STIMSON stuk UNSW SYDNEY

NONPROLIFERATION

REPORT

SLAFKA

Demonstrating the Potential for Distributed Ledger Technology for Nuclear Safeguards Information Management

By Cindy Vestergaard, Edward Obbard, Edward Yu, Guntur Dharma Putra, and Gabrielle Green

SLAFKA Prototype

Blockchain in Practice Program

THE STIMSON CENTER promotes international security, shared prosperity & justice through applied research and independent analysis, deep engagement, and policy innovation.

For three decades, Stimson has been a leading voice on urgent global issues. Founded in the twilight years of the Cold War, the Stimson Center pioneered practical new steps toward stability and security in an uncertain world. Today, as changes in power and technology usher in a challenging new era, Stimson is at the forefront: Engaging new voices, generating innovative ideas and analysis, and building solutions to promote international security, prosperity, and justice.

More at **www.stimson.org**.

Acknowledgments

The authors are grateful to the Finnish Radiation and Nuclear Safety Authority (STUK) and the Carnegie Corporation of New York (CCNY) for their generous support in funding this research. Additionally, the authors give their sincerest thanks to STUK and the various organizations from the nuclear safeguards and distributed ledger technology (DLT) community who participated in various discussions, virtual roundtables, and demonstrations. Their candid feedback provided space to understand how new technologies such as DLT may create greater efficiencies in safeguards information management in the years to come.

Abstract

SLAFKA is a prototype distributed ledger technology (DLT) platform built in collaboration between the Finnish Radiation and Nuclear Safety Authority (STUK), the Stimson Center, and the University of New South Wales. SLAFKA demonstrates how DLT manages data and allows for information sharing between the operator and national/regional/international regulators, offering a new and secure way to communicate safeguards data. SLAFKA illustrates how a permissioned blockchain platform aligns with confidentiality of nuclear accounting information and can readily provide an intuitive, cloud-based user interface that can be accessed by logging in from any web browser.

About the Authors

Dr Cindy Vestergaard is a Senior Fellow and Director of the Stimson Center's Blockchain in Practice Program and its Nuclear Safeguards Program. Her research on nuclear safeguards focuses on the impact of evolving international obligations and emerging technology on states and industry while her research on blockchain technology considers and tests the potential for the tech to increase transparency, security and efficiencies in international security regimes.

Gabrielle Green MSc (International Relations) is currently a Research Associate with the Blockchain in Practice and Partnerships in Proliferation Prevention Programs at the Stimson Center. Her research focuses on blockchain technology, nuclear safeguards, United Nations Security Council Resolution 1540 assistance programs, and chemical weapons-related material security.

Dr Edward G. Obbard is a Senior Lecturer in nuclear engineering at UNSW Sydney. His research focuses on nuclear materials and new solutions to nuclear safety and safeguards problems.

Edward Yu BEng (Hons.), BCom, took part in the development of both SLAFKA and its predecessor SLUMBAT as a researcher at UNSW Sydney. He has commercial experience in financial auditing (KPMG) and is pursuing a career in forensic accounting (Clayton Utz).

Guntur Dharma Putra BEng, MSci (computer science) is currently a Ph.D. candidate in the School of Computer Science and Engineering, UNSW Sydney. His research interest covers distributed systems and the Internet of Things.

I. Introduction

An ongoing challenge in the implementation of nuclear safeguards is the need to utilize and keep pace with emerging technologies for better streamlining of reporting and inspection procedures to accomplish more with limited resources. Currently, nuclear material accounting records are based on electronic documents, which involve inefficiencies related to data integrity and correctness. Moreover, with growing cyber threats, the need for greater information and systems security increases significantly. To address these challenges, a partnership formed in 2019 between the Finnish Radiation and Nuclear Safety Authority (STUK), the Stimson Center in Washington, D.C., and the University of New South Wales (UNSW) in Sydney, Australia, to develop the world's first distributed ledger technology (DLT) prototype for safeguarding nuclear material. The DLT prototype, called SLAFKA, tests the potential to increase efficiency, trust, and transparency in the management of nuclear safeguards information. The prototype is based on Finland's system of accounting and control, which uses a centrally stored database called SAFKA. Thus, the name SLAFKA emerges from a "shared ledger SAFKA."

Officially launched in Helsinki on 10 March 2020, SLAFKA demonstrates how DLT (1) validates and improves the management of safeguards data and (2) enhances permissioned information sharing between operator and regulators on nuclear material transactions (movements and processing). SLAFKA tests DLT as a novel method to track nuclear material, detect diversion, and monitor treaty compliance for Finland's State System of Accounting and Control (SSAC). The prototype is a first step in illustrating how a permissioned DLT platform aligns with the confidentiality requirements of nuclear accounting information to provide a new and secure way to communicate safeguards data.

II. Nuclear Safeguards in Finland

Nuclear safeguards are a set of technical measures that are applied to nuclear materials and activities to ensure they are used only for peaceful purposes. These measures are based on commitments made by parties to the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) and include nuclear material accountancy and reporting of nuclear fuel cycle–related activities to the International Atomic Energy Agency (IAEA). Finland was among the first group of countries to sign the NPT when it opened for signature on 1 July 1968 and, on 9 February 1972, it also became the first state with a Comprehensive Safeguards Agreement to enter into force with the IAEA.[1] This Agreement was replaced with Euratom's Comprehensive Safeguards Agreement with the IAEA (INFCIRC/193) when Finland joined the European Union in 1995. In 2004, an additional protocol to Euratom's agreement entered into force (INFCIRC/193.Add.8).[2] The IAEA and the European Commission (Euratom) therefore have independent mandates to evaluate and verify Finland's nuclear activities.

Finland's Nuclear Energy Act (990/1987) implements Finland's safeguards obligations and measures at the facility level, such as Finland's four operating nuclear power plants and the facilities at the Technical Research Centre of Finland (VTT), the University of Helsinki, and Posiva, the company that is responsible for the permanent disposal of spent fuel in Finland. Operators report directly to the European Commission as required by Commission Safeguards Regulation No 302/2005, while STUK collects, inspects, and reviews safeguards data and submits national declarations to both the Commission and the IAEA.

Although Finland's nuclear power program is relatively small with four reactors, nuclear energy provides 34.7 percent of Finland's total electricity given that these reactors are some of the most productive in the world.[3] This share is expected to increase to 45 percent when a fifth reactor is anticipated to come online at the Olkiluoto 3 site in 2022. A sixth reactor is also planned to be built at the Hanhikivi 1 site, which would bring Finland's total nuclear share close to 60 percent, if the operational time of old units is extended.[4] Finland's nuclear program is also unique as it is the first country in the world to begin construction of a deep geological repository (DGR), which is expected to receive spent nuclear fuel in the mid-2020s and continue for 100 years until final closure.[5]

The basic reporting unit for the IAEA is known as a Material Balance Area (MBA). An MBA is a physical area in which a balance of nuclear material can be made. Within an MBA, increases and decreases of material are recorded and physical inventories can be taken. If a nuclear facility has more than one MBA, then all movement of nuclear material between MBAs

1 STUK (Olli Okko, ed.), "Implementing Nuclear Non-proliferation in Finland: Regulatory Control, International Cooperation and the Comprehensive Nuclear-Test-Ban Treaty," *Annual Report* 2019, p. 12: https://www.julkari.fi/bitstream/handle/10024/139830/stuk-b246. pdf?sequence=1&isAllowed=y.

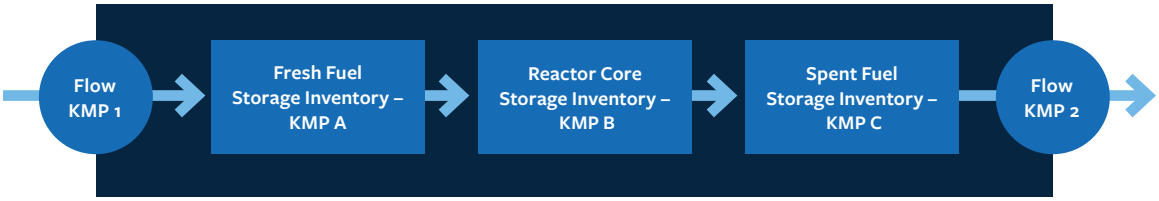
2 Protocol Additional to the Agreement between the Republic of Austria, the Kingdom of Belgium, the Kingdom of Denmark, the Republic of Finland, the Federal Republic of Germany, the Hellenic Republic, Ireland, the Italian Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Portuguese Republic, the Kingdom of Spain, the Kingdom of Sweden, the European Atomic Energy Community and the International Atomic Energy Agency in implementation of Article III, (1) and (4) of the Treaty on the Non-Proliferation of Nuclear Weapons, INFCIRC/193/A.8, 12 Jan 2005: https://www.iaea.org/sites/default/files/publications/documents/infcircs/1973/infcirc193a8.pdf.

3 As of 2019. See: Power Reactor Information System, "Finland," IAEA: https://pris.iaea.org/PRIS/CountryStatistics/CountryDetails.aspx?current=FI. Accessed 5 October 2020.

4 Ibid.

5 Posiva, "General Time Schedule for Final Disposal," http://www.posiva.fi/en/final_disposal/general_time_schedule_for_final_disposal#.X10XyshKg2w. Accessed 12 September 2020.

Figure 1: Structure of a Material Balance Area (MBA) representing a nuclear reactor. The MBA contains inventory and flow Key Measurement Points (KMP).



within the same facility must be reported.[6] Finland's SSAC involves 16 MBAs.[7]

The possible structure of an MBA is illustrated in Figure 1. MBAs consist of two types of Key Measurement Points (KMPs): Inventory KMPs and Flow KMPs. Inventory KMPs, such as KMP A, B, and C in the diagram, are locations where material appears in a form that can be measured to determine inventory. At Flow KMPs, such as KMP 1 and 2 in the diagram, material appears in a form that can be measured to determine changes in inventory, known as flows. Examples of flows include receipts of nuclear material, shipments, terminations, and accidental losses of material.

