PNNL-28050

Pacific Northwest
NATIONAL LABORATORY

Evaluating Safeguards Use Cases for Blockchain Applications

October 2018

1 SL Frazar
2 CA Joslyn
3 RK Singh
4 AM Sayre

U.S. DEPARTMENT OF ENERGY

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

DISCLAIMER

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

PNNL-28050

Evaluating Safeguards Use Cases for Blockchain Applications

October 2018

1 SL Frazar
2 CA Joslyn
3 RK Singh
4 AM Sayre

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

Pacific Northwest National Laboratory
Richland, Washington 99352

OFFICIAL USE ONLY

Executive Summary

The International Atomic Energy Agency (IAEA or the Agency) provides credible assurances to the international community that countries are meeting their obligation not to divert nuclear material or misuse nuclear programs for non-peaceful purposes. The IAEA conducts a variety of verification activities, including onsite inspections, collection of open-source information, and use of instrumentation installed at facilities to collect and transmit data between facilities and IAEA headquarters. Based on these activities, the IAEA prepares and transmits to States computerized reports that summarize the results of its inspections and visits and communicates the results of its overall verification activities to the public through electronic reports. As the number of nuclear facilities and amount of nuclear material increases, the digital information that the IAEA must collect, protect, manage, evaluate, assimilate, and report becomes more complex and dynamic.

Meanwhile, the environment in which the IAEA must perform the aforementioned activities remains politically charged. Member States have no presumption of trust in each other's nuclear activities, nor do they always trust the IAEA. Yet, they rely on the IAEA's assurances to the international community that State nuclear programs remain dedicated to peaceful use.[1] To assert the independence and trustworthiness of its activities, the IAEA maintains a commitment to non-discriminatory verification approaches that feature technical criteria and objective factors about State activities.[2] Regardless, political disagreements remain, and they continue to be resolved through traditional mechanisms of communication, cooperation, negotiation, and arbitration.[3] Such traditional mechanisms can be limited in their effectiveness because their success ultimately depends on States maintaining a strong foundation of trust.

In 2009, the introduction of the digital currency Bitcoin and its underlying technology, the blockchain, presented a new variable into this politically charged environment. With rapid public acceptance of these two technologies, community stakeholders could begin to consider the variety of services cryptographically secure distributed ledgers (DLs) like blockchain could contribute to safeguards. Specifically, when applied in the right context, DLs could strengthen a foundation of trust among stakeholders while increasing the efficiency, lowering the cost, maintaining stakeholder privacy, and ensuring security surrounding digital transactions. Recognizing these benefits, the Pacific Northwest National Laboratory (PNNL) initiated a study in 2017 with sponsorship from the Nonproliferation and Arms Control Program (NPAC) at the National Nuclear Security Administration to explore the potential application of blockchain technology to international safeguards.[4]

As part of that effort, PNNL clarified key terms that were used to construct a conceptual methodology for evaluating different use cases for blockchain technology. In 2018, using the methodology as a guide, PNNL developed domain-agnostic evaluation criteria to determine whether a given use case might benefit from a DL solution. As part of this work, PNNL examined seven safeguards use cases involving digital

[1] Fact Sheet #3: Information Relevant to the IAEA General Conference. 2014. "Topic: Safeguards Resolution." Vienna, September 2014. http://www.nonproliferation.org/wpcontent/uploads/2014/09/2014_IAEA_GC_QA_Safeguards.pdf.

[2] IAEA. 2014. "Supplementary Document to the Report on the Conceptualization and Development of Safeguards Implementation at the State Level (GOV/2013/38). GOV/2014/41. August 13, 2014. https://armscontrollaw.files.wordpress.com/2014/09/iaea-state-level-safeguards-document-august-2014.pdf

[3] Paragraphs 3 and 22 of the Comprehensive Safeguards Agreement (INFCIRC/153) emphasize the cooperative nature of safeguards while providing options for issues resolution in the form of negotiation and arbitration, respectively.

[4] Frazar, Sarah, Mark Schanfein, Ken Jarman, Curtis West, Cliff Joslyn, Sam Winters, Sean Kreyling, and Amanda Sayre. 2017. "Exploratory study on potential safeguards applications for shared ledger technology," Pacific Northwest National Laboratory, February 2017.

transactions, including (1) transit matching, (2) UF_6 cylinder tracking, (3) computerized inspection and complementary access reports, (4) the noncompliance process, (5) nuclear material accounting reporting, (6) unattended monitoring systems and state-of-health transmissions, and (7) communicating safeguards information through the Safeguards Information Report. Eventually, the nuclear material accounting reporting use case and the computerized inspection/complementary access reports use case were combined into a single use case called Information Management and Reporting.

PNNL identified several key findings and recommendations from this evaluation.

- The terms, definitions, and concepts presented herein serve as a foundation for a defensible evaluation methodology that the IAEA can use to evaluate new use cases as they arise. This work aims to enable the IAEA and NPAC to make sound investment decisions in DL technology, given a set of use case conditions.
- DLs are designed to solve very specific types of problems, and while a DL may offer some benefits to various safeguards use cases, they do not necessarily provide a unique solution, making further investment questionable.
- PNNL recommends further exploration of the UF_6 cylinder tracking and transit matching use cases. However, indicators also suggest information management and the noncompliance process use cases might warrant further study.
- PNNL also considered multi-lateral Fuel Bank exchanges during its 2017 study. Although it was not evaluated under the 2018 study, based on the findings from the 2018 work, PNNL recommends conducting further research into this use case due to the number and types of digital transactions taking place, an apparent desire for decentralization to promote trust among stakeholders, and the lack of existing technical solutions to meet these needs.
- Finally, once a suitable use case is deemed worthy of further exploration, significant work is required to develop technical user requirements and explore stakeholder perceptions about the technology's deployment before the designing, developing, and testing of different ledger designs can proceed.

Acknowledgments

PNNL wants to acknowledge the thoughtful feedback and contributions provided by several safeguards and computer science experts, including Sean Kreyling, Brent McGinnis, John Oakberg, Mark Schanfein, Cindy Vestergaard, Curt West, Benjamin Wilson, and Sam Winters. PNNL also wishes to thank the NPAC at the National Nuclear Security Administration for its continued support for this work.

Acronyms and Abbreviations

CFR	Code of Federal Regulations
DL	Distributed ledger
DLT	Distributed ledger technology
ICR	Inventory change reports
MBR	Material balance reports
NNSA	National Nuclear Security Administration
NPAC	Nonproliferation and Arms Control
PoS	Proof of Stake
PoW	Proof of Work
SDP	State Declarations Portal
SIR	Safeguards Information Report
SL	Shared ledger
SoH	State of health
UMS	Unattended and Surveillance Monitoring System
IAEA	International Atomic Energy Agency
NMA	Nuclear material accounting
PNNL	Pacific Northwest National Laboratory

Contents

Figures

Tables

1.0 Introduction

The International Atomic Energy Agency (IAEA or the Agency) provides credible assurances to the international community that countries are meeting their obligation not to divert nuclear material or misuse nuclear programs for non-peaceful purposes. The IAEA conducts a variety of verification activities that generate, evaluate, and communicate data and information. Specifically, the IAEA collects, manages, analyzes, and assimilates State declarations consisting of inventory change reports (ICRs), physical inventory listings (PILs), material balance reports (MBRs), concise notes, and textual reports, which are typically submitted electronically to the IAEA. Broadly speaking, these declarations serve as a basis for inspection activities and the IAEA's safeguards conclusions; more narrowly, the IAEA reconciles information contained in ICRs to keep track of nuclear material shipments between facilities. The IAEA also collects open-source information such as academic papers, satellite imagery, and third party information, sharing and storing them internally as digital files. Unattended monitoring systems collect and transmit digital files containing surveillance images, non-destructive assay measurements, nuclear material flow measurements and state of health (SoH) information. The IAEA prepares and transmits to States computerized reports that summarize inspection results and complementary access visits and communicates overall verification results to the public through an electronic Annual Report and Safeguards Information Report. As the number of nuclear facilities and amount of nuclear material increases, the digital information that the IAEA must collect, protect, manage, evaluate, assimilate, and report becomes more complex and dynamic.

Meanwhile, the environment in which the IAEA must perform the aforementioned verification activities remains politically charged. Member States have no presumption of trust in each other's nuclear activities, or in the IAEA at times. Yet, States rely on evidence generated through the IAEA's verification activities that other States remain recommitted to their nonproliferation obligations. In the process, States continue to emphasize to the IAEA the importance of maintaining objectivity and pursuing non-discriminatory safeguards verification approaches.[1] To assert the independence and trustworthiness of its activities, the IAEA maintains a commitment to use non-discriminatory verification approaches featuring technical criteria and objective factors about State activities.[2] Regardless, political disagreements remain and continue to be resolved through traditional mechanisms of communication, cooperation, negotiation, and arbitration.[3] Such traditional mechanisms can be limited in their effectiveness because their success depends on States maintaining a strong foundation of trust.

In 2009, the introduction of the digital currency Bitcoin, and its underlying technology, the blockchain, presented a new variable into this politically charged environment. With rapid public acceptance of these two technologies (which will be described in Section 2.0), community stakeholders had a promising technical solution that could strengthen the foundation of trust underlying the safeguards system while increasing the efficiency, lowering the cost, maintaining stakeholder privacy, and ensuring the security of various digital transactions. Recognizing these benefits, the Pacific Northwest National Laboratory (PNNL) initiated a study in 2017 with sponsorship from the Nonproliferation and Arms Control Program

[1] Fact Sheet #3: Information Relevant to the IAEA General Conference. 2014. "Topic: Safeguards Resolution." Vienna, September 2014. http://www.nonproliferation.org/wpcontent/uploads/2014/09/2014_IAEA_GC_QA_Safeguards.pdf.

