Pacific Northwest
NATIONAL LABORATORY

PNNL-29527

Transit Matching Blockchain Prototype

November 2019

Sarah Frazar
Cliff Joslyn
Rustam Goychayev
Alysha Randall

U.S. DEPARTMENT OF ENERGY

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

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

Printed in the United States of America

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

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

PNNL-29527

Transit Matching Blockchain Prototype

November 2019

Sarah Frazar
Cliff Joslyn
Rustam Goychayev
Alysha Randall

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

Pacific Northwest National Laboratory
Richland, Washington 99354

Summary

This document describes the technical work performed in Fiscal Year 2019 to incorporate distributed ledger technology into a nuclear safeguards application/problem. It outlines the nuclear safeguards problem used, the team's reasoning for selecting the problem, and their design choices. Lastly, this document introduces the resulting product, including screenshots of the demonstration, key findings, and recommendations for future work. This work builds on the studies conducted by the Pacific Northwest National Laboratory in 2017 and 2018. The two studies and the work performed were funded by National Nuclear Security Administration's Office of Nonproliferation and Arms Control to explore how distributed ledger technology could benefit the International Atomic Energy Agency's work.

Acronyms and Abbreviations

ACL	Access Control Language
BNA	Business Network Archive
DL	Distributed Ledger
FY	Fiscal Year
IAEA	International Atomic Energy Agency
ICR	Inventory Change Reports
IDE	Integrated Development Environment
MBA	Material Balance Area
MBR	Material Balance Reports
PNNL	Pacific Northwest National Laboratory
SA	State Authority

Contents

Figures

Tables

1.0 Introduction

This document describes the technical work performed in Fiscal Year (FY) 2019 to incorporate distributed ledger (DL) technology into a nuclear safeguards application/problem. The following pages describe the nuclear safeguards problem used, the team's reasoning for selecting the problem, and their design choices. Lastly, this document introduces the final product, including screenshots of the demonstration, key findings, and recommendations for future work plans. This work builds on the studies conducted by the Pacific Northwest National Laboratory (PNNL) in 2017[1] and 2018[2]. The two studies and the work performed in FY2019 were funded by National Nuclear Security Administration's Office of Nonproliferation and Arms Control to explore how DL technology could benefit the International Atomic Energy Agency's (IAEA) work.

In FY2017, PNNL completed a study that explored whether international safeguards might be expected to benefit from potential incorporation of blockchain technology. PNNL developed an analytical methodology for evaluating whether and to what extent different DL designs could help solve to different safeguards problems. In FY2018, PNNL explored seven safeguards use cases that might benefit from a DL solution: [3]

- Transit matching
- UF_6 cylinder tracking
- Computerized inspection and complementary access reports
- Noncompliance process
- Nuclear material accounting reporting
- Unattended monitoring systems and state-of-health transmissions
- Communicating safeguards information through the Safeguards Information Report.

The study concluded that further exploration of the transit matching use case was highly warranted as the use case met six out of eight evaluation criteria described in section 4.2 of the report. Transit matching refers to the process of matching reports of domestic and international shipments and receipts of nuclear material between facilities. While different types of changes to nuclear material inventories may occur, transit matching is implemented only for those reports that indicate nuclear material was shipped from or received into a material balance area (MBA). Under the current transit matching process, the IAEA uses a computer algorithm to match 95% of domestic reports and 25% of foreign transfer reports. IAEA analysis matches remaining reports by hand.[4]

In FY2019, the PNNL team transitioned the work from the conceptual stage into a DL prototype that models the transit matching process. The prototype was designed for the IAEA to test whether the technology might benefit the IAEA's transit matching process. A key finding was

---

[1] Frazar, Sarah, Mark Schanfein, Ken Jarman, Curtis West, Cliff Joslyn, Sam Winters, Sean Kreyling, and Amanda Sayre. 2017. "Exploratory study on potential safeguards applications for shared ledger technology," Pacific Northwest National Laboratory, February 2017.
[2] Frazar, Sarah, Cliff Joslyn, R Singh, Amanda Sayre. 2018. "Evaluating Safeguards Use Cases for Blockchain Applications," Pacific Northwest National Laboratory, February 2018.
[3] Ibid.
[4] Frazar, Sarah, Mark Schanfein, Ken Jarman, Curtis West, Cliff Joslyn, Sam Winters, Sean Kreyling, and Amanda Sayre. 2017. "Exploratory study on potential safeguards applications for shared ledger technology," Pacific Northwest National Laboratory, February 2017.

that a DL could potentially improve the timeliness of detection while increasing confidence in safeguards conclusions. Specifically, this report includes three findings:

1) A DL could improve the timeliness of detection of diversion of nuclear material through real-time match attempts of all transactions posted to the ledger.
2) A graded score applied to all match attempts could help inform inspection activities.
3) Transparent documentation of IAEA match attempts on a tamper-proof ledger can increase confidence in IAEA safeguards conclusions.[1]

Of the three findings, the first two are supported by currently available automated workflow environments, in addition to a DL, while the third key finding is enabled only by the immutability and cryptographic surety that the blockchain provides.

This study describes the range of issues that influenced PNNL's design decisions and development process. It describes how information is reported to facilitate transit matching, the types of data submitted to the IAEA process, likely users of a DL designed for safeguards purposes, the permissions governing their interactions with the ledger, how information would be reflected on a ledger, and how the IAEA might use the information to improve its safeguards verification activities. It provides screenshots of the final prototype ledger and discusses key findings and additional issues for future researchers to consider.

The audience for this work includes the National Nuclear Security Administration's Office of Nonproliferation and Arms Control, which sponsored the research; IAEA inspectors and analysts; technology enthusiasts; software developers; safeguards and computer science experts at National Laboratories, universities, and thinktanks; and safeguards professionals around the world. PNNL hopes future researchers will improve the design and development process described here.

[1] Changes are tamper proof in a sense that it is extremely computationally difficult to accomplish and it becomes evident to experts what the changes were and who made them.

2.0 Prototype Design

Prior to software development, the team considered various factors likely to affect the ledger's design, including the detailed workflow of the transit matching process, the transit matching dataset, the scope of the DL design (transit matching vs. mass balance), and the optimal DL software platform.

2.1 Transit Matching Process

In a series of meetings with safeguards experts, PNNL articulated the current process by which transit matching occurs. Specifically, the team analyzed the parties involved in transit matching, their interactions, conditions that should be applied to their interactions on the ledger (e.g., who has permission to view certain types of information), key documentation processes, and the core "information artifacts" (forms and records) used in the matching processes. This examination established the foundation for the prototype's design document (Appendix A).

2.2 Transit Matching Data

In order to model interactions between MBAs and the IAEA, the team created a surrogate dataset (Appendix B) of simulated Inventory Change Reports (ICRs) based on a sample ICR template and expert interviews. The dataset for this project initially included simulated transactions between eight MBAs in order to completely capture all possible transaction variations. The possible batch transaction combinations included in the dataset are the following:

- "One to one," representing a single shipment documented as a single shipment upon receipt.
- "One to many," representing a single shipment separated into separate batches upon receipt.
- "Many to many," representing several small shipments documented as several shipments upon receipt.
- "Many to one," representing several small shipments combined into a single batch upon receipt.

The original dataset accounted for foreign and domestic transactions, as well as transactions that accounted for possible "re-batching", with batches being subtracted from, added to, and/or renamed, within an MBA before being recorded on a physical ledger. The PNNL team debated whether a re-batching process, as recorded in the ICR, was part of the transit matching process or more relevant to determining an overall mass balance in the safeguards system. Logically, modifying or renaming batches after receipt of shipment is part of a mass balance problem and not part of the transit matching process. To design the simplest prototype that would still support or refute the hypothesis being tested, the team decided to defer the more complex set of mass balance-related operations, such as re-batching operations, to future research. This allowed the team to limit the dataset to include only transactions between MBAs.

2.3 Platform Selection

The team reviewed various blockchain platforms to select the option for the transit matching use case. The examination included two prominent, freely available platforms, Ethereum and Hyperledger.

Table 1 illustrates the similarities and differences between the main platforms evaluated.

