Exploring the Application of Shared Ledger Technology to Safeguards and other National Security Topics

Sarah Frazar, Sam Winters, Sean Kreyling, Cliff Joslyn, Curtis West, Mark Schanfein, and Amanda Sayre, Pacific Northwest National Laboratory

Abstract:

In 2016, the Office of International Nuclear Safeguards at the National Nuclear Security Administration within the Department of Energy commissioned the Pacific Northwest National Laboratory to explore the potential implications of the digital currency Bitcoin and its underlying technology, blockchain, on the safeguards system. The authors found that the general class of technologies to which blockchain belonged, Shared Ledger Technologies (SLT), offers a spectrum of potential benefits to the safeguards system. While further research is needed to validate assumptions and findings in the paper, preliminary analysis suggests that both the International Atomic Energy Agency and Member States can use SLT as part of a new system to promote efficient, effective, accurate, and timely reporting. The novel architecture of SLT would lead to significant increases to trust and transparency in the safeguards system without sacrificing confidentiality of safeguards data. This increased transparency and involvement of Member States in certain safeguards transactions could lead to increased trust and cooperation among States and the public. This paper describes these benefits and the analytical framework for assessing SLT applications for specific safeguards problems. The paper also describes other national security areas where SLT could provide benefits.

I. Introduction:

The International Atomic Energy Agency (IAEA) is responsible for providing credible assurances that countries are meeting their obligations to not divert or misuse nuclear materials or facilities for non-peaceful purposes. To fulfill these responsibilities, the IAEA is developing and applying in a limited context the State Level Concept (SLC), which is a comprehensive approach to implementing safeguards that uses all relevant information about a State's nuclear program to draw safeguards conclusions. Key principles underlying the SLC are that implementation should be "non-discriminatory," "independent," and "objective."[i] Despite significant investments in IAEA infrastructure and operations to support a transition to the SLC in ways that are aligned with these principles, some States continue to voice "suspicions that the approach is discriminatory and allows for the use of political, rather than objective technical factors to guide safeguards implementation. The use of intelligence information provided by Member States also plays into this concern."[ii] In short, despite significant efforts to demonstrate a commitment to objectivity and nondiscrimination, the IAEA is still confronted with mistrust by some States. This environment creates a compelling rationale to examine new technologies that could contribute to more trusting relationships that might strengthen commitment to and compliance with nonproliferation obligations.

In 2009 a similar impetus in the financial technology community resulted in Bitcoin, which was introduced to the public to promote privacy among multiple parties engaged in financial transactions. At a time when trust in traditional, centralized currency systems was diminishing, Bitcoin and its underlying technology, the blockchain, offered users an alternative solution that was perceived to be private, secure, and reliable, without relying on the paradigm of centralized trust of the traditional banking system.

The central technology facilitating Bitcoin transactions is an electronic shared ledger, known as a blockchain. Multiple parties in the Bitcoin network maintain an independent copy of the ledger to record transactions. Other parties post transactions pseudonymously, meaning their identities are protected but details about the transaction remain transparent. Computer programs run by validators (those storing full copies of the ledger), rather than one centralized authority, competitively process the financial transactions taking place on the ledger based on a secure system rooted in cryptography and financial incentives.

The Bitcoin blockchain ledger system served as an encouraging proof of concept to technologists. Those familiar with blockchain technology recognized its ability to facilitate non-financial transactions by designing similar systems to different specifications. Blockchain technology was a potentially paradigm shifting technology due to its ability to provide, in a decentralized and trustless way, five key services through different ledger designs:[iii]

- **Consistency:** All blockchain participants see the same information across all copies of the ledger.
- **Validity:** All transactions must meet a certain set of predetermined conditions (e.g., green flags) before being added to the blockchain.
- **Immutability:** Once information is posted to the ledger, the information is effectively immutable, meaning it cannot be altered.
- **Uniqueness:** There are no duplicate or conflicting transactions.
- **Authentication:** All transactions are uniquely tied to a specific individual via private key.

Blockchain technology relies heavily on a combination of cryptography and economic incentives to fulfill the above services, which results in a very secure system.

