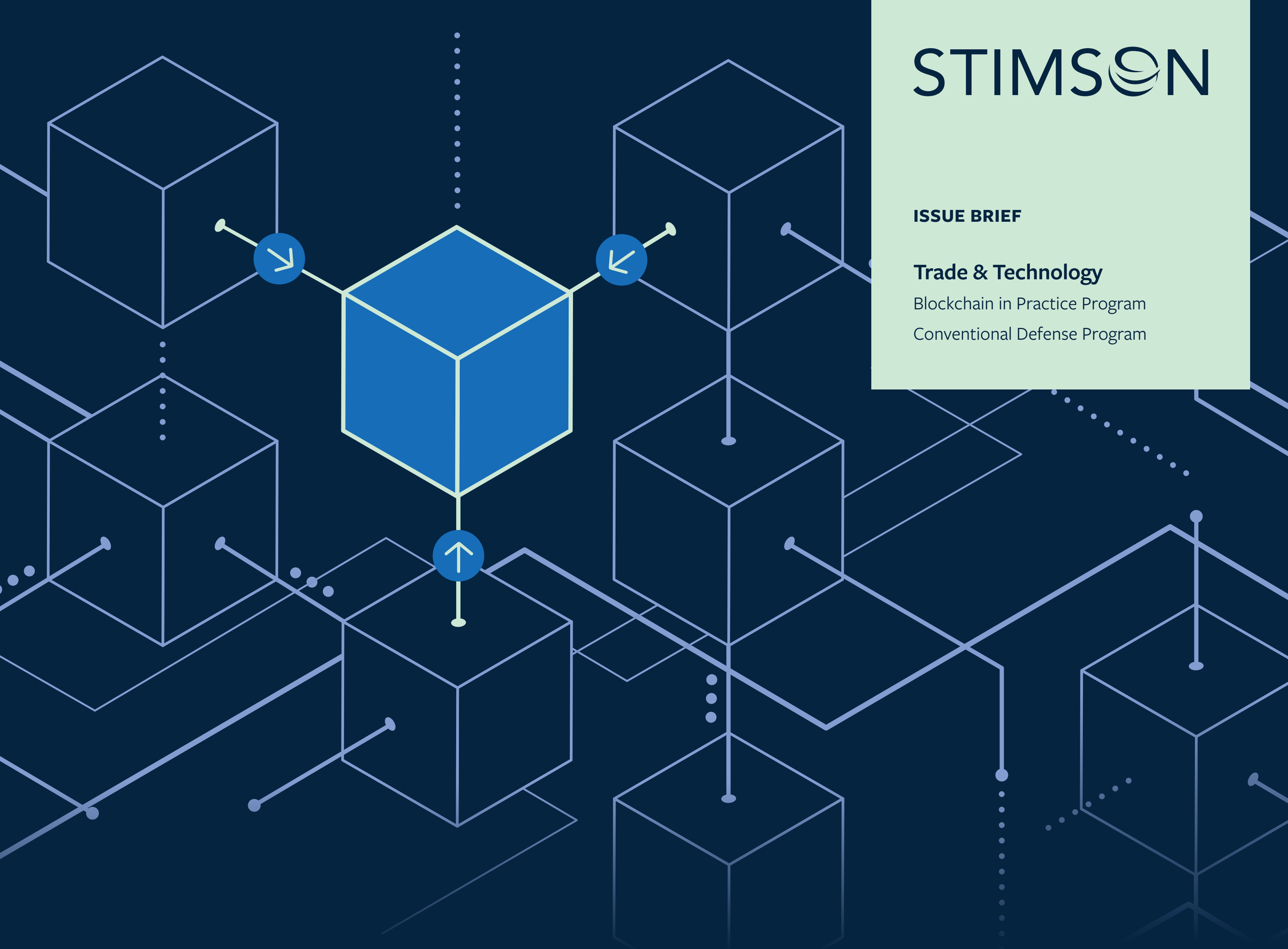


STIMSON

ISSUE BRIEF

Trade & Technology

Blockchain in Practice Program

Conventional Defense Program

Issue Brief: Distributed Ledger Technology for Arms Control and Management

Elias Yousif & William Marshall

September 2023

ABOUT STIMSON

The Stimson Center promotes international security and shared prosperity through applied research and independent analysis, global engagement, and policy innovation.