In Finland, safeguards reporting is based on Commission Regulation (Euratom) No. 302/2005, with Annexes III-V of the document being similar in content to the IAEA's Model Subsidiary Arrangement Code 10 (Code 10),[8] which specifies three types of reports to be made by SSAC agencies to the IAEA: Inventory Change Reports (ICRs), Physical Inventory Listings (PILs), and Material Balance Reports (MBRs).[9] ICRs report changes in inventory, PILs report the result of physical inventories, and MBRs provide aggregate material balances for each type of material at specified locations. STUK carries out about 40 inspections and 60 inspection days annually. International inspections are approximately 25 days per year.[10]

Current software for Finland's national nuclear material database (SAFKA) generally operates well in ease of use and checking for data consistencies in reporting on inventory changes, but its ability to validate data is less dependable. In a survey conducted by Stimson and UNSW,[11] operators noted that inefficiencies were mainly related to mistakes/corrections in reporting as well as software errors, alongside implementation of new functions. It was also noted that STUK manually runs script to check domestic shipments and match them to receipts. This only works if the receipt and shipment are domestic. Similarly, while incoming reports from operators are received by secure lines to STUK (without cryptography) and stored and rendered unchangeable in STUK's digital document handling system, operators report to the European Commission (EC) over unencrypted email, which is less secure. As new cyber threats emerge, transfer of data to STUK and Euratom become increasingly vulnerable to cyberattacks, which serves as one of the motivations for STUK in considering how advances in technology can strengthen information security and the integrity of safeguards data. Moreover, the inspectorates (STUK, EC, and the IAEA) do not compare the

6 International Atomic Energy Agency, INFCIRC/153, 1972.

7 STUK (Olli Okko, ed.), "Implementing Nuclear Non-proliferation in Finland: Regulatory Control, International Cooperation and the Comprehensive Nuclear-Test-Ban Treaty," *Annual Report* 2019, p. 16: https://www.julkari.fi/bitstream/handle/10024/139830/stuk-b246.pdf?sequence=1&isAllowed=y.

8 International Atomic Energy Agency, 2017. "Subsidiary Arrangement Code 10: Contents, Format and Structure of Reports to the Agency." SG-FM-1172. IAEA. https://www.iaea.org/sites/default/files/sg-fm-1170-subsidiary-arrangement-code-10-labelled.pdf.

9 Ibid, p. 1.

10 STUK (Olli Okko, ed.), "Implementing Nuclear Non-proliferation in Finland: Regulatory Control, International Cooperation and the Comprehensive Nuclear-Test-Ban Treaty," *Annual Report* 2019, p. 10: https://www.julkari.fi/bitstream/handle/10024/139830/stuk-b246.pdf?sequence=1&isAllowed=y.

11 Survey was conducted in September 2019.

nuclear material balances in their databases, and conceivable errors may be unnoticed over extended periods of time.

Another motivation for STUK in developing a DLT prototype is Finland's DGR. Its long operating lifetime (100 years) raises the issue of long-term data management and presents new verification challenges, given that the inventory of the facility will change on a continual basis. At the same time, physical inspection becomes impossible once the material is placed more than 400 meters underground. Spent nuclear fuel contains fissile material such as plutonium, which the IAEA considers as "direct use material" for the manufacture of nuclear explosives and is therefore of highest proliferation concern. STUK has worked closely with Euratom and the IAEA to ensure that safeguards have been a part of the DGR's design from the beginning. One of the biggest challenges going forward is how to ensure enduring confidence that the inventory below ground is the same as what is reflected in records above ground. As noted by STUK, safeguarding spent fuel underground presents new challenges where "the significance of data integrity is immense."[12]

12 STUK (Olli Okko, ed.), "Implementing Nuclear Non-proliferation in Finland: Regulatory Control, International Cooperation and the Comprehensive Nuclear-Test-Ban Treaty," *Annual Report* 2019, p. 39: https://www.julkari.fi/bitstream/handle/10024/139830/stuk-b246.pdf?sequence=1&isAllowed=y.

III. The Potential of Distributed Ledger Technology

DLT is a software architecture for validating, storing, and sharing data. There is generally a large overlap between what may be accomplished with more conventional, centralized data storage architecture and what works on a DLT platform. For some problems in data storage, in which the functional requirements of the problem match the inherent characteristics of DLT, it may provide an elegant solution. Part of the success and simplicity of SLAFKA comes about because the essential nuclear safeguards requirement of sharing trusted, immutable records so closely matches the basic premise of DLT.

A blockchain – a chain of blocks – is a type of DLT. DLT is the catch-all category for decentralized digital databases that can include a wide range of participants from multiple locations.[13] A database is considered a DLT when it

> (i) enables a network of independent participants to establish a consensus around (ii) the authoritative ordering of cryptographically validated ("signed") transactions. These records are made (iii) persistent by replicating the data across multiple nodes, and (iv) tamper evident by linking them by cryptographic hashes. (v) The shared result of the reconciliation/consensus process – the "ledger" – serves as the authoritative version for these records.[14]

DLT is a result of bringing together three fundamental information technologies: hashing, encryption, and networking.

Hashing

A hashing algorithm is a mathematical function that may be applied to any string of input characters – whether numbers, text, whole documents, large files such as a video, or even a whole operating system – and generate a unique, fixed-length output as illustrated in Figure 2.[15]

Hashing is the basis of authentication. At its most basic, the ubiquitous password login is an authorization provided when a server verifies that the current hash of a user's password, generated during login, matches the previously stored password hash for that user. A key attribute of hashes is their unidirectional quality. This means that even if a malicious actor obtains the (disclosed) password hashes on the server, with currently available technology it is impossible to deduce the original (secret) password string, except by trial and error. Some hashing algorithms intentionally incorporate a degree of computational work, which makes it harder to reveal passwords by "brute force" attacks that are aimed at accomplishing this.[16]

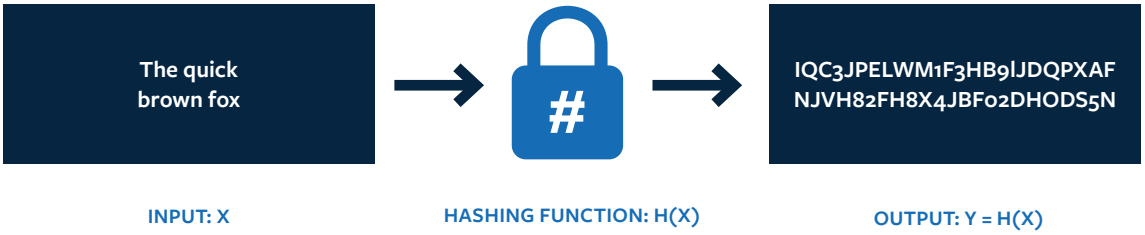
13 Lovely Umayam and Cindy Vestergaard, "Complementing the Padlock: The prospect of blockchain for strengthening nuclear security," Policy Paper, 26 June 2020: https://www.stimson.org/2020/complementing-the-padlock-the-prospect-of-blockchain-for-strengthening-nuclear-security/. Accessed 5 October 2020.

14 Michel Rauchs et al., Distributed Ledger Technology Systems: A Conceptual Framework, Cambridge Centre for Alternative Finance, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-10-26-conceptualising-dlt-systems.pdf.

15 Anyone who has downloaded and installed bespoke software may be familiar with the 'md5 check-sum', which is one kind of hashing algorithm. When used to "hash" a piece of downloaded software, the check-sum creates a reliable output that the user can compare with a corresponding check-sum published by the software creator, and in doing so verify that all of the software has been downloaded correctly, and moreover that it has not been corrupted during transmission.

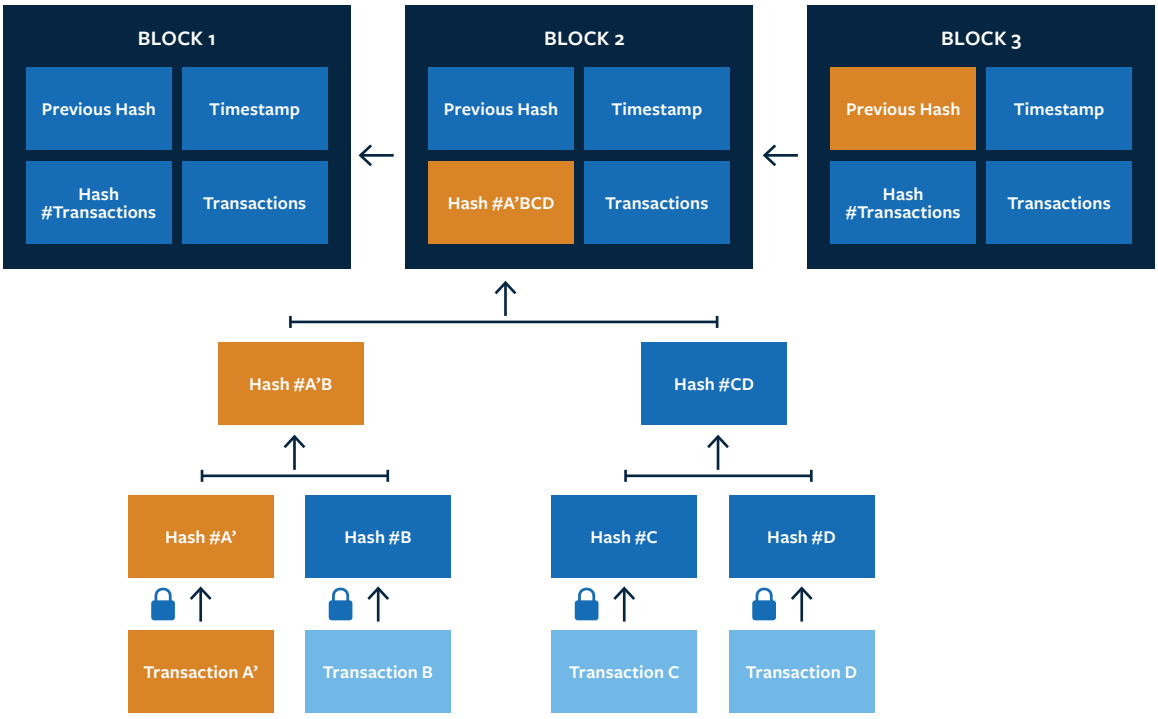
16 A brute force attack uses trial-and-error to guess passwords or encryption keys. It involves excessive forceful attempts to gain access to accounts and network resources. See: Kaspersky, "Brute Force Attack: What You Need to Know to Keep Your Passwords Safe," https://www.kaspersky.com/resource-center/definitions/brute-force-attack. Accessed 6 September 2020.

Figure 2: Hashing



A blockchain is a tamper-evident data storage architecture that exploits the one-way, digital fingerprinting properties of hashing (as depicted in Figure 3). Data, often representing transactions of assets or currency, are grouped sequentially into blocks. The sequence of transactions may be determined chronologically, with blocks containing later transactions being appended to the blockchain, forming a ledger. The blocks can include further metadata, including hashes incorporated to reference and validate any relevant data stored externally to the blockchain. Crucially, each block stores the hash of its predecessor. The implication of this chain of internal cross-referencing is for any potential modification in the data or metadata stored in any block to be immediately verifiable by reevaluating the correct hash of each block. If there has been a modification, the hash of the modified block will not match the historical hash stored in its successor. The blockchain is therefore practically immutable.[17]

Figure 3: Immutability – If Transaction A was modified to Transaction A', then Block 2 would be stored as #A'BCD, which would no longer correspond to the previous hash stored in Block 3.



17 This is not the same as functionally immutable, as being carved in a single-write storage medium, but rendered practically immutable by the ability of a participant to check for unauthorized changes.