Table 1. Platform Attributes

Metric/Characteristic	Ethereum	Hyperledger
Description	Generic blockchain platform	Modular blockchain platform
Ideal for	Business to Consumer businesses and general applications	Business to Business businesses
Network	Permissionless, public or private	Permissioned, private
Consensus Protocol	Proof-Of-Work. Proof-Of-Stake Casper Implementation Ledger level	Allows multiple approaches (pluggable consensus algorithm), supports Practical Byzantine Fault Tolerance Transaction level
Smart Contracts	Smart contract code (e.g., Solidity)	Chaincode (e.g., Go, Java)
Scalability	Existing scalability issue	Not prevalent
Governance	Ethereum Developers	Linux Foundation
Cryptocurrency	Ether is used to execute contracts	Not prevalent

2.3.1 Platform

Based on the comparison in Table 1, PNNL chose Hyperledger Fabric,[1] an enterprise-grade permissioned DL framework currently deployed for various applications. Its modular and versatile design satisfies a broad range of industry use cases. It offers a unique approach to consensus that enables performance at scale while preserving privacy. Originally developed by IBM, Hyperledger Fabric is under the Hyperledger project umbrella of open-source blockchain tools and services started by the Linux Foundation in 2015.[2] According to Thirteenth EuroSys Conference paper published in 2018 by majority IBM associate authors,

> "Hyperledger Fabric is the first truly extensible blockchain system for running distributed applications. It supports modular consensus protocols, which allows the system to be tailored to particular use cases and trust models. Fabric is also the first blockchain system that runs distributed applications written in standard, general-purpose programming languages, without systemic dependency on a native cryptocurrency. This stands in sharp contrast to existing blockchain platforms that require 'smart contracts' to be written in

[1] "Hyperledger Fabric." *Hyperledger* (blog). Accessed September 17, 2019. https://www.hyperledger.org/projects/fabric.
[2] "About Us." *The Linux Foundation* (blog). Accessed September 17, 2019. https://www.linuxfoundation.org/about/.

> domain-specific languages or rely on a cryptocurrency. Fabric realizes the permissioned model using a portable notion of membership, which may be integrated with industry-standard identity management. To support such flexibility, Fabric introduces an entirely novel blockchain design and revamps the way blockchains cope with nondeterminism, resource exhaustion, and performance attacks." [1]

Notably, Hyperledger Fabric as a generic blockchain DL does *not* necessarily implement or require an actual cryptocurrency capability.[2] Such a dependency was deemed neither necessary nor supportable in the safeguards context, as States would be highly unlikely to be willing to "pay" in cryptocurrency to report safeguards information.

2.3.2 Coding Environment

Once the platform was chosen, the team needed to select a coding environment. PNNL chose to use the publicly available Hyperledger Playground Integrated Development Environment (IDE). This IDE is a user-friendly coding environment that allows the developer to test code functionality and generate a business network archive (BNA) file that can be deployed as a blockchain. Importantly, the team later discovered that two different users are not able to sign on to the IDE and access the same Hyperledger's blockchain from two different computers using the same BNA to conduct transactions independently. Hyperledger Playground is a framework for rapid development and deployment to model a limited business network in a matter of weeks versus months. Other larger development teams may want to consider a more robust system.

---

[1] Androulaki, Elli, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, et al. "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains." In *Proceedings of the Thirteenth EuroSys Conference on - EuroSys '18*, 1–15. Porto, Portugal: ACM Press, 2018. https://doi.org/10.1145/3190508.3190538.
[2] Ibid.

3.0 Prototype Development

Having selected the platform and IDE, the team wrote a software program to code the transit matching process (see Appendix C). This section summarizes the questions addressed:

1. What information is posted to the ledger?
2. Who would post information to the ledger?
3. Under what conditions or with what permissions would they interact with the ledger?
4. When would they post transactions?
5. How are transactions matched in a ledger?
6. How do matched transactions appear in a ledger?
7. How would they make corrections or update posted data?

3.1 Information Reporting/Posting

In the typical safeguards system, States submit Material Balance Reports (MBRs), ICRs, and Physical Inventory Listings to the IAEA on a monthly basis. Reporting data on a monthly basis is not relevant in a DL, since users post transactions as other users validate them on a continuing basis. Thus, while information once posted to the ledger does not change, when and how it is reported does. In effect, a DL serves as a single continuous ICR, with transactions indexed by unique line numbers.

3.2 Users and User Permissions

As discussed in PNNL's FY2017 study, three different types of DLs exist: Public, private, and consortium.[1] The transit matching DL prototype PNNL selected models a consortium ledger, which is limited to certain participants. Within the group of valid participants, different users can be distinguished with access to different forms of information:

- **State Authorities (SAs):** SAs enter the ICR codes associated with domestic shipments, foreign shipments, domestic receipt, and foreign receipt onto a DL.[2]
- **Central Authority:** The IAEA has the right to review and confirm transit matches and to correct submissions by SAs by entering "Clarification Records" to the DL.
- **Observers:** Other parties who, while not Authorities, have read-only access to aspects of the DL. Other parties could include facilities associated with a shipment or receipt.

3.3 Sensitive versus Non-sensitive Data

A related issue to users and user permissions involves the type of data they post to the ledger. The team defined "non-sensitive data" as information that States would be willing to share with all consortium participants in the interest of demonstrating safeguards compliance, while "sensitive data" refers to information States would prefer to share only with the IAEA and specific SAs. In PNNL's model, the only non-sensitive data posted to the ledger would be

[1] Frazar et al. "Exploratory study." February 2017.
[2] IAEA. 2011. "Contents, Format, and Structure of Reports to the Agency." SG-FM-1172. https://www.iaea.org/sites/default/files/sg-fm-1172_-_model_subsidiary_arrangement_code_10_labelled.pdf.

information recording the submission by a particular MBA on a particular date, and its status as "matched" or “unmatched” in the DL (see below). All other information about masses, elements, etc., is considered sensitive.[1]

3.4 Understanding Matching in a Digital Ledger

To better understand the process of matching transactions and addressing unmatched transactions, it is important to understand more precisely what it means to "match" a transaction. For example, is matching considered to be "crisply" either "matched" or "not matched", or can there be *degrees* of matching? How "close" does a given Shipment Domestic (SD)/Receipt Domestic (RD) pair of transit records need to be before they're considered "matched"? Most importantly, would such degrees of matching improve the effectiveness of safeguards verification?

To explore these issues, we adapted the following formal model, as recorded in Appendix A:

- **Match Candidates:** First, certain crisp criteria are needed before considering certain transit records as matching. These include having the batch name, element, and appropriately matching MBA numbers.
- **Match Score:** Once these crisp criteria are met, assign a "match score" to any potential match. This score varies from zero (indicating a complete mismatch) to 1 (indicating a complete match). Within this score, certain "free parameters" are available for "tuning" by the model users, or subject matter experts. These indicate various "weights" reflecting the relative importance (or lack thereof) of different components of the score and certain tolerances that can be expected to be overlooked.
- **Mass Penalty:** The greater the extent to which the (potentially clarified) masses are not equal subtracts as a penalty from a score of 1. Mass penalty has both a weight (comparing it to other score components) and a tolerance (a *deminimus* acceptable discrepancy).
- **Time Penalty:** The greater the extent to which the dates of shipping and receipt vary subtracts as a penalty from a score of 1. Time penalty has both a weight and very critical tolerance, initially set to 60 days per Code 10.[2]
- **Items Penalty:** The greater the extent to which the number of items in the shipping and receipt vary subtracts as a penalty from a score of 1.

3.5 Matching Transactions in a Digital Ledger

As discussed previously, the DL does not explicitly represent current ICRs on a monthly, batched basis. Similarly, matches, partial matches, and failed matches are represented in the DL in a mathematical form. As the DL is immutable, information about prior records are never changed. Rather, the ledger is appended with additional records indicating a change in the status of prior information. As a result of this inherent design feature in a DL, the concept of “Match Records” indicates that certain transit records have sufficiently matched in real time.

To satisfy all purposes, the following general mechanism facilitates transaction matching. Each DL record contains a field for the status labeled "Match" that can have one of four values:

---

[1] Due to limitation of Hyperledger Composer, the PNNL team was unable to fully implement the access controls as stated here, due to the constraints implemented the Hyperledger Composer. This limitation is further described in Appendix C - Developer Notes.

[2] Code 10 of the General Part of the Subsidiary Arrangements under the Comprehensive Safeguards Agreement specifies the format of nuclear material accounting report.