Acknowledgments

The brief was authored by Elias Yousif, Research Analyst with the Stimson Center's Conventional Defense program, and William Marshall with the Blockchain in Practice program. The authors were also supported by Rachel Stohl, Stimson's Vice President and Director of the Conventional Defense program, and Cindy Vestergaard, Non-Resident Fellow with the Blockchain and Practice and Nuclear Security programs. This brief was funded by generous support from the government of Switzerland. The authors also thank members of their expert workshop and peer reviewers who generously provided input and feedback.

Please Cite this Publication As

Elias Yousif and William Marshall, 2023, *Issue Brief: Distributed Ledger Technology for Arms Control and Management*. The Stimson Center, Washington D.C., USA.

Table of Contents


0-23547
DANGER
KEEP AWAY

Introduction

The global arms trade is a vast, dynamic, and complex enterprise, with numerous actors in multiple countries involved in facilitating the transfer of conventional weapons around the world. The arms trade is already a multi-billion-dollar sector: Rising great power tensions, proliferating armed conflict, and growing unease around the global security landscape have all contributed to a worldwide surge in international arms transfers while increasingly intricate networks of longstanding and emerging stakeholders are moving conventional weapons across the globe. These trends are straining national regulatory and arms control ecosystems intended to ensure responsible transfers; prevent illicit movement of arms; mitigate arms diversion; and ensure appropriate tracing, stewardship, and custody of defense articles.

Despite the growing burden on industry and national governments to ensure responsible arms transfers, many national governments still rely on outdated technologies and processes to manage their arms transfer control systems, which can strain administrative capacities, increase the margin for error throughout a given transaction, and leave such processes and related documentation vulnerable to manipulation and/or malicious activities.

New technological solutions may offer an opportunity to both meet rising global demand for materiel while ensuring appropriate responsibility and oversight of arms transfers. The application of distributed ledger technology (DLT) for customs regulation and other regulatory and commercial ecosystems offers potential value in assisting governments, industry, and other stakeholders in securing, streamlining, and increasing transparency in international arms transfers, reducing the burden of compliance and potentially mitigating the risks of weapons loss or diversion.

This Issue Brief explores the potential utility of applying DLT in arms control and arms transfer management processes. The brief is organized into two sections and an annex. Section 1 identifies several practical challenges, gaps, and inefficiencies in contemporary arms transfer control and management ecosystems that could be aided by the tailored application of DLT. Section 2 contains recommendations for follow-on research to expand on initial findings. The Annex offers three hypothetical scenarios of different DLT-enabled ecosystems that could improve the efficacy of various elements of arms transfer control and management systems.

Methodology

The findings and recommendations of this Issue Brief are drawn from several sources. First, the Stimson Center conducted scoping desk research, including an in-depth literature review of academic articles and industry publications. Second, Stimson examined DLT applications in analogous industries and identified common themes and trends. Third, Stimson undertook one-on-one consultations with government officials, academics, and private sector stakeholders engaged in arms transfer controls or relevant research activities. Finally, Stimson conducted an expert roundtable to discuss initial insights and findings and receive feedback on the scope and feasibility of DLT use for arms transfer controls.

What is DLT?

Distributed ledger technology (DLT) streamlines data sharing and authentication between numerous and diverse stakeholders using an immutable, distributed digital ledger. This authoritative ledger is shared by all participants, streamlining information flows, and reducing administrative processes. DLT is sometimes referred to as a “trust machine” because all participants agree to share information according to specific guidelines enacted by group consensus, while each participant or group maintains ownership of their own data.