[2] IAEA. 2014. "Supplementary Document to the Report on the Conceptualization and Development of Safeguards Implementation at the State Level (GOV/2013/38). GOV/2014/41. August, 13 2014. https://armscontrollaw.files.wordpress.com/2014/09/iaea-state-level-safeguards-document-august-2014.pdf

[3] Paragraphs 3 and 22 of the Comprehensive Safeguards Agreement (INFCIRC/153) emphasize the cooperative nature of safeguards while providing options for issues resolution in the form of negotiation and arbitration, respectively.

(NPAC) at the National Nuclear Security Administration (NNSA) to explore the potential application of blockchain technology to international safeguards.[1]

As part of that effort, PNNL clarified key terms used to construct a methodology for evaluating different use cases for blockchain technology. Many of these terms warrant reiteration here as they set the stage for the follow-on work performed in 2018. The blockchain is one example of a *distributed ledger* (DL), which is "a type of database spread across multiple sites, regions, or participants," in which users maintain individual copies of the ledger while seeing the same information, thereby eliminating the need for a centralized authority to maintain the ledger.[2] While all blockchains are considered DLs, not all DLs are blockchains. By comparison, *a shared ledger* (SL) is one in which a large community of users access and see the same information on a single ledger. For purposes of this study and unless otherwise specified, the authors will use the term DL technology (or DLT) to represent the collection of technologies (blockchain, DL, and SL) because it is the distributed nature of the ledger that portends the most significant impact on the safeguards system.

Returning to the 2017 study[3], PNNL asserted that DLs could play a role in helping the IAEA fulfill certain strategic objectives associated with increasing trust and transparency in the safeguards system, but it did not articulate a specific use case that might benefit from a DL, how that ledger might be designed, or the conditions under which that ledger could be deployed.

Accordingly, PNNL began a follow-on study in 2018 to articulate the specific safeguards use cases that would most benefit from a DL solution. PNNL performed the work in three steps:

1. PNNL identified seven use cases involving digital transactions of safeguards data for evaluation. These use cases included (1) transit matching, (2) UF_6 cylinder tracking, (3) computerized inspection and complementary access reports, (4) the noncompliance process, (5) nuclear material accounting (NMA) reporting, (6) unattended monitoring systems and SoH transmissions, and (7) communicating safeguards information through the Safeguards Information Report (SIR). Eventually, the NMA reporting use case and the computerized inspection/complementary access reports were combined into a single use case called Information Management and Reporting.
2. PNNL developed domain-agnostic evaluation criteria to determine whether a given use case might benefit from a DL solution.
3. PNNL applied the criteria to each use case, identifying cases for further evaluation and validating the salient finding from the 2017 study that DLT offers a spectrum of benefits to a number of safeguards use cases.

As will be discussed in Section 4.0, the authors delineated this spectrum along the lines of feasibility and desirability. Feasibility refers to the technical possibility that DLs could be designed to meet certain safeguards objectives. Desirability refers to the level of desire or need for a DL solution to help a State or the IAEA fulfill a strategic objective. The use cases that met both feasibility and desirability criteria were excellent candidates for further evaluation by the IAEA.

---

[1] Frazar, Sarah, Mark Schanfein, Ken Jarman, Curtis West, Cliff Joslyn, Sam Winters, Sean Kreyling, and Amanda Sayre. 2017. "Exploratory study on potential safeguards applications for shared ledger technology," Pacific Northwest National Laboratory, February 2017.

[2] Buntinx, JP. 2017. "Distrubuted Ledger Technology v. Blockchain Technology." *The Merkle.* March 25, 2017. Available at: https://themerkle.com/distributed-ledger-technology-vs-blockchain-technology/

[3] Frazar, Sarah, et al. 2017. "Exploratory," Pacific Northwest National Laboratory. February 2017.

This study describes the work performed in 2018 with the intent to inform future investment decisions relating to DL technology for safeguards purposes. The study begins with a reiteration of the history and evolution of Bitcoin and its underlying technology (Section 2.0). Section 3.0 reviews key terms and summarizes the analytical methodology developed in 2017. Section 4.0 describes the methodology pursued in 2018 while Section 5.0 discusses the application of evaluation criteria against each use case. Section 6.0 describes key findings and recommends next steps.

2.0 Overview of Blockchain Technology

Bitcoin[1] is a digital currency and payment software system built on a cryptographically secure, replicated, electronic ledger called a "blockchain". Bitcoin was intended to disrupt the traditional paradigm of trust in financial systems where a centralized authority (such as a bank) retains a single, authoritative copy of a ledger of transactions, thus giving it sole authority to manage and regulate it while charging users an access fee. Under that system, users trust the authority will not manipulate the ledger in the process of managing transactions. By comparison, some participants in a blockchain-enabled financial system (those playing the role of "validators" or "miners") retain their own copy of the ledger and use computer algorithms and consensus protocols to validate and record a history of transactions.[2] As described in a previous paper by the authors[1]: "Parties post transactions pseudonymously, meaning their identities are protected but details about the transaction remain transparent. Computer programs run by validators … competitively process the financial transactions taking place on the ledger based on a secure system rooted in cryptography and financial incentives." In this way, the blockchain enables all participants, including validators and other users, to conduct the same types of financial transactions with more efficiency, transparency, and security than previously experienced, which can result in higher levels of trust in the overall system.

Since its inception, as public enthusiasm for Bitcoin increased, public interest in blockchain's capabilities grew as well. Experts in these technologies recognized that the blockchain designed to facilitate Bitcoin transactions to disrupt the traditional paradigm of trust did not necessarily capitalize on the variety of ways DLs might be used. On the contrary, DLs could be designed to facilitate transactions involving money, information, or any combination of digital items. Smart contracts were designed to both introduce complex logic and programming languages to blockchain transactions while other mechanisms help connect these digital workflows to physical actions in the world. Some began to predict that DLs would become a "game changer" for international transactions, dramatically changing information sharing, supply chain management, transaction auditing, and regulatory compliance.[3],[4]

Indeed, the blockchain market exploded, with the number of digital currencies and DL solutions increasing commensurately with the number of problems people hope it will solve. For example, while Bitcoin remains the premier digital currency, competitors such as Bitcoin Cash[5] (an earlier version of

[1] Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." https://bitcoin.org/bitcoin.pdf.
[2] Jaikaran, Chris. 2018. "Blockchain: Background and Policy Issues." *Congressional Research Service.* February 28, 2018. Accessed on 30 May 2018. https://fas.org/sgp/crs/misc/R45116.pdf.
[3] Crowe, Portia. 2016. "There Is a 'Game Changer' Technology on Wall Street and People Keep Confusing It with Bitcoin," *Business Insider*. Accessed May 17, 2016. http://www.businessinsider.com/what-is-blockchain-2016-3.
[4] Williams-Grut, Oscar. 2015. "Goldman Sachs: 'The Blockchain Can Change... Well Everything'," *Business Insider* (2015), Accessed May 17, 2016. http://www.businessinsider.com/goldman-sachs-the-blockchain-can-change-well-everything-2015-12?r=UK&IR=T.
[5] https://www.bitcoincash.org/. Accessed on 22 August 2018.

Bitcoin itself) and Litecoin[1] have gained considerable market share. Ethereum[2] demonstrates the promise of using DLs with a higher level of built-in computational power for automating workflows. Corporate engagement also increased, with IBM's adoption of Hyperledger[3] marking a significant entry, and distributed cryptographic technologies such as Guardtime[4] rising in prominence in applications like smart power grid technology. A growing diversity of core blockchain technologies also emerged, including:

- Ripple, which uses permissions to link their DL closely to fiat currencies for banking applications[5]
- ZCash[6] and Monero,[7] which introduce higher levels of cryptographic design to avoid potential loss of anonymity of Bitcoin
- Iota,[8] which uses an innovative cryptographic architecture called the "tangle" to enable Internet of Things applications.

Despite the growing acceptance of these various technologies, understanding why and how they disrupt common notions around information sharing, supply chain management, transaction auditing, and regulatory compliance can be challenging. To facilitate this understanding, the following sections introduce a key concepts about blockchain functionality and DL services, which were introduced in the 2017 study and will become relevant during the use case evaluation.

2.1 Blockhain Transaction Cycle

The key steps within blockchain transactions are outlined below and in Figure 1.[9]

[1] https://www.litecoin.com/. Accessed on 22 August 2018.
[2] https://ethereum.stackexchange.com/. Accessed on 22 August 2018.
[3] https://www.hyperledger.org/. Accessed on 22 August 2018.
[4] https://guardtime.com/. Accessed on 22 August 2018.
[5] https://ripple.com/. Accessed on 22 August 2018.
[6] https://z.cash/. Accessed on 22 August 2018.
[7] https://getmonero.org/. Accessed on 22 August 2018.
[8] https://www.iota.org/. Accessed on 22 August 2018.
[9] Botjes, Edzo. 2017. "Pulling the Blockchain apart. The transaction life-cycle." *Medium.* Accessed on July 31, 2018. https://medium.com/ignation/pulling-the-blockchain-apart-the-transaction-life-cycle-7a1465d75fa3.