Encryption

Encryption uses a mathematical function to process an input string and generate a unique indecipherable output, as a function of the encryption key applied. Unlike hashing, encryption is reversible if the key is known.

Data stored on a blockchain may be encrypted. If the data or metadata that is stored is encrypted, then a participant without the encryption key can still check hashes and maintain the tamper-proof integrity of the blockchain, even though they are unable to read the underlying information. This is a key attribute of DLT, because it means that all participants can contribute to building trust in the system in a way that does not depend on their individual data access privileges. A participant with the encryption key can read the data, but they are still unable to edit it in place, by virtue of blockchain immutability described above. This is another key attribute, because it means that even those participants with extensive access privileges are still bound by the append-only structure of the ledger.

Networking

Networking in DLT is based on the same types of protocols, end-to-end encryption, and hardware virtualization technologies that underpin the World Wide Web. While hashing and encryption are the enabling technologies of DLT, without networking they would not create the kind of re-evaluation of possibilities in trusted data storage that is implied by DLT. Because participants can trust that data on the blockchain is both immutable and confidential, this logically enables the participants to share copies of the ledger between themselves, creating a network of distributed ledgers. This final step has the most far-reaching consequences because it creates a distributed, jointly maintained, trusted, potentially still confidential ledger that participants can consult for an authoritative version of their own and others' data.[18] This aspect of DLT allows it to build a "trust machine" where trust is no longer facilitated through a singular, centralized authority, but by a combination of the data itself, which is immutable, and by the direct participation of a broad cross-section of stakeholders in maintaining and checking the records.

Hashing, encryption, and networking establish the essential characteristics of the shared ledger. Built on these are the final two further components of DLT that enable real work applications: smart contracts and endorsement policy.

Smart contracts

A smart contract (known as a chaincode in Hyperledger Fabric[19]) is a piece of code that defines the rules of transactions that are executed by participants in the shared ledger. Execution of smart contracts usually results in appending new blocks to the blockchain. Smart contracts may execute at the time that a participant orders a transaction, or they can be preprogrammed to execute at a certain time or when certain conditions are fulfilled. In this sense, because they have power to modify the ledger and because they can be set in motion on pre-agreed terms, they are like a legal contract. Although a blockchain is decentralized in terms of data storage, it is fully uniform in terms of its transaction logic for all nodes, this being enforced by smart contracts.

Endorsement policy

When a participant in a blockchain requests a transaction in response to some operational need, they are unlikely to have authority to execute that transaction directly on their copy of the ledger. How they obtain that authorization for a transaction, which ultimately becomes executed globally by a smart contract, is determined by the system's endorsement policy (also called consensus mechanics or consensus protocol). This endorsement policy is the final component that makes a blockchain operational. For example, a participant would submit a transaction proposal to a list of endorser peers specified in the endorsement policy. The endorser peers check the

18 "What Is the Difference Between DLT and Blockchain?," BBVA, 2018, https://www.bbva.com/en/difference-dlt-blockchain/. Accessed 5 September 2020.

19 "Chaincode Tutorials,"Hyperledger Fabric, https://hyperledger-fabric.readthedocs.io/en/release-1.3/chaincode.html. Accessed 15 September 2020.

consistency of the transaction against agreed rules for the transaction specified by the endorsement policy, before the transaction instructions are broadcast to all nodes for execution. Transactions therefore conform to a set of predefined rules, which facilitates data integrity and trust.

Overall, DLT platforms are decentralized, as they give multiple participants a role in maintaining the ledger.[20] They can be open systems, such as blockchain technology underpinning cryptocurrencies (such as Bitcoin) where anyone with an internet connection can participate in a system of buying and selling digital currencies. They can also be private or permissioned, restricting access and actions to specified participants and certain records. Some permissioned blockchains such as Hyperledger Fabric may additionally permit different roles for different members, allowing peers to have different read and write permissions.[21] These platforms are therefore partially centralized, as different participants may take on different levels of responsibility in maintaining the ledger.

Permissioned DLT platforms are being tested and used in a wide range of government and private services, from tracking global shipping and the provenance of high-value minerals to improving access to and security of personal health records and tracking supply chains that deliver food items and other goods globally.[22] Industries, governments, and international organizations are also interested in exploring the potential for DLT because of its resilience against cyberattacks. In order to edit or manipulate data within a DLT platform, a cyberattack would need to simultaneously attack every copy of transactions. This differs from attacks on centralized databases, where changes to a single ledger may go undetected. In a nuclear safeguards context, DLT allows regulators to control participation as aligned with strict confidentiality rules for safeguards information management where information regarding storage areas, transport routes, or schedules of fuel is classified as restricted.

The attractiveness of blockchain technology to nuclear safeguards information management arises from its contributions to trust and decentralization. Data integrity, immutability, and transparency underpin trust in data, given the inability of network participants to reverse or modify a transaction once accepted by network peers. A shared, authoritative ledger also allows for greater participation and transparency among participants in the management of safeguards information.

20 Sarah Frazar, Cindy Vestergaard, Ben Loehrke, and Luisa Kenausis, "Evaluating Member State Acceptance of Blockchain for Nuclear Safeguards," December 2019, *Nuclear Weapons Readout and Recommendations*, p. 8.

21 Androulaki, E. et al. (2018) 'Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains', in Proceedings of the Thirteenth EuroSys Conference. New York, NY, USA: ACM (EuroSys '18), pp. 30:1–30:15. http://dx.doi.org/10.1145/3190508.3190538. Accessed 5 October 2020.

22 Daniel Palmer, "IBM, Maersk's Blockchain Platform TradeLens Is Shipping to Russia," Coindesk, 12 June 2019. https://www.coindesk.com/ibm-maersks-blockchain-platform-tradelens-is-shipping-to-russia; E-Estonia, "Healthcare." E-Estonia, n.d., https://e-estonia.com/solutions/healthcare/e-health-record/. See also: K. Wiggers, "Everledger Raises $20 Million to Track Assets with Blockchain Tech," *VentureBeat* (24 Sep 2019); "Learning from the Estonian e-Health System," *Health Europa*, 11 Jan 2019.

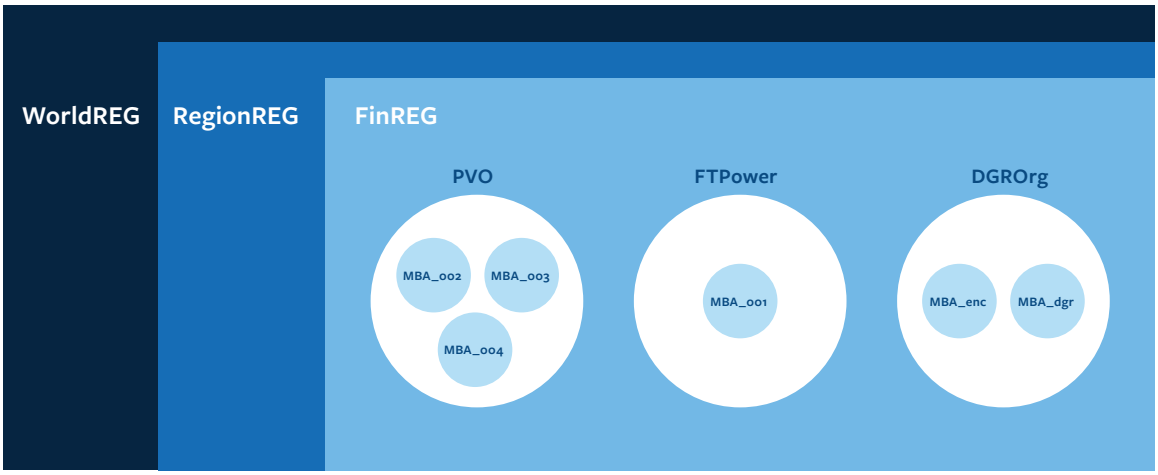
IV. Developing SLAFKA

SLAFKA is a small-scale prototype developed to demonstrate the potential for DLT to be applied to nuclear safeguards information management. Although fictional, SLAFKA is based on Finland's SSAC and is made up of two kinds of participants as outlined in Figure 4: three operators (FTPower, PVO, and DGROrg) and three regulators (FinREG, RegionREG, and WorldREG). FTPower and PVO represent nuclear power plants, and DGROrg represents the deep geological repository. For the regulators, FinREG represents the national regulator, RegionREG the regional authority (such as Euratom), and WorldREG the international regulator (with a similar function to the IAEA).

The user requirements within SLAFKA are based on existing documentation (specifically Commission Regulation No 302/2005[23]), which describes requirements for nuclear material accounting in Finland. A basic scope was agreed upon with STUK at the start of the project and updated as SLAFKA was developed. STUK provided the operational requirements that would determine how SLAFKA could be integrated with their safeguards system. The main challenges during development were to define how the prototype would achieve specific functions. As the software provider for SLAFKA, UNSW was an integral partner in proposing, testing, and modifying solutions. These solutions and subsequent changes were based on Stimson's framing of the ideal prototype within safeguards policy research and STUK's wider objectives in creating SLAFKA.

SLAFKA was designed with a user interface to input and display information to users from the operator, who may not be familiar with different types of information technology. They would be able to use SLAFKA in their day-to-day setting, and input changes in their nuclear material inventories. The user interface (www.slafka.org) is hosted on a web server and displayed to individual users via their web browser. The principal functions of the user interface are to enable convenient interaction between users and the blockchain back-end and to provide graphical representation of the structure and procedures for blockchain transactions.

Figure 4: SLAFKA Participants - The three nuclear operators are in the national jurisdiction of FinREG. Each has a number of different MBAs. FinREG is a hypothetical State regulator inside the jurisdiction of RegionREG, which in turn is within the overall jurisdiction of WorldREG.



23 Commission Regulation (Euratom) No 302/2005 of 8 February 2005 on the application of Euratom safeguards – Council/Commission statement. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005R0302.