- **UNMATCHED:** Initially, all records are assigned a status of UNMATCHED. These are then called "unmatched transits", which are available "to be matched" by the DL.
- **MATCHED:** Once a shipping and a receiving record, possibly combined with a clarification record (see below), are deemed to be "sufficiently" matched (see Understanding Matching in a Digital Ledger), then their status is changed to MATCHED, and they are no longer available for later matching.
- **PARTIAL:** If a record is matched but falls below a determined threshold calculated by the aforementioned penalties, the record will be labeled as PARTIAL, until perhaps a Clarification Record is submitted, at which point it will be re-evaluated for a MATCHED status.
- **DEPRECATED:** A record will be deprecated, or downgraded, if it is not necessary anymore due to a clarification or correction. It will not be evaluated in any further transactions but available to view.

3.6 IAEA Clarifications and State Corrections

When automatic matching fails in the PNNL model, the CA can issue new "clarification" records into the DL, which can add or subtract amounts of elements to transit (shipping or receiving) ICR lines. These are distinct from the CORRECTION TO entries, which SAs make while updating previously filed transit records. Such corrections are explicitly represented in the DL through a different mechanism. A record will then be matched or deprecated as a result of the clarification or correction.

3.7 Matching Improves Efficiency and Effectiveness

The aforementioned method of evaluating and matching transaction records on a DL demonstrates why a DL improves the effectiveness and efficiency of the transit matching process. In today’s safeguards system, when computer matching fails, the IAEA attempts to match reports by hand. If the IAEA is unable to match a report, it proceeds to investigate through further questioning of the State and safeguards inspections. Armed with limited information about why the report remains unmatched, the corresponding inspection can be onerous. The previously listed mechanisms, and the concept of applying a threshold to determine if certain transit records are “sufficiently” matched, are important for the IAEA because records are assigned a “MATCHED” label *with the underlying reason* for that label. For example, if two transit records have an above-threshold discrepancy in batch mass and/or number of items, the records are labeled as “partially” matched with the discrepancies observable to the IAEA. Having the ability to see the underlying mathematical reason as to why records have a certain match value can allow the IAEA to a) facilitate a match at a future point, and b) inform a more precise inspection plan of a related MBA.

4.0 Prototype DL

The prototype DL is demonstrated in this section via screenshots of the Hyperledger Composer Playground IDE. These screenshots illustrate the process for issuing identities (IDs) for participants in the blockchain, executing the different types of transactions, and viewing the immutable ledger.

4.1 Issuing IDs and Accessing Blockchain Network

Admins must create identities and issue new IDs for all participants. Under the *user tab*, select “ID Registry” (Figure 1).

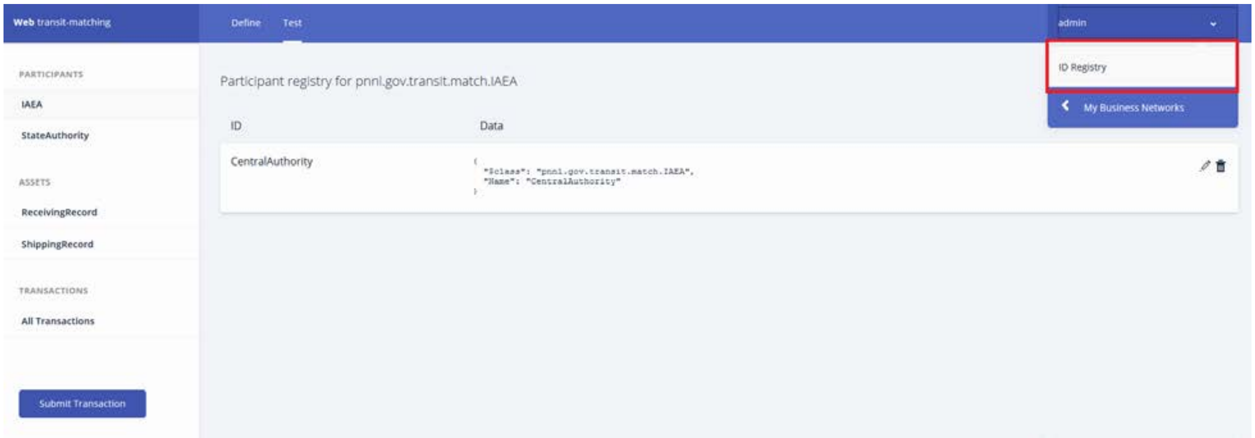

Figure 1. ID Registry

Click “Issue New ID” and an existing persona can now be issued an ID for use by clicking “Create New” (Figure 2).

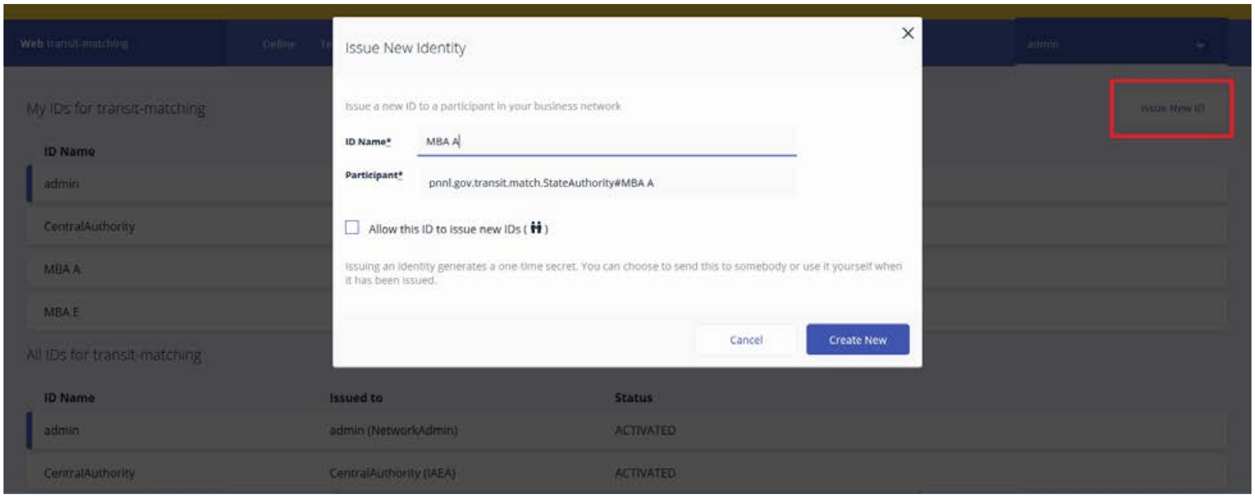

Figure 2. Issuing ID

Figure 3 shows the main page of the Composer Playground and the different IDs that can access the Transit-Matching blockchain network.

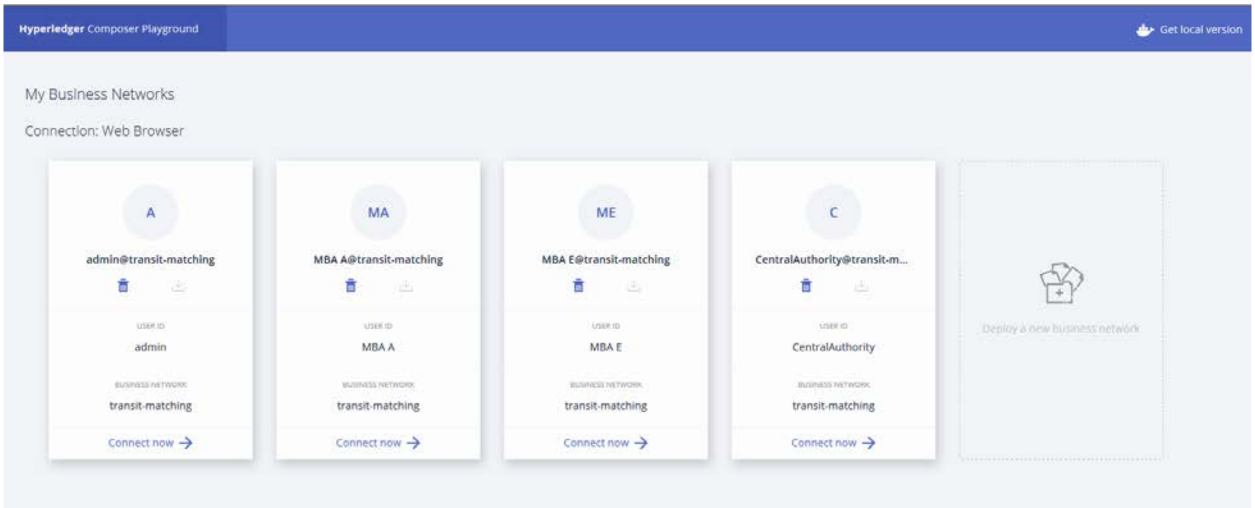

Figure 3. Main Page

4.2 Transactions

The “Submit Transaction” button within the test section is where a transaction would be submitted by a participant. Here, a participant chooses a transaction to execute (Figure 4):