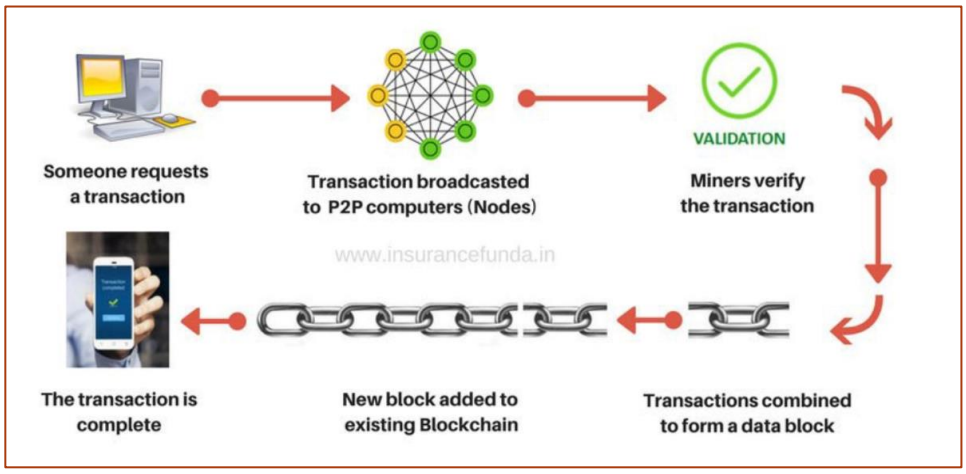

Figure 1. Blockchain Transaction Cycle (Botjes, 2017)

- **Transaction Initiation:** An originating node (computer) connected to the blockchain's peer-to-peer network requests a specific transaction, which is broadcast to all the other nodes (peers).
- **Validation:** "Miner" nodes in the network receive a collection of these broadcasted transaction candidates and attempt to validate the legitimacy of a collection ("block") of them through a computationally expensive algorithm. This process is computationally expensive because a cost is associated with running a blockchain node in terms of hardware, installation, and electrical power. This power requirement is driven by different "consensus algorithms" running on the blockchain, such as Proof of Work (PoW) or Proof of Stake (PoS). These algorithms decide which block of transactions should be trusted and added to the chain.
  - **Proof of Work:** PoW is the most expensive to run as each “miner” on the network uses a large amount of computing power (i.e., many computers) to compete with the other miners on the network to see who can be the first to complete a cryptographic puzzle and validate a new transaction. Those who solve the puzzle first apply the transaction to the block and earn some Bitcoin as a "reward". PoW does not scale well and is vulnerable to pooling, meaning miners can combine efforts to solve a puzzle and share in the earnings.
  - **Proof of Stake:** Pooling can lead to effective centralization of the network. That, combined with the cost of running PoW on a ledger, prompted the development of alternative consensus algorithms, such as PoS. Under PoS, one node or “validator” is selected to validate all the transactions in a block. A computer algorithm selects a single validator to cryptographically sign the block based on stake (percent ownership, wealth) held by the validator. Compared to a PoW approach, PoS requires less computing power and is therefore less expensive and more scalable. Moreover, with PoS no block reward is associated with the block generated so validators only get the transaction fee paid by the user. Hence, PoS validators are not incentivized to pool their efforts for profits, hence decentralization of the network is not threatened.
- **Publication:** The successful miner adds the candidate transactions as a block to the distributed database that records the ledger, and broadcasts the success to the network.
- **Consensus and Chaining:** If a conflict exists between multiple miners, the majority or the consensus of miners decide which block should be applied to the ledger, thus forming the chain.

2.2 Permissions

Blockchains can be implemented in various ways based on user needs. In a *permissioned* ledger only authorized parties can validate blocks and access the ledger, and a certain level of trust is required for parties to be a part of such a network in the first place. By comparison, in a *permissionless* ledger like Bitcoin, every node is responsible for maintaining consensus to decide the legitimacy of a transaction or whether it is valid, and anyone can participate in validating the blocks based on various consensus algorithms. Section 3.0 describes the permissions in various ledger designs in more detail.

2.3 Smart Contracts

Smart contracts are computer programs stored on a DL and executed by its peer nodes as part of the transaction validation process. They can thus perform calculations whose results are consistent across all the network nodes, reaching consensus on the result of the contract. These contracts can be written by anyone to conduct any deterministic computational operations, which could include exchange of money, digital assets, authorities and keys, or any digital work. Since Smart Contracts run on a blockchain itself, they produce transparent, efficient, conflict-free results without middlemen. These contracts can be triggered automatically based the results of other calculations or on the occurrence of certain events (conditions) (Figure 2).[1]

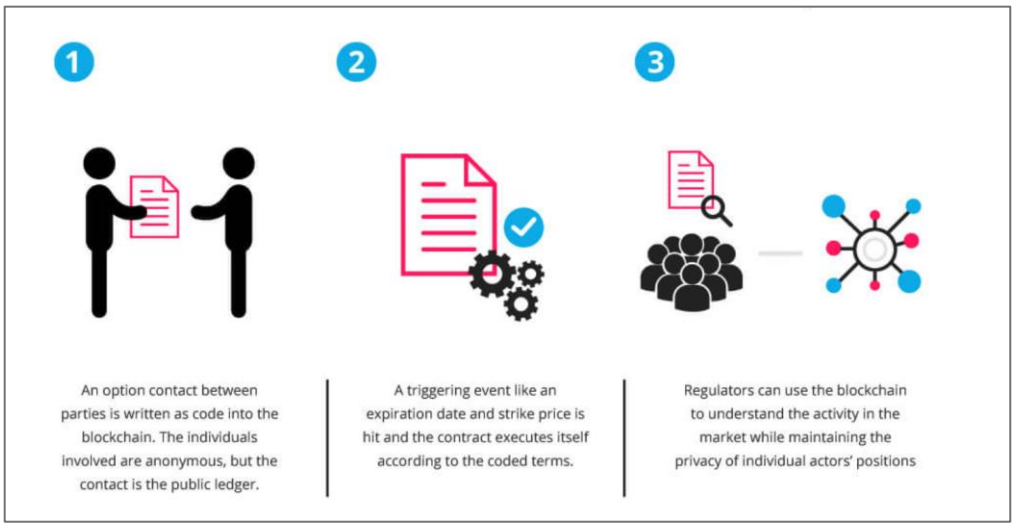

Figure 2. Smart Contract Methodology (Blockgeeks 2018)

2.4 The Future of Blockchain Technologies

Blockchain technologies have risen to high prominence recently, and promise serious disruption, both good and bad. Financial speculation and criminal activity run rampant in the DL space, and regulators eye the fast-moving developments warily. Nonetheless, DL technologies are also maturing while a range of actors come to understand their legitimate and productive role in the digital technology landscape. These

[1] "Smart Contracts: The Blockchain Technology That Will Replace Lawyers: A Beginner's Guide to Smart Contracts." *Blockgeeks.* Accessed July 31. 2018. https://blockgeeks.com/guides/smart-contracts/.

and other emerging DL technologies could impact the design of future ledgers that could be applied to safeguards and related workflows.

3.0 Summary of Analytical Methodology for Evaluating Potential Safeguards Use Cases (FY17)

When PNNL initiated its research into Bitcoin, blockchain, and DLs, the technologies were relatively nascent and rapidly evolving. Nearly two years later, the DL landscape has expanded and evolved significantly, yet the core services that PNNL described in 2017 remain relevant. These services establish the framework for the methodology developed in 2017 and applied in 2018 against the seven use cases.

As described in PNNL's 2017 report, DLs offer five core services that collectively improve transaction efficiency, transparency, and security, leading to higher levels of trust among ledger users[1]:

- ***Consistency***: Parties can see the same details about the shared fact.
- ***Validity***: Proposed transactions submitted to a system are validated against predefined rules, before being added to the ledger.
- ***Uniqueness***: Two transactions, even if both are valid, must not conflict with each other.
- ***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.

Next, the authors presented definitions for different types of ledger designs (see Table 1):

- ***Localized***: Has a single, authoritative copy (e.g., banks).
- ***Distributed***: Many copies of the ledger are maintained by a consensus protocol that provides a consistent view of each ledger.
- ***Centralized:*** Certain participants (a singular entity or a subset of entities) have permission to maintain the state of the ledger.
- ***Decentralized:*** All users have equal privilege in maintaining the consistent state of the ledger.

When these characteristics are combined, they offer different benefits to ledger users.

A Localized/Centralized Ledger is referred to as a ***private ledger***. Private ledgers are for single entities that maintain control over a single ledger. A centralized entity seeking to assert security and authority over ledger transactions is often attracted to this type of system, which is why they are often used in traditional banking systems.

A Distributed/Decentralized Ledger is referred to as a ***public ledger.*** Each party maintains a copy of the ledger and has equal access to the ledger. No single party is given special privileges for either submitting or validating transactions, viewing the ledger, or maintaining consistency of the ledger. The Bitcoin ledger is a good example of a public ledger. Users who desire greater transparency and individual control over their transactions are attracted to this type of system.

[1] Frazar, Sarah, et al. 2017. "Exploratory." Pacific Northwest National Laboratory. February 2017.

A Distributed/Centralized Ledger is referred to as a ***consortium ledger***. Under this system, a group of trusted users each maintains a copy of the ledger and executes distributed consensus protocol of the system. The group will agree on the permissions of the ledger, including who can make transactions (and with whom), who can read the ledger, etc. Users who value security and operate in regulated environments yet also desire a greater level of transparency and trust in that environment are attracted to this type of system. Use cases where a consortium ledger might be most applicable are those involving extensive sharing of declaration and inspection information among small groups of entities, such as the Brazilian-Argentine Agency for Accounting and Control or European Atomic Energy Community. The International Fuel Bank could also be viewed as a consortium.

Given logical inconsistency in combining a localized ledger, which refers to a single authoritative copy, and a decentralized ledger, which enables all users to maintain copies of the ledger, no alternative term for the combination exists.

Table 1. Combination of different ledger designs

	Centralized (permissioned)	Decentralized
Localized	Private	Not applicable
Distributed	Consortia	Public

These concepts were assimilated into a table showing generically how each ledger model might achieve the five blockchain services.

Table 2. Analytical Framework Assessing Blockchain Applications to Safeguards

		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		

As explained in the 2017 study:

> "Table 2 shows that three services (namely validity, uniqueness, and authentication) are common to all three models as they are available today using existing IT solutions, such as electronic databases, digital reporting software, digital signatures, and digital certificates. They can be engineered into any

model and provide sufficiently secure authentication of users. The primary difference between the models is how consistency and immutability are provided, and this is where we see the most potential to change the level of trust and transparency in a given system.

Put simply, it is unnecessary to use consensus mechanisms in a private ledger; a single entity maintains the ledger. By comparison, the use of [DLs] in a public or consortium system requires the incorporation of consensus protocols and possibly permissions. *Ultimately, it is the problem being addressed that determines the type of model that will be followed, the extent to which permissions are applied and to which users, and the type of consensus protocol that would be engineered into the ledger's design*."

