, smart contracts allow for facilitation, verification, and execution of an arbitrary agreement without the need for mutual trust or a trusted third party.[28,29] One organization, the Decentralized Autonomous Organization (DAO), is the first experiment in what some call "programmable governance"; DAO is run without managers or executives, but through business rules engrained in smart contracts.[30] Meanwhile, a company called Everledger[31] is using blockchains to track and certify high value commodities such as diamonds for insurance and law enforcement purposes. These are only a few of the emerging companies that are starting to experiment with blockchain technology.

Interest in blockchain applications has seeped into the security sphere as well. The U.S. Defense Advanced Research Projects Agency is researching the use of blockchain to create a secure messaging and transaction platform.[32] A U.K. cybersecurity company plans to develop a security infrastructure for U.K. nuclear power plants using blockchain technology.[33] Two researchers at King's College London are investigating "feasibility of distributed ledger technologies for monitoring and control of weapons and hazardous materials".[34]

Each of these experimental applications serves as a compelling surrogate for exploring questions of importance to safeguards. For example, the DAO experiment explores the relationship between decentralized authority and trust. One of the implicit hypotheses being tested is whether organizations driven and governed by "immutable, unstoppable, and irrefutable computer code" garner greater levels of trust among its membership. Another question is whether such a model actually increases the level of commitment to the organization's goals and objectives. To extrapolate to the safeguards context, it is worth questioning whether a greater reliance on objective computer codes rather than third parties to verify the fulfillment of selected safeguards obligations might increase the efficiency or effectiveness of IAEA safeguards or lead to greater cooperation and trust among states.

The Ethereum model raises interesting questions about the future of enforcement and the role third parties play in the process. Rather than simply record a transaction on a ledger, parties record the terms of a contract (as expressed in a programming language) into the ledger. The software that controls the ledger

[27] https://www.ethereum.org/

[28] Buterin, Vitalik, "A Next-Generation Smart Contract and Decentralized Application Platform." https://github.com/ethereum/wiki/wiki/White-Paper.

[29] G. Zyskind, O. Nathan and A. '. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," Security and Privacy Workshops (SPW), 2015 IEEE, San Jose, CA, 2015, pp. 180-184. doi: 10.1109/SPW.2015.27

[30] Paul Vigna, "Chiefless Company Rakes in More Than $100 Million," *Wall Street Journal* (2016), Accessed May 16, 2016 at http://www.wsj.com/article_email/chiefless-company-rakes-in-more-than-100-million-1463399393-lMyQjAxMTA2NDExNjYxNjY1Wj.

[31] Information about Everledger can be found at http://www.everledger.io/.

[32] Frank Pound, "Secure Messaging Platform," (2016), Accessed May 17, 2016 at https://sbir.defensebusiness.org/%28X%281%29S%28sdehyicwygn4ngxvrwpzwmc5%29%29/topics?AspxAutoDetectCookieSupport=1#topic27859.

[33] Levich, Andrew. "Guardtime: Blockchain to guard nuclear power plants." *Coinfox.* 4 January 2016. Available at: http://www.coinfox.info/news/4316-guardtime-using-blockchain-to-guard-industries

[34] Peter McBurney, "King's of the Block: Blockchains and Distributed Ledgers," (2016), Accessed May 18, 2016 at http://www.dcs.kcl.ac.uk/staff/mcburney/blockchain.html

then executes the contract (through the programming language), taking sole control of ensuring that the terms of the contract are executed as specified. In the safeguards context, the integration of self-executing mechanisms into information management systems might improve the quality and timeliness of State reporting or possibly lower costs associated with it. Further, such mechanisms might positively influence the transit matching process by reducing the number of person days spent resolving transmit matching issues.

Finally, the Everledger model explores the relationship between data authenticity, security, and quality assurance. In the safeguards context, this model could be used to track UF6 cylinders or contribute to item accounting in a nuclear facility.

When considering how these technologies might impact safeguards, it is important to note that blockchain really refers to a specific implementation of a shared ledger, with linked "blocks" of transactions.[35] However, as Richard Gendal Brown, CTO of R3[36], notes, "If you don't have bitcoin's business problem, then be very wary of those trying to sell you something that looks like a bitcoin solution."[37] That is to say, blockchains are capable of satisfying very specific functional requirements. In the absence of bitcoin's specific requirements, a blockchain designed around cryptocurrencies may not solve your problem. The benefit of thinking more broadly about shared ledger technologies, rather than focusing on one distinct application (i.e., bitcoin), is the ability to consider core attributes of shared ledger designs and to "…treat them as a *menu* from which to select and customise… different combinations, in different flavours, for different business problems."[38] These five services are:

- **Consistency:** Parties involved with a shared fact (transaction, status report, etc.) are guaranteed to see the same details about the shared fact.
- **Validity:** Proposed transactions submitted to a system must be deemed valid, according to predefined rules, before being added to the ledger.
- **Uniqueness:** Two transactions, even if both are valid, must not conflict with each other (e.g., one party may not indicate that they sent the same physical good to two distinct parties).
- **Immutability:** Once a transaction is committed to the ledger, that transaction cannot be changed.
- **Authentication:** Every action in the system is associated with a secure private key that is unique for each involved party.

These services and additional system characteristics may be blended together and implemented in many ways as part of a SLT.[39]

The broader space of SLT is not as well defined or explored as that specifically of blockchain. This is not surprising: as a hugely popular system, bitcoin has provided a very well defined and successful implementation and use case for blockchain. However, the extensibility of SLT as a general set of

[35] Anatonopoulos. Ch 7.

[36] R3 is a technology company exploring applications of shared ledger technology for a consortium of 45 financial institutions. http://r3cev.com/

[37] https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/

[38] Ibid.