V. SLAFKA Transactions

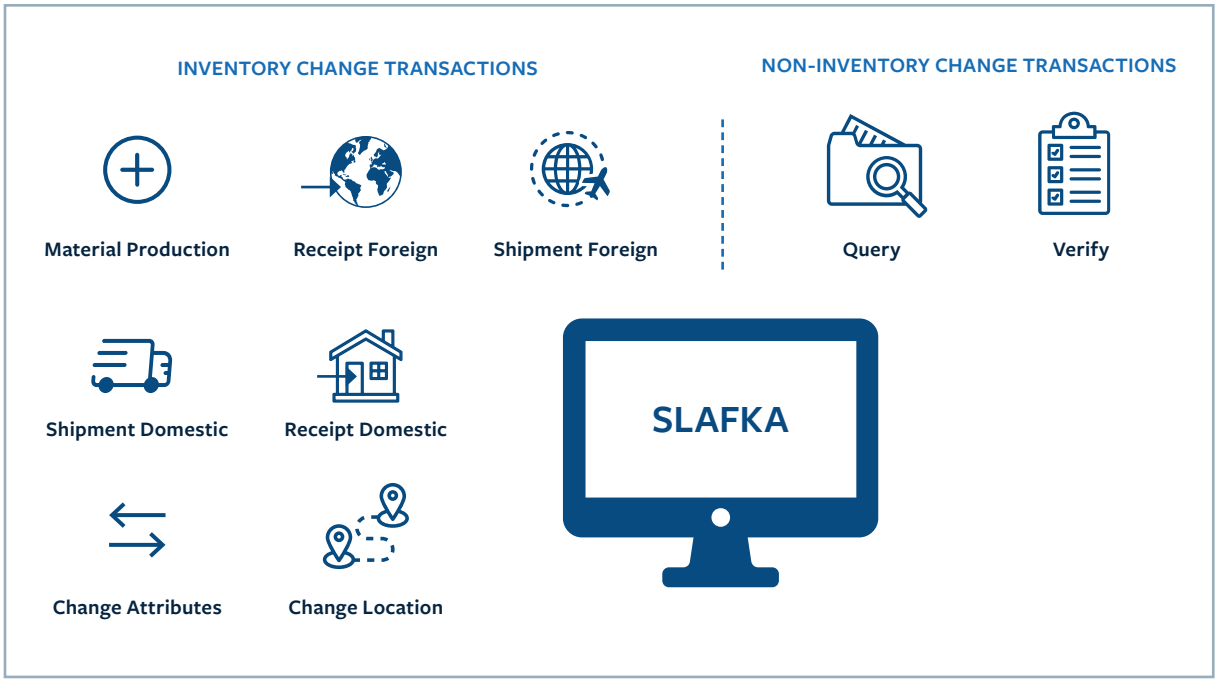
SLAFKA needed to demonstrate that it can input, store, display, and output nuclear material accounting information to meet reporting requirements for the IAEA and Euratom. The three types of reports are ICRs, PILs, and MBRs. SLAFKA transactions include domestic and international shipment/receipt, remeasurements, nuclear loss, nuclear production, change attributes, rebatching, underground disposal, and verification by the regulator.

Figure 5 shows the SLAFKA transactions divided into inventory change transactions and non-inventory change transactions. Inventory change transactions range from Material Production to Change Attributes. The non-inventory change transactions are Query and Verify.

A batch in SLAFKA is a digital asset representing a physical batch of nuclear material, as well as a safeguards accounting unit. A batch is given a unique numerical identity, e.g., BATCH_001.

All operations on SLAFKA are called transactions, which operate on the basis of a batch. SLAFKA transactions are grouped into four types: batch assets creation, batch ownership modification, batch attributes modification, and other transactions.

Figure 5: SLAFKA Transactions



Creating new batches/new material

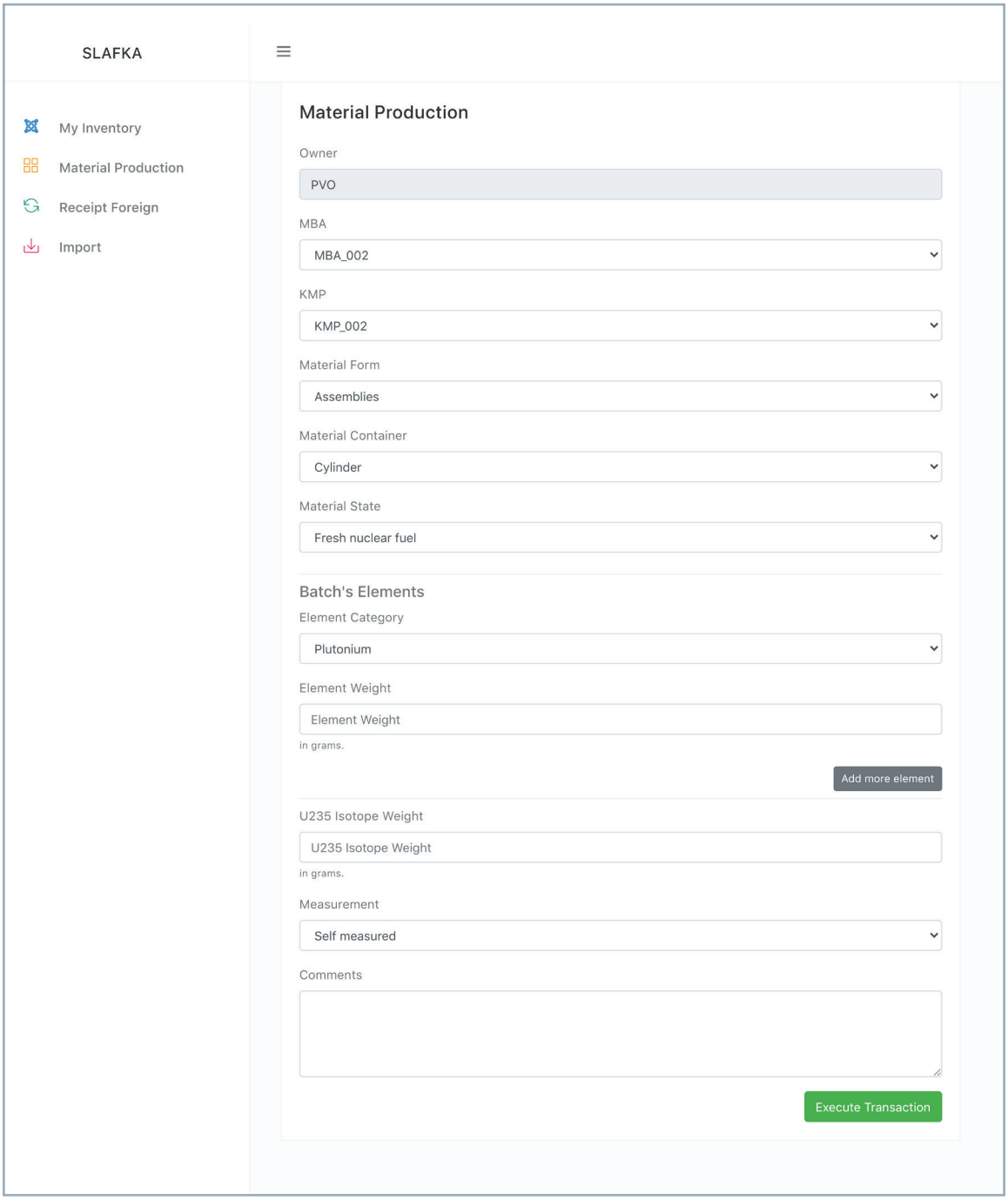
Material Production

Material production initializes a new batch asset. The required inputs for the transaction include the name of the batch and the name of the MBA where the batch is located. Upon successful material production, a new batch will be listed on the inventory table. MBAs within the same (e.g., FinREG's) jurisdiction are named according to the form 'MBA_123', where '123' is a unique number. MBAs outside of the same jurisdiction are equivalent to a country code, e.g., France is MBA_F and Russia is MBA_R. The name of the KMP is supplied also in the form of 'KMP_123'. The KMP in SLAFKA is the lowest-level identifier of the physical location of the batch of nuclear material.

Further options are Material Form (may be Ores, Concentrates, Solutions, Powder, Ceramics, Metal, Fuel, or Canisters); Container Type (Cylinder, Pack, Drum, Discrete Fuel Unit, Birdcage, Bottle, Tank, or Other); Material State (Fresh Nuclear Fuel, Irradiated Nuclear Fuel, Waste, or Irrecoverable Material); and Measurement Basis (Self-Measured, Self-Estimated, Another-Measured, or Another-Estimated).

The number of elements that may be present in a batch is arbitrary. To specify the composition of the batch, the Material Production (see Figure 6) accepts three lists of strings corresponding respectively to element category, element weight, and isotope weight.

Figure 6: Material Production



Receipt Foreign

Similar to material production, Receipt Foreign initializes a new batch when an import of nuclear material is received, with the attributes as specified by the recipient. The owner is always the creator/recipient of the batch. This transaction acts as the receipt of nuclear materials from outside SLAFKA. To simultaneously create batches, SLAFKA can import multiple batches from a correctly formatted text file. Receipt Foreign is illustrated in Figure 7.