At this juncture, the team referred to the IAEA's strategic goals (Improve and contribute to timely detection, build confidence and trust in Member State declarations, and build confidence and trust in the IAEA conclusions) and used a series of decision trees to determine preliminary design requirements for a variety of use cases, including transit matching, information reporting, and information management via the SIR.[1,2]

The 2017 paper thus laid the analytical foundation for evaluating safeguards use cases in fiscal year (FY) 2018. The approach to evaluate use cases in 2018 draws on the salient point from 2017: *DLs are designed to solve very specific types of problems*. As a reminder, Bitcoin and its underlying technology were initially designed to solve a particular financial problem—a desire to increase efficiency, security of, and trust in financial transactions while removing central decision makers from the transaction. As depicted in Table 2, the problems people are typically concerned about when exploring DLs (data uniqueness, validation, and authentication) can all be solved with a combination of existing databases, software programs, and encryption solutions. Once people recognize the type of problem they are trying to address, they often conclude that they do not need a DL to solve it.

Similarly, a number of safeguards use cases may benefit from or be solved with a DL solution, yet they could also be sufficiently addressed with existing non-DL information technologies. Other safeguards use cases' characteristics may be difficult, if not impossible, to solve with existing information technologies. The use cases where DLs provide benefits and help the IAEA fulfill one of its strategic objectives merit further investment and development.

4.0 Methodology

This section describes how the team selected use cases for evaluation, developed evaluation criteria, applied weights to different criteria, and ultimately scored the desirability and feasibility of different use cases.

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

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

4.1 Use Case Selection

Based on a review of safeguards verification activities as described in IAEA guidance documents,[1] the team identified activities involving different types of digital transactions that could be incorporated into computer algorithms run on a DL. Articulating the purpose of an activity provides the first indication as to whether the use case might benefit from a DL solution. Data reconciliation and information monitoring are traditional functions DLs tend to facilitate. Transmission of information can be facilitated through existing, non-DL technologies; decentralizing the transmission process does not ostensibly add value, although there may be exceptions. Table 3 lists each use case and aligns it with a specific function the ledger is intended to facilitate:

Table 3. Alignment of Ledger Purpose with Safeguards Use Case

Safeguards Use Case(s)	Purpose
Transit matching, NMA reporting	Data reconciliation
UF_6 cylinder tracking	Information monitoring
Unattended monitoring and SoH data	Data transmission
SIR, computerized inspection and complementary access reports, and noncompliance process	Information communication

For each use case, the authors drew upon peer-reviewed journal articles, presentations, and expert opinion to create a matrix aligning specific safeguards verification challenges against a DL service (e.g., immutability) and a specific safeguards requirement (e.g., timeliness of reporting, timeliness of detection). This activity clarified safeguards challenges that might be solved with DL services. For example, the authors selected the following statement from a peer-reviewed journal: "Batch identification declared in shippers/receivers must be identical but the receiver sometimes doesn't know shipper's batch ID and vice versa, which leads to unmatched reports and delays."[2] This type of challenge relates closely to the safeguards requirement "timeliness of reporting," and might be considered a "validation issue" in DLT context, so it was placed in the matrix in alignment with these two factors. This research provided the necessary information for evaluating each use case.

4.2 Criteria Development

Next, the team developed selection criteria for evaluating potential use cases and listed them under one of two categories: feasibility and desirability. If a use case met some or all of the feasibility criteria, it meant certain use case characteristics could be addressed with a DL solution. However, as discussed, many existing non-DL IT, software, and database solutions might also provide these benefits. Due to the significant investment and effort required by the IAEA and Member States to explore, develop, and incorporate new technologies into existing workflows, *a technology that does not enable the IAEA to*

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

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

fulfill a strategic objective is unlikely to receive significant interest from IAEA staff. Thus, the team developed desirability criteria. If a use case met some or all of the desirability criteria, it meant the incorporation of a DL might enable the IAEA to increase trust in Member State declarations, increase trust in IAEA safeguards conclusions, or increase the timeliness of detection.

Table 4 and Table 5 show the two categories of criteria. The ranking methodology used in these tables is dedicated to the idea that while seeking conditions to *justify* the use of a DL, on a technical basis it is perhaps more important to recognize conditions where a DL is actually counter-indicated. Thus the rankings recognize the "modality" of a criteria:

- **Promoters:** A promoter criterion argues in favor of using a DL. A use case that meets a promoter criterion suggests value in pursuing a DL for that purpose. However, failure to meet a promoter criterion not necessarily mean a DL is disadvantageous. For example, a use case that does not require a high level of data security may still benefit from a DL solution.
- **Demoters:** A demoter criterion argues against use of a DL for that use case. A use case that meets a demoter criterion suggests there is no value in pursuing a DL for that purpose. However, failure to meet the criterion ("Does not Meet") does not necessarily conclude that a DL would be the right solution. For example, in Table 3, use cases that can be solved with existing IT would argue *against* the use of a DL, while failing to meet that does not necessarily suggest a DL. The conclusion is neutral; other solutions may be a better fit.

Table 4. Feasibility Criteria

Feasibility Criteria	Modality
Use case requires high level of data security Information can only be shared with designated entities	Promoter
Use case requires auditable data trail Stakeholder confidence in current data depends on confidence of past transactions	Promoter
Use case would benefit from faster transaction completion Stakeholders would benefit from faster processing data (~every 10 minutes)	Promoter
Use case would benefit from higher confidence in data validation Stakeholders desire greater understanding of transaction provenance, uniqueness, and identification	Promoter

Table 5. Desirability Criteria

Desirability Criteria (as driven by IAEA strategic goals)	Modality
Existing information technologies solve use case challenges	Demoter
Use case would lead to an improvement of trust Stakeholder interests currently unaligned; no trust among stakeholders is presumed	Promoter
Use case requires a centralized authority, even if a DL is implemented	Demoter
Use case would improve the timeliness of detection Primary function of the use case directly supports IAEA ability to detect diversion of nuclear material or undeclared activities	Promoter

4.3 Use Case Scoring

A use case that fully met a promoting criterion received a 1; those that partially met a given promoting criterion received a 0.5; and use cases that did not meet the given promoting criterion received a 0. For demoting criteria, these values were negated, with a use case that fully met a demoting criterion receiving a -1, etc. The team additionally applied a weighting scheme to the criteria to differentiate the use cases. Each *feasibility* criterion was weighted by a factor of 1 to establish a baseline for comparison. *Desirability* criteria were given a weight of 2 to emphasize the importance of meeting strategic objectives when considering DL technologies applications in a given use case. Each use case received a feasibility score, a desirability score, and an overall score. For example, the average of all the feasibility scores was 3.1, so a use case with a feasibility score exceeding 3.1 was highlighted as a use case that fulfilled feasibility requirements. A use case with a score exceeding .66 fulfilled desirability requirements. Following this approach, the team expected some use cases to be feasible but not desirable; others might be desirable, but not yet feasible. Use cases that fulfilled both sets of requirements were considered worthy of further exploration.

5.0 Safeguards Use Cases

This section describes each use case's concept of operation, highlighting specific safeguards challenges reported by subject matter experts or in open literature. The team examined all use cases involving digital transactions to provide a rich dataset for comparison. The team anticipated that some, and possibly none, of the use cases might call for or benefit from a DL solution. After each description, a table reflects how each use case was evaluated using the methodology in Section 4.0.

5.1 Information Management and Reporting

The Information Management and Reporting use case presents a standard ledger-type problem in that it involves reconciliation of large amounts of digitized data. The IAEA's role is not to independently track nuclear material worldwide. Rather, the Agency verifies information provided by States about the status of nuclear materials and activities in their countries. This process generates hundreds of thousands of accounting records and other communications from both the IAEA and Member State that require submission, tracking, and reconciliation within certain timeliness parameters. Existing IAEA databases are disjointed, requiring individuals to look in multiple places for information. To address this issue, the IAEA launched the MOSAIC project to, "enable staff to search information across the entire repository."[1] MOSAIC is an existing information management technology that provides some of the same services as DLT (e.g., information protection, auditability), and the IAEA recently invested significant funding to ensure it is capable of meeting future information reporting needs. Thus, comparing the two technical approaches can help to determine whether DLs provide unique value beyond that which is offered via MOSAIC.

The rationale for this comparison emerged during a meeting with IAEA staff hosted by Cindy Vestergaard of the Stimson Center.[2] During this meeting, IAEA staff recognized the importance of reducing or eliminating certain manual activities while maintaining or improving data security. This desire for increased efficiency and security appears to be driving initial interest in DLs. However,

[1] IAEA. 2017. "MOSAIC: The Modernization of Safeguards Information Technology." https://www.iaea.org/sites/default/files/17/01/mosaic.pdf.

[2] The meeting was hosted by Cindy Vestergaard of the Stimson Foundation and funded by the Stanley Foundation. The meeting was conducted March 13, 2018, at the Vienna Center for Disarmament and Nonproliferation. All discussions were held under Chatham House rules.

participants also noted that merely freeing resources from one activity so they can be applied to another is unlikely to convince the IAEA and its Member States to invest significant resources in exploring and developing an emerging technology such as DLT. In fact, many of the Member States with large commercial nuclear fuel cycle operations have laws in place that do not allow the state to require actions on the part of an operator that are not strictly required by a safeguards agreement. Recognizing this constraint, the participants asserted that the emerging technology would have to enable the IAEA to achieve something unprecedented or facilitate additional reporting from Member States before the Agency would commit significant resources to developing and incorporating the technology into existing infrastructure and workflows. In other words, this use case likely would have to exceed both the average feasibility and desirability scores to justify further investment in a DL solution for information management purposes by the IAEA. Thus, as part of the evaluation of this use case PNNL considered the capabilities that reside in MOSAIC.

