Pacific Northwest
NATIONAL LABORATORY

PNNL-30525

Exploration of Potential Application of Distributed Ledger Technology for Managing Transactions Under Joint Technology Development and Transfer Agreements

September 2020

1 Sarah L Frazar
2 Rustam Goychayev
3 Alysha Randall
4 Cliff Joslyn
5 Aaron Melville
6 Kevin Whattam

U.S. DEPARTMENT OF ENERGY

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

DISCLAIMER

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

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
www.osti.gov
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

PNNL-30525

Exploration of Potential Application of Distributed Ledger Technology for Managing Transactions Under Joint Technology Development and Transfer Agreements

September 2020

1 Sarah L Frazar
2 Rustam Goychayev
3 Alysha Randall
4 Cliff Joslyn
5 Aaron Melville
6 Kevin Whattam

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

Pacific Northwest National Laboratory
Richland, Washington 99354

Executive Summary

In 2017, the Pacific Northwest National Laboratory (PNNL) initiated a project exploring distributed ledger technology (DLT) applications for export control. The resulting study, which was delivered to the National Nuclear Security Administration (NNSA) Office of Nonproliferation and Arms Control (NPAC), identified two export control use cases for future exploration: 1) the authorization processes governed by Part 810 of Title 10, Code of Federal Regulations and managed by the website e810 and 2) validation and verification of export license with shipping documentation.[1] The study also referenced NPAC management's suggestion to examine a new use case, namely intellectual property (IP) transactions occurring under a joint technology development and transfer agreement (JTDTA). This document summarizes the findings from the team's evaluation of the JTDTA use case.

As part of this examination, PNNL focused on addressing whether DLT could be used to manage transactions occurring under a JTDTA to promote civil nuclear cooperation without raising proliferation concerns. PNNL further dissected this question into two separate, but related challenges of concern to parties of JTDTAs:

- Strengthening the monitoring and enforcement of IP protections applied to nuclear-related materials and technology developed and exchanged under a JTDTA; and
- Detecting or deterring the misuse of protected, nuclear-related material or technology developed and transferred under the JTDTA, an issue of particular concern to the U.S. Government.

Strengthening IP enforcement can help protect national commercial interests, thereby providing a critical incentive for parties to participate in these agreements. Failure to prevent technology misuse raises the proliferation risk associated with these types of collaborative arrangements, which can disincentivize parties from participating in them. Indeed, in 2018, a JTDTA Implementing Arrangement between the United States and China, along with associated license application reviews involving the development and transfer of technologies relating to the Travelling Wave Reactor (TWR),[2] were halted due to concerns over the illegal diversion of civil nuclear technology for military or unauthorized purpose. There is value to the U.S. Government to determine whether new technologies, such as DLT, could address these issues simultaneously in measurable, cost-effective ways.

This research suggests that while DLT <u>can</u> be used to strengthen IP protections between authorized parties to a JTDTA, it does not provide a <u>unique</u> solution for addressing this challenge. Moreover, DLT is not readily a capability that can be targeted to prevent technology misuse. *The particular capabilities and advantages of DLT systems are not significant compared to the capabilities of other, well-established technologies that can be used to document transfers of ownership, monitor access to protected information, and support legal enforcement of IP infringement. DLT may introduce additional efficiencies to the process via use*

[1] Frazar S, M Schanfein, K Jarman, C West, C Joslyn, S Winters, S Kreyling and A Sayre. 2017. "Exploratory study on potential safeguards applications for shared ledger technology," Pacific Northwest National Laboratory, February 2017. PNNL-26229.

[2] U.S. Department of Energy. "DOE Announces Measures to Prevent China's Illegal Diversion of U.S. Civil Nuclear Technology for Military or Other Unauthorized Purposes." 11 October 2018. Available at: https://www.energy.gov/articles/doe-announces-measures-prevent-china-s-illegal-diversion-us-civil-nuclear-technology. Accessed on 3 September 2020.

of secure automated workflows, but this benefit may not be worth the cost of political or technical investment to deploy DLT for this purpose. Regarding the challenge of technology misuse, neither existing technologies nor DLT prevent parties from misusing technologies for use in a nuclear weapons program.

Based on these findings, PNNL recommends that NNSA explore the full suite of functions and capabilities in existing software and database applications. NNSA also should engage with the developers of e810 to understand the extent to which a DLT platform might be integrated with existing software and database solutions. PNNL does not recommend considering current DLT platforms as a solution that could prevent unauthorized users from obtaining and sharing sensitive information outside of the JTDTA context.

Acronyms and Abbreviations

AEA	Atomic Energy Act
DLT	distributed ledger technology
DOE	U.S. Department of Energy
IA	information artifacts
IAM	identity access management
IP	intellectual property
JTDTA	joint technology development and transfer agreement
NNSA	National Nuclear Security Administration
NPAC	Nonproliferation and Arms Control
NRC	U.S. Nuclear Regulatory Commission
PNNL	Pacific Northwest National Laboratory
TWR	Travelling Wave Reactor

Contents

1.0 Introduction

In 2017, the Pacific Northwest National Laboratory (PNNL) initiated several projects aimed at exploring the potential application of distributed ledger technology (DLT) to nonproliferation challenges. Between 2017 and 2018, PNNL explored whether and how DLT might benefit international safeguards. In the process, PNNL identified several use cases involving digital transactions for future exploration and developed a methodology for evaluating those use cases to determine which, if any, might benefit from DLT deployment.[3,4] This methodology aims to evaluate each use case using a standard approach to identify objective indicators as to whether DLT might benefit, or even potentially disadvantage, a particular use case.

In parallel, PNNL initiated a separate project exploring DLT applications for export control, applying the same methodology to seven use cases devised in 2018.[5] This project resulted in a study delivered to the National Nuclear Security Administration (NNSA) Office of Nonproliferation and Arms Control (NPAC) in 2018. That study identified two export control use cases for future exploration: 1) the authorization processes governed by Part 810 of Title 10, Code of Federal Regulations,[6] managed by the website e810,[7] and 2) validation and verification of export license with shipping documentation. It also referenced NPAC management's suggestion to apply the evaluation methodology to an eighth use case, namely intellectual property (IP) transactions occurring under a joint technology development and transfer agreement (JTDTA). This document summarizes the findings from the team's evaluation of the JTDTA use case.

As part of this exploration, PNNL sought to address the question of whether and how DLT might support joint technology development or transfer for the purpose of promoting U.S. nonproliferation objectives and civil nuclear cooperation between two countries. In this context, PNNL specifically examined two separate but related challenges of concern to parties of JTDTAs:

- Strengthening the monitoring and enforcement of IP protections applied to nuclear-related materials and technology; and
- Detecting or deterring parties from misusing protected, nuclear-related material or technology that was developed and transferred under the JTDTA, an issue of particular concern to the U.S. Government.

With regard to the first challenge, IP protections typically include copyright, patent, trade secrets, etc., and are applied by one party to protect its unique idea, concept, or invention, or

[3] Frazar S, M Schanfein, K Jarman, C West, C Joslyn, S Winters, S Kreyling and A Sayre. 2017. "Exploratory study on potential safeguards applications for shared ledger technology," Pacific Northwest National Laboratory, February 2017. PNNL-26229

[4] Frazar S, C Joslyn, R Singh and A Sayre. 2018. "Evaluating Safeguards Use Cases for Blockchain Applications," Pacific Northwest National Laboratory, February 2018. PNNL-28050

[5] Frazar S, C Joslyn and GT Hoffman. 2018. "Evaluating Export Control Use Cases for Distributed Ledger Technology: Interim Report." Pacific Northwest National Laboratory, October 2018. PNNL-28777.

[6] Assistance to Foreign Atomic Energy Activities, 10 C.F.R § 810.6. (2011). Available at: https://www.ecfr.gov/cgi-bin/text-idx?SID=654145adc6ebe16a58aeeb82fb5381e8&mc=true&node=pt10.4.810&rgn=div5.

[7] The e810 site allows exporters of nuclear technology to submit and track their license requests and General and Specific Authorization reports with DOE/NNSA. This website is centrally maintained by DOE/NNSA. More information can be found at https://e810.energy.gov/FAQ/Index

jointly by parties that collaborated in the development of the unique idea, concept, or invention. Strengthening IP enforcement provides a critical incentive for parties to participate in these agreements, thereby protecting national interests while promoting civil nuclear cooperation between two countries.

With regard to the second challenge, whenever one party retransfers something of value to another party (for this use case a foreign party), there is a risk that the other party may misuse the item or information. In the case of a JTDTA, any party to the agreement has the potential to misuse protected nuclear material or technology that was jointly developed and/or transferred under the JTDTA. This can be done either by creating counterfeit versions of nuclear-related materials or technologies or retransferring them to unauthorized parties, both of which can be used in clandestine nuclear programs. Notably, a JTDTA Implementing Arrangement between the United States and China and associated license application reviews involving the development and transfer of technologies relating to the Travelling Wave Reactor (TWR)[8] was halted in 2018 due to concerns over the illegal diversion of civil nuclear technology for military or unauthorized purpose.

Given these two challenges, it is worth considering whether emerging technologies, such as DLT, might strengthen IP enforcement while also preventing unauthorized transfer of protected, sensitive nuclear technology. Addressing these challenges might create a compelling incentive for parties to return to the table to promote civil nuclear cooperation without raising proliferation concerns.

This research suggests that while DLT <u>can</u> be used to strengthen IP protections between authorized parties to a JTDTA, it does not provide a <u>unique</u> solution for addressing this challenge. Moreover, DLT is not readily a capability that can be targeted to prevent technology misuse. *DLT can be used to document transfers of IP-protected technology between authorized parties to a JTDTA. However, the particular capabilities and advantages of DLT systems are not significant compared to the capabilities of other well-established technologies that can be used to document transfers of ownership, monitor access to protected information, and support legal enforcement of IP infringement. DLT may introduce additional efficiencies to the process via use of secure automated workflows, but this benefit may not be worth the cost of political or technical investment to deploy DLT for this purpose. Regarding the challenge of technology misuse, neither existing technologies nor DLT prevent parties from misusing technologies to create counterfeit products or retransfer to unauthorized parties for use in a nuclear weapons program.*

The following sections provide a brief summary of DLT functionality and potential value proposition for parties to JTDTAs, an exemplar JTDTA use case, the methodology used to evaluate the exemplar use case, a summary of findings, and recommendations for consideration.

[8] U.S. Department of Energy. "DOE Announces Measures to Prevent China's Illegal Diversion of U.S. Civil Nuclear Technology for Military or Other Unauthorized Purposes." 11 October 2018. Available at: https://www.energy.gov/articles/doe-announces-measures-prevent-china-s-illegal-diversion-us-civil-nuclear-technology. Accessed on 3 September 2020.

2.0 Summary of Distributed Ledger Technology

DLT refers to a broad class of digital, cryptographic, distributed ledgers that store transactions between people or entities. Blockchains are the primary technologies used in successful distributed ledgers, for example being the underlying technology that facilitates Bitcoin transactions. Blockchains were designed to disrupt the traditional paradigm of trust in financial systems, where a centralized authority such as a bank retains a single, authoritative copy of a transaction ledger. In blockchain-enabled systems, cryptographic algorithms operating on a shared, public database replace the role of the bank, enabling parties to retain their own copy of a cryptographically secure ledger and validate the surety of all transactions posted on the ledger. Blockchain systems, and DLT more broadly, store information such as account balances, asset ownership, state of transactions, or any data into blocks that are chained together cryptographically to assure validity and immutability. The improvement in security, efficiency, trust, and transparency offered by DLT makes it attractive to entities that seek to avoid either needing to trust each other or to jointly invest their trust in a central authority to manage the process.

Returning to the JTDTA context, the parties to the agreement presumably already trust each other sufficiently to collaborate, but the risk of technology misuse for national interests sustains a certain level of mistrust that is currently mitigated through standard legal agreements, export licenses, and IP controls—all of which are difficult to enforce because parties can simply download and copy or photograph protected information. The distribution of DLT systems and reliance on computer algorithms to provide cryptographic surety of transactions posted on the ledger suggested not only that protected information could remain secure through their use but also that violations might be more easily enforced. The potential for DLT to protect sensitive information while promoting confidence and trust among JTDTA parties was thus sufficiently attractive to nuclear professionals as to warrant the further examination.

3.0 Summary of Joint Technology Development and Transfer Agreement Use Case

Joint technology development and transfer agreements are both generally common and tailored to meet the needs of the associated parties. Universities, research institutions, and commercial companies have entered these types of agreements for years to advance the development of their respective inventions for future commercialization.[9] While JTDTAs involving nuclear-related technologies are not as common, variation among the terms and conditions of those agreements and associated agreements and legislation warranted establishment of a reference JTDTA for the purpose of this project.

PNNL's reference JTDTA is based on the 2018 Implementing Arrangement established between the United States and China to cover the joint development and transfer of technology

[9] Himmelrich NT. "Technology Transfer Agreements: Don't be an Amateur." Gordon Feinblatt, LLC. 17 December 2001. Available at: https://www.gfrlaw.com/what-we-do/insights/technology-transfer-agreements-don%E2%80%99t-be-amateur#:~:text=A%20Tech%20Transfer%20agreement%20is,Transfer%20must%20recognize%20outside%20interests. Accessed on 4 September 2020.

associated with the TWR.[10] This 2018 Implementing Arrangement was established in accordance with the Atomic Energy Act of 1954, as amended (AEA), and under the Agreement for Cooperation Between the United States and the People's Republic of China Concerning Peaceful Uses of Nuclear Energy of [July 23, 1985] (also referred to as the U.S.-China "123 Agreement" after the relevant section of the AEA). The Implementing Arrangement serves as the Special Authorization required by Section 57.b.(2) of the AEA, indicating the Secretary of Energy has determined the transfer will not be inimical to the interest of the United States. U.S. persons under the Implementing Arrangement must also obtain a relevant export license from the U.S. Nuclear Regulatory Commission (NRC). Within this legal framework, authorized persons under this Implementing Arrangement may also apply IP protections to various ideas, concepts, and inventions relevant to the TWR brought to the Arrangement or jointly developed under it.

The reference JTDTA can be described as a collection of parties, or entities, from two countries. These entities include multiple U.S. companies; multiple foreign companies; support organizations, such as law firms, on both sides; and government agencies such as the U.S. Department of Energy (DOE) and NRC. Over the course of the execution of the agreement, these entities, which are designated as authorized persons to the JTDTA, exchange a variety of information artifacts (IA) such as documents, records, designs, software codes, blueprints, etc. Any of these IAs may have one or more IP protections applied to them, such as patent and copyright filings, trademark and trade secret determinations, licenses, etc. These IP protections are generally applied as needed: one type of protection (e.g., a nondisclosure agreement) need not have to be in place to trigger another type of protection (e.g., a patent application). While these IAs are primarily sent among the entities who are party to the JTDTA, in some cases authorized persons could potentially interact with entities outside of the JTDTA, like additional companies outside the JTDTA, and countries beyond the two countries in question. Such interactions with parties outside of the JTDTA are considered unauthorized as they are going to unauthorized entities and may be being misused for purposes not sanctioned by the JTDTA. These entities, IAs, and transactions are depicted in the diagram in Appendix A.

4.0 Use Case Evaluation

The PNNL team worked with experts in export control and IP to apply the standard evaluation methodology developed in 2018[5] to the referenced JTDTA. The evaluation is available in Appendix B and its score in relation to the other export control use cases that were evaluated in 2018 is shown in Appendix C. Its score of 4 out of a possible 10 was low, both absolutely and relatively to the other use cases considered. This indicates that the JTDTA use case likely does not possess features that would call for a distributed ledger. This section highlights key points from the evaluation for consideration.

Confidence in Data Security and Validation: The team considered all transactions between authorized persons as occurring in a secure environment similar in primary ways to those used for handling classified information. Specifically, while all authorized parties interact with each

[10] Implementing Arrangement between the United States of America and the Government of the People's Republic of China under the Agreement for Cooperation between the Government of the United States of America and the Government of the People's Republic of China Concerning Peaceful Uses of Nuclear Energy, 78 Fed. Reg. 243 (December 18, 2013).

other within the information systems of the JTDTA, some authorized parties may have permission to access certain information that others do not. In this context, the primary requirement is a document repository with access controls and alerts that provide high levels of data security and validation about which users are accessing which IAs, for both reading (accesses) and writing (changing, copying, or deleting). State-of-the-art technologies with sufficient access controls can adequately maintain a high level of confidence in data security and validation. Standard modern solutions available in cloud computing platforms have several resources that could be used collectively to provide file storage, identity access management (IAM), and logs based on access or changes.

One example may be Amazon Web Services where permissions can be set with the IAM console to allow certain users to read and write to certain locations in the file system (S3) and the Amazon CloudWatch can provide observability and monitoring based on those systems.[11] Other cloud computing services examples include Microsoft's Azure and Digital Ocean. Outside of cloud services, other solutions could include personalized software that monitors file system change notifications and raises events when a directory, or a file in a directory, changes.[12] Using the software, metadata could also be added to IA files as they evolve through the system for additional tracking. Access permissions would be set by an administrator for this shared drive/directory. Digital rights management technology/software that can be readily purchased today as well.

When addressing transactions outside the JTDTA, the challenge evolves from one that is largely focused on document management and protection to one that is primarily focused on detecting and preventing information diversion and misuse. These are two separate but related challenges, where the former can be addressed with existing technologies and a distributed ledger while the latter remains unaddressed by both existing technologies and DLT.

Current Use Case Processes Hinder Legitimate Commerce: As noted previously, the 2018 Implementing Arrangement was halted by U.S. concerns over the potential for retransfer of sensitive technology to unauthorized entities. Improving IP protection and enforcement can help incentivize countries to joint JTDTAs in the future.

Decentralization: Due to U.S. export control laws, the DOE plays a central role in defining the terms of the JTDTA and enforcing U.S. laws. The DOE cannot be removed from this role, removing the possibility of taking advantage of the full benefits of a decentralized DLT system.

Decentralized ledgers are those in which there is a substantial community of users who may have different privileges in maintaining the consistent state of the ledger. The benefits of decentralized ledgers, which rely on computer algorithms rather than people to validate and post transactions, are increased transparency and trust among parties, at the cost of efficiency. By comparison, the benefit of using a private ledger, where a central authority maintains control over the ledger, is increased efficiency at the cost of transparency and trust. Under a consortium system, predetermined users maintain their own copy of the ledger and execute distributed consensus protocols to validate transactions. Consortia platforms are a compromise solution for parties that wish to limit access to the ledger to certain parties and exhibit some control over how those parties interact with the ledger without sacrificing the benefits of increased transparency. Thus, parties to the JTDTA might derive some benefit in terms of efficiency and auditability through use of a consortium system to document and monitor transactions among

[11] For more information about these capabilities, visit https://aws.amazon.com/cloudtrail/.
[12] For more information, visit https://aws.amazon.com/iam/.

authorized parties on a distributed ledger. However, existing database and software solutions also offer many of the same desired features, such as automated access alerts, without sacrificing too much transparency. Without further development and testing, it is unclear whether potential benefits of using a consortium platform would outweigh the costs of integrating that platform with other existing systems, such as the e810 site. Deploying and integrating existing software and database solutions is likely more cost effective.

5.0 Summary of Findings

Based on this research, PNNL offers the following findings:

DLT can be used to strengthen IP protections between authorized parties to a JTDTA, but it does not provide a unique solution for addressing this challenge. *DLT can be used to document transfers of IP-protected technology between authorized parties to a JTDTA. However, existing technologies also can be used to document transfers of ownership, monitor access to protected information, and support legal enforcement of IP infringement. DLT may introduce additional efficiencies to the process via use of secure automated workflows, but this benefit may not be worth the cost of political or technical investment in deploying DLT for this purpose.*

DLT cannot be used to prevent technology misuse. *Neither existing technologies nor DLT prevent parties from misusing technologies to create counterfeit products or retransfer IA to unauthorized parties for use in a nuclear weapons program.* Items within the JTDTA system could be available inside and outside the blockchain through screenshots, downloads, and other functions that cannot be tracked nor prevented with a distributed ledger. Nondisclosure agreements and patents would still be required for those with access to IP, and then legal action would take place as it is the same today.

6.0 Recommendations

Based on the findings from this research, the project team offers the following recommendation for consideration:

1. DOE/NNSA should explore the full suite of functions and capabilities in existing software and database applications to determine the extent to which user permissions and monitoring capabilities can strengthen IP enforcement mechanisms. It also might be worth considering other practices that are used to protect sensitive information, including those that might be used to protect classified information. Specific tools and approaches offered by Amazon Web Services could be considered to assist in legal recourse include:
   - *Deploying software capability that works with cloud infrastructure to track access*. Such capability would act as a 'container' to the file repository on the cloud and use metadata to document changes or activities that occur within its domain, such as authorized or unauthorized attempts to upload or download files. This type of software would support improved cyber forensics in the event that a breach occurs.[13]

[13] According to the AWS website, "AWS Identity and Access Management (IAM) enables you to… create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources." For more information, visit https://aws.amazon.com/iam/.

- *Creating a portal in cloud infrastructure to monitor duplication attempts*. A portal can be used as the only way to view IAs and might be able to track any screensharing or screenshot attempts. This option would not have the ability to track activities performed *outside* the system, such as attempts to photograph and distribute sensitive information. However, this portal would create a more secure and trackable access to the information artifact.[14]
- *Attaching an image recognition capability to the cloud infrastructure portal*. This capability would help detect indications of attempts to copy the contents on the screen from *inside* the system. This, for example, could prevent an attempt by a user to take photography of the screen using a digital camera or a phone. The image recognition software would detect the camera and either report the activity or shut down the system to prevent unauthorized image acquisition. This also means that the requirement for accessing the system through the cloud portal would require a webcam device to always face a user. One existing software that might be applicable for this purpose is a Tensor Flow-Object Detection model. The model would run in the background while a webcam is active in the user space.[15] As soon as it detects a camera, it would shut down the application and notify system administrators. This addition will not necessarily prevent all attempts at unauthorize duplication of IAs, but it would raise the deterrence threshold.

2. As part of this exploration of existing software and database applications to support joint technology development and transfer, DOE/NNSA should engage with the developers of e810 to understand the extent to which that platform might be integrated with existing software and database solutions that enable sensitive information management, monitoring, and distribution among JTDTA parties. An integrated system would further strengthen efforts to monitor and reconcile authorized activities with activities being conducted under a JTDTA.
3. As discussed in this study, few, if any, tools are available to definitively prevent unauthorized users from obtaining and sharing sensitive information outside of the JTDTA context. Without the introduction of new technologies or approaches, distributed ledgers do not currently appear to have a specific value for this purpose.

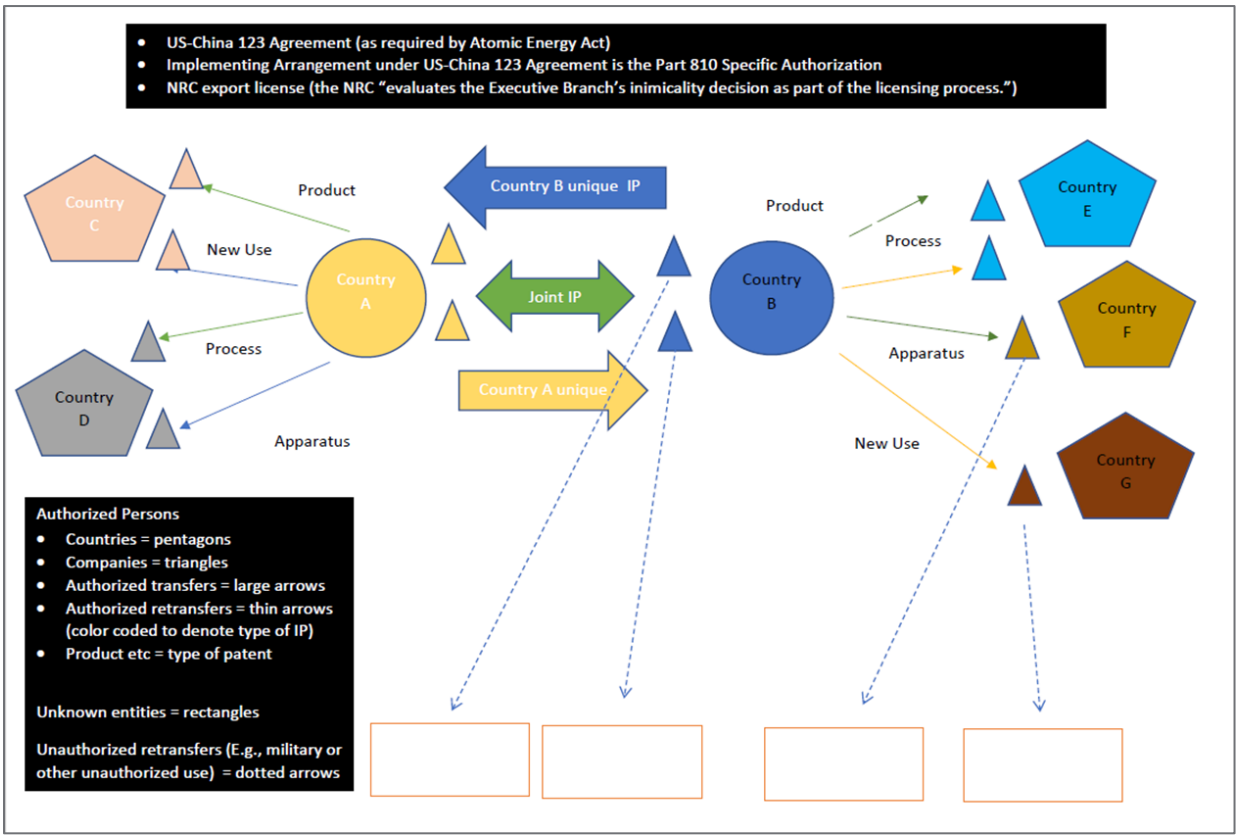
7.0 Conclusion

DLT provides important benefits to the export control system, particularly in the areas of supply chain management, transborder shipments, license authorizations, and government-to-government assurance processes. These use cases were highlighted in PNNL's previous exploration of potential DLT applications for export controls.[16] Subsequently, researchers at non-profit organizations have highlighted DLT's ability to "protect data from tampering, theft and hacking…ensure data integrity and provenance…and establish a link between digital identities and actual items."[17] Additional research is needed to better understand the extent to which DLT might benefit the aforementioned use cases. As this study demonstrates, DLT may bring these

[14] AWS CloudTrail is a service that enables users to, "…monitor, and retain account activity…and provides event history of your AWS account activity." For more information, visit https://aws.amazon.com/cloudtrail/'.
[15] More information about this software can be found at https://github.com/pjreddie/darknet/wiki/YOLO:-Real-Time-Object-Detection.
[16] Frazar S, C Joslyn and GT Hoffman. 2018. "Evaluating Export Control Use Cases for Distributed Ledger Technology: Interim Report." Pacific Northwest National Laboratory, October 2018. PNNL-28777.
[17] Candano D. "Blockchain for Export Controls." 6 April 2020. Stimson Center. Available at https://www.stimson.org/2020/blockchain-for-export-controls/. Accessed on 19 September 2020.

benefits to joint technology development and transfer agreements. However, existing solutions could also be used. Moreover, DLT is unlikely to address the significant challenge of preventing unauthorized duplication and sharing of sensitive information outside the JTDTA context. Few, if any, technology solutions will prevent someone from photographing information once it has been accessed or sharing information verbally with unauthorized parties. While this challenge remains, export control professionals and governments engaging in joint technology development and transfer agreements can take advantage of existing solutions and new technologies, such as DLT, to strengthen IP protections wherever possible. DLT remains a promising solution for many problems, but it is not the unique solution that will solve challenges associated with joint technology transfers.

Appendix A – Flow of Transaction under a Notional JTDTA



Appendix B – JTDTA Use Case Evaluation

Criteria	Joint Tech Development	Scores
Use case requires high level of data security (information can only be shared with designated entities)	Yes, combination of proprietary and controlled information.	Meets
Use case requires auditable data trail	Yes, U.S. Government is trying to increase stringency of the full reporting that is required. Once a joint venture is formed, more stringent controls will be needed under this goal.	Meets
Use case would benefit from faster transaction processing (enabled by proof of work)	Transaction speed is less relevant in this case. Auditability is more important, for example, if someone checks out a document. There are no complaints about long wait times for transaction processing.	Does not meet
Use case would benefit from higher confidence in data validation	This is not as a significant risk any more. Pulling a drawing, people know exactly where to go. The document control system will only give you the latest version. The document will not be posted unless document has been approved by all parties. Approval processes may use human validation or automated approvals. Electronic signoffs are used. There is already high confidence. Under JV, China will implement the same security standards/approval protocols. There may by efficiencies that could be introduced in the security protocols. Terrapower uses electronic signatures for approvals in Agile system.	Does not meet
Existing information technologies solve use case challenges	Not really. Once JV is formed, document is created based on information from another document. Or technology in document created by U.S. and China. So, what is the source of the information in document—China or U.S.? How much of that technology is U.S. origin v Chinese origin? If the Chinese take the information and put it into another reactor and claim Chinese origin technology. How do we identify downstream?	Partial
Improves Trust: Stakeholder interests are not aligned with central authority	Yes: Parties trust each other sufficiently to come together in technology transfer agreement but such agreements break down due to lack of trust regarding potential for technology misuse.	Meets
Improves Trust: Central authority required (decentralization does not undermine effectiveness; may bring value)	Yes. DOE has authority over overall database, and there is some 810 involvement as well. While DOE cannot be removed as the authority, aspects of the authorization review process could be decentralized, such as the Department of State engagements. International agreements/national law requires DOE oversight.	Meets
Current use case processes hinder legitimate commerce	Yes; 2018 Implementing Arrangement was halted due to proliferation concerns.	Meets

Current use case processes alert stakeholders about activity or behavior of concern	Current use case processes do not alert. Technology transfer from Terrapower to China—controls are adequate and alerted sufficiently if something is transferred out of Implementing Arrangement. If technology is jointly developed and they take the technology and use it for something else, no adequate alerting is in place. An audit trail is needed to help alert activity of concern.	Partial

Appendix C – JTDTA Use Case Evaluation Scores

Criteria for Application	Part 810 (score)	EAR commercial (score)	ITAR military (score)	NSG Denials (score)	NISS reporting (score)	Shipping Documentation (score)	"Self-Reg" (score)	JTDTA (score)	Meets Criteria	Partially meets criteria	Does not meet Criteria	Weight
Use case requires high level of data security (information can only be shared with designated entities)	1	1	1	0.5	1	1	1	1	1	0.5	0	1
Use case requires auditable data trail	1	1	1	1	1	1	1	1	1	0.5	0	1
Use case would benefit from faster transaction processing (enabled by proof of work)	1	0.5	0.5	0.5	0	0.5	1	0	1	0.5	0	1
Use case would benefit from higher confidence in data validation	1	0.5	0.5	0	0.5	1	0	0	1	0.5	0	1
FEASIBILITY SUBTOTALS	**4**	**3**	**3**	**2**	**2.5**	**3.5**	**3**	**2**				Average
Existing information technologies solve use case challenges	-1	-1	-1	-2	-1	0	0	**-1**	-1	-0.5	0	2
Improves Trust: Stakeholder interests are not aligned with central authority	2	2	2	2	1	2	2	**2**	1	0.5	0	2
Improves Trust: Central authority required (decentralization does not undermine effectiveness; may bring value)	-1	-2	-2	0	0	0	0	**-2**	-1	-0.5	0	2
Current use case processes hinder legitimate commerce	2	2	2	0	2	2	0	**2**	1	0.5	0	2
Current use case processes alert stakeholders about illegitimate commerce	2	2	2	0	2	0	-1	**1**	1	0.5	0	2
DESIRABILITY SUBTOTALS	**4**	**3**	**3**	**0**	**4**	**4**	**1**	**2**				Average
	8	**6**	**6**	**2**	**6.5**	**7.5**	**4**	**4**	**5.71429**			

Pacific Northwest National Laboratory

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

www.pnnl.gov