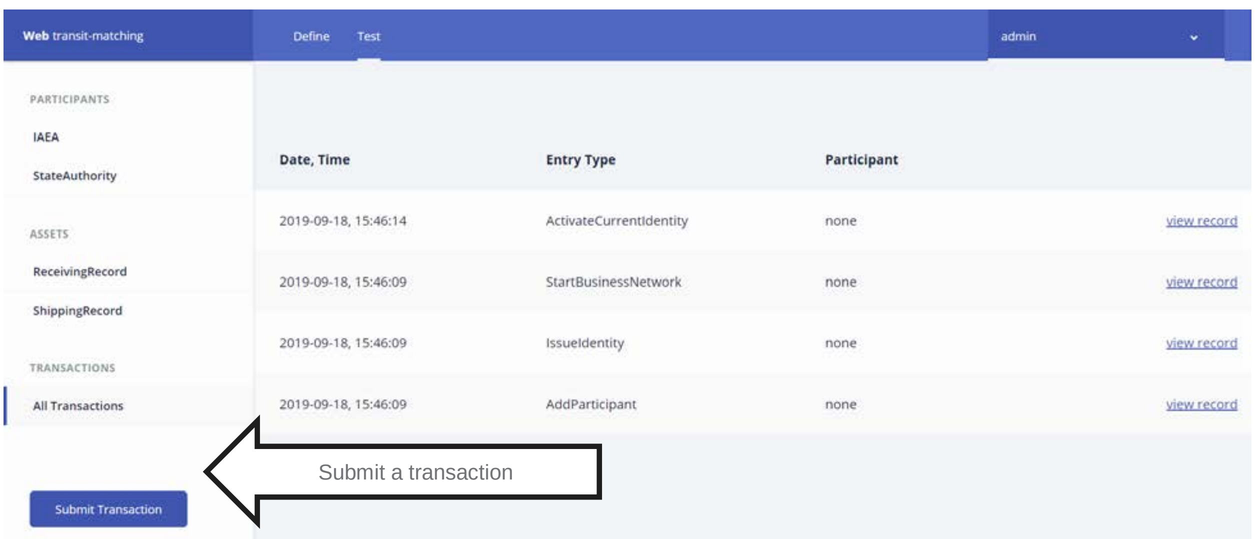

Figure 4. Transactions

As shown in Figure 5, a user chooses the transaction they want to execute.

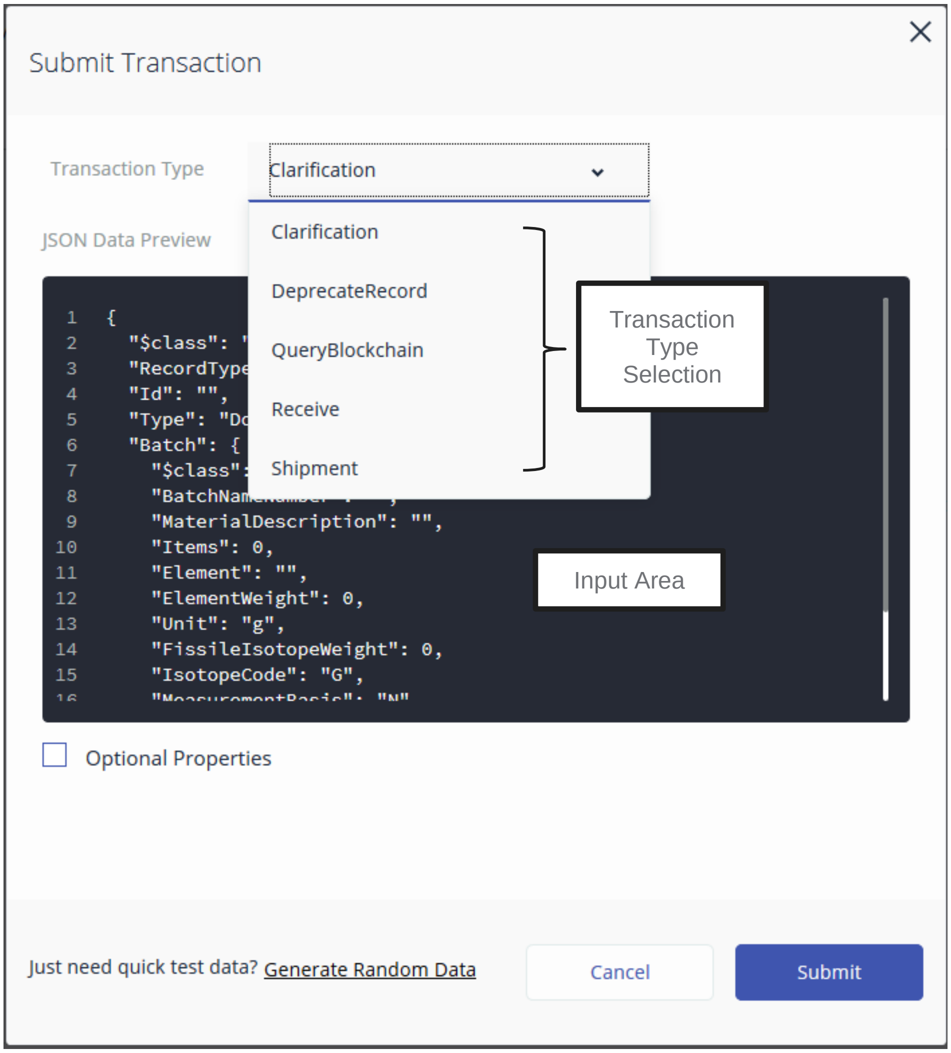

Figure 5. Submitting a Transaction

A **Shipment** transaction will generate a ShippingRecord.

A **Receive** transactions will generate a ReceivingRecord. Upon clicking “Submit,” the record will compare with all the existing ShippingRecords that do not have a match status of “MATCHED” or “DEPRECATED” according to the algorithm described above and detailed in Appendix A. Upon finding a partial match or a full match, a **MatchStatus** event will be attached to the ReceivingRecord with details of which record ID it matched with, the weight penalty, time penalty, and items penalty.

The **Clarification** transaction is visible to both the StateAuthority and CentralAuthority participants; however only the CA can make changes to existing records. Upon clicking “Submit” the record will be updated and a field will be added to the record stating who made the latest change. An algorithm will check for matched records of the opposing record type and update the “Match” field if a partial match or full match is discovered. An event, **ClarificationNotice**, will also be attached to every Clarification transaction stating who modified the record and the change time and date of the change.

The **DeprecateRecord** transaction requires an input of an ID and record type, and will change the “Match” field of the record to “DEPRECATED.” An original record will deprecate when a SA edits a record. The original entry deprecates, while the new one is used for matches. The deprecated record will exist for auditing purposes but will not be available to match with other records.

The **QueryBlockchain** transaction is only available to the CentralAuthority participants. A number of true/false choices are available to specify the view of the aggregated data from the blockchain. First, the participant must choose the record type (ShippingRecord/ReceivingRecord) and mark the queries they would like to view: “Find all matched”, “partial matches”, “unmatched”, “deprecated”, “corrected” and “clarified” records. The distinction of corrected records are the “Clarification” transactions submitted by StateAuthority participants, and the clarified records are the “Clarification” transactions submitted by CentralAuthority participants.

4.3 Viewing the Ledger

All transactions can be viewed by clicking the “All Transactions” section within “Transactions.” Specifics of any record, including the “Events,” can be viewed by clicking the “view record” link within the “Transactions” section. See Figure 6 and Figure 7 show an example ledger “Receive” transaction, followed by the event that was emitted with it.