The electronic Verification Package (eVP) housed in MOSAIC "consolidates into a single application activities associated with safeguards in-field verification, including planning, reporting and review…also referred to as the "Inspectors' App." By their account the IAEA claims eVP will "remove the need for hundreds of thousands of paper documents each year."[1] Furthermore, the Field Activity Reporting application assists the inspector in generating relevant reports. The Collaborative Analysis Platform will "give [IAEA] users the ability to search, collect, and integrate multiple data and information sources" increasing the effectiveness and efficiency of state evaluations.[2] The State Declarations Portal (SDP) is designed to allow relevant parties to exchange information such as NMA Reports; Additional Protocol Declarations; requests for termination, exemption, and re-application of safeguards; information provided under voluntary arrangements (e.g., neptunium/americium, international trafficking database); and requests for approval or clarification.[3] This exchange of information is performed using standard VPN, two factor authentication.

The SDP may be an area in which DLs have applicability by providing a more efficient, secure, and automated means for transmitting additional information regarding the batch identity, location, movement, contract association, corporate information, sample analysis, etc. A DL could allow the operator to go beyond what is typically required under Code of 10 of the model Subsidiary Arrangement and attach more detail regarding the information on a "batch" that, if distributed, could be verified using an expanded set of information. Such provision of additional information would increase the IAEA's situational awareness of State nuclear activities.

Despite the links between these new applications, it is still unclear whether MOSAIC will help the IAEA substantially increase its transparency and therefore trust by Member States. What is known is that the SDP allows States and regional authorities to share information with the IAEA and vice versa without violating the confidentiality commitments in INFCIRC/153 (para 5) and INFICRC/540 (Art. 15). Ultimately, while MOSAIC may not necessarily solve all problems associated with stakeholder trust, its ability to improve efficiency within the IAEA's information management system may be a sufficient near-term solution.

[1] Fisher, Matt. 2017. "New Application Increases Efficiency and Effectiveness of Safeguards Verification." IAEA. https://www.iaea.org/newscenter/news/new-application-increases-efficiency-and-effectiveness-of-safeguards-verification

[2] Ibid.

[3] IAEA. 2018. "The IAEA Safeguards State Declarations Portal." https://www.iaea.org/sites/default/files/sg-sdp.pdf.

Table 6. Evaluation of Information Management and Reporting Use Case

Criteria	Information Management and Reporting	Determination
Feasibility Requirements		
Use case requires high level of data security (information can only be shared with designated entities)	In accordance with INFCIRC/153 and INFCIRC/540 state-supplied information and the results of safeguards activities are protected to prevent inappropriate disclosure. However, metadata are shared in the SIR to provide support for safeguards conclusions. State information is treated as safeguards confidential so digital reports are sent via VPN/encrypted email. However, metadata are shared among Safeguards Evaluation Groups as they prepare the SIR to provide evidence of safeguards conclusions, but all findings are protected as safeguards confidential.	**Meets**
Use case requires auditable data trail	An audit trail of all corrections is critical. The closing balance for an MBR from a prior material balance period must match the opening balance for the current period. The period covered by the statement must be constant in covering the period from the end of the previous statement. In the current system, if an error exists in a submitted transaction, a separate new transaction must be entered to correct the error and it is keyed back to the original entry error. The original entry cannot be changed. The integration of safeguards reports into the State Declaration Portal does not change this capability. A DL would provide for a more efficient means for connecting a "correction" to a previous entry, say to correct an identified bias, through cryptographically secure workflows.	**Meets**
Use case would benefit from faster transaction processing (enabled by PoW)	While timeliness of safeguards reporting is important, there is no driving need for submitting real-time PILs/MBRs/ICRs. Nevertheless, the sooner the IAEA received accounting reports, the sooner it can draw a safeguards conclusion. Information reporting must be submitted by deadlines reflected in the Comprehensive Safeguards Agreement, namely as soon as possible but, due no later than 30 days after the end of the month in which the ICR occurred, or 30 days after a physical inventory taking for PILs and MBRs. States tend to have more stringent reporting timelines and quantities to address nuclear security concerns that could also benefit international safeguards reporting, which could be an adoption incentive if the IAEA decides to use DL for information reporting purposes.	**Partial**
Use case would benefit from higher confidence in data validation	Clerical errors do happen. Increasing confidence in data provenance and identification could add value.	**Meets**
Desirability Requirements		

Existing information technologies solve use case challenges	MOSAIC and the State Declaration Portal effectively support consistent, timely reporting and analysis of information.	**Meets**
Improves Trust: Stakeholder interests are not aligned with central authority	There is no presumption of trust. By definition, NMA reporting is necessary so the IAEA can verify State declarations.	**Meets**
Improves Trust: Central authority required (decentralization does not undermine effectiveness; may bring value)	The IAEA will always remain a central authority in the safeguards system because of the role inspectors play in verifying State-provided information. However, DLs could provide a means for the IAEA to reduce the level of effort while strengthening the confidence that the international safeguards community has in the conclusions drawn by the IAEA. More research is required to determine the extent to which IAEA effort could be reduced via DLs.	**Meets**
Improves timeliness of detection (use case function)	NMA reporting is critical to detecting diversion and undeclared activities. Thus, NMA reporting directly support the IAEA's strategic goal to improve the timeliness, correctness, and completeness of reporting.	**Meets**

5.2 Transit Matching

Transit matching was identified in PNNL's 2017 study as a potential safeguards use case due to the large number of nuclear material transactions involved and the activity's focus on data reconciliation. Although related to the Information Management and Reporting Case above, this use case takes a deeper look at the process of reconciling the content of specific reports rather than the presence and timeliness of the reports themselves. The following description of the transit matching process was drawn from the 2017 study:

> "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 one regional authority). 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 3,000-4,000 records remained unmatched each quarter.[1] 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.[2] 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."

Due to the number of ICRs requiring hand matching (~25%, the majority of which report foreign transfers),[3] identifying and quantifying the issues resulting in the need for manual intervention can be challenging. Regardless, immutable, transparent monitoring of these data would increase situational awareness and quickly flag transactions that could not be automatically reconciled. Such features would save the IAEA considerable resources while promoting transparency and trust among stakeholders. That said, Member States would need to take steps to improve their reporting practices, such as requiring their operators to declare transfers in a manner that allows for machine matching and update their matching rules.[4] While DLs could introduce efficiencies, such Member State reporting practices could undermine a DL's effectiveness at improving the effectiveness and efficiency of transit matching.

Table 7. Evaluation of Transit Matching Use Case

Criteria	Transit Matching	Determination
Feasibility Requirements		
Use case requires high level of data security (information can only be shared with designated entities)	State regulations on transfer of confidential information vary. Many do not trust encryption. A DL would improve data security. However, States that do not trust encryption will most likely not use a DL either.	Meets
Use case requires auditable data trail	Batch identification declared by the shippers and receivers must be identical. However, the receiver sometimes does not know the shipper's batch identification (or batch name) and vice versa, which leads to unmatched reports by software and consequently delays in matching. Clerical issues in reporting (e.g., noting a wrong country in the shipper invoice) can result in mismatched reports. DLs could help with automating reconciliation of identification information and create an immutable audit trail for monitoring and analysis purposes.	Meets

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

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

[3] Oakberg, J.A., Gilligan, K.V., Whitaker, J.M. 2013. "IAEA NPT Transit Matching: Current Methodologies and Challenges." Oak Ridge National Laboratory. ORN/TM-2013/160.

[4] Benjamin Wilson, email message to author, September 17, 2018.

Use case would benefit from faster transaction processing (enabled by PoW)	Reporting delays happen due to long shipment delays (e.g., UF_6 cylinders). No indication whether undeclared activities were performed in the event of a diverted shipment or misuse of a facility. Containment and surveillance helps mitigate. Global transparency is desired.	Meets
Use case would benefit from higher confidence in data validation	Batch identification declared in shippers/receivers must be identical but receiver sometimes does not know shipper's batch ID and vice versa, which leads to unmatched reports and delays. Clerical issues in reporting (e.g., noting wrong country in shipper invoice) can result in mismatched reports.	Meets
Desirability Requirements		
Existing information technologies solve use case challenges	Technologies exist but have not reduced the number of unmatched reports, sometimes because States ignore requests for information from the IAEA. Some States may not update matching rules, undermining the effectiveness of existing IT solutions. In 2012 alone, approximately 600,000 ICRs were generated by 55 States. Approximately 3,000-4,000 remain unmatched each quarter.	Partial
Improves Trust: Stakeholder interests are not aligned with central authority	IAEA reconciliation of shipper/receiver data is necessary so the IAEA can verify State declarations about shipments and receipts. There is no presumption of trust between the IAEA and Member States.	Meets
Improves Trust: Central authority required (decentralization does not undermine effectiveness; may bring value)	As envisioned by the scenario in the study, transit matching is a reconciliation process that could be performed on the ledger by computer nodes running consensus algorithms on a shared peer-to-peer network. Transactions would be visible to the IAEA and any State interested in monitoring movements of nuclear material worldwide.	Does not Meet
Improves timeliness of detection (use case function)	Improving the effectiveness and efficiency of the transmit matching process directly impacts the IAEA's strategic objective to improve the timeliness of detection. No human matching is performed on unmatched reports of small (de minimis) amounts, which are defined by the IAEA. Immediate detection of missing material is not always possible through transit matching because the reporting timeliness can vary greatly. Different Code 10 record structures result in differences on how many records are reported to indicate a shipment or receipt. Comprehensive, automated transaction reconciliation improves situational awareness and enables better tracking and monitoring of nuclear material subject to international safeguards.	Meets

As reflected in Table 7, this use case scored relatively high, so it is worth envisioning how a DL might be applied. Upon shipment of material, a facility might add metadata drawn primarily from inventory change

and shipping documentation, and depending on Code 10 format, include the encoder's name, reporting period, facility code, the shipper's ICR number, and the recipient's country inventory report number.[1] If States provided this information consistently today, many of the challenges inherent in the transit matching process would be resolved. That said, DLT could introduce other benefits not seen today.