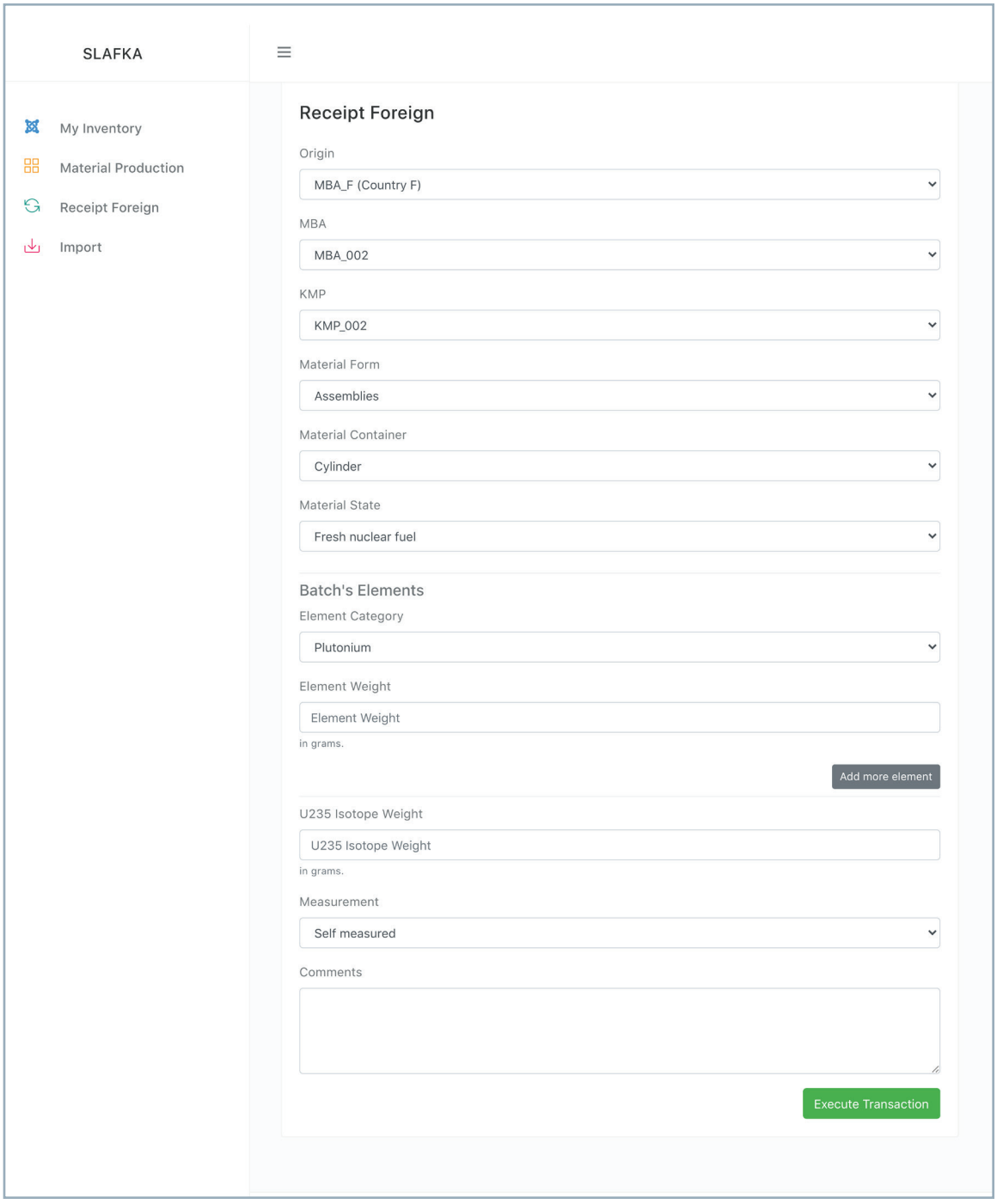
Nuclear transformation – Production

Nuclear transformation transactions update the inventory of nuclides in a batch and are designed to be executed by nuclear operators when fuel is irradiated in a reactor. Although the nuclear transformation transaction is grouped here with other material production transactions, as it creates new nuclear material, it is executed on an existing batch. The nuclear transformation input parameters are changes in the element weights and, for uranium, change in the enrichment level. New elements can be added to a batch, e.g., adding plutonium during fuel irradiation.

Nuclear transformation – Loss

There is a corresponding nuclear loss transaction to enter material lost during irradiation, such as burn-up of U-235. Generally, the nuclear loss/production transactions would be executed in succession to represent irradiation of a batch (loss of U-235 and production of plutonium).

Figure 7: Receipt Foreign page



Batch ownership modification

Shipment Domestic

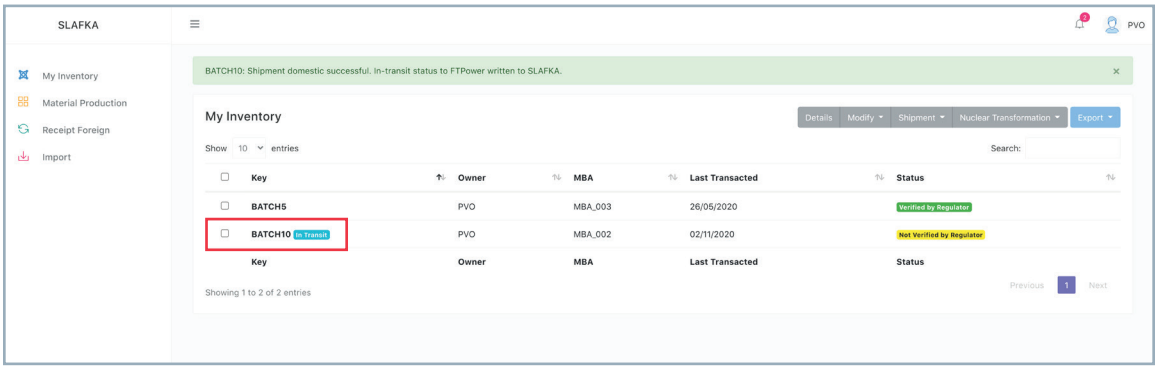
Shipment Domestic initiates transfer of a batch to another holder within the same national jurisdiction. Inputs are the name of the batch being transferred and the name of the holder to which the batch is being sent. Shipment Domestic changes the ownership of a batch to another nuclear operator in SLAFKA. Upon successful transaction execution, a success message will be displayed at the top and an 'In Transit' badge indicates that the batch is currently being shipped, as in Figure 8.

Once the DestinedTo attribute has a value, the batch is flagged by the batch owner's (consignor's) user interface as being 'In transit'. At the same time, if the intended recipient of the batch runs a SLAFKA query transaction (see below), finding this batch with its DestinedTo attribute referring to their own identity will trigger a notification that a batch is destined to them.

Shipment to DGROrg

Similar to Shipment Domestic, Shipment to DGROrg changes the ownership of a batch to DGROrg.

Figure 8: Successful Shipment Domestic execution

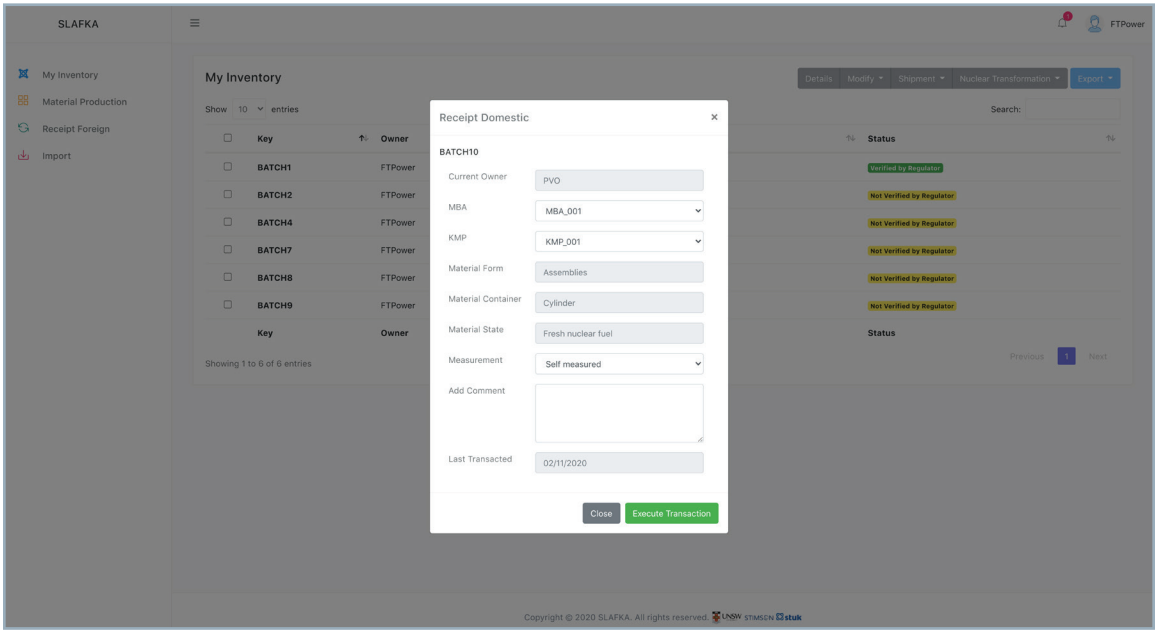


Receipt Domestic

A Receipt Domestic transaction (Figure 9) is used to take ownership of a batch. After a nuclear operator (consignor) executes the Shipment Domestic transaction, the consignee receives a notification.

Executing the transaction updates the owner attributes of the batch to the recipient, updating MBA and KMP attributes to specified values. Receipt Domestic transactions do not give the recipient an opportunity to change any attributes of the batch except those described here. This enforces consistency of transit matching on any transaction. Any shipper/receiver difference needs to be entered separately as a remeasurement transaction.

Figure 9: Receipt Domestic pop-up dialog



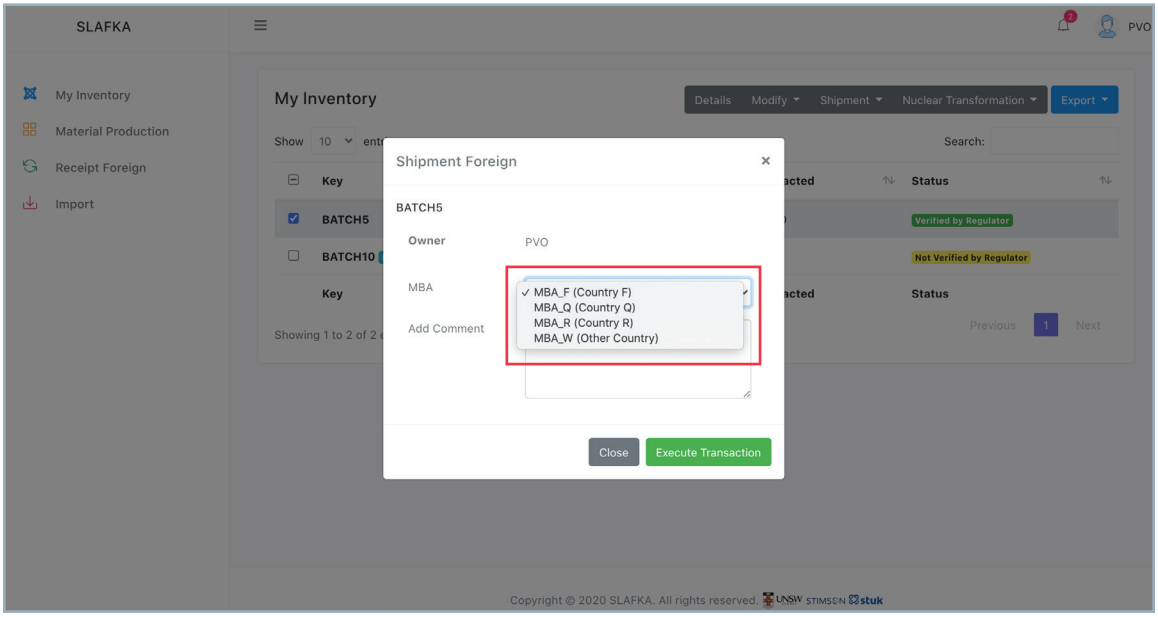
Shipment Foreign

This transaction changes the ownership of a batch to 'FinREG' for record-keeping purposes and updates the MBA to the country code of the country batch exported to. In reality, the batch is not owned by FinREG but rather leaves its jurisdiction.

All SLAFKA's holders of nuclear materials are in a single State. This introduces a dilemma in how to execute a foreign shipment. While the batch cannot have no owner, it is also not consistent with the properties of the blockchain ledger to delete the batch when it leaves FinREG's jurisdiction. The solution was to change the owner of an exported batch to FinREG, to represent export of a batch to a third country, with the MBA code being selected from a special set of MBAs that are in effect country codes as in Figure 10. As a result, provenance and continuity of knowledge of the batch are ensured and, in practice, FinREG has visibility over a list of country-code MBAs, the contents of each one providing records of material that has been shipped.

The only input to the Shipment Foreign transaction is the batch name and country code, with FinREG as the only possible recipient.