An example of how these services work in the financial context may be useful here. In the Bitcoin context,

> If Party A wants to send money to Party B, the proposed transaction is broadcast to the validators of the network with a digital signature that authenticates Party A as the sender. Once a transaction is proposed, validators compete to post it to a 'block', in which computer algorithms have determined the funds are available (valid) and no double-spending is taking place (unique). Once the transaction is confirmed to be valid and unique, a network validator (computer) propagates the confirmation to other nodes to which it is currently connected.[iv] If the

transaction is determined to be invalid, the node will reject it and synchronously return a rejection message to the originator. The ledger, once updated, is functionally immutable as a result of the hash functions[v] and other cryptographic structures used in the software.[vi] Meaning, the ledger cannot be altered.[vii]

While this is one manifestation of a blockchain ledger, other ledger designs also run on blockchain technology. Specifically, while some ledgers facilitate financial transactions (e.g., Bitcoin), others facilitate transaction workflows involving information about physical goods (e.g., Everledger). Other ledgers such as Ethereum facilitate "smart contract" systems, which combine financial information with computer programs that automatically and securely execute contracts as transactions proceed. As will be discussed in this paper, these other ledger designs become relevant when exploring non-financial problems, such as those in the nonproliferation and arms control contexts.

Certain ledger designs can introduce high levels of trust and transparency into systems involving multiple parties who do not know or trust each other. These characteristics suggest potential benefit in exploring whether blockchain technology might be useful to nonproliferation and arms control. Both systems are politically charged and consistof multiple states that must find ways to trust their respective efforts to comply with various agreements, protocols, or resolutions. Such trust is difficult to maintain when certain Member States voice concern about discriminatory implementation of SLC or when arms control negotiations break down due verification challenges.

To lend urgency to this discussion, growing public acceptance of these rapidly evolving technologies suggest they may come to alter, if not dominate, current financial, information, and commercial transaction systems. Such transactions are critical elements of the nonproliferation and arms control system, so it behooves specialists in these areas to evaluate and understand the risks and opportunities they pose.

Against this backdrop and with sponsorship from the National Nuclear Security Administration's Office of International Safeguards, the Pacific Northwest National Laboratory (PNNL) conducted a study in fiscal year (FY) 2017 that explored the potential application of blockchain technology to safeguards.[viii] The study argued that blockchain technology "…can be used to promote efficient, effective, and timely reporting," but the true value proposition comes from the technology's ability to "increase transparency in the safeguards system without sacrificing confidentiality of safeguards data..."[ix]

This paper summarizes the findings from that study and offers additional scenarios that might benefit from the application of blockchain technology. The paper is structured in five sections:

- Section II presents a common nomenclature establishing a foundation for an analytical methodology used to assess various blockchain applications.
- Section III describes the analytical methodology.

- Section IV describes an approach for applying the methodology to nonproliferation and arms control use cases.

II. Establishing a Common Nomenclature

With Bitcoin's rapid public acceptance came greater appreciation for the variety of ways blockchain technology could be used to solve different non-financial applications. The companies and individuals involved realized that blockchain's value proposition resides in a broader consideration of existing state-of-the-art cryptographic techniques, modern IT tools, and distributed electronic ledgers. Experts began referring to this collection of system characteristics and services as SLT. As described in PNNL's FY17 study, to better understand how SLT can solve different problems, it is necessary to classify the different types of shared ledgers that can be created:

> *Localized* ledgers are those that have a single, authoritative copy. There are copies of the primary ledger that are accessed for viewing, but there is only one copy that represents the definitive state of the system. In contrast, *distributed* ledgers are those where many copies of the ledger are maintained by a consensus protocol that provides a consistent view among ledgers. The consensus process reconciles differences between ledger copies that may exist for short periods of time...[x] Distributed ledgers have a distinct advantage over localized ledgers in that they do not have a single point of failure. In order for an adversary to corrupt or delete a local ledger, they must only attack the single copy. To do this for a distributed ledger, a large portion of the ledgers would all have to be attacked at once, which is significantly more difficult…
>
> *Centralized* ledgers are those that give certain participants roles of trust in maintaining the state of the ledger. This could mean either a singular entity or a subset of entities are responsible for validation... In contrast, *decentralized* ledgers are those in which all users have equal privilege in maintaining the consistent state of the ledger….A component of a centralized ledger is that it is permissionable. By having a centralized power structure, permissions or 'roles' can be granted to certain users to allow them to interact with the ledger in privileged or limited ways. For example, a 'read-only' role may be granted permissions only to view transaction meta-data on the ledger, while a 'read/write' role may be granted to allow a user to submit transactions to the ledger…[xi]

Table 1 depicts the four possible combinations to make different SLT frameworks. Combination (d) is not possible: the nature of a localized ledger, given that it exists on a single machine run by a single entity, runs counter to the concept of being decentralized, which requires that no single user have disproportionate control over the ledger. Therefore, it was not included in the team's analysis.