For example, any information added to a DL would be immutable, thus preventing facilities from manipulating the data. DLT could allow Member States to be granted access to transit records by the declaring State. It would then be possible for a group of countries to agree to share information and establish a transit-consortium, thus promoting transparency and possibly trust that States are reporting the nuclear material inventories transferred to other material balance areas. Upon receipt of the material, the two transactions are automatically reconciled using Code 10 data and added to the ledger. Any discrepancies in the metadata are flagged for the IAEA. Since the entire reconciliation process would be performed via consensus algorithms on the ledger, it could take place without the IAEA's involvement but not without IAEA awareness. Using a DL for this purpose, machine matching would become an intrinsic part of the ledger, possibly decreasing the number of transactions requiring hand matching. The IAEA would still receive ICRs and be required to verify the information contained in those reports through inspection activities. However, this component of the information management and reconciliation process could be decentralized without undermining IAEA effectiveness.

Use of DLs for this purpose may also increase the international safeguards community's confidence in the ability to detect possible collusion between States to divert nuclear material from peaceful to non-peaceful purposes. A DL would provide more transparency for scenarios in which Non-nuclear Weapons States ship material to a Nuclear Weapons State under an agreement that restricts the Nuclear Weapons State from using their material for non-peaceful purposes.

5.3 Safeguards Implementation Report

The IAEA prepares an annual SIR to summarize its safeguards inspection results. A summary of this report referred to as the *Safeguards Statement* is released to the public.[2] In this report, the IAEA presents its safeguards conclusions, listing each country in accordance with the types of safeguards agreements the country implements. The report discusses how the IAEA derived its conclusions based on the types of verification activities performed under the country's safeguards agreements. The IAEA also prepares a more detailed SIR that contains quantitative data measuring the extent to which States fulfill their reporting obligations. This more detailed report is treated as safeguards confidential and is not released to the public. Although this case study is also related to the Information Management and Reporting Case above, the SIR process involves a one-way provision of information, as opposed to reconciliation of information. Thus, the team included the transmission of this report as a case study to explore whether a DL or SL might improve communications between the IAEA and Member States or strengthen the reports' transparency and effectiveness as a reporting mechanism.

As reflected in Table 8, this use case did not receive high scores primarily due to existing mechanisms for transmitting the SIR and little to no driver for decentralizing the process. However, the preparation of the SIR within the IAEA is a highly confidential process with tight deadlines and all information assembled from the divisions must be correctly and accurately assimilated into the SIR. Bringing together all of the information within the Department, in various forms, is a time-consuming process that might benefit from a cryptographically secure, automated workflow or Smart Contract that runs on top of a DL.

[1] IAEA. 2011. "Contents, Format, and Structure of Reports to the Agency." SG-FM-1172. https://www.iaea.org/sites/default/files/sg-fm-1172_-_model_subsidiary_arrangement_code_10_labelled.pdf.
[2] IAEA. 2016. "Safeguards Statement for 2016." https://www.iaea.org/sites/default/files/statement_sir_2016.pdf.

Table 8. Evaluation of Safeguards Information Report

Criteria	Safeguards Implementation Report	Determination
Feasibility Requirements		
Use case requires high level of data security (information can only be shared with designated entities)	The process of preparing the SIR is a highly protected process. The results are eventually released to the public in electronic format annually for informational purposes to allow Member States to monitor IAEA activities.	Partial
Use case requires auditable data trail	Public trust in the data reported in the SIR relies on maintaining a clear audit trail.	Meets
Use case would benefit from faster transaction processing (enabled by PoW)	The SIR is released annually and features a single transmission of information. No exchange of information that would requires a PoW calculation.	Does not Meet
Use case would benefit from higher confidence in data validation	As data are collected and reported in the SIR, this criterion does not directly apply to the use case.	Does not Meet
Desirability Requirements		
Existing information technologies solve use case challenges	The SIR is released annually and features a single transmission of information. Efforts are under way to make this report more dynamic and informative using existing software and data analysis solutions.	Meets
Improves Trust: Stakeholder interests are not aligned with central authority	There is no presumption of trust among the stakeholders interested in SIR content. In fact, through release of the SIR the IAEA seeks to improve transparency and trust in the safeguards conclusions that are derived from the Agency's verification activities.	Meets
Improves Trust: Central authority required (decentralization does not undermine effectiveness; may bring value)	As the SIR is released by the IAEA, it would be impossible to decentralize the process.	Meets
Improves timeliness of detection (use case function)	While the SIR data are gathered in direct support of the strategic objective to improve the timeliness of detection, the report itself does not directly support this objective.	Does not Meet

5.4 UF_6 Cylinder Tracking

Uranium hexafluoride or UF_6 cylinders are standardized steel cylinders used for storing and transporting UF_6 between conversion, enrichment, fuel fabrication, and material recovery facilities. Cylinders are 30 or 48 inches in diameter fabricated to the ISO 7195 and ANSI N14.1 standards with several models in production for industrial scale transportation of depleted natural and low enriched uranium (e.g., Model

30B, 48X, 48Y, and 48G).[1] Depending on its size and its contents, a cylinder can contain between 2 and 12 metric tons of depleted, natural, or low-enriched UF_6. International transportation standards require cylinders to display a metal nameplate with identifying information including owner, serial number, and certifications. However, the value of this information is diluted by the fact that cylinders are often given additional non-standard markings by facilities to aid with internal operations. In any case, the identification information is not typically tracked by the owner, manufacturer, or receiver via database or digital exchanges of information. Rather, the receiver verifies the number of the cylinder based on the sale/transit manifest.

The weaknesses in this asset tracking system make nuclear material in cylinders vulnerable to diversion during transit. As the former Director of Safeguards at the IAEA, Olli Heinonen, explains,

> "About 100,000 UF_6 cylinders are currently in worldwide use. Most of them are used to store depleted uranium, but there are annually about 15,000 movements of cylinders containing low-enriched or natural uranium. These cylinders move from country to country often overseas between uranium conversion, enrichment and fuel fabrication plants on journeys and voyages, which last several weeks. While industry is good at tracking valuable materials, it may take several weeks before missing cylinders are detected and the cylinders are located."[2]

Continuing, Heinonen states,

> "Cylinders in transit or stocks can be diverted by a state or obtained by subnational groups or black market vendors. There are several diversion scenarios including diverting a known, declared cylinder for uranium enrichment in a clandestine facility, or misusing a declared cylinder without reporting to the regulatory body or the IAEA in a declared, safeguarded facility, or using an undeclared cylinder at a safeguarded facility."[3]

Due to these concerns, safeguards experts studied the concept of a applying a unique ID to cylinders, referred to as a Global ID, to facilitate cylinder tracking.[4] Further development of a Global ID concept could involve establishing a shared database that would be similar to a SL in that multiple parties could access and monitor the same information. Assuming a ledger could be designed to incorporate digital Global ID numbers, the number of digital transactions each year would total approximately 150,000. These digital transactions do not exist for this purpose just yet. While a DL would certainly improve the efficiency and effectiveness of UF_6 cylinder tracking and increase the level of situational awareness among stakeholders, a DL would add value by enabling parties worldwide to maintain an immutable history of transactions, reducing the opportunity for facilities to manipulate the shared database to hide cylinder diversion. Thus, as reflected in Table 9, this use case received relatively high scores.

---

[1] WNTI. 2017. WNTI Standard: UF_6 Cylinder Identification. Accessed 4 April 2018. https://www.wnti.co.uk/media/87140/WNTI%20STANDARD%20-%20UF6%20Cylinder%20Identification%20-%20Version%20--%20Final%20-%202017.pdf.

[2] Ibid.

[3] Heinonen, Olli. 2014. "Why the Monitoring of Movements of UF_6 Cylinders Matters." Harvard Kennedy Center: Belfer Center for Science and International Affairs. 29 April 2014. https://www.belfercenter.org/publication/why-monitoring-movements-uf6-cylinders-matters. Accessed March 28, 2018.

[4] Whitaker, M., J. L. White-Horton, and J. M. Morgan. 2013. "Preliminary Concept of Operations for a Global Cylinder Identification and Monitoring System." Oak Ridge National Laboratory, August 2013. ORNL/TM-2013/278.

Table 9. Evaluation of UF_6 Cylinder Tracking Use Case

Criteria	UF6 Cylinder Tracking	Determination
Feasibility Requirements		
Use case requires high level of data security (information can only be shared with designated entities)	As with all safeguards information, the need for security and auditability of databases tracking cylinder movements is a top priority to facilities, States, and the IAEA. The spoofing or hacking of these databases or ledgers could lead to undetected diversion of nuclear material.	Meets
Use case requires auditable data trail	No clear need exists to improve the audit trail for UF_6 cylinders. Identification and tracking formats can vary widely across industry as each cylinder owner will establish its own specific identification format. Even within an organization, the format may change.	Meets
Use case would benefit from faster transaction processing (enabled by PoW)	Some companies automated their inventory practices by applying supplemental, machine-readable identifiers (e.g., barcodes); the inspectorates cannot readily use these because the identifiers vary between cylinder owners and are randomly or not permanently attached to the cylinders. Thus, their verification activities remain a labor-intensive, time-consuming manual process. The challenges in reading the cylinder identification can lead to reading and transcription errors that require additional time to resolve.	Meets
Use case would benefit from higher confidence in data validation	Stronger validation is needed for cylinder identification numbers as cylinders change owners. Cylinder identification is a string of alpha-numeric characters provided by the purchaser—typically a UF_6 conversion plant or enrichment plant. Once stamped or engraved, the identification number typically remains unchanged over the entire service life of the cylinder (which can extend 40 years or longer). Occasionally, an identification number may be changed if a cylinder is sold, tested, and certified, and the new owner desires a new number with a different format.	Meets
Desirability Requirements		
Existing information technologies solve use case challenges	IAEA does not have the general requirement to track any nuclear material through its lifecycle, although some tracking is performed in specific cases.	Does not Meet
Improves Trust: Stakeholder interests are not aligned with central authority	The stakeholders involved in UF_6 cylinder shipments are facilities, State Authorities, and the IAEA. There is no presumption of trust between the IAEA and States, although trust is slightly higher between facilities engaged in nuclear material shipments with each other.	Meets

Improves Trust: Central authority required (decentralization does not undermine effectiveness; may bring value)	While the IAEA verifies material inventories at facilities and confirms the cylinder contents received into or leaving a material balance area, the IAEA does not have a requirement for tracking cylinders throughout their lifecycle. Heterogeneous cylinder identification makes the verification process quite time consuming. A database or ledger that would enable real-time tracking of UF_6 cylinders could be designed with the IAEA as a clear beneficiary, but without IAEA oversight.	Does not Meet
Improves timeliness of detection (use case function)	Improving real-time monitoring of UF_6 cylinders directly supports the IAEA's objective to improve detection timeliness. Inspection frequency at certain facilities may be low depending on the quantity and type of nuclear material stored/processed; a considerable amount of time could elapse before a theft or diversion of material in a UF_6 cylinder is determined and confirmed.	Meets

5.5 Unattended Monitoring Systems/State of Health

Unattended monitoring systems were identified in PNNL's 2017 study as a potential safeguards use case due to the transmission and monitoring of large data flows. Thus, this section draws its description directly from that report.