Figure 10: Shipment Foreign pop-up dialog



Modifying batches

Change Location

Change Location updates the MBA and KMP of a batch. Input parameters are the new MBA and KMP location for the batch. Change Location is used only to change MBA and KMP to values within the jurisdiction of the batch owner. It cannot be used to transfer ownership of a batch. Shipment Domestic or Shipment Foreign is used for this purpose.

Change Attributes

A Change Attributes transaction updates attributes that do not affect location, composition, or ownership of the batch. These are the batch name, material form, material container, and material state. To execute the transaction, the user specifies the attribute to be changed and a new value.

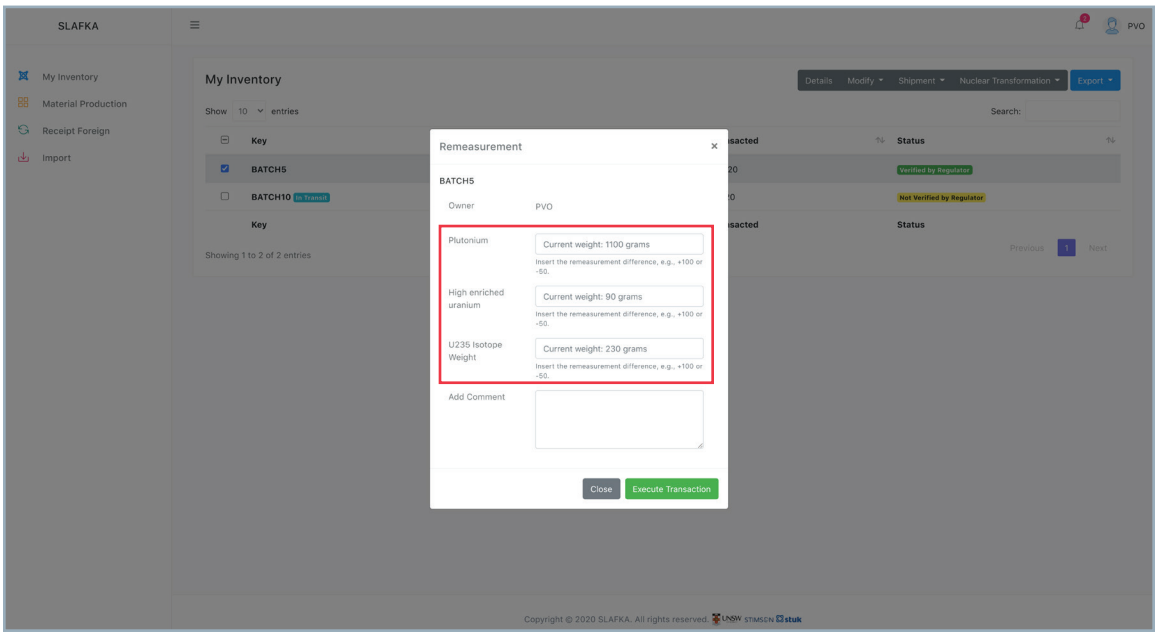
Remeasurement

SLAFKA Remeasurement allows the owner of a batch to update the element weights. In this sense, it is like a subset of the functionality of the nuclear transformation transactions; however, it does not allow the user to add any new element to the batch. Remeasurement is illustrated in Figure 11.

Rebatching

SLAFKA rebatching allows the user to transfer material between batches that they own. Material is transferred to/from an existing batch, or the rebatching transaction can specify the creation of a new batch to transfer the material. Rebatching creates 'Rebatched from' comments in any new batch specifying the provenance of the material.

Figure 11: Remeasurement pop-up dialog



Non-inventory Change transactions

Other SLAFKA transactions are used for viewing batches and for regulator verification.

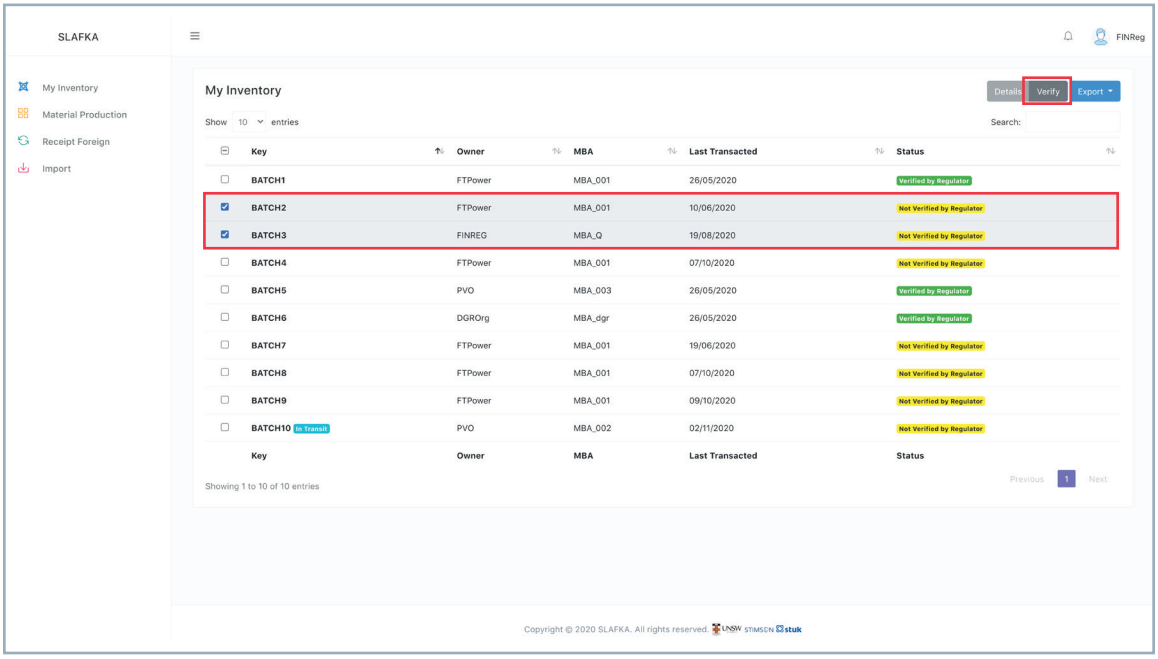
Query

The Query transaction is used to show batch information in the graphical user interface. If the user is a regulator, then their permission also allows them to read the MBA history of the batch and to read the trail of rebatching comments. In this way, the Query transaction allows a regulator to establish provenance of batches. A user is only able to see batch provenance as it relates to their own MBAs.

Verify

Each time the batch is transacted by any holder and in any of the above transactions except for Query, the Verify flag is reset to False. The regulator has a special Verify transaction to indicate verification of batch. When executed, the Verify flag is set to True. Only the regulator has permission to execute this transaction. In the current SLAFKA, there is only one kind of regulator verification, but this could be extended to show verification by different authorities, with each one having sole permission to set their Verify flag. To verify a batch or multiple batches, the user can select desired batches and click the Verify action button, as shown in Figure 12.

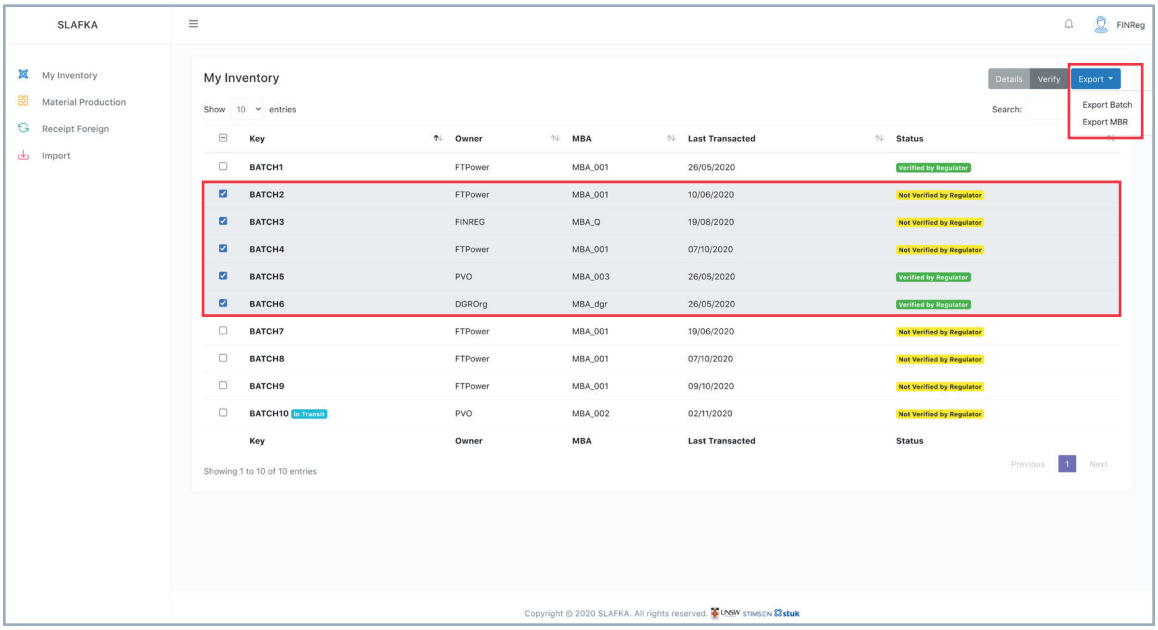
Figure 12: Verify multiple batches



Export Data

SLAFKA supports data exporting in two different formats: PATI-like and MBR text file. To export data, the user selects the desired batches to be exported and exports them to a text file of the chosen format. In the export-to-PATI option, the selected batches will be exported into a structured text file. The formatting of this text file is similar to text files used to import/export batch data from PATI, which is the fuel management software used by some Finnish nuclear power operators. For export to MBR, SLAFKA exports a Material Balance Report (MBR) of selected batches to a text file. SLAFKA's export menu is illustrated in Figure 13.