[39] As will be discussed later in the paper, use of SLT may be transparent to the user and may be engineered to integrate with existing systems, such as IAEA mailbox system.

capabilities is clear, and the recent trend has been toward a broader set of ledgers than just the one designed to facilitate bitcoin transactions. As more entities experiment with different forms of SLT applications, new questions will arise about how the concepts being tested could benefit or hinder safeguards activities. Due to the rapidly evolving development of SLT, the team developed an analytical framework to bound the discussion and underpin future research on the topic. To this end, the team identified existing models and concepts to provide a common nomenclature for discussion.

5.0 A Common Nomenclature for SLT

The discussion about a common nomenclature begins with a classification of the different types of shared ledgers that can be created, driven by the problem to which the ledger is being applied. Shared ledgers can be classified into two dichotomous pairs of terms: *localized* and *distributed and decentralized* and *centralized*.[40,41] Each of these pairs serves as useful units of analysis. In addition, some terms can be combined into meaningful models for analysis and other combinations of terms can be immediately dismissed because they contain logical inconsistencies. Further distinctions can be made between concepts such as *public ledgers, private ledgers* and *consortium ledgers*. Each of these concepts and terms are defined in this section.

5.1 Localized vs. Distributed

Localized ledgers are those that have a single, authoritative copy. There are copies of the primary ledger that are accessed for viewing, but there is only one copy that represents the definitive state of the system. In contrast, *distributed* ledgers are those where many copies of the ledger are maintained by a consensus protocol that provides a consistent view among ledgers. The consensus process reconciles differences between ledger copies that may exist for short periods of time due to the “mining” mechanism. [42] Distributed ledgers have a distinct advantage over localized ledgers in that they do not have a single point of failure. In order for an adversary to corrupt or delete a local ledger, they must only attack the single copy. To do this for a distributed ledger, a large portion of the ledgers would all have to be attacked at once, which is significantly more difficult. Distributed ledgers are the underlying technology for bitcoin.

5.2 Decentralized vs. Centralized

Centralized ledgers are those that give certain participants roles of trust in maintaining the state of the ledger. This could mean either a singular entity or a subset of entities are responsible for validation. Given that a centralized system can have either one or many entities, there is a spectrum of the degree to which a ledger is “centralized”. In contrast, *decentralized* ledgers are those in which all users have equal privilege in maintaining the consistent state of the ledger. Bitcoin is a decentralized SLT. Decentralized ledgers

[40] https://medium.com/@arthurb/a-functional-nomenclature-of-cryptographic-ledgers-e836cb0e6864#.hzyjze6fn

[41] https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[42] There are a variety of different consensus algorithms in computer science. Bitcoin uses a proof-of-work based “emergent consensus.” For more information on bitcoin’s approach, see Antonopolous, Mastering Bitcoin, Ch. 8. We will not elaborate on consensus approaches, as there are many, and that is beyond the scope of this project.

often offer increased transparency and trust, at the cost of efficiency, as a result of the cryptographic consensus protocol used in these systems.

A component of a centralized ledger is that it is permissionable. By having a centralized power structure, permissions or “roles” can be granted to certain users to allow them to interact with the ledger in privileged or limited ways. For example, a “read-only” role may be granted permissions only to view transaction meta-data on the ledger, while a “read/write” role may be granted to allow a user to submit transactions to the ledger. It is possible to grant users (some or all) outside of the consortium full permissions to view the ledger, or grant them no permissions and only allow consortium members to use and view the ledger. This is highly customizable and can be implemented as needed for a given use case. Because a decentralized ledger lacks a central authority that can grant permissions, this model is not permissionable, which can be exemplified by bitcoin.

5.3 SLT Models with Characteristics

Given the aforementioned pairs of characteristics and features, there are four possible combinations to make different SLT frameworks (see Table 2).

Table 2. Combinations for SLT frameworks

	Centralized (certain users have permissions)	**Decentralized (all users maintain)**
Localized (single ledger copy)	(a): Private Ledgers	(d)
Distributed (many ledger copies)	(b): Consortium Ledger	(c): Public Systems

However, the nature of a localized ledger, given that it exists on a single machine run by a single entity, runs counter to the concept of being decentralized, which requires that no single user have disproportionate control over the ledger. It is possible to imagine what this combination could be—perhaps interested parties compete to control the single copy, and whoever controls the ledger at that time is responsible for the contents. However, these possible designs are very unlikely to be useful for our uses; therefore, option (d) is not addressed in the paper.

This report analyzes the following combination of characteristics:

a) Localized, Centralized (e.g., bank)

b) Distributed, Centralized (no obvious example)

c) Distributed, Decentralized (e.g. bitcoin)

Once these characteristics are combined into different models, they can be framed as public, private or consortium ledgers.

5.4 Public vs. Private vs. Consortium Ledgers

There are varying levels of “openness” to a shared ledger. In one extreme, there are totally public systems, like bitcoin. *Public systems* correspond with combination (c): distributed and decentralized. In a

Public System, any party can use the system and no one party is given special privileges for either submitting or validating transactions, viewing the ledger, or maintaining consistency of the ledger. All other combinations of characteristics fall under a group of ledgers with varying levels of privacy. According to Vitalik Buterin, co-founder of Ethereum, *private ledgers* are for single entities that maintain the ledger. An organization in charge of a private ledger may choose to apply permissions, limiting who is able to do things such as submit transactions or view the ledger, or run fully permissionless and allow the public to fully interact with the ledger. In this sense, a private ledger represents combination (a): localized and centralized. [43,44]

Under a *Consortium System*, a finite group of predetermined users maintains a ledger of their private interactions. Consortia rely on a trusted set of users to each maintain a copy of the ledger and execute distributed consensus protocol of the system. From the outset, the consortium will agree on the permissions of the ledger, including who can make transactions (and with whom), who can read the ledger, etc. As such, a consortium approach is distributed, centralized, and with the option to be permissioned. As such, combination (b): distributed and centralized. A consortium approach becomes less centralized as the size of the consortium grows.