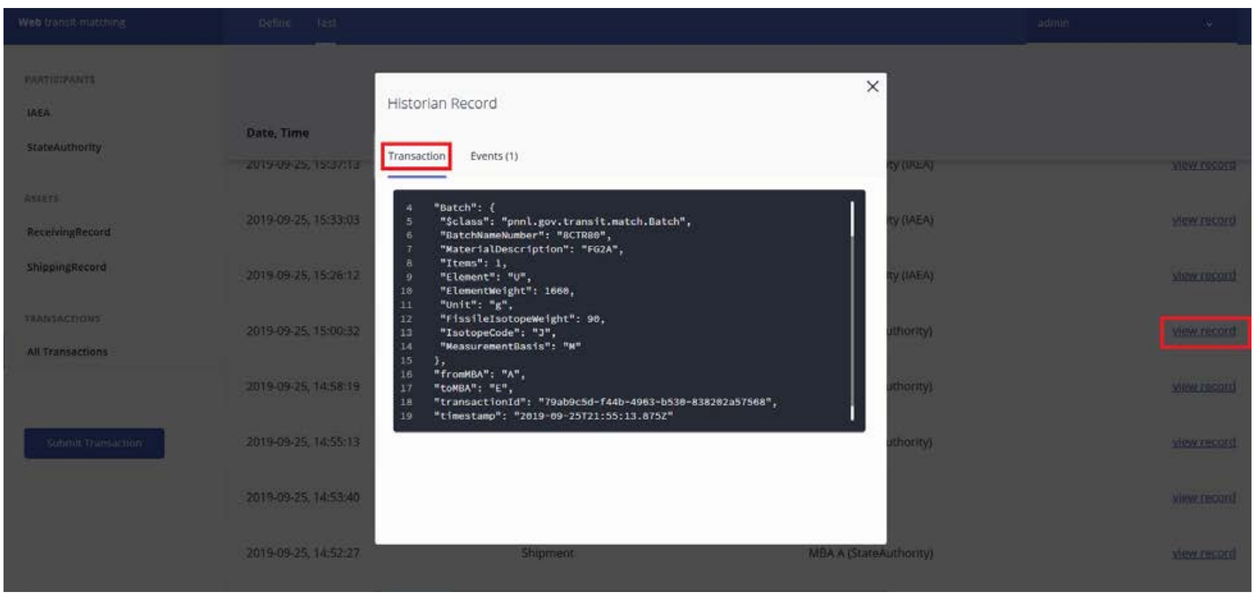

Figure 6. Historian Transaction

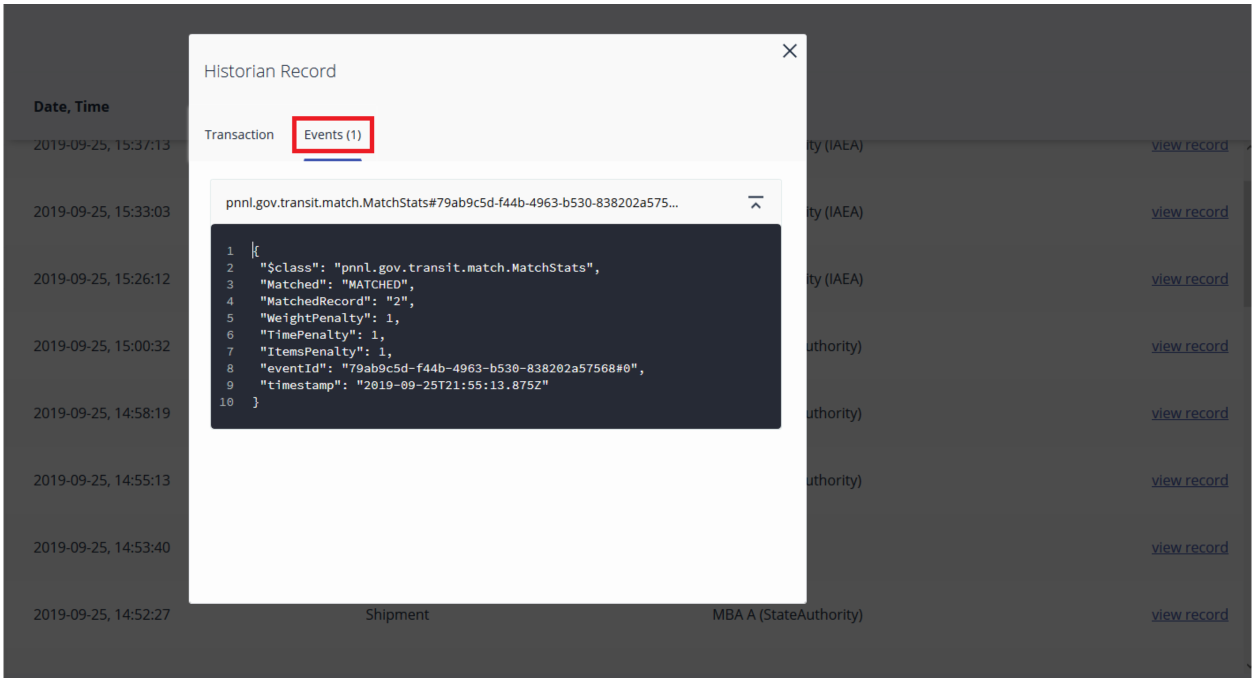

Figure 7. Historian Event

5.0 Outcomes

As discussed in this document, PNNL developed a prototype ledger that may potentially improve timeliness of detection of diversion of nuclear material while providing all parties involved with an tamper-proof record of transactions. Specifically, a DL designed for transit matching could improve the efficiency of the transit matching process through real-time match attempts of all transactions posted to the ledger. Meanwhile, a graded score applied to each match attempt could help inform inspection activities, thereby increasing the effectiveness of safeguards inspection activities. Performing these functions on a tamper-evident record of transactions increases confidence in IAEA safeguards conclusions through transparent reconciliation of transit matching reports.

Of the three findings observed in this study, the first two are supportable by currently available automated workflow environments, in addition to a DL. Meanwhile, the third key finding is enabled only by the immutability and cryptographic surety that the blockchain provides—this is what makes the DL technology stand out from the computer science software/tools available today.

5.1 Future Plans

The work conducted by PNNL in FY2019 can be further expanded upon in several ways:

- **Incorporating the physical inventory listing and MBR into the Hyperledger Fabric to account for re-batching**: As stated previously, the team debated whether an MBA re-batching process, as recorded in the ICR, was occurring *within* an MBA or *between* MBAs when the batch was being renamed. The team eventually settled on renaming batches being part of a mass balance problem and not part of the transit matching process, and in fact would not affect the transit matching process within the blockchain. The next step in the development and improvement of the DL is to incorporate the mass balance problem into the process and test whether the more complex transactions still support the initial hypothesis of this study.

- **Port the business network with the code to a custom blockchain and test with various parties (move from Composer Playground IDE)**: The Composer Playground is a convenient framework to quickly build and test business networks and conduct transactions. However, two different users are not able to sign on to the IDE and access the same Hyperledger's blockchain from two different computers using the same BNA to conduct transactions independently. Future researchers may wish to deploy a newly created Hyperledger Fabric instance instead.

  Additionally, it was discovered that Access Control Language (ACL) rules, which are applied to the results of queries, restrict what information is returned from a query for a specific participant (i.e., the list of assets returned by a query are processed by the ACL rules and only those that are allowed are added to the results returned). Because of this limitation, all SAs had to be able to read each other's records in order to find matches with other SA records, which would not be feasible under today's safeguards system.

  The current IDE setup is a convenient way to conduct current research and develop a quick prototype using Hyperledger. The next step would be to deploy the Business Network in a Hyperledger Fabric instance with multiple organizations and actors to fully test the blockchain. Further research will be necessary to determine if development should continue in a blockchain that is more malleable or perhaps build a blockchain from scratch.

- **Add graphical user interface for users:** Lastly, an average user must have an easy and intuitive way of navigating the transit matching Hyperledger. This will also allow the user to analyze and understand the current data. Therefore, further efforts should concentrate on creating a graphical user interface that acts as an interface and connects to the Hyperledger back-end.

Appendix A – DL System Design

Safeguards Blockchain Design

Cliff Joslyn, Sarah Frazar, Rus Goychayev, Alysha Randall

Revised November, 2019

Contents

List of Tables

1 Assumptions and Questions

1. In real life material balance areas (MBAs) submit one or more inventory change reports (ICRs) containing one or more lines, labeled by "Report #", and included a number of disinct, numbered pages, on a roughly monthly basis. Here we will assume that each MBA has a single rolling ICR with an indefinitely growing number of lines. Thus for us, months don't matter, and in fact, there are no ICRs proper, but rather ICR lines. MBA and ICR line number as thus sufficient to identify any ICR line.