Figure 13: SLAFKA Export Menu

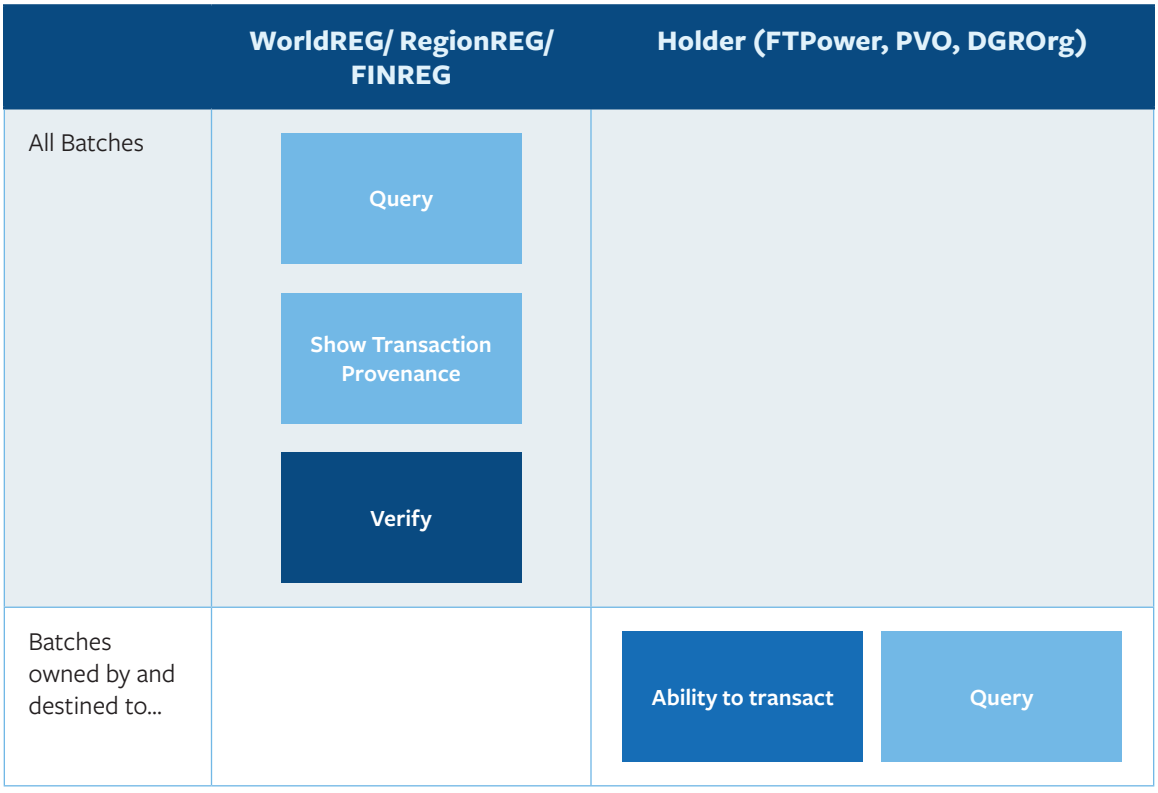


VI. SLAFKA Permissions

The purpose of building SLAFKA on a permissioned blockchain was twofold: (1) to act as a realistic test on the feasibility of blockchain for safeguards, and (2) to provide a genuine educational experience for users to interact with a real blockchain system for nuclear materials accounting. In line with confidentiality rules for nuclear safeguards data, SLAFKA's access controls allow holders of nuclear material (FTPower, PVO, and DGROrg) to input and view their own inventories (not the inventories of other holders), and regulators have visibility of operator inventories. Peers maintain copies of SLAFKA and participate in the execution and validation of transactions. Regulators are not given the ability to transaction except for the Foreign Shipment and Verify transactions described above. Figure 14 illustrates the permissions within SLAFKA.

SLAFKA permissions specify the role of each participant. RegionREG and FinREG have permission to query and show provenance of all batches in their jurisdiction (in practice, this means all SLAFKA batches, because it is based on a single State). In addition, RegionREG and FinREG are permissioned to verify batches through an inspection, which nuclear material holders do not have. The third regulator, WorldREG, has the same permissions as RegionREG and FinREG, except that WorldREG's Query transaction does not extend down to KMP visibility. The project team purposefully designed the Query distinction between regulators to demonstrate how regulators further up the regulatory hierarchy do not necessarily need to have the greatest authority in SLAFKA. In fact, the holders of nuclear material in some ways have greater permissions than the regulators, given they have the ability to transact batches. These transactions include those described above, such as Ship Domestic, Change Attributes, etc. A distinction is made between batches owned by and batches destined to a holder by a domestic shipment. In the latter case, the only

Figure 14: SLAFKA access controls



available transactions are to query the batch, which is necessary for the consignee to be aware of its existence, and the Receipt Domestic transaction, which places the batch into the consignee's MBA and completes the transfer of ownership. Crucially, the consignee has no ability to modify or otherwise transact a batch before they have taken full possession of and responsibility for it.

The SLAFKA permissions work together with the participant jurisdiction to encode the regulatory structure into blockchain permissions for batch visibility and the authority to execute transactions. In this way, complex regulatory relationships can be readily mapped to a DLT system that can potentially include multiple regulators and jurisdictions. This role/jurisdiction mapping was one of the principle innovations that made SLAFKA possible, making it suitable for implementation in a DLT architecture.

For the development of SLAFKA there were no requirements relating to security or to the specific functionality of the blockchain architecture behind the user interface. Given SLAFKA is a first step, and is fictional, SLAFKA was not designed to provide a secure environment to preserve privacy to the level required by nuclear safeguards. The focus was on user interaction with a DLT system and on providing a genuine experience to users in the process and flow of transactions that are working on a real DLT system.

Hyperledger Fabric

SLAFKA was built in Hyperledger Fabric, a private, permissioned blockchain framework developed by an IBM-led consortium under the auspices of the Linux Foundation's Hyperledger project. Hyperledger Fabric includes features that preserve the confidentiality of data and restrict user permissions over reading and writing data. This functionality aligns with confidentiality rules governing nuclear safeguards. Together, these provide assurance that certain transactions will be broadcasted only to relevant parties rather than all participants as in traditional blockchain models. A key Hyperledger feature exploited in SLAFKA is smart contracts, referred to as chaincode, which in SLAFKA both executes the transactions and restricts what particular users can do. Further Hyperledger features such as private data collections, channels, and endorsement policies would be valuable in future implementations of a safeguards tool like SLAFKA but were not used in the prototype.

SLAFKA archived permissioning by building access control into the chaincode. For example, the chaincode for a Shipment Domestic transaction checks whether the peer proposing it is within a list of approved "holder" nodes and has permission to transact that particular batch. SLAFKA also checks whether the node being used matches that of the owner of the asset. Similarly, a node seeking to read information about a batch would execute a transaction for reading batch attributes. The Chaincode for the Query transaction will only execute successfully if the node proposing the transaction meets conditions specified in the Chaincode (in this case, being a holder and being an owner of the batch). SLAFKA does not perform further verification, such as by checking the transaction against endorsement policies. This area of access control capabilities in Hyperledger Fabric is therefore not exploited in the current implementation of SLAFKA and is one clear area for developing future work.

VII. A New Way of Safeguards Reporting

The conceptual differences between present-day and SLAFKA reporting are outlined in Figure 15. Current safeguards reporting (depicted on the left) is unidirectional from holders of nuclear material to the (national or regional) regulator and then up to the IAEA. Holders of nuclear materials are nuclear power plants, DGRs, or holders of small quantities of nuclear materials such as universities, laboratories, or hospitals. In SLAFKA, instead of holders/operators reporting directly to a regulator, they digitally transact between one another and the regulator(s) observe and verify the transactions.

While the regulators' ability to fulfill their essential oversight functions is fully preserved, in some ways their role in checking and authorizing transactions is simplified, because some of these functions (notably transit matching, reconciliation of transactions, and data entry on behalf of participants) are taken over by logic built into the smart contract or even eliminated.

SLAFKA therefore encourages higher levels of transparency – where transparency is appropriate – and greater participation among stakeholders in a national SSAC. Blockchain decentralization is the way DLT systems give multiple participants a role in maintaining the state of the ledger, underpinning the consensus protocol that enables creation of a trusted environment. The innovation that makes this possible is the concept of breaking down the characteristics of stakeholders in the nuclear material supply chain into roles and jurisdictions for the SLAFKA participants. This enabled the essential requirements of nuclear material accounting to be met by the innate characteristics (and advantages) of DLT for this application.

Figure 16 highlights how the attributes of trust and decentralization are linked. Transparency, data integrity, and immutability of blockchain data storage underpin the trust attribute. The integrity of data results from the requirement that transactions conform to a set of predefined rules and be authorized according to a consensus

Figure 15: Present-day safeguards reporting and SLAFKA safeguards reporting

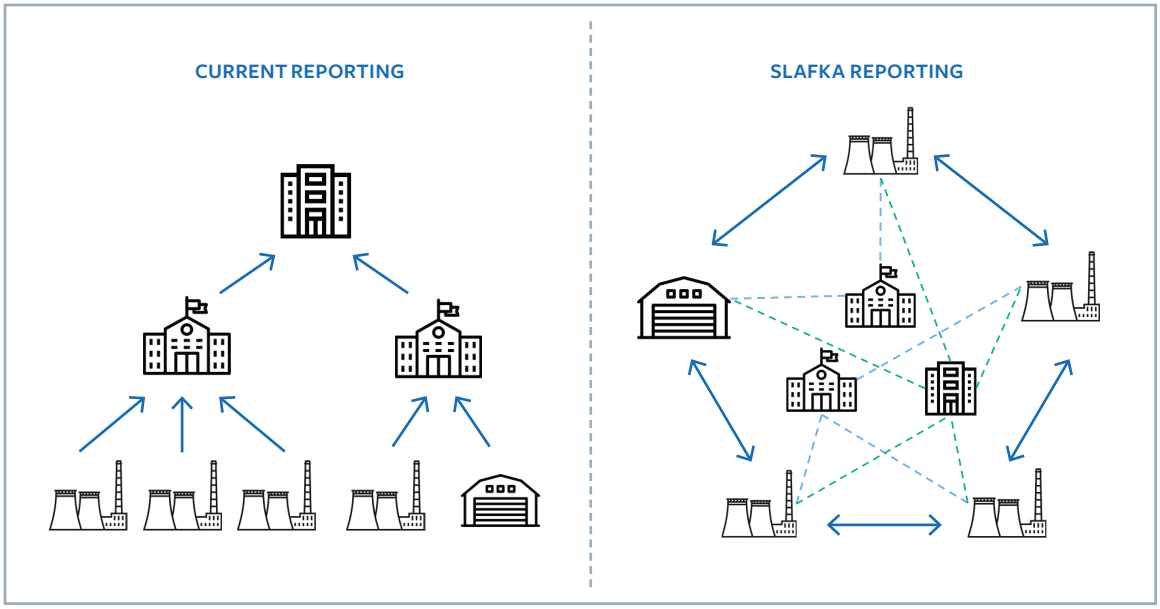
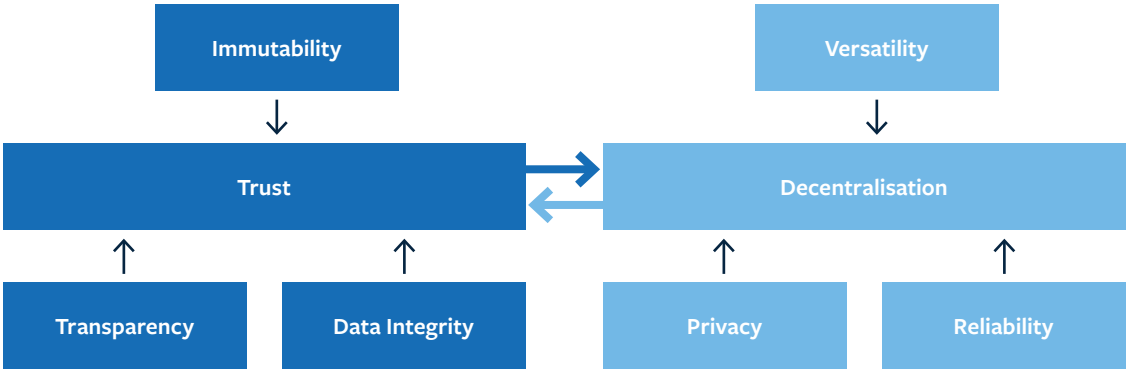


Figure 16: DLT attributes of trust and decentralization



protocol as well as the practical immutability of blockchain.