Buterin suggests that, while a private ledger more or less represents a traditional, centralized ledger system, a consortium approach begins to offer the benefits of increased trust and transparency that are typically associated with a less centralized and distributed approach, without completely opening the door as with a public model. Thus, this distinction between private ledgers and consortium ledgers becomes important when exploring potential applications and benefits to safeguards, because the IAEA follows the more traditional private approach in their interactions. A shift from standard database or private ledger approaches to less centralized, consortium ledgers could lead to greater trust and transparency in the system while removing single points of failure but without undermining privacy protections or data security.

The next section describes each combination of SLT characteristics and features within the safeguards context. The goal is to explore how such models might work if implemented as part of the safeguards system. It is important to note that any "decentralizing" from a central authority is only in regard to maintaining the ledger of the data (encrypted or not) and transactions. There is still the need for a trusted authority to review the data, perform inspections to confirm reports, and perform regulatory action. *There is no intent to pass judgment about the viability or desirability of any model* rather to provide an initial understanding if an SLT could achieve any of the earlier mentioned strategic goals.

6.0 An Analytical Framework for Assessing Blockchain Applications to Safeguards

Table 3 lists the five services offered by shared ledger technology and three different SLT models.

1. Centralized, localized – referred to as a Private System

[43] https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[44] Model (B) may be hard to conceptualize—simultaneously being private and permissionless. An example of this might be something like Wikipedia or the comment section on an online article. Even though a single entity is maintaining and running the servers for the website, any one person is able to write an update and view the updates performed by others.

2. Centralized, distributed – referred to as a Consortium System
3. Decentralized, distributed, permissionless – referred to as a Public System.

The table depicts how each SLT model would achieve the five services. Three of the services, namely validity, uniqueness, and authentication, are available today using existing IT solutions, such as electronic databases, digital reporting software, digital signatures, and digital certificates. The three services could be built into any software program and provide sufficiently secure authentication of users; there is no SLT model that serves as a unique provider of these three services.

Table 3. Comparison of How SLT Models Fulfill SLT Services

		Model Type		
		Centralized, Localized (Private)	Centralized, Distributed (Consortium)	Decentralized, Distributed (Public)
Service	Consistency Immutability	Trusted Central Authority (e.g., IAEA)	Member State Consortium Consensus	Open Style Consensus (e.g., bitcoin Proof of Work)
	Validity	Implementation-specific, rule-based software protocol that checks for complete transactions		
	Uniqueness	Implementation-specific, rule-based software protocol that checks that a proposed transactions does not conflict with the current state of the ledger		
	Authentication	Implementation-specific modern IT solution		

The primary difference between the models is how consistency and immutability are provided, and this is where the potential to change the level of trust and transparency in a system exists.

6.1 Private System (Centralized, Localized)

A *Private System* model strongly resembles the status quo. Under this type of model, a trusted authority (i.e., the IAEA) would be responsible for maintaining the single authoritative copy of a shared ledger that would record all States' transactions, much in the style of a traditional ledger. As such, any increased trust or transparency would likely be marginal and come from implementation decisions, such as granting certain permissions (e.g., the ability to view meta-data of other Member States' reports). More robust and modern software and IT solutions (e.g., improved digital reporting with spot-checking software and secure encryption) would ensure consistency and immutability of data while protecting safeguards confidential information. In a private system, consistency and immutability are assured through the faithful actions of a trusted authority.

6.2 Consortium System (Centralized, Distributed)

A *Consortium System* represents a significant departure from the traditional IAEA reporting scheme. Under a Consortium System, copies of the ledger would be distributed across separate entities involved in safeguards-related activities, such as Member States, nuclear facilities, state regulatory authorities, locations outside facilities etc. The IAEA can be in the consortium or not. It would require further analysis to be determine if this makes a significant difference in terms of enhancing trust and transparency in the safeguards system.

When an entity reports something like an inventory change report, which would traditionally be sent to the IAEA, it would instead broadcast that information to the ledger consortium. If the consortium deems the submission to be valid, unique, and authenticated, the transaction would be added to the ledger. Due to its distributed nature, this ledger would be visible to all members of the consortium (i.e., Member States and the IAEA) at all times. However, a distributed ledger does not necessarily mean that data will be exposed to all entities. The submitting party could encrypt any sensitive data such that it is only consumed by specific entities, such as the IAEA, by use of public/private key encryption. Meaning, it is possible to share metadata that entities deem suitable for sharing, allowing a broader community of members to see certain information while a smaller portion of that community, which might consist of only one entity, has permission to see more sensitive information. It is important to assert here that Member States may perceive greater risk in exposing sensitive data via distributed ledgers, despite use of modern cryptography. However, Member States already rely on these same encryption techniques to send sensitive information via email to the IAEA. Distributed ledgers rely on the same underlying principle that the cost to decrypt any piece of data is greater than the value of the information being shared.[45] Ultimately, Member States will need to assess whether they are willing to accept a small amount of increased risk to generate greater overall transparency in the system.

In a consortium system, appropriate consensus mechanisms, rather than the faithful actions of a trusted authority, would ensure immutability and consistency. There are a variety of consensus mechanisms that could be considered, but their consideration remains outside the scope of this project. Through involvement in the multi-party consensus process, Member States will become more involved, promoting increased confidence in the system.