Table 1. Combinations for SLT frameworks

	Centralized (certain users have permissions)	**Decentralized (all users maintain)**
Localized (single ledger copy)	(a): Private Ledgers (e.g., bank)	(d)
Distributed (many ledger copies)	(b): Consortium Ledger (no obvious example)	(c): Public Systems (e.g., Bitcoin)

Once these characteristics are combined into different models, they can be framed as public, private, or consortium ledgers. Under *public systems* any party can use the system and no one party is given special privileges. *Private ledgers* are for single entities that maintain the ledger, choosing whether or not to apply permissions.[xii] Under a *Consortium System*, a trusted set of users each maintains a copy of the ledger and executes distributed consensus protocol of the system. From the outset, the consortium will agree on the permissions of the ledger, including who can make transactions, who can read the ledger, etc.

As discussed in the 2017 paper,

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

III. Analytical Framework for Assessing Blockchain Use Cases

Having established a foundational nomenclature to support the analysis of various uses cases, it is possible to establish a structured framework for an analytical approach. Table 2 depicts this framework, showing generically how each SLT model might achieve the five blockchain services.

Table 2. Comparison of How SLT Models Fulfill SLT Services

		Model Type		
		Centralized, Localized (Private)	Centralized, Distributed (Consortium)	Decentralized, Distributed (Public)
Service	Consistency	Trusted Central Authority (e.g., IAEA)	Member State Consortium Consensus	Open Style Consensus (e.g., Bitcoin Proof of Work)
	Immutability			
	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		

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 distributed ledgers 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. The next section describes some of the problems that might require a shared ledger and how a user might decide the type of ledger that would be most appropriate.

IV. Applying the Methodology

As people learn more about SLT's potential to serve complex problems involving large-scale transactions, they often start explore potential blockchain applications with an erroneous question: how might blockchain technology be applied to this problem? However, as more blockchain researchers are beginning to document, the type of problem being addressed drives whether it

makes sense to use blockchain and how a ledger might be designed. [xiv,xv] In many cases, there is no need to turn to blockchain. For example, as blogger Gideon Greenspan bluntly reports, "If your requirements are fulfilled by today's relational databases, you'd be insane to use a blockchain."[xvi]

Thus, users should first articulate the strategic-level goals being pursued when solving the particular problem: when designing a solution to a problem, is the goal to promote transparency and trust among parties that do not typically trust each other or to obtain greater data security and transactional efficiency within the system? Users should consider specific characteristics of a given problem such as:

- Is there a central authority currently managing a system of interactions among multiple parties?
- Do the parties engaged in the system necessarily know or trust each other?
- Is a central authority either unavailable or unwelcome? (Parties do not always trust the central authority to be an objective arbiter.)
- Are the parties exchanging large-scale datasets?
- Do the datasets contain sensitive information (e.g., proprietary, business sensitive information)?

To help navigate these types of high-level questions, the study presented a series of decision trees for consideration. (As research evolved since the publication of the FY17 study, a number of other experts offered variations on the simple decision trees described here.) [xvii]