SLAFKA demonstrates that DLT platforms will not change what safeguards information is reported or undermine security and confidentiality rules – some of the most politically charged issues for the international safeguards community. DLT does not replace the need for inspection by regulatory bodies, and STUK, Euratom, and IAEA inspectors would continue to visit facilities and verify physical inventories against information recorded in the ledger. Participants at a workshop in June 2019 on acceptability of DLT to member states of the IAEA noted that the integration of a DLT platform into existing systems as a reporting tool would not lead to additional safeguards information beyond what is already required by safeguards agreements. Participants also did not anticipate that safeguards agreements would need to be updated if blockchain technology was adopted.[24]

SLAFKA illustrates how DLT could improve the timeliness for detecting diversion. For example, inspectors and analysts can monitor changes to inventories as they are entered instead of waiting 30 to 60 days after a change has occurred to receive an ICR. This capability can improve the effectiveness of routine inspection plans and inform where the IAEA conducts Complementary Access under the Additional Protocol and its ability to detect undeclared nuclear activities. It would also enable the IAEA to provide more immediate feedback about the quality of information reported.[25]

One concern with erasing the line between operator and state records is that operators are currently required to submit changes in inventory once a month. Reporting and operational procedures are therefore designed for monthly reporting to allow validation and reconciliation before submission, which calls into question when one or more transactions could be considered an official report. One way around this is to have a private DLT platform within a company/facility, which could still track daily movements of material as per company policy but post reconciled data to a separate, shared DLT with the IAEA or regional authority. Another is to consider how daily changes can be reflected in a shared ledger with the regulator in a way that allows for holders to move material between MBAs as needed operationally. Given that DLT allows for traceability of batches as they move between MBAs, this can facilitate reconciliation monthly, without each change requiring a "Verified by the Regulator" validation until physical inspection is scheduled.

24 Sarah Frazar, Cindy Vestergaard, Ben Loehrke, and Luisa Kenausis, "Evaluating Member State Acceptance of Blockchain for Nuclear Safeguards," December 2019, p. 8.

25 Ibid., p. 9.

Discussions on DLT platforms for nuclear safeguards have also considered how DLT enables data analytics to identify patterns, which is an important function as the International Atomic Energy Agency focuses on a State's nuclear activities as a whole.[26] Moreover, a DLT layer could be integrated into existing databases at the IAEA, which would give it the capability to access and link source documentation with inventory data, replacing a function currently performed manually. It is important to underscore that the integration of databases would have to be voluntary, as there is no legal basis for such integration in INFCIRC/153. If the IAEA decided to integrate the systems, it could see benefits, such as an immediate provision of up to date accounting information to the IAEA.

Moreover, a shared database among the inspectorates (national regulators, Euratom, and the IAEA) would allow them access to the same information on nuclear material balances. Currently, the inspectorates do not compare the nuclear material balances in their databases, meaning errors may go unnoticed for extended periods of time.

SLAFKA illustrates that despite the reputation of blockchain technology as disruptive, permissioned DLT presents an evolutionary opportunity in the way safeguards information is reported and managed. A tamper-evident, transparent ledger facilitates trust in data integrity and reinforces confidence in safeguards reporting even as corrections are continually appended to the ledger. Overall, these improvements create greater analytical efficiency and trust in State- and operator-provided information, which can transform how regulators review and prepare information. This is particularly relevant at the international level when the IAEA Board of Governors considers cases of non-compliance. Figure 17 lists the benefits of DLT for stakeholders in nuclear safeguards information management.

Figure 17: Benefits of DLT for Stakeholders

PROPERTIES/ CHARACTERISTICS	REGULATOR BENEFITS	OPERATOR/ INDUSTRY BENEFITS
Immutable data storage	Enduring record of provenance and (read only) records of inventories and transactions Trust in data when investigating cases of non-compliance	Authoritative records shared across ecosystem

26 Ibid.

PROPERTIES/ CHARACTERISTICS	REGULATOR BENEFITS	OPERATOR/ INDUSTRY BENEFITS
Networked architecture and distributed data storage	Enhanced resilience of records for very long-term data storage (e.g., DGR) One ledger, the single authoritative version of the truth Greater sense of involvement and participation among stakeholders Allows inspectorates (STUK, EC, IAEA) to share (and compare) nuclear materials balances, reducing likelihood of errors going unnoticed over extended periods of time	Enhanced security (especially against deletion/loss of records) State and operator records are the same, reducing errors and delays in reconciliation Greater sense of involvement and participation among stakeholders
Batches as assets – inherent checking and reconciliation of transactions	All transactions are broken into discrete steps; reduced likelihood of cutting corners in reporting	Reduced frequency of errors
Transactions mediated by smart contract/Chaincode	Regulator input in defining the transaction logic up front	Streamlining of regulatory relationships – operators can freely transact with their inventories, within a trusted network
Access controls and encryption of data	Regulators can see all MBAs	Facilities can only see nuclear material in their own inventories or being sent to them
Trust and data integrity	Transactions are immutable and append only	
Permissioning and confidentiality	Automated verification and encryption – very difficult for data to be tampered with	

VIII. Next Steps and Future Research

Given that Finland is a member of Euratom, any DLT for safeguards information management would have to be regional for it to be adopted. Health and travel restrictions related to the COVID-19 global pandemic limited the ability of the SLAFKA team to present the prototype to Euratom in person. Once restrictions are lifted, next steps are to demonstrate SLAFKA to Euratom officials and explore the potential for further development and testing of SLAFKA within the wider Euratom safeguards system.

SLAFKA is a first step in exploring the potential of DLT to be applied to nuclear safeguards. SLAFKA illustrates how a permissioned DLT platform can input, store, and display nuclear materials accounting information to meet reporting and confidentiality requirements of Euratom and the IAEA. It demonstrates how DLT facilitates a new way in reporting safeguards that involves greater participation and transparency among stakeholders within a shared, authoritative ledger. SLAFKA also provides an intuitive, cloud-based user interface that can be accessed by logging in from any web browser, allowing for a more user-friendly environment.

Future research will need to further develop and test security and specific functionality of the blockchain architecture. Given that SLAFKA is fictional and to be used for demonstration purposes publicly, it was not designed to provide a secure environment. It also assumes that participants have already agreed upon consensus in data validation. SLAFKA attains confidentiality by building permissions at the level of transactions, that is, smart contracts. For instance, a node seeking to read information about a batch would execute a transaction for reading batch attributes. The chaincode corresponding to the transaction will execute successfully only if the node proposing the transaction meets conditions specified in the smart contract.

A significant gap highlighted by the creation of SLAFKA is a complete description of endorsement policies for nuclear material transactions in a system like SLAFKA. Currently, the validity of proposed transactions is affirmed only by the node proposing the transaction. While the SLAFKA user interface does not allow users to submit invalid transactions that do not meet the rules of the network, theoretically, nodes can propose and endorse invalid transactions. One reason SLAFKA did not include transaction endorsement policies is that information about their likely structure and function is not presently available. Further research is needed to discover what endorsement policies are most beneficial for the stakeholders in a nuclear material accounting system and, crucially, to create and reach consensus on the nature of these endorsement polices where they are not presently known. This exercise will promote valuable dialogue, with or without its envisioned application in a future DLT platform for nuclear safeguards.

SLAFKA also did not test aspects related to reporting under the Additional Protocol (AP). This was by design given the focus was to first understand how DLT can be used to streamline reporting from operators to STUK and to Euratom as required by Commission Safeguards Regulation No 302/2005. The IAEA uses a separate protocol reporter (PR3) software for AP declarations which has its own built in database, separate from reporting under Comprehensive Safeguards Agreements. Many EU member states and nuclear operators use CAPE software (Commissions Additional Protocol Editor) specifically designed for AP reporting via European Commission. Future research and prototype development can test AP transactions as well as demonstrate the ability of DLT to integrate existing systems and their databases.

In SLAFKA, holders of nuclear materials are located within a single State. Future research is needed to explore how transactions related to imported and exported material function in line with Nuclear Cooperation Agreements (NCAs). These bilateral agreements outline specific export controls and bilateral (or trilateral, with the

IAEA) reporting requirements between trading partners in nuclear material and technology. This research would include more participants in a DLT platform and would have to address a variety of export control regulations specific to NCAs.

Future research would also benefit from including not only safeguards information, but also data related to nuclear security and safety as required by national regulations. Given that batch attributes such as location and composition are also necessary for nuclear security and safety information, a DLT platform that incorporates the "3S" principles of safeguards, security, and safety would increase understanding about the applicability of DLT to increase efficiencies in storing and reporting data within operators as well as within a State. This research could first focus on a specific industry operator to understand operational as well as regulatory practices and regulations. It would also address the transport of nuclear material.

Lastly, a common question when presenting SLAFKA to stakeholders usually relates to the correctness of information placed on the blockchain. Incorrect information or "bad data" put on a blockchain is still incorrect. Human error is not erased by the technology. As with current safeguards reporting, physical inspection is used to verify records, and corrections are in turn appended to the ledger. An area for further investigation is how SLAFKA and DLT platforms can be integrated with remote monitoring hardware, and how this hardware can contribute to the trust in and the security (or vulnerabilities) of the overall system. There are strong precedents for this research in existing remote monitoring hardware and expertise routinely employed by the IAEA for verification purposes, and the rapidly growing research area outside of nuclear safeguards connecting blockchain technology to the internet of things.

SLAFKA is a first step among many in researching and testing the functionality, usability, and acceptability of DLT for nuclear safeguards information management. More study is needed on broader safeguards applications such as those related to bilateral trade agreements or the Additional Protocol and also to the wider issue of the costs for development (and whether benefits outweigh costs). SLAFKA was developed by an interdisciplinary team whose members each provided specific policy, technical, and operational requirements. The prototype demonstrates not only that DLT can cover safeguards transactions and permissions, and strengthen data integrity and confidentiality, but also that the inherent characteristics of DLT are suited to the peculiarities and highly governed structure of nuclear safeguards. As the world's first blockchain prototype for safeguarding nuclear materials, SLAFKA shows the potential for safeguards powered by blockchain.