6.3 Public System (Decentralized, Distributed)

A *Public System* is more difficult to imagine and fraught with political and technical challenges. An envisioned Public System would totally shift the responsibility for collecting and managing State reporting from the IAEA to citizens or organizations. This system would be a truly open system, in the

[45] Bruce Schneier offers a useful explanation about the effectiveness of cryptography provides Different algorithms offer different degrees of security; it depends on how hard they are to break. If the cost required to break an algorithm is greater than the value of the encrypted data, then you're probably safe. If the time required to break an algorithm is longer than the time the encrypted data must remain secret, then you're probably safe. If the amount of data encrypted with a single key is less than the amount of data necessary to break the algorithm, then you're probably safe. I say "probably" because there is always a chance of new breakthroughs in cryptanalysis. On the other hand, the value of most data decreases over time. It is important that the value of the data always remain less than the cost to break the security protecting it." Schneier, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C. "Security of Algorithms". John Wiley & Sons. 1996.

style of bitcoin. This means that any interested party (public, industry, government, etc.) could submit transactions to the ledger, maintain a full copy of the ledger, and participate in the consensus mechanisms. It is worth noting that consensus mechanisms used in a public system may differ from those implemented in a consortium system. With correct incentives to get a large enough group of validators,[46] it is possible that a Public System would be able to secure sensitive data (encrypted or not) and provide both a consistent and immutable ledger. This system might enable the IAEA to shift more resources to its onsite inspections, offering a significant benefit to the IAEA. However, opening the system to the public introduces both known and not yet discovered vulnerabilities that would have to be evaluated. In short, this type of system is a dramatic departure from current practices. If the IAEA and its Member States were to pursue this approach, much more research would be needed to understand its execution and potential impact on the IAEA's legal authorities.

Table 4 summarizes analysis about each SLT model against the goals described in Section 3.0. The rating is to help determine the potential value of each model and if there are any models worth ruling out or investigating further. To fill out this table, the team asked one question of each SLT model in relation to the respective functional requirement: "What is the likelihood that this model could contribute to the IAEA functional requirement?" The cell color denotes the team's assumption of that particular combination, where green means "likely" and red means "unlikely". A yellow cell indicates whether it is "not likely, but not unlikely" or "unclear" that the model will address the safeguards outcome. For a detailed description of the coloring, see Appendix A.

Table 4. Assessment of Blockchain Models against IAEA Objectives and Function Requirements

	Model Name Characteristics & Features	Private Localized, Centralized	Consortium Distributed, Centralized	Public Distributed, Decentralized
IAEA Strategic Goals	Improve and Contribute to Timely Detection	🟩	🟩	🟩
	Build Confidence & Trust in Member States	🟨	🟩	🟨
	Build Confidence & Trust in the IAEA	🟥	🟩	🟨

This table is based on the current state of the SLT ecosystem and literature, which is immature and rapidly evolving. As such, the table is certainly speculative, but it suggests there are areas that merit further exploration by the IAEA to determine which models might offer the most significant benefits to IAEA operations or practices. In Section 7.0, we will explore use cases well suited for shared ledgers, and imagine what possible SLT implementations might entail.

7.0 Approach for Considering SLT Models

The previous sections defined key terms and clarified why SLT is particularly useful for promoting transparency and trust in various systems. This section describes an approach for determining how the different SLT models could be assigned to a specific safeguards problem.

[46] In the case of bitcoin, these are miners.

As stated earlier, an SLT must provide five services: authentication, validity, uniqueness, immutability, and consistency. For a given safeguards problem, we first outline how the SLT must accomplish the three services we determined to be model agnostic: authentication, validity, and uniqueness. These services can be addressed through a combination of rulemaking and engineering. First, rules must be made for what it means for a submission or transaction to be authenticated, valid, and unique. Then, an engineering solution must be designed that will be able to check and ensure these to be true. These decisions will be driven by the nature of the use case and specified functional requirements.

This leaves the consistency and immutability services remaining. How these services are provided will vary depending on which model is chosen. To identify which model might be most effective in addressing a given problem, one must navigate one of two decision trees. Decision Tree A (Figure 1) offers a choice between a localized ledger (private), and a more transparent, distributed (non-private) ledgers. This tree would be chosen if the primary characteristic of the tree was related to trust and transparency. Decision Tree B (Figure 2) offers a choice between a decentralized (public) ledger, v. more centralized, permissionable (non-public) ledgers. Decision Tree B should be used if the driving factor for model selection is related to controllability (permissionability) of the ledger.

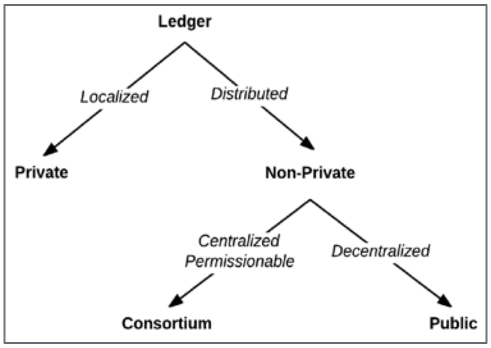

Figure 1. Decision Tree A

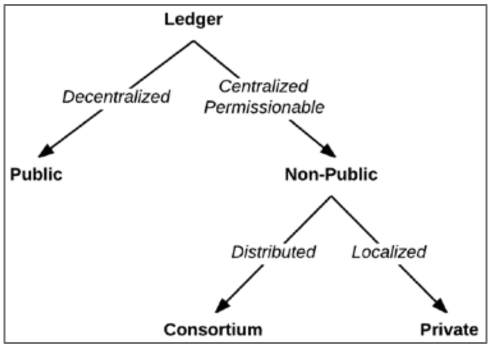

Figure 2. Decision Tree B

After navigating the two decision trees, further branches of the tree can be traversed depending on the desired characteristics of the ledger. Each decision requires extensive analysis of the functional requirements and their associated costs and benefits. Once a model has been chosen, decisions can be made about how to implement immutability and consistency for that given model. While this choice is relatively trivial for a private ledger, how to provide these services in consortium and public systems is an evolving area and would require a thorough investigation of options.

In the following section, we will demonstrate this process with use cases deemed relevant to SLT.

8.0 Illustrative Safeguards Example

This section will begin to explore the envisioned application of SLTs to specific safeguards use cases. This is purely an illustrative exercise. We are not asserting that certain use cases are well suited for certain ledger models. Rather, the objective of this section is to illustrate an essential point of this paper: Certain problems are suitable for ledger solutions, including the uses cases described here. The particular requirements or problems specified by a given use case will define the type of ledger that is ultimately selected. In the safeguards context, such requirements could include a desire for more trust, transparency, State cooperation, security, efficiency, effectiveness or lower implementation costs.