Description	Notation	Type	Note/Restriction
Code	C	`String`	See below, from Code 10
From MBA	$Mf = j$	`Unsigned`	For some $1 \leq j \leq N$.
To MBA	$Mt = j$	`Unsigned`	For some $1 \leq j \leq N$.
Time	t	`Date`	Date stamp.
Batch Name	B	`String`	
Items	I	`Unsigned`	
Material Description	D	`String`	As specified in Code 10.
Element	E	`Char`	As specified in Code 10.
Weight	W	`Unsigned Float`	The weight of element E.
Unit	u	`String`	Units 'g' or 'Kg'.
Isotope Code	c	`Char`	One of 'G', 'J', or 'K'.
Correction	ρ	`Unsigned`	> 0=ICR line corrected

Table 1: ICR fields.

2. The following are unresolved:
   - Can matched shipping lines be at different times?
   - Can matched receiving lines be at different times?
   - Is the 60 day window over the whole set of times?
3. The below only addresses the transit matching problem. The material balance is not addressed.
4. We do not believe facility to be relevant.
5. "KMP code", "weight of fissile isotopes", and "measurement basis" are not addressed.

2 ICR Lines

Assume a set of N MBAs, denoted by $M^i, 1 \leq i \leq N$.

2.1 ICR Line Syntax

Let L^i_k be the k'th line of the ICR of the reporting MBA M^i, for $k > 0$. Lines are of the form

$$L^i_k = \langle C, Mf, Mt, t, B, I, D, E, W, u, c, \rho \rangle,$$

whose components are listed in Table 1.

2.2 ICR Line Issues and Constraints

- For convenience, each of the above may appear scripted, so e.g. E^i_k is the element of the k'th line of MBA i's ICR.

ICR Code	Blockchain record type	Blockchain record notation	Authority	Record Type	Comment
SD	SD	S_k^i	State	Transit: ICR	Ship domestic
SF	SF	S_k^i	State	Transit: ICR	Ship foreign
RD	RD	R_k^i	State	Transit: ICR	Receive domestic
RF	RF	R_k^i	State	Transit: ICR	Receive foreign
	CP	P_k^i	Central	Transit: Clarification	Batch increase
	CM	M_k^i	Central	Transit: Clarification	Batch decrease
	AT		Central	Match	Complete transit match
	AP		Central	Match	Partial transit match

Table 2: Blockchain record types.

- MBAs can only report on the *own* activity. Specifically, for each ICR line L_k^i, either $Mf_k^i = M^i$ or $Mt_k^i = M^i$, but not both.
- Reporting MBA i and reporting date t are non-sensitive. All other fields are sensitive.
- Lines must be sequential in time, so that for two lines $L_k^i, L_{k'}^i$, $k < k'$ iff $t_k^i < t_{k'}^i$.
- For corrections, $\rho_k^i = 0$ indicates that there is no correction, while $\rho_k^i > 0$ indicates that line $L_{\rho_k^i}^i$ is deleted (more specifically, that its MatchStatus is set to DEPRECATED, see Sec. 3.1).
- It is required that $\rho_k^i < k$, so that only past lines can be corrected by future lines.

2.3 ICR Codes

ICR lines are coded by C_k^i, and these codes put constraints on some of the other values, which have to be checked for:

Shipping, SD or SF: Sending MBA $Mf = M^i$ sends to MBA Mt.

Receiving, RD or RF: Receiving MBA $Mt = M^i$ receives from MBA Mf.

3 Blockchain

Establish a blockchain $\mathcal{B}$ containing records of different types, see Table 2.

3.1 Transit Records

Transit records are claims as to outgoing shipments, incoming receptions, or adjustments to quantities of material. All transit records are appended with a MatchStatus field, with the following possible values:

UNMATCHED (default): Line L_k^i is available for matching.

MATCHED: Line L^i_k has been matched within the matching threshold, and is no longer available for matching.

PARTIAL: Line L^i_k has been matched, but *not* within the matching threshold, and remains available for matching.

DEPRECATED: Line L^i_k has been corrected by a subsequent line $L^i_{k'}$, or clarified by the central authority, and is no longer available for matching.

- Unmatched and Partially matched records are called Unmatched Transits (UTs).
- All records have MatchStatus=UNMATCHED when created.
- MatchStatus is not sensitive.

3.1.1 ICR Records

Establish four Transit:ICR blockhain record types, one for each ICR code, including all ICR data fields. These are claims by MBAs about ICR activity. Shipment records with ICR codes SD and SF are notated as S^i_k, while receipt records for ICR codes RD and RF are notated as R^i_k.

If $\rho^i_k > 0$, then the MATCHSTATUS for line $L^i_{\rho^i_k}$ is set to DEPRECATED.

3.1.2 Clarification Records

Establish two Transit:Clarification blockchain record types which do not correspond to ICR codes. These are claims by central authority about corrections to ICR activity. While not claims by a state authority, they are given ICR lines for a particular MBA i, and thus invested with a distinct new ICR line number k.

Clarification Increase CP: Central authority is using code C =CP to record that MBA i on line L^i_k is increasing batch B by weight W. Notated P^i_k. Weight W^i_k will be positive.

Clarification Decrease CM: Central authority is using code C =CM to record that MBA i on line L^i_k is decreasing batch B by weight W. Notated M^i_k. Weight W^i_k will be negative.

- Clarification records have only a reporting MBA i, shipping and receiving MBAs Mf, Mt are null.
- The intention is that there be zero or one, but not more, clarification records, either CM or CP, for any batch B for any MBA i.

3.2 Match Records

These are claims by the central authority that certain collections of UTs (unmatched or partial transit records) are "good" matches.

Transit match records are of the form $\langle i, k, j, l, k', l', \Sigma \rangle$, where:

- There is a transit record UT S_k^i with recipient MBA $Mt = M^j$;
- There is a transit record UT R_l^j with shipping MBA $Mf = M^i$;
- k' and l' indicate the existence of optional clarification record UTs $*_{k'}^i, *_{l'}^j$, where $*$ is either P or M, for MBAs i and j respectively. k' or l' may be zero, indicating that there is no clarification record for MBA i or j, respectively. If so, then the corresponding weights $W_0^i, W_0^j = 0$. It is also required that $k' \cdot l' = 0$, so that only up to one clarification record is present for the match.
- The shipping and receiving elements are the same: $E_k^i = E_l^j$; and
- The shipping and receiving batch names are the same: $B_k^i = B_l^j$.

Matches are scored as $\Sigma = \prod \sigma_\bullet$ for a sequence of **score penalties** $0 < \sigma_\bullet \leq 1$, so that $0 < \Sigma \leq 1$. $\Sigma = 1$ means that it's a perfect match. Penalties are as follows, also incorporating **penalty weighting factors** $w_\bullet$ which should be tuned as as needed:

Weight Penalty: The (optionally clarified) shipping and receiving weights should be proportionately close:

$$\sigma_W = w_W \cdot \left(\left| \ln \left(\frac{W_k^i + W_{k'}^i}{W_l^j + W_{l'}^j} \right) \right| + 1 \right)^{-1}$$

where weights W are scaled appropriately for shipping and receiving units u_k^i, u_l^j. If desired, a **weight deminimus threshhold** ϵ_W can be established, so that instead

$$\sigma_W = \min \left(1, w_W \cdot \left(\left| \ln \left(\frac{W_k^i + W_{k'}^i}{W_l^j + W_{l'}^j} \right) \right| + 1 \right)^{-1} + \epsilon_W \right)$$

so that there is no penalty for discrepancies below deminimus.

Time Penalty: The shipping and receiving dates should be close enough in time. Establish a **time deminimus** ϵ_t, typically 60 days. The gaps between shipping and receiving dates larger than that should be penalized:

$$\sigma_t = \frac{w_t}{\max(0, t_k^i - t_l^j - \epsilon_t) + 1}$$

Items Penalty: No deminimus here, items really have to match.

$$\sigma_I = \frac{w_I}{|I_k^i - I_l^j| + 1}$$

Assume a global **match threshold** Θ.

- If $\Sigma \leq \Theta$ so that the match score is below the threshold, then the match is deemd **complete**. Then a complete match record AT is posted to $\mathcal{B}$, and the MatchStatus field for ICR lines L_k^i and L_l^j, and if $k', l' > 0$, then $L_{k'}^i, L_{l'}^j$, are set to MATCH, and are no longer available for other matches.
- If $\Sigma > \Theta$, then the match is deemd **partial**, a partial match record AP is posted to $\mathcal{B}$, and the MatchStatus field for ICR lines L_k^i and L_l^j, and if $k', l' > 0$, then $L_{k'}^i, L_{l'}^j$, are set to PARTIAL, and remain available for other matches.