> "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 onsite 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 SoH 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.[1]
>
> 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…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."[2]

As discussed in Table 10, this use case did not receive high desirability scores primarily because solutions exist for monitoring these data and it is impossible to decentralize the workflow.

[1] Frazar, Sarah, et al. 2017. "Exploratory." Pacific Northwest National Laboratory. February 2017.
[2] Ibid.

Table 10. Evaluation of UMS Use Case

Criteria	Unattended Monitoring Systems State of Health Data	Determination
Feasibility Requirements		
Use case requires high level of data security (information can only be shared with designated entities)	The central authority lacks full trust in the installed systems. A facility might attempt to hack the system for the purpose of spoofing the data.	Meets
Use case requires auditable data trail	Auditability of data is critical as these systems provide important information that can be used to support verification of nuclear material inventories and ensure continuity of knowledge at the facility.	Meets
Use case would benefit from faster transaction processing (enabled by PoW)	Effectively all UMS data are transmitted every 24 hours to the IAEA. There is no driving need for faster processing of data.	Does not Meet
Use case would benefit from higher confidence in data validation	The central authority lacks full trust in the installed systems. A facility might attempt to hack the system for the purpose of spoofing the data.	Meets
Desirability Requirements		
Existing information technologies solve use case challenges	Numerous tools can be used for monitoring data, using ledgers to maintain an audit trail. The IAEA and various Member States began successfully sharing UMS and SoH data before the existence of DL.	Meets
Improves Trust: Stakeholder interests are not aligned with central authority	The central authority lacks full trust in the installed systems. A facility might attempt to hack the system for the purpose of spoofing the data.	Does not Meet
Improves Trust: Central authority required (decentralization does not undermine effectiveness; may bring value)	The workflow features one-way transmission of data from the facility to the IAEA. It would be impossible to decentralize the workflow without undermining the purpose of the safeguards workflow.	Meets
Improves timeliness of detection (use case function)	Maintaining confidence in unattended remote monitoring streams directly supports the IAEA's strategic objective to improve the timeliness of detection.	Meets

5.6 Noncompliance Process

The noncompliance process was selected as a use case due to its inclusion of electronic communications exchanged during a broader governance process that occurs within the IAEA to resolve questions about a State's nuclear activities. As Josh Stark, a blockchain consultant, observed, DLs are being considered to

facilitate governance processes. Stark offers the following definition for governance as the "rules, laws, institutions, processes, rights and customs that, used together, become a system that enables organizations to make decisions."[1] Such decision-making activities can be facilitated through self-executing computer programs such as Smart Contracts that allow for facilitation, verification, and execution of an arbitrary agreement without the need for mutual trust or a trusted third party.[2,3] Stark's definition, coupled with the capabilities offered via Smart Contracts, raises the question whether the noncompliance process, a highly politicized governance process, might benefit from some form of DL. Recognizing the significant organizational, political, and policy changes required to support the incorporation of a DL into the noncompliance process, the inclusion of this case study was designed to question the ostensibly unconventional applications the IAEA might consider for the future.

Paragraph 19 of the Comprehensive Safeguards Agreement states that when the IAEA is "not able to verify that there has been no diversion of nuclear material required to be safeguarded under the Agreement to nuclear weapons or other nuclear explosive devices…," it may initiate the transmission of a series of reports to resolve the issue.[4] This noncompliance process is described in Article XII (C) of the IAEA Statute as the following:

> "…The inspectors shall report any noncompliance to the Director General who shall thereupon transmit the report to the Board of Governors. The Board shall call upon the recipient State or States to remedy forthwith any noncompliance which it finds to have occurred. The Board shall report the noncompliance to all members and to the Security Council and General Assembly of the United Nations..."[5]

Despite the significant impact noncompliance acts have on safeguards verification, surprisingly little guidance is provided to help the IAEA or its Member States navigate the process. Thus, authors seeking to understand how the IAEA handles such cases of noncompliance attempt to add a bit more color to the process:

> "When an 'anomaly' is detected by inspections, or these days by any other validated source of information, a report will be prepared for the [Deputy Director General for] Safeguards, who, depending on the seriousness of the case, may deal directly with state authorities in an attempt at its resolution. If the issue is more serious or if the initial approach to the state, starting with the SSAC [State system of accounting for and control of nuclear material] if one exists, does not work, the [Director General] will be informed. The [Director General] may then communicate with the nuclear authorities in the state concerned at the highest level. If the result is unsatisfactory and the issue not resolved, a report will be prepared for the [Board of Governors]."[6]

---

[1] Stark, Josh. 2018. "Making Sense of Blockchain Governance Applications." *Coindesk.com.* 20 Nov 2016. Accessed May 31, 2018. https://www.coindesk.com/making-sense-blockchain-governance-applications.

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

[3] Zyskind, Guy, Oz Nathan, and Alex Pentland. 2015. "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.

[4] IAEA. 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." June 1972.

[5] IAEA. "The Statute of the IAEA."

[6] Findlay, Trevor. 2012. "Unleashing the Nuclear Watchdog: Strengthening and Reform of the IAEA," Centre for International Governance Innovation, 2012. http://www.cigionline.org/sites/default/files/unleashing_the_nuclear_watchdog.pdf.

Former PNNL staff member Andrew Kurzrok captures the dynamic, fluid nature of the Agency's deliberations in his study exploring potential improvements to this process:[1]

> "According to long-time IAEA staff members, 'there is no firm mechanism for how [a case] goes from the [Deputy Director General for Safeguards] to the DG'[2] and 'no hard and fast rule for when [the Director General] tells the Board.'[3] The development of a Board report is a collaborative, iterative process that includes the Director General's staff (formerly EXPO, now the Director General's Office for Coordination), the Office of Legal Affairs, and the Deputy Director General for Safeguards. It also includes other relevant staff from the Department of Safeguards. Since potential safeguards violations 'take a while to resolve,' follow-up reporting to the Board may be necessary."[4]

In his study, Kurzrok argues to standardize some governance-related activities, such as a standardized reporting template that cognizant IAEA staff could evaluate and reach a decision. Kurzrok notes, "The Secretariat could develop a standardized reporting template for specific reports to the Board of Governors… a standardized reporting template might help the Secretariat become more transparent in its decision-making and make it increasingly obvious when a state is not cooperative."[5] It might be possible to then incorporate such standardized reports into a DL facilitating a Smart Contract workflow thereby increasing efficiency and minimizing perceptions that the process is subjective, politicized, or discriminatory.

Turning to this use case evaluation, the team considered whether the noncompliance process was similar to the problems DLs typically solve. Recognizing the relative paucity of electronic transactions involved in this process, the team considered whether something could be technically facilitated with a DL and whether a desire to do so exists. Ultimately, some indicators suggest the process could be facilitated with a DL solution, but whether the process might be decentralized and still function is unclear.

To elaborate, the noncompliance process aims to deliberate and resolve questions about State compliance with its safeguards agreement. As such it is inherently a governance process ripe for allegations of abuse and politicization. Nima Gerami, a research fellow at the National Defense University, writes, "the Board Members, who have their own national interests and agendas, do not address cases of potential noncompliance 'with a common sense of purpose.'"[6,7,8] Indeed, politics are a prominent feature of noncompliance deliberations, despite IAEA efforts to rely on technical criteria and independent verification measures as a basis for their safeguards conclusions. When noncompliance deliberations are reported in the news, disagreements among IAEA staff and countries become exacerbated, thus increasing the lack of trust within the safeguards community. If a technical solution could automate the governance process and improve its trust level, it would directly support the IAEA's ability to assure the international community that a State's nuclear program remains dedicated to peaceful activities. Actions that can mitigate these issues and improve trust are a worthwhile investment.

---

[1] Kurzrok, Andrew. 2014. "Improving the International Atomic Energy Agency's Safeguards Noncompliance Reporting Process." Pacific Northwest National Laboratory. September 2014.
[2] Interview with Olli Heinonen, former IAEA Deputy Director General for Safeguards, February 26, 2014.
[3] Interview with Laura Rockwood, former IAEA legal officer, April 25, 2014.
[4] Ibid.
[5] Kurzrok. "Improving." 2014.
[6] Ibid.
[7] Gerami, "An Organizational Perspective," *op. cit.*
[8] While the UN Security Council also maintain political power, particularly under its Chapter VII mandate, this paper will focus on the relative power balance among actors within the IAEA.

Continuing the speculative discussion about the feasibility of decentralizing parts of the noncompliance process, a scenario could exist in which metadata from State declarations, inspection reports, and other relevant safeguards information (e.g., satellite imagery) might be populated into a standard template securely managed and maintained on an electronic ledger. While the IAEA would maintain full NMA records (as they do today for verification purposes), metadata from these reports could be processed on a DL for review by all States, particularly in times when politically charged discussions might dilute or distract from the more salient issues under consideration. Such transparency would allow the IAEA to build a strong, objective noncompliance case when a State refuses to cooperate in the resolution of discrepancies or anomalies. The security and immutability of the metadata would provide further trust in IAEA conclusions.