As part of their obligations under INFCIRC 153, States are required to submit a variety of reports to the IAEA, including inventory change reports (ICR)[47], material balance reports[48], physical inventory listings[49], and concise notes[50]. The IAEA currently receives approximately 900,000 of such reports annually.[51] The IAEA expects all reports to be complete, correct, and submitted in accordance with required deadlines.[52] The information contained in these reports is considered safeguards confidential, which means the IAEA cannot share the detailed contents. An SLT designed to facilitate the transmission of these reports to the IAEA must fulfill each of the five services, beginning with authentication, validity, and uniqueness.

- **Authentication:** An authentication requirement might be that both the submitter (i.e., a member state) and the receiver (i.e., the IAEA) of a report must digitally sign all submissions. Digital signatures can be performed with public/private key cryptography. There are many examples and implementations of this in both the SLT ecosystem, such as the public/private key scheme that Bitcoin employs, and in more conventional environments, such as Entrust.[53]
- **Validity:** While not an exhaustive list of rules, a "valid" report might be required to provide all necessary values and report values that are within realistic ranges and are consistent with known information about a country. Further, a report may only be valid if the sender is a State Regulatory Authority (SRA) and the receiver is the IAEA. Through use of spot-checking software, an SLT could be designed to check all fields and immediately notify the sending State and the IAEA of any gaps or errors in a submittal, dramatically accelerating the reconciliation process.
- **Uniqueness:** For a report to be "unique," it might be required that two reports with the same identification number not be submitted or two reports from the same SRA cannot be submitted within the same time window. For certain reports that might track distinct objects at an item facility, uniqueness could mean that the same item is not said to be in two different places in different forms. Similar to validity, spot-checking software could be implemented into the SLT implementation that would check that these rules are being followed.

[47] An Inventory Change Report is an accounting report provided by the State to the IAEA changes in the inventory of nuclear material for each Material Balance Area at a Facility. All definitions and additional information are drawn from the IAEA's Safeguards Glossary available at: http://www-pub.iaea.org/MTCD/publications/PDF/nvs-3-cd/PDF/NVS3_prn.pdf

[48] A Material Balance Report is an accounting report provided by the State to the IAEA showing the material balance based on a physical inventory of nuclear material actually present in the material balance area.

[49] A Physical Inventory Listing is a report provided by the State to the IAEA in connection with a physical inventory taking by the operation listing all batches separately and specifying material identification and batch data for each batch.

[50] Concise notes contain information supplied by the State to the IAEA and accompany inventory change reports for the purposes of explaining the inventory changes and describing the anticipated operational program, particularly the taking of a physical inventory.

[51] Gilligan, Kimberly, Katy Snow, Michael Whitaker, John Oakberg "Best Reporting Practices for Transit Matching"
Proceedings of the 57th Annual Meeting of the Institute of Nuclear Materials Mangagement. 2016.

[52] For example, according to the model Comprehensive Safeguards Agreement, ICRs must be dispatched to the IAEA as soon as possible and in any event within 30 days after the end of the month in which the inventory changes occurred or were established (60 days in the case of a regional authority).

[53] https://www.entrust.com/

It is at this point that it is no longer possible to make decisions based purely on the use case; rather, the IAEA's strategic objectives and the desired goals for SLT must be factored into the process:

- **Distribution:** Perhaps the IAEA seeks to increase trust and transparency in their reporting process and wants timestamped, encrypted reports to be visible to either Member States or the public. Such transparency may contribute to an increased sense of trust and involvement in the safeguards system. As mentioned earlier, another reason to move to a distributed model is to provide resilience to attacks or failures through redundancy.
- **Localization:** Perhaps a distributed ledger is deemed to be fraught with too much potential for manipulation, or states are not comfortable with sharing data, even in an encrypted form.
- **Decentralization:** Perhaps there is a time when neither the IAEA nor States can be fully trusted to maintain a ledger correctly. A decentralized model could be explored that provides incentives in the style of bitcoin for an accurate ledger to be maintained. It is also possible that there may be a desire for increased involvement of, or accountability to, the general public for certain applications, such as the IAEA's annual safeguards reporting or societal verification, and a public facing ledger that is fully transparent might be a good solution.
- **Centralization:** For many cases, the concept of decentralization may seem irresponsible to surrender the control of centralized authority. If a service is absolutely critical to treaty enforcement, then maintaining strict control over that is important. Additionally, any system that requires permissions must be centralized.

In this hypothetical case, given the above, assume that the system must first and foremost be centralized. It is important that the system be permissionable, so only certain entities (federal governments, SRAs, etc.) are able to see who is reporting. Additionally, perhaps a fully decentralized system is too much of a political leap for some Member States. This leads us to choose a non-Public System. At this point, we have the option of a private model, which is mainly the status quo, or a consortium model, which offers potential benefits in regards to trust and transparency. In this hypothetical case, we imagine that some States are beginning to feel as though the IAEA is not acting fairly toward them, and is being influenced by certain States. Perhaps they are concerned that some States may submit incomplete reports or do not submit information on time. In a different scenario, some may feel as though the IAEA's yearly reports about States' reporting performance is insufficient, and they want to be able to hold their fellow Member States accountable in real time. Both of these scenarios point to the preferred model being one that allows increased participation and transparency: the distributed model. As such, this results in the consortium model shown in Figure 3.