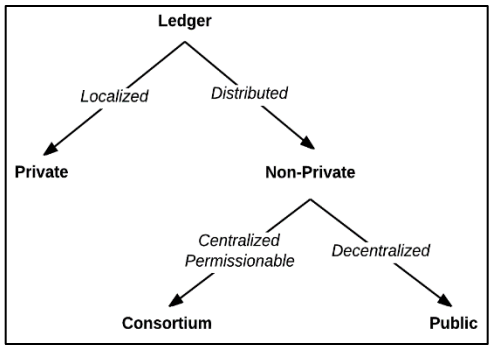

Figure 1. Decision Tree A

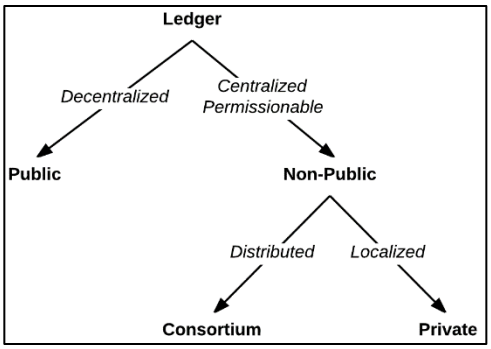

Figure 2. Decision Tree B

Decision Tree A (Figure 1) offers a choice between a localized ledger (private) and a more transparent, distributed (non-private) ledgers. This tree is optimal if the driving factor for model selection was related to trust and transparency. Decision Tree B (Figure 3) offers a choice between a decentralized (public) ledger versus more centralized, permissionable (non-public) ledgers. Decision Tree B should be used if the driving factor for model selection is related to controllability (permissionability) of the ledger. Once the strategic goals are defined, the user can select a ledger design and make decisions about whether and how to apply permissions and use consensus protocols.

The PNNL study introduced a number of specific safeguards problems involving digital transactions that merit future exploration to determine whether they might benefit from a shared ledger solution. Those problems included the following:

- Improving the efficiency and effectiveness of nuclear material accounting while protecting safeguards confidential data
- Introducing efficiencies into the transit matching process
- Improving the transparency and effectiveness of the IAEA's Safeguards Information Report
- Improving transparency among and reporting from States about nuclear material shipments

Other safeguards problems currently being evaluated involve the standardization of the IAEA's noncompliance process and tracking and securing transactions involving physical items and data.

The export control and arms control domains offer other problems that might be solved with blockchain technology. For example, in the area of export control, U.S. and international licensing processes involve multiple parties that exchange large-scale datasets that include sensitive proprietary information. Specific research questions focus on whether smart contracts are a desirable way to automate certain export license transactions, improve pattern detection, or highlight indicators associated with suspicious or legitimate transactions using blockchain technology.

At the time of this publication, no obvious research has been conducted into potential blockchain applications to arms control problems. This domain is potentially ripe for future research as it involves a system of stakeholders who do not always trust each other to comply with the terms of extant bilateral and multi-lateral arms control treaties and agreements. The strategic question of interest in this context is whether use of distributed electronic ledgers that enable parties to verify each other's compliance with treaty obligations might enable or promote treaty verification in unprecedented ways.

V. Conclusion:

Based on the 2017 study described in this paper, PNNL made two observations:

(1) SLT offers a spectrum of potential benefits to the nonproliferation system. SLT can be used to promote efficient, effective, and timely reporting, but SLTs are not unique in offering this solution. Modern databases and information technology solutions may be just as if not more effective to advance these objectives.
(2) SLT is unique in its ability to increase transparency in the nonproliferation system without sacrificing confidentiality of data. This unique ability warrants further research into understanding whether, and to what extent, SLT might be used to solve specific safeguards, export control, and arms control problems.

Once the specific problems for future research have been selected, long-term research will involve exploration of the desireability and feasibility of using shared ledgers to solve the selected

problems. That exploration will include definition of the specific functional requirements for the ledger and testing of the ledger's design to validate assumptions about its potential applicability.

---

[i] International Atomic Energy Agency. "The Conceptualization and Development of Safeguards Implementation at the State Level." GOV/2013/38. 12 August 2013.

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

[iii] Ledger designs differ in terms of the types of roles and permissions that are applied to various users of the ledger.

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

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

[vi] Ch 8, Mastering Bitcoin, Andreas Antonopolous

[vii] Frazar, SL, KD Jarman, CA Joslyn, SJ Kreyling, AM Sayre, MJ Schanfein, CL West, ST Winters. "Exploratory Study on potential safeguards applications for shared ledger technology." Pacific Northwest National Laboratory. August 2016. PNNL-26229

[viii] Ibid.

[ix] Ibid.

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

[xi] Frazar, SL et al. "Exploratory Study."

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

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

[xiv] Wust, K, and A Gervais. "Do you need a blockchain?" *Cryptology* ePrint Archive, Report 2017/375, 2017. Available at: http://eprint.iacr.org/2017/375.pdf. Accessed on 5 June 2017.

[xv] Greenspan. "Avoiding."

[xvi] Greenspan, G. "Avoiding the pointless blockchain project: How to determine if you've found a real blockchain use case." *Private Blockchains.* Posted 22 November 2015. Available at: http://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project.

[xvii] A list of different decision trees can be found at: https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1.