Table 11. Evaluation of Noncompliance Process Use Case

Criteria	Noncompliance Process	Determination
Feasibility Requirements		
Use case requires high level of data security (information can only be shared with designated entities)	According to one former IAEA staff member, clarifying information can be disseminated during technical briefings. However, these technical briefings are closed to the public. While it is the IAEA's prerogative to maintain the confidentiality of its proceedings, the Board's frequent derestricting the Director General's reports immediately (which are then posted to the IAEA's public website) strongly suggests that there is a norm of public transparency and accountability.	Partial
Use case requires auditable data trail	Any data exchanged as part of a governance and/or investigative process should be auditable by cognizant stakeholders of the process.	Meets
Use case would benefit from faster transaction processing (enabled by PoW)	As a governance process, faster processing of governance decisions is not needed.	Does not Meet
Use case would benefit from higher confidence in data validation	As a governance process, documentation of the provenance and record of key decisions is always needed.	Meets
Desirability Requirements		
Existing information technologies solve use case challenges	Existing technologies do not address challenges inherent in this use case.	Does not Meet
Improves Trust: Stakeholder interests are not aligned with central authority	Due to the political nature of noncompliance discussions, there is no presumption of trust between Member States, Member States under investigation, and the IAEA.	Meets
Improves Trust: Central authority required (decentralization does not undermine	Aspects of the noncompliance process could be decentralized, but with little value added without significant investment in additional tools that would be necessary to automate governance processes.	Partial

effectiveness; may bring value)		
Improves timeliness of detection (use case function)	Improving the transparency and apolitical nature of the noncompliance process would directly support the IAEA's strategic objective of promoting trust in IAEA conclusions. This does not directly relate to the IAEA's ability to improve the timeliness of detection.	Does not Meet

As summarized in Table 12, two use cases (transit matching and UF_6 Cylinder Tracking) meet all the feasibility and desirability requirements, making them worthy of further exploration in the near term. Three use cases (information management and reporting, unattended monitoring/SoH systems, and noncompliance process) did not score high enough to warrant further investigation or investment. However, a detailed assessment of the information management and noncompliance use cases may be warranted, as they were at or just below the average score. The last use case (focused on the SIR) received a negative score. The score spectrum reflected in Table 12 demonstrates the methodology's ability to differentiate use cases objectively and defensibly, given a set of use case conditions. The full scores are provided in Appendix A.

Table 12. Summary of Evaluation Scores by Use Case

	Information Management and Reporting	Transit Matching	Safeguards Implementation Report	UF6 cylinder tracking	Unattended Monitoring/ State of Health Data	Noncompliance	
Feasibility	3.5	4	1.5	4	3	2.5	Score is 3.1 or above
Desirability	0	3	-2	4	-2	1	Score is .66 or above
Overall Score	**3.5**	**7**	**-0.5**	**8**	**1**	**3.5**	Score is 3.75 or above

6.0 Key Findings and Final Thoughts

The FY18 study produced several key findings and recommendations.

First, the study aimed to position the IAEA to be a knowledgeable consumer when making investment decisions related to DL applications. To this end, the terms, definitions, and concepts presented herein serve as a foundation for a defensible methodology for evaluating use cases for DL solutions. With this methodology in hand, the IAEA will be in a good position to evaluate new use cases as they arise and make sound decisions about whether to pursue further investment in a DL solution, given a set of use case conditions.

Ultimately, the salient message of the FY18 study is that DLs are designed to solve very specific problems. While a DL may offer some benefits to various safeguards use cases, they do not necessarily provide a unique solution, making further investment questionable. To warrant future investment by

organizations such as NPAC and the IAEA, a use case should ideally meet both feasibility and desirability criteria. As demonstrated in FY18, UF_6 cylinder tracking and transit matching merit further exploration. Additionally, information management and the noncompliance process use cases may warrant further study as their scores fell just below the average score.

Once a suitable use case is identified, significant work is required to develop technical user requirements and explore stakeholder perceptions about the technology's deployment before the design, development, and testing of different ledger designs can proceed.

Finally, one use case that PNNL explored during its initial FY17 study was multi-lateral Fuel Bank exchanges. This use case was not examined in FY18 because it was not considered part of a State's obligations to the IAEA. However, based on the number and types of digital transactions taking place, an apparent desire for decentralization to promote trust among stakeholders and the lack of existing technical solutions to meet these needs, this use case might receive high scores when evaluated using the methodology presented herein. The Fuel Bank combines aspects of three use cases already evaluated, specifically the transit case, UF_6 case, and SIR (implementation reporting case). Since the bank would only feature a maximum 60 30B UF_6 cylinders held by the IAEA (INFCIRC/916),[1] there may not be any significant confidentially issue with the IAEA fully releasing all the nuclear material accountancy records via a DL. If the containers were tracked with a Global ID, their movements and utilization could be tracked with a DL made available to all Member States. At the same time, given the Fuel Bank's purpose to supply assurance and the IAEA in-effect implementing safeguards on its's own facility, the need for transparency is quite high. In this way, the Fuel Bank may represent an application that combines the most attractive features all the cases examined in the study.

[1] IAEA. 2017. "Agreement between the International Atomic Energy Agency and the Government of the Republic of Kazakhstan regarding the Establishment of the Low Enriched Uranium Bank of the International Atomic Energy Agency in the Republic of Kazakhstan." INFCIRC/916. March 22, 2017. https://www.iaea.org/sites/default/files/publications/documents/infcircs/2017/infcirc916.pdf.

Appendix A

Scoring Results

Appendix A

Scoring Results

Table 13. Scores for Information Management and Transit Matching Use Cases

Criteria for Application	Information Management and Reporting (Determination)	Information Management and Reporting (Score)	Transit Matching (Determination)	Transit Matching (Score)	Meets Criteria	Partially meets criteria	Does not meet Criteria	Weight	Total
Use case requires high level of data security (information can only be shared with designated entities)	1	1	1	1	1	0.5	0	1	
Use case requires auditable data trail	1	1	1	1	1	0.5	0	1	
Use case would benefit from faster transaction processing (enabled by proof of work)	0.5	0.5	1	1	1	0.5	0	1	
Use case would benefit from higher confidence in data validation	1	1	1	1	1	0.5	0	1	
FEASIBILITY SUBTOTALS		**3.5**		**4**				Average	3.08333
Existing information technologies solve use case challenges	-1	-2	-0.5	-1	-1	-0.5	0	2	
Improves Trust: Stakeholder interests are not aligned with central authority	1	2	1	2	1	0.5	0	2	
Improves Trust: Central authority required (decentralization does not undermine effectiveness; may bring value)	-1	-2	0	0	-1	-0.5	0	2	
Improves timeliness of detection (use case function)	1	2	1	2	1	0.5	0	2	
DESIRABILITY SUBTOTALS		**0**		**3**				Average	0.66667
Total Score		**3.5**		**7**	Average	**3.75**			

Table 14. Scores for Safeguards Implementation Report and UF_6 Cylinder Tracking

Criteria for Application	Safeguards Implementation Report (Determination)	Safeguards Implementation Report (Score)	UF6 Cylinder Tracking (Determination)	UF6 Cylinder Tracking (Score)	Meets Criteria	Partially meets criteria	Does not meet Criteria	Weight	Total
Use case requires high level of data security (information can only be shared with designated entities)	0.5	0.5	1	1	1	0.5	0	1	
Use case requires auditable data trail	1	1	1	1	1	0.5	0	1	
Use case would benefit from faster transaction processing (enabled by proof of work)	0	0	1	1	1	0.5	0	1	
Use case would benefit from higher confidence in data validation	0	0	1	1	1	0.5	0	1	
FEASIBILITY SUBTOTALS		**1.5**		**4**				Average	3.08333
Existing information technologies solve use case challenges	-1	-2	0	0	-1	-0.5	0	2	
Improves Trust: Stakeholder interests are not aligned with central authority	1	2	1	2	1	0.5	0	2	
Improves Trust: Central authority required (decentralization does not undermine effectiveness; may bring value)	-1	-2	0	0	-1	-0.5	0	2	
Improves timeliness of detection (use case function)	0	0	1	2	1	0.5	0	2	
DESIRABILITY SUBTOTALS		**-2**		**4**				Average	0.66667
Total Score		**-0.5**		**8**	Average	**3.75**			

Table 15. Scores for Unattended Monitoring and State of Health Data and Noncompliance Process

Criteria for Application	(Unattended Monitoring Systems & State of Health Data (Determination)	Unattended Monitoring Systems State of Health Data (Score)	Noncompliance Proceess (Determination)	Noncompliance Process (Score)	Meets Criteria	Partially meets criteria	Does not meet Criteria	Weight	Total
Use case requires high level of data security (information can only be shared with designated entities)	1	1	0.5	0.5	1	0.5	0	1	
Use case requires auditable data trail	1	1	1	1	1	0.5	0	1	
Use case would benefit from faster transaction processing (enabled by proof of work)	0	0	0	0	1	0.5	0	1	
Use case would benefit from higher confidence in data validation	1	1	1	1	1	0.5	0	1	
FEASIBILITY SUBTOTALS		**3**		**2.5**				Average	3.08333
Existing information technologies solve use case challenges	-1	-2	0	0	-1	-0.5	0	2	
Improves Trust: Stakeholder interests are not aligned with central authority	0	0	1	2	1	0.5	0	2	
Improves Trust: Central authority required (decentralization does not undermine effectiveness; may bring value)	-1	-2	-0.5	-1	-1	-0.5	0	2	
Improves timeliness of detection (use case function)	1	2	0	0	1	0.5	0	2	
DESIRABILITY SUBTOTALS		**-2**		**1**				Average	0.66667
Total Score		**1**		**3.5**	Average	**3.75**			

Pacific Northwest
NATIONAL LABORATORY

www.pnnl.gov

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

U.S. DEPARTMENT OF
ENERGY