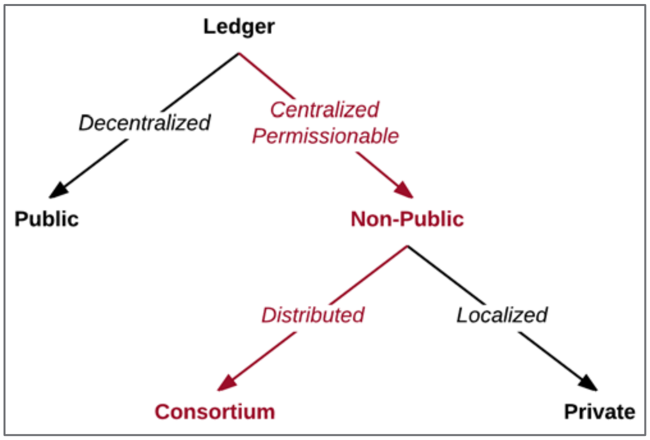

Figure 3. Consortium model

There are many possible realizations of this model. As part of the consortium, each Member State will maintain a copy of the ledger. When a report is submitted, it would be encrypted and sent out to the network. After the software verifies the authentication and proves the report valid and unique, the Member States would add the signed timestamp and the encrypted data to their ledgers. This would provide credible assurances in real time to other Member States and the public that States are honoring their safeguards obligations to submit complete and timely reports. However, the IAEA would still need to provide assurances to the international community that the contents of the report are accurate through appropriate verification measures. No longer would states have to wait for an annual IAEA report that says whether or not other Member States are submitting on time. When the IAEA needs to review the reports, it would be able to access the data and use the necessary private decryption key to view the contents of the report. Other states, even though they had the encrypted reports, would not be able to view the actual contents unless they were able to somehow break the encryption. Given this model, we have to decide an approach to consistency and immutability.

- **Consistency:** For a distributed system an appropriate consensus mechanism must be chosen. There are many examples of possible approaches, with a prominent class of techniques know as Byzantine Fault-Tolerant algorithms.[54] We will not suggest a specific algorithm for consistency because this is an area of active research and development, and there are many possible options.
- **Immutability:** Immutability is tightly coupled with consistency, so the approach would depend on the chosen consensus algorithm.

9.0 Other Potential Application Areas

The above use case is only one example. It is not suggesting a consortium approach is the only viable or most interesting approach. To provide an exhaustive list of examples would be both arduous and speculative. This paper is merely recommending a process by which to assess models. Any number of private, consortium, or public systems could be explored for future use. It is just as possible at this point that the IAEA could create a custom private solution or take advantage of something like a public Ethereum platform but execute all of its affairs through private smart contracts. Ultimately, the ecosystem

[54] http://pmg.csail.mit.edu/papers/osdi99.pdf

is very young and anything could be possible in the future, although not a lot is necessarily well understood right now. Further research into the similarities and differences between IAEA's specific information management needs compared to other organizations also approach SLT is an intriguing area of future study. However, it is important to scope out other IAEA tasks that could take advantage of SLT. Below are a few possible areas PNNL safeguards experts identified.

9.1 Transit Matching Declarations

ICRs indicating transfers of nuclear material between material balance areas are subject to transit matching. Transit matching is the process for relating or "matching" reports of domestic and international shipments and receipts. Currently, there are approximately 900,000 reports on nuclear material transfers that are submitted to the IAEA. There are different types of changes to inventories, but transit matching is implemented only for those reports that indicate material has been shipped from or received into a material balance area. Non-nuclear Weapons States are required to submit their ICRs within 30 days of the end of the month in which the transaction occurred (60 days for regional authorities). Nuclear Weapon States are required to submit reports as soon as possible. Upon receiving these declarations, the IAEA processes them into its safeguards information system. Approximately every 14 days, the staff initiates software algorithms to perform "machine matching". This means an algorithm determines which shipper and receiver records should be matched and connects the necessary matching information in the database. IAEA staff review and confirm the results of machine matching, and a manual process is started for those remaining records that are not matched by the software algorithms.

A number of issues arise as a result of this process. Even when States submit accurate and complete declarations within the required timeframe, the significant lag in processing time makes accurate reconciliation difficult. Moreover, the IAEA software can automatically match (i.e., machine match) about 95% of the domestic transfers and 25% of the foreign transfers. Analysts at the IAEA, who review the matches made by machine, match the remainder and make corrections by hand. As of 2014, approximately 3,000-4000 records remained unmatched each quarter.[55] To compound these challenges, the shipper or receiver may fail to report a transfer or may report the transfer differently, further hindering the reconciliation process.[56] Despite the gaps in information, the IAEA must keep States informed of the transit matching status for all foreign and domestic transfers of nuclear material. Periodically, reports are sent to the States, advising them of any unmatched records and requesting additional information that may assist the IAEA in completing the transit matching process.

Transit matching experts have made several recommendations to tackle these challenges.[57] In this context, SLT may help introduce certain efficiencies into the transit matching system, which would help achieve these recommendations. It is also possible that SLT could simultaneously improve overall transparency within this system, providing unknown benefits to safeguards. Additional testing is

[55] Gilligan, K.V., Oakberg, J.A., Whitaker, J.M. "Transit Matching for International Safeguards." Presented at the *Symposium on International Safeguards.* 20-24 October 2014. Oak Ridge National Laboratory. Available at: https://www.iaea.org/safeguards/symposium/2014/home/eproceedings/sg2014-slides/000193.pdf

[56] Canadian Nuclear Safety Commission. "Transit Matching Best Practices." *Best Reporting Practices for Nuclear Material Accountancy Next Generation Safeguards Initiative.* Presented by Jennifer Sample. 23-24 February, 2016. Oak Ridge, TN. Available at: http://www.nuclearsafety.gc.ca/eng/pdfs/Presentations/CNSC_Staff/2016/20160223-Jennifer-Sample-Transit-Matching-Best-Practices-eng.pdf

[57] Gilligan, K.V. et al. "Transit Matching for International Safeguards."

necessary to identify any unforeseen benefits from increasing the level of transparency in the transit matching process.

- Ensure all related processes, procedures, and information systems are well documented.
- All states should voluntarily submit ICRs to the IAEA more frequently.
- States should review and respond to IAEA statements and communications in a timelier manner.
- The IAEA should adopt a consistent batch reporting structure
- States should add container IDs to the ICRs
- States should use the same batch name for shipments and receipts of the same material.

9.2 Unattended and Surveillance Monitoring System

An Unattended and Surveillance Monitoring System (UMS) is a system that automatically monitors the flow of nuclear materials 24 hours a day and 365 days a year without the need for human interaction. It is permanently installed in a nuclear facility by the IAEA. The UMS may use a variety of sensors such as radiation, pressure, temperature, flow, optical, vibration, and electromagnetic fields to collect qualitative or quantitative data. All external components are in tamper indicating enclosures to ensure integrity of the data. The UMS is computer based for data retrieval either on-site or remotely by an IAEA inspector. Not all States allow the remote electronic transmission of data across international borders, but many do. The type of information transmitted to the IAEA includes a) IAEA state of health data giving information about the status of the IAEA equipment only, b) safeguards data without images (such as seal information, and detector response), and c) safeguards images. All of these data are encrypted prior to transmission outside of the IAEA cabinet.

UMS data are not typically shared with the facility if it is an IAEA owned system. There are special cases where IAEA UMS data may be shared on a delay to the facility. There are other cases where Joint-Use systems are shared by both the IAEA and the operator. For the cases where the operator already receives IAEA data, as in the case of delayed receipt, or where a systems data is shared, these data are shared locally. One possible benefit for the use of SLT, might be if there is value in sharing meta data, such as the positive remote transmission of data from the facility to the IAEA. Since the risk of data tampering is relatively low, the next major concern with unattended monitoring systems involves a failure to transmit data, which is not always a State issue. Primary causes for data transmission failure include: freezing or failure of the modem, loss of connectivity with the service provider, failure of IAEA data transmission equipment, and general loss of mains power. In the case where a modem freezes, arrangements exist for the facility operator to reboot the modem.

Further research is necessary to determine whether or how SLT might enhance the security, effectiveness, efficiency, or transparency, if desired, of the UMS. In this case, the authors hypothesize that further research may reach the conclusion that there is no benefit to using SLT in this application.

9.3 IAEA Reporting to States: A living Safeguards Implementation Report

Currently, the IAEA verifies State declarations through onsite inspections. Although the goal is to resolve reporting discrepancies during an inspection, the IAEA may continue to transmit requests for amplification or clarification to States to resolve a question. States continue to transmit responses to these questions until the issue is resolved. Throughout the year, the IAEA informs each State of the results of each inspection and the conclusions it has drawn. While the details of each report is safeguards confidential, meta data might be shared via a SLT to show that the IAEA is meeting its obligations to the States. Additionally, the IAEA prepares a confidential safeguards evaluation report about its inspection activities in each State, and integrates these findings into an annual Safeguards Implementation Report, which is issued to its Board of Governors. The IAEA then publishes a summary of the report on its website to highlight the main achievements, developments, and concerns from the previous year. 58 As summaries, such statements contain few details about country-specific inspection activities or about the costs associated with such efforts. Discussions are ongoing about ways to improve the transparency and effectiveness of IAEA reporting to States via SLT solutions.

Thus far, the discussions remain theoretical. As part of this study, the authors documented high level data flows that includes the IAEA, State, Board of Governors, and the public. For example under the State we include: Reports (ICR, MBR), shipments and receipts of nuclear material, mailbox declarations, design information questionnaire, and provision of information under the Additional Protocol. For the IAEA, we include 90a & 90b statements, Comprehensive Safeguards Agreement notifications, Complementary Access notifications under the Additional Protocol, and Safeguards Implementation Report. We then looked at SLT as both the transmission mechanism and the transparency mechanism. For transmission we could see, for example, where the IAEA would give credit to a State for meeting reporting requirement deadlines as soon as their report was posted to the ledger. For the transparency mechanism we assure that sensitive data is encrypted and transparency data like dates and content titles would be open for viewing by those who can see the SLT but are not the involved party. This transparency opens the system so it could give confidence to all participants that the system is working and all parties are meeting their obligations. Or conversely, show those that are not meeting their obligations.

9.4 Nuclear Material Shipment Tracking

Through contractual agreements, nuclear material is shipped both internationally and domestically under strict regulations that address safety, security, and safeguards issues as well as protect the financial value of the material. In accordance with the State's safeguards agreement, the IAEA has the right to verify shipments and receipts of nuclear material.[59] Under today's shipping technology, the use of global positioning system (GPS) tracking on all forms of transport is routine. Yet, real time reporting of this

[58] All Safeguards Statements from the years 2000-2014 can be found here: https://www.iaea.org/Publications/Reports/.

[59] IAEA - International Atomic Energy Agency. 1972. The Structure and Content of Agreements Between the Agency and States Required in Connection with the Treat on the Non-Proliferation of Nuclear Weapons. INFCIRC/153, International Atomic Energy Agency, Vienna, Austria. Para. 91-94. Available at https://www.iaea.org/publications/documents/infcircs/structure-and-content-agreements-between-agency-and-states-required.

tracking information is not a current requirement of international safeguards. Instead, the States involved in the shipment “shall make suitable arrangements to determine the point at which the transfer of responsibility [for the nuclear material] will take place.”[60] Subsequently, the exporting State must notify the IAEA of the probable date that the receiving State will assume responsibility for the material. If the material will not be placed under safeguards in the receiving state, the IAEA should be notified within three months of the time when the recipient State confirms receipt of the nuclear material. In addition, States are only required to report approximate dates of when the material actually leaves or arrives at a facility. In short, there is a lack of precision in the reporting requirements governing shipments of nuclear material. Such imprecision can prevent the IAEA from having full insight into the location and movement of nuclear material around the world and impact its ability to efficient carry out verification activities.

While adding reporting requirements would certainly give the IAEA greater insight into such shipments, it is not easy—and it is arguably unnecessary—to do so. Some version of a SLT solution might enable States to voluntarily report GPS data throughout the shipping process.[61] However, due to obvious security concerns about sharing GPS information about nuclear material shipments, such data would be encrypted, enabling on certain users to view the raw data. Such voluntary reporting might then promote more effective and efficient verification activities, creating some incentive for the IAEA to encourage use of SLTs for this purpose. The only apparent incentive for States to use a SLT to share GPS information would be to demonstrate transparency and cooperation with the IAEA. Such transparency and cooperation would enable the IAEA to adjust inspection schedules to efficiently and effectively perform verification activities at facilities.