4 More Blockchain Details

4.1 Data Sensitivity

Reporting MBA i, reporting date t, and MatchStatus are non-sensitive. All other fields are sensitive.

4.2 Users and Permissions

There are three user types:

State Authorities (SA): SAs compile ICR lines from their MBAs, and have the rights to publish and observe all of their shipping SD and SF and receiving RD and RF; and to observe all non-sensitive information in the blockchain $\mathcal{B}$.

Central Authority (CA): The IAEA and possibly others have the right to publish clarification CM and CP records, and matching AT records; and to observe all information in the blockchain $\mathcal{B}$.

Observers (O): Other users have the right to observe the blockchain $\mathcal{B}$ and all non-sensitive data.

Appendix B – ICR Surrogate Data

INVENTORY CHANGE REPORT (ICR) FORM R.01.1/c

COUNTRY..................
FACILITY.................................
MATERIAL BALANCE AREA......MBA A......

PERIOD COVERED BY REPORT FROM.................. TO.........................
REPORT NO..................................
PAGE NO...... OF ....PAGES
SIGNATURE

	ENTRY NO.	CONTINUATION	DATE OF INVENTORY CHANGE	MBA/COUNTRY FROM	MBA/COUNTRY TO	TYPE OF INVENTORY CHANGE	KMP CODE	NAME OR NUMBER OF BATCH	NUMBER OF ITEMS IN BATCH	MATERIAL DESCRIPTION	ELEMENT	WEIGHT OF ELEMENT	UNIT kg/g	WEIGHT OF FISSILE ISOTOPES (URANIUM ONLY) (g)	ISOTOPE CODE	MEASUR. BASIS	CONCISE NOTE	CORRECTION TO: REPORT NO.	CORRECTION TO: ENTRY NO.	1
	1	3	4	10	14	18	20	21	29	33	37	38	46	48	56	72	73	74	78	80
*	1			MBA A	MBA G	SD	513	ATG61Z	1	BQ2F	N	800	g	7	G	M				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2

INVENTORY CHANGE REPORT (ICR) FORM R.01.1/c

COUNTRY..................
FACILITY.................................
MATERIAL BALANCE AREA......MBA B......

PERIOD COVERED BY REPORT FROM.................. TO.........................
REPORT NO..................................
PAGE NO...... OF ....PAGES
SIGNATURE

	ENTRY NO.	CONTINUATION	DATE OF INVENTORY CHANGE	MBA/COUNTRY FROM	MBA/COUNTRY TO	TYPE OF INVENTORY CHANGE	KMP CODE	NAME OR NUMBER OF BATCH	NUMBER OF ITEMS IN BATCH	MATERIAL DESCRIPTION	ELEMENT	WEIGHT OF ELEMENT	UNIT kg/g	WEIGHT OF FISSILE ISOTOPES (URANIUM ONLY) (g)	ISOTOPE CODE	MEASUR. BASIS	CONCISE NOTE	CORRECTION TO: REPORT NO.	CORRECTION TO: ENTRY NO.	1
	1	3	4	10	14	18	20	21	29	33	37	38	46	48	56	72	73	74	78	80
	1			MBA F	MBA B	RF	P1	ST3PM	1	FW1F	E	10	g	2	G	M				2
	2			MBA F	MBA B	RF	P6	RMF76Z	3	BD1A	E	15	g	2	G	M				2
	3			MBA E	MBA B	RD	P6	CAR47I	1	DJ1J	P	7	g			M				2
	4			MBA D	MBA B	RD	L15	P4TSM	2	NJ8E	U	32	g	4	J	N				2
1-2 *	5			MBA D	MBA B	RD	L15	P4TSM	1	NJ8E	U	32	g	4	J	N				2
*	6			MBA D	MBA B	RM	L15	P4TSM	1	NJ8E	U	32	g	4	J	N				2
*	7			MBA D	MBA B	RP	L15	P4TSMA	1	NJ8E	U	16	g	2	J	N				2
*	8			MBA D	MBA B	RP	L15	P4TSMB	1	NJ8E	U	16	g	2	J	N				2
1-3 *	9			MBA C	MBA B	RD	D3	EL3M4	4	GG2C	N	200	Kg	158.2	G	M				2
*	10				MBA B	RM	D3	EL3M4	4	GG2C	N	200	Kg	158.2	G	M				2
*	11				MBA B	RP	D3	ABC1	1	GG2C	N	121	Kg	155.2	G	M				2
*	12				MBA B	RP	D3	ABC2	1	GG2C	N	23.5	Kg	1	G	M				2
*	13				MBA B	RP	D3	ABC3	2	GG2C	N	55.3	Kg	2	G	M				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2

INVENTORY CHANGE REPORT (ICR) FORM R.01.1/c

COUNTRY...................
FACILITY...................................
MATERIAL BALANCE AREA........MBA C........................

PERIOD COVERED BY REPORT FROM.................. TO...........................
REPORT NO...................................
PAGE NO...... OF ....PAGES | SIGNATURE

				MBA/COUNTRY							ACCOUNTANCY DATA							CORRECTION TO		1
	ENTRY NO	CONTINUATION	DATE OF INVENTORY CHANGE	FROM	TO	TYPE OF INVENTORY CHANGE	KMP CODE	NAME OR NUMBER OF BATCH	NUMBER OF ITEMS IN BATCH	MATERIAL DESCRIPTION	ELEMENT	WEIGHT OF ELEMENT	UNIT kg/g	WEIGHT OF FISSILE ISOTOPES (URANIUM ONLY) (g)	ISOTOPE CODE	MEASUR. BASIS	CONCISE NOTE	REPORT NO.	ENTRY NO.	
	1	3	4	10	14	18	20	21	29	33	37	38	46	48	56	72	73	74	78	80
*	1			MBA C	MBA B	SD	30	EL3M4	4	GG2C	N	200	Kg	158	G	M				2
	2			MBA D	MBA C	RD	57	PRT347	1	GG2C	D	373.7	g	27.6	K	M				2
	3			MBA E	MBA C	RD	03	7MRB	7	BU2G	E	562.2	g	75	G	M				2
	4			MBA E	MBA C	RD	75	48TBR	2	BU2G	N	1234	g	105.7	G	M				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2

INVENTORY CHANGE REPORT (ICR) FORM R.01.1/c

COUNTRY...................
FACILITY...................................
MATERIAL BALANCE AREA........MBA D........................

PERIOD COVERED BY REPORT FROM.................. TO...........................
REPORT NO...................................
PAGE NO...... OF ....PAGES | SIGNATURE

				MBA/COUNTRY							ACCOUNTANCY DATA							CORRECTION TO		1
	ENTRY NO	CONTINUATION	DATE OF INVENTORY CHANGE	FROM	TO	TYPE OF INVENTORY CHANGE	KMP CODE	NAME OR NUMBER OF BATCH	NUMBER OF ITEMS IN BATCH	MATERIAL DESCRIPTION	ELEMENT	WEIGHT OF ELEMENT	UNIT kg/g	WEIGHT OF FISSILE ISOTOPES (URANIUM ONLY) (g)	ISOTOPE CODE	MEASUR. BASIS	CONCISE NOTE	REPORT NO.	ENTRY NO.	
	1	3	4	10	14	18	20	21	29	33	37	38	46	48	56	72	73	74	78	80
	1			MBA D	MBA C	SD	605	PRT847	3	GG2C	D	373.7	g	27.6	K	M				2
	2			MBA D	MBA B	SD	PR	P4TSM	1	NJ8E	U	15	g	4	J	M				2
*	3			MBA E	MBA D	RD	7T	3CTP50	1	FG2A	U	1565	g	115	J	M				2
2-1 *	4			MBA E	MBA D	RD	7T	8CTR80	1	FG2A	U	1660	g	90	J	M				2
*	5				MBA D	RM	7T	3CTP50	1	FG2A	U	1565	g	115	J	M				2
*	6				MBA D	RM	7T	8CTR80	1	FG2A	U	1660	g	90	J	M				2
*	7				MBA D	RP	7T	BRST49	4	FG2A	U	3223.5	g	209	J	M				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2

INVENTORY CHANGE REPORT (ICR) FORM R.01.1/c

COUNTRY..................
FACILITY.................................
MATERIAL BALANCE AREA......MBA G......