Blockchain, a subset of DLT, works by encoding transactional data into a “hash” that is combined with others to form “blocks” of encrypted data that are continuously replicated across a network of participants. This constant replication provides blockchain’s signature immutability, and in combination with the algorithmic encryption of each hash, ensures that all records are append-only, granting participants full provenance of the history of each transaction. In this way, blockchain technology enables greater consistency and auditability of data across an entire ecosystem or network of participants.

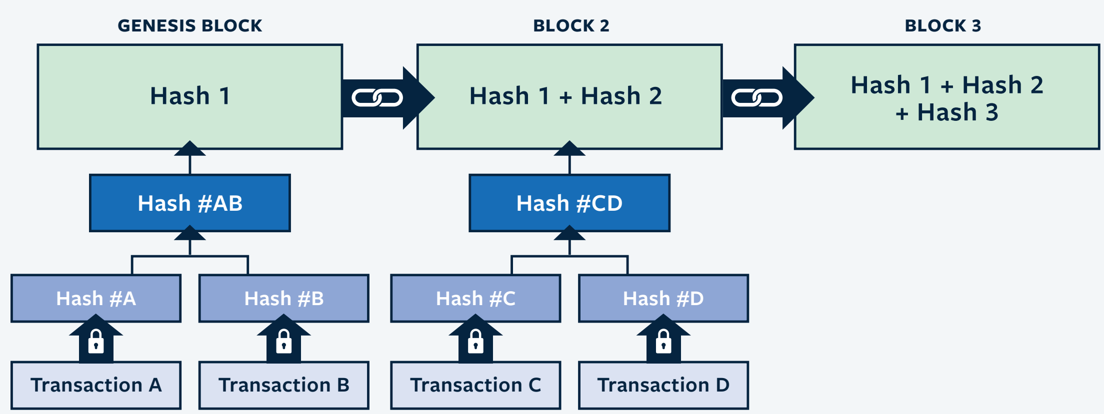
Unlike traditional databases that rely on a central authority to validate transactions, a blockchain can be fitted with permissioned protocols to provide participants information at specific locations or time frames, depending on their level of access. This is especially beneficial for processing high-value assets and demonstrating compliance that require real-time access to information across multiple organizations, automating manual data entry or, in some cases, supplementing more traditional/physical data-management processes. Data stored in a DLT platform does not have to be sensitive information itself — rather, certain metadata can be hashed that corroborates the chain of custody for a particular set of data or real-world asset, for example, by providing access logs or information on the condition and location of a weapon system.

Benefits of DLT

Some of the potential benefits of employing a blockchain for supply chain management include:

- *Decentralization*: Multiple participants in different locations can access and share data without the need for a centralized authority or database. Blockchain networks are not susceptible to a single point of failure.
- *Distribution*: Each blockchain network represents a digital ecosystem in which participants, or "nodes," can share data using a single, shared ledger. This reduces the time required to process transactions, reconcile data, and demonstrate compliance.
- *Confidentiality*: A permissioned DLT platform enforces strict access controls for each participant, in line with confidentiality rules implemented according to regulations and group consensus. Each user's level of access and the types of transactions they may perform are decided by these permissions.
- *Security*: The cryptographic "hashing" of transactions and inherent immutability of blockchain technology protects the ownership of each participant's data and ensures that all records are "tamper evident." Hashed records cannot be overwritten, only appended with new information. New hashes will contain copies of previous hashes, but the original hash will remain on the blockchain as an immutable record of the original transaction.

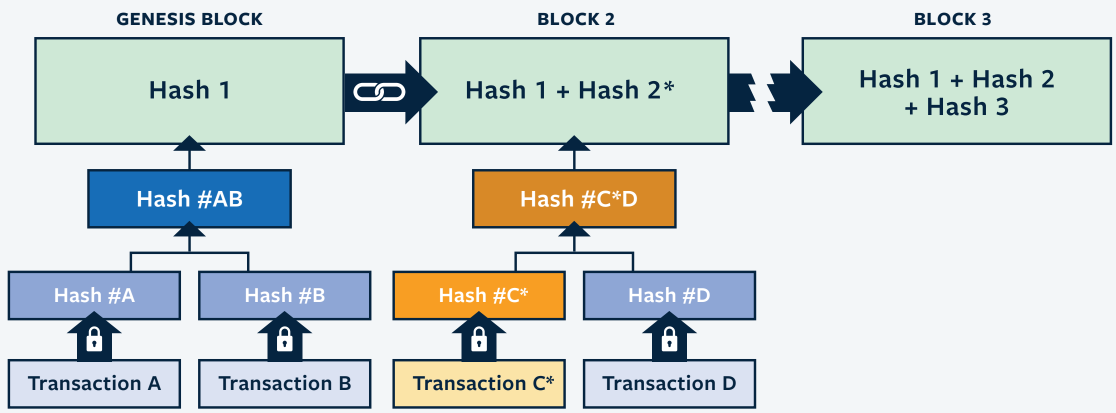
Figure 1: Blockchain Immutability



If there is an attempt to alter the record of a transaction, the corresponding hash will no longer match the duplicates of the previous version dispersed throughout other blocks stored throughout the blockchain. In this way, blockchain is highly "tamper evident" ensuring the consistency, integrity, and security of data within the ecosystem.

Figure 2: Blockchain is "Tamper Evident"

If the data recorded in Transaction C is altered (Transaction C ▸ Transaction C), the new hash that results will no longer match duplicates of the previous hash located in other blocks dispersed throughout the blockchain network.*



There are three main types of DLT platforms: public, permissioned or private, and hybrid (also known as consortium) (see Figure 3).

Figure 3: Types of DLT Platforms

Public	Permissioned (private)	Hybrid/consortium
▹ Access is open to public participation ▹ Usually, a large number of users ▹ No central authority ▹ Examples include cryptocurrencies such as Bitcoin and Ethereum	▹ Access is restricted to specific users ▹ The number of users is restricted ▹ Controlled by one authority or a group ▹ Examples include IBM's Food Trust, Walmart Canada's DL Freight platform, De Beer's Tracr platform, and SLAFKA (see below)	▹ Combination of public and permissioned infrastructure ▹ Members decide who participates and/or which transactions are made public ▹ Users may share equal rights to transact, view, or append or modify transactions, but identity of users is anonymous. Can also be controlled by one or more authorities ▹ Examples include Circulor and MATCH (see below)

Blockchain in Practice: Commercial, Government, and Prototype Applications

A growing number of commercial and government initiatives focus on the potential of DLT to improve supply chain provenance, enhance logistics, and track the transfer and custody of physical goods. Blockchain solutions are also increasingly being employed by organizations and companies to guarantee the quality and safety of products, mitigate the risk of supply-chain disruptions, and streamline regulatory reporting by increasing transparency and efficiency, reducing operating costs. A review of recent initiatives offers some insight into the ways in which DLT addresses a host of information-sharing challenges in complex, multistakeholder supply chains, many of which hold parallels to international arms transfers, including:

- IBM's Food Trust solution, based on the permissioned Hyperledger Fabric platform, works to reduce the risk of foodborne outbreaks in partnership with global food suppliers, like Walmart.[1] IBM Food Trust offers commercial food retailers and suppliers a single digital ledger from which to track and provide provenance over the manufacture and transit of food products, in some cases reducing the time to trace a product's lifespan from an average of seven days to just 2.2 seconds.[2] Specifically designed to aid food retailers in complying with the 2011 US Food Safety Modernization Act, IBM Food Trust offers producers, shippers, retailers, and regulators real-time tracking of food products using only a stock keeping unit (SKU) identifier.[3]

- Walmart Canada introduced the Hyperledger Fabric-based DL Freight platform in March 2021 to reduce invoice discrepancies in freight shipping among 70 Canadian carrier companies.[4] Prior to implementing the DL Freight platform, nearly 70% of invoices were subject to dispute. As of 2022, Walmart Canada reports discrepancies in less than 1% of freight invoices. Moreover, discovering and resolving disputes has become significantly easier, reducing the risk that carriers will experience delays of weeks or months in receiving compensation.

- The De Beers Tracr platform, based on IBM's blockchain cloud service and Hyperledger Fabric, enables greater supply chain transparency and tracking of diamond products from mine to customer across De Beers Group's operations in four partner countries. Tracr also validates the integrity of De Beers' supply chain for regulators and authorities. Launched in 2018 as an exploratory pilot to test the ability of DLT to provide enhanced provenance over diamond production, the De Beers Group's Tracr blockchain platform now covers over a quarter of the company's production value.[5] The De Beers Group plans to expand Tracr to cover a majority of the company's diamond production, including tracking the origin of each diamond, by 2030.

- Circulor utilizes the permissioned Oracle Blockchain Platform to enable automated "end-to-end" oversight of its mineral mining supply chain and validation of compliance with ethical sourcing regulations.[6] Established in 2018, the company's "Circulor Protocol" offers facial recognition technology, GPS location monitoring, container tracking, and QR code reading to better track the source, transfer, and sale of sensitive mineral products, like cobalt. The Oracle Blockchain platform is also capable of tracking mined diamonds using "40 metadata points" to provide customers with digital proof that each diamond was responsibly sourced.[7]

- The Republic of Korea's Customs Service (KCS) began a pilot program in 2018 to test the application of DLT to increase the efficiency of export clearance for e-commerce in partnership with 50 companies, including ten companies in Singapore and Vietnam.[8] Based on Hyperledger Fabric, Samsung SDS' permissioned e-C/O blockchain platform instantly clears low-value e-commerce exports from South Korea and partner countries and enables real-time information sharing between e-commerce transport companies and KCS.[9] KCS announced in 2022 that the platform was in the process of becoming fully operationalized and would be integrated into its existing UNI-PASS digital customs clearance system.[10]

- "SLAFKA," the world's first blockchain prototype for nuclear safeguards information management, was launched in Helsinki, Finland on March 10, 2020.[11] A collaborative project among Finland's Radiation and Nuclear Safety Authority, the Stimson Center's Blockchain in Practice program, and the University of New South Wales, SLAFKA demonstrated how a DLT platform can support national compliance with international safeguards obligations. SLAFKA was built using Hyperledger Fabric, a permissioned DLT platform that allows simulated national, regional, and international inspectorates access to the same authoritative ledger with different access controls in line with real-world confidentiality rules. Using a single authoritative ledger, operator and State records are identical, eliminating the time currently spent by inspectors to reconcile such records.[12]

- The Stimson Center's Monitoring and Tracking Chemicals (MATCH) project is a DLT proof-of-concept that demonstrates the potential of blockchain to reconcile transfer data for commonly traded dual-use chemicals regulated under the Chemical Weapons Convention. The MATCH prototype platform simulates chemical transfers and regulatory reporting between hypothetical industry entities and States Parties using a single, authoritative digital ledger, simplifying the complexities of different countries' reporting requirements and reducing the occurrence of discrepancies.[13] Developed in partnership with Global Affairs Canada's Weapons Threat Reduction Program and DLT developer OARO, MATCH was built using Hyperledger Besu and operates on the public-permissioned LACChain blockchain network.

Assessing DLT's Application for Arms Transfer Management and Control

Contemporary Arms Transfer Control and Management Ecosystems

International arms transfers represent an expansive set of overlapping enterprises spanning different sectors, stakeholders, and national boundaries. To assess the potential utility and practical application of DLT for arms transfers, it is worth considering generalizable flows of materials and information along a given transfer chain, as well as the various institutional nodes that are involved in the life cycle of a transfer. Stimson researchers identified the following ecosystems, pertaining specifically to arms transfer processes, to better understand the potential applicability of DLT.

STAKEHOLDERS[14]

National Authorities

National authorities encompass a range of government agencies and actors involved in regulating, facilitating, approving, overseeing, or otherwise engaging in the export, import, or transit of conventional arms. Generally, these include:

- *Legislatures:* Legislative bodies can play various roles in the international arms transfer enterprise. In addition to defining the national laws that govern how other competent authorities regulate or control arms transfers, many will also play a more direct oversight role in adjudicating arms transfer decisions, as is the case in the United States, the world's largest international arms exporter.

- *Licensing authorities*: Licensing authorities are, generally, government institutions charged with administering and verifying compliance with national arms control regimes and foreign policy prerogatives, including by issuing requirements for the export of defense articles or services verified through a licensing process. Licensing systems vary substantially, but they often encompass a range of compliance, verification, vetting, and policy considerations to permission either individual transactions, batches of transactions, and/or to authorize the activities of private sector and commercial stakeholders. Licensing processes, though often administered by a single institution, can also encompass a number of government bodies, requiring intra and inter-agency communication and consultation.

- *Customs authorities:* Customs authorities are government bodies charged with managing the physical import, export, and transit of defense articles across national boundaries and ensuring their compliance with national control regimes and licensing requirements, especially at points of departure and entry. In many cases, customs authorities will be charged with verifying that defense articles being imported, exported, or in transit have the appropriate authorizations, including licenses, and that physical goods at various ports of entry and egress are accurately reflected in documentation. Customs authorities, therefore, will commonly need to confer and share information with licensing authorities as well as private sector stakeholders.

- *Law enforcement and investigative authorities:* Law enforcement authorities are generally charged with detecting, investigating, and prosecuting cases where actors have violated national arms control regulations and laws. Though typically concerned with illicit trades in defense articles, detection and investigation requires broad access to information on arms transfers, including legal transactions.

Private Sector

Private sector stakeholders include a range of commercial actors involved in the manufacture, sale, shipping, compliance, and other services required to transact an international arms transfer. Though there may be significant overlap between these actors, they generally include:

- *Manufacturers*: These are the commercial actors who produce, assemble, and make available defense articles for export. Typically, they are the actors submitting license applications to licensing authorities and who are responsible for complying with relevant arms control regulations and statutes. In short, these are the stakeholders who are instigating the international transactions regulated by national control systems. These manufacturers will have direct knowledge and information on the military items being exported, the designated end user, and the stipulations surrounding the transfer — information that may be required for licensing and commercial reasons.

- *Transporters*: Transporters are, generally, commercial actors tasked with physically moving defense articles from points of departure to points of destination. Though circumstances may vary, their custody defense articles are incidental, and a transporter's awareness or familiarity with any military hardware in their possession will be limited to commercial or customs control necessities.

- *Freight forwarders*: Freight forwarders are commercial actors specializing in the international transport of military goods, arranging the logistics, customs compliance, documents, and cargo accommodations with transporters. Acting on behalf of importers and exporters, they organize and administer various logistical and administrative aspects of transport.

- *Brokers*: Brokers are any entity or individual acting as an intermediary compensated to arrange or facilitate arms transfer transactions. Brokering can encompass a wide variety of activities, including managing financial, administrative, customs, or managerial processes on behalf of clients.

Each of these stakeholders maintains various overlapping, parallel, or isolated information ecosystems that must, to some degree, connect with each other for a transfer to move from the point of manufacture to the point of delivery. In other words, in any given arms transfer transaction, the physical movement of defense articles between different custodians is accompanied by intersecting but highly contingent information flows between and among these private and public sector stakeholders, each with their own equities and data requirements.

Key Nodes and Information Flows for International Arms Transfers

Though the physical movement of defense articles and their associated information flows will differ substantially based on context, generalizable trends can illustrate how various nodes in a transfer chain communicate with one another to transact an international arms transfer. The illustration below offers insights into the architecture a DLT system would have to service for the purposes of arms transfer control and management.

Figure 4: Nodes in a Conventional Arms Transfer Ecosystem