10.0 Findings and Recommendations

Based on this exploration of the potential implications of bitcoin, blockchain, and SLT for the safeguards system, the team established two outcomes. First, we developed a nomenclature to describe SLT from which we created a set of conceptual SLT models. Given our set of SLT models, we have proposed an approach for model assessment within a given safeguards context. This nomenclature and associated analytical approach will help inform future investment decisions involving different SLT applications for safeguards purposes.

Second, we discovered that SLT offers a spectrum of benefits to the safeguards system. SLT can be used to promote efficient, effective and timely reporting through spot-checking software and generally improved digital reporting. But we note that SLTs are not unique in offering this solution. Modern databases and IT solutions may be just as, if not more, effective to advance these objectives. However, SLT solutions also increase the amount of shared meta-data and the ability to share that information quickly, enabling States to participate in the safeguards system in ways they haven’t experienced before. As such, SLTs are unique in their ability to increase transparency in the safeguards system without sacrificing confidentiality of safeguards data. This increased transparency and involvement of Member States in certain safeguards transactions could lead to increased trust and cooperation among States. Greater reliance on SLT to support activities such as safeguards reporting or transit matching might allow

[60] Nuclear weapon states

[61] It is unclear what combination of shared ledger features might be most effective in facilitating such reporting (e.g., localized, centralized, permissioned).

the IAEA to redirect resources away from information management and more toward safeguards inspections. The combination of more effective, efficient, and secure data transmission processes, coupled with greater levels of transparency and trust in the safeguards system, might also encourage States to voluntarily, or indirectly, report more safeguards information, which could lead to the timely detection of nuclear material diversion. For example, many nuclear fuel cycle supplier activities are linked among many States, so one could envision where more information from one State might reveal an issue with, or resolve a question in, another State.

Based on the current analysis, we can only speculate about what might be possible. Further testing of different SLT environments that are specifically addressing safeguards problems is needed to validate these projections about how we think the technology will grow. A variety of actions can be taken to explore the collective benefits and contributions to effectiveness, efficiency, security, transparency, and trust which type of ledgers offer the most benefit or the most compelling set of benefits to safeguards:

- Identify opportunities for industry engagement. SLT is a rapidly developing area, garnering the attention of both entrepreneurs and large corporations. As the technology develops, more commercially available platforms will become available that the IAEA could potentially adopt. Similar to the types of engagements NNSA is pursing with the small modular reactor industry, NNSA could establish working groups or bilateral collaborations with companies that are specifically exploring alternative applications for SLT. These collaborations will help NNSA monitor advancements that could help validate or refute the concepts explored in this study.
- NNSA's Office of International Nuclear Safeguards could team with the Office of Research and Development to fund S&T research related to SLT (e.g., consortium consensus mechanisms, homomorphic encryption, etc.). Such research might involve design and development of a pilot SLT that is specifically designed around a set of safeguards requirements selected by NNSA and IAEA.
- Socialize the concept of SLT with the IAEA and selected Member States and document the feasibility and desirability of implementing SLT for safeguards purposes.

At the end of the day, the authors do not assert that SLT will solve a specific safeguards problem in a dramatic fashion. What we do see is a novel approach to strengthen the nonproliferation regime by increasing the level of trust and transparency across IAEA/State reporting commitments while maintaining data security and improving efficiencies. More research is necessary to determine how SLT solutions might be designed to solve selected safeguards problems and how much benefit might be derived in doing so. Specific investigations could explore stakeholder acceptability, establish functional requirements for a safeguards specific SLT, and evaluate the extent to which SLT designs might contribute to increasing the level of trust in the safeguards system.

Appendix A

Elaboration on Table 4

Appendix A

Elaboration on Table 4

Assessment of Blockchain Models against IAEA Objectives and Function Requirements

	Model Name	Private	Consortium	Public
	Characteristics & Features	Localized, Centralized	Distributed, Centralized	Distributed, Decentralized
IAEA Technology Functional Requirements	Improve and Contribute to Timely Detection	🟩	🟩	🟩
	Build Confidence & Trust in Member States	🟨	🟩	🟨
	Build Confidence & Trust in the IAEA	🟥	🟩	🟨

This Appendix provides justification for the colors given in the table above.

<u>Improve and Contribute to Timely Detection</u>

- Private: These systems will require improved and standardized digital submissions. This allows for information to be submitted more often, spot checked, etc. and makes reporting and resolution of deficiencies easier and more frequent—which leads to faster and increased detection.
- Consortium: Same as private.
- Public: Same as private.

<u>Build Confidence & Trust in Member States</u>

- Private: Member States could receive meta-data indirectly through IAEA, but they would be unable to confirm the authenticity directly from other Member States or necessarily confirm that other Member States are seeing the same thing. Confidence or trust might increase if additional information is submitted, but the same authenticity issues would apply.
- Consortium: Member States directly receive submissions (likely with some degree of confidentiality) and are more involved in the process, so they have more confidence that other nations are fulfilling their obligations
- Public: With a pseudonymous system, Member States are able see data/meta-data if they are maintaining a ledger but are unable to attribute the reporting to specific entities. This assumes that Member States would not be able to determine identity based on the transactions in the system.

<u>Build Confidence & Trust in the IAEA</u>

- Private: Member States still have to trust the IAEA to do what it is doing now, so change is unlikely.
- Consortium: The IAEA allows others to participate in the process, which shows its impartiality and willingness to be more transparent.

- Public: The international community will have more information, but cannot attribute it to a source that they care about, nor can they verify the validity (like a "societal verification" tip line) of a claim.

Pacific Northwest
NATIONAL LABORATORY

U.S. DEPARTMENT OF
ENERGY

Proudly Operated by **Battelle** *Since 1965*

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)

www.pnnl.gov