PERIOD COVERED BY REPORT FROM.................. TO.........................
REPORT NO..................................
PAGE NO...... OF ....PAGES
SIGNATURE

	ENTRY NO.	CONTINUATION	DATE OF INVENTORY CHANGE	MBA/COUNTRY FROM	MBA/COUNTRY TO	TYPE OF INVENTORY CHANGE	KMP CODE	NAME OR NUMBER OF BATCH	NUMBER OF ITEMS IN BATCH	MATERIAL DESCRIPTION	ACCOUNTANCY DATA: ELEMENT	WEIGHT OF ELEMENT	UNIT kg/g	WEIGHT OF FISSILE ISOTOPES (URANIUM ONLY) (g)	ISOTOPE CODE	MEASUR. BASIS	CONCISE NOTE	CORRECTION TO: REPORT NO.	ENTRY NO.	1
	1	3	4	10	14	18	20	21	29	33	37	38	46	48	56	72	73	74	78	80
1-1 *	1			MBA A	MBA G	RD	16	ATG61Z	1	BQ2F	N	800	g	7	G	M				2
*	2			MBA G	MBAH	SF	2D1	BR1TC7	1	GQ2G	D	500	g	4	K	M				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2

INVENTORY CHANGE REPORT (ICR) FORM R.01.1/c

COUNTRY..................
FACILITY.................................
MATERIAL BALANCE AREA......MBA F......

PERIOD COVERED BY REPORT FROM.................. TO.........................
REPORT NO..................................
PAGE NO...... OF ....PAGES
SIGNATURE

	ENTRY NO.	CONTINUATION	DATE OF INVENTORY CHANGE	MBA/COUNTRY FROM	MBA/COUNTRY TO	TYPE OF INVENTORY CHANGE	KMP CODE	NAME OR NUMBER OF BATCH	NUMBER OF ITEMS IN BATCH	MATERIAL DESCRIPTION	ACCOUNTANCY DATA: ELEMENT	WEIGHT OF ELEMENT	UNIT kg/g	WEIGHT OF FISSILE ISOTOPES (URANIUM ONLY) (g)	ISOTOPE CODE	MEASUR. BASIS	CONCISE NOTE	CORRECTION TO: REPORT NO.	ENTRY NO.	1
	1	3	4	10	14	18	20	21	29	33	37	38	46	48	56	72	73	74	78	80
	1			MBA F	MBA B	SF	BRT	ST3PM	1	FW1F	E	10.3	g	2	g	M				2
	2			MBA F	MBA B	SF	255	RMF76Z	3	BD1A	E	15.9	g	2	g	M				2
*	3			MBA F	MBA E	SF	SPT	Z13P2	3	DD1F	N	3	Kg	600	G	M				2
*	4			MBA F	MBA E	SF	M2R	73Z72	1	FE2Z	D	6247.00	g	500	G	m				2
*	5			MBA F	MBA E	SF	B5	DLM54X	2	FG2A	E	700	g	79	G	m				2
*	6			MBA F	MBA E	SF	7T	B4ALM6	1	FG2A	E	35.2	g	3	G	m				2
*	7			MBA F	MBA E	SF	Z8	T1MX	2	GQ2D	T	7.3	Kg	97	G	m				2
2-3 *	8			MBA E	MBA F	RF	PL	BIRD5	1	FG3C	D	2361.9	g	400	G	m				2
*	9			MBA E	MBA F	RF	SMG	7ABR20	2	FJ4G	N	4.3	Kg	603.7	G	M				2
	10				MBA F	RM	B7	B1RD5	1	FG3C	D	2361.9	g	400	G	M				2
	11				MBA F	RM	B7	7ABR20	2	FJ4G	N	4.3	Kg	603.7	G	M				2
	12				MBA F	RP	B7	B1RD5A	6	FG35	D	2000	g	350	G	m				2
	13				MBA F	RP	B7	B1RD5B	2	FG35	D	35.2	g	50	G	M				2
	14				MBA F	RP	B7	7XMBT	2	F54G	N	603.7	Kg	603.7	G	M				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2
																				2

INVENTORY CHANGE REPORT (ICR) FORM R.01.1/c

COUNTRY..................
FACILITY................................
MATERIAL BALANCE AREA.........MBA H.........................

PERIOD COVERED BY REPORT FROM.................. TO.........................
REPORT NO..................................
PAGE NO...... OF ....PAGES
SIGNATURE

1 5 9 13 19 25 28 31 70 74 80

																			1
			MBA/COUNTRY						ACCOUNTANCY DATA								CORRECTION TO		
ENTRY NO.	CONTINUATION	DATE OF INVENTORY CHANGE	FROM	TO	TYPE OF INVENTORY CHANGE	KMP CODE	NAME OR NUMBER OF BATCH	NUMBER OF ITEMS IN BATCH	MATERIAL DESCRIPTION	ELEMENT	WEIGHT OF ELEMENT	UNIT kg/g	WEIGHT OF FISSILE ISOTOPES (URANIUM ONLY) (g)	ISOTOPE CODE	MEASUR. BASIS	CONCISE NOTE	REPORT NO.	ENTRY NO.	
1	3	4	10	14	18	20	21	29	33	37	38	46	48	56	72	73	74	78	80
1-1 * 1			MBA G	MBA H	RF	013	BR1TC7	1	BQ2F	D	500	g	4	K	M				2
																			2
																			2
																			2
																			2
																			2
																			2
																			2
																			2
																			2
																			2
																			2
																			2
																			2
																			2
																			2
																			2
																			2
																			2
																			2
																			2
																			2

Appendix C – Developer Notes

The Hyperledgers' business network framework feature three key components. The model file describes the objects and transactions while the script file determines the logic for executing transactions and events. The access control file describes the rules governing the permissions applied to participants. Lastly, an optional query file is used to extract specific data from the blockchain.

The PNNL model features two participants: StateAuthority and IAEA. The model also features two assets: ShippingRecord and ReceivingRecord, JSON example for ReceivingRecord:

```
asset ReceivingRecord identified by id {
 o String id
 o Type Type
 o Batch Batch
 o DateTime DateTime
 o String toMBA
 o String fromMBA
 --> StateAuthority SA // state authority owns this Batch/MBA
 o String LastModifiedBy default = ‘N/A’
 o Match Match default = 'UNMATCHED'
}
```

Batch is a concept:

```
concept Batch {
 o String BatchNameNumber
 o String MaterialDescription
 o Integer Items
 o String Element
 o Double ElementWeight
 o Unit Unit
 o Double FissileIsotopeWeight
 o IsoCode IsotopeCode
 o Measurement MeasurementBasis
}
```

Unit, IsoCode, Type, Measurement, and Match are all enums.

There are two events:

```
event MatchStats {
 o String Matched
 o String MatchedRecord
 o Double WeightPenalty
 o Double TimePenalty
 o Double ItemsPenalty
}

event ClarificationNotice {
 o String Message
}
```

Finally, there are five transactions.

```
transaction DeprecateRecord {
 o RecordType RecordType
 o String Id
}

transaction QueryBlockchain {
 o RecordType RecordType
 o Boolean FindAllMatchedRecords default = true
 o Boolean FindAllPartialMatchRecords default = false
 o Boolean FindAllUnmatchedRecords default = false
 o Boolean FindAllClarifiedRecords default = false
 o Boolean FindAllCorrectedRecords default = false
 o Boolean FindAllDeprecatedRecords default = false
}

transaction Clarification {
 o RecordType RecordType
 o String Id
 o Type Type
 o Batch Batch
 o String fromMBA
 o String toMBA
}

@returns(ShippingRecord)
transaction Shipment {
 o Type Type
 o Batch Batch
 o String fromMBA
 o String toMBA
}

transaction Receive {
 o Type Type
 o Batch Batch
 o String fromMBA
 o String toMBA
                                   }
```

Limitations and Future Development

1. In Hyperledger Composer it was discovered that ACL rules applied to the results of queries allow the restriction of what information is returned from a query for a specific participant (i.e., the list of assets returned by a query is processed by the ACL rules and only those that are ALLOWED are added to the results returned). Because of this limitation, All StateAuthorities had to be able to read each other's records to find matches with other StateAuthority records'.
2. Composer Playground offered a small sandbox for one developer to make a rudimentary prototype but is not ideal for testing at scale or demonstration purposes. Solutions include:

a. Create independent blockchain of governance.
b. Create user interface to better display results and design.
c. Implement a full scale Peer-To-Peer network where each user’s computer becomes a file server as well as a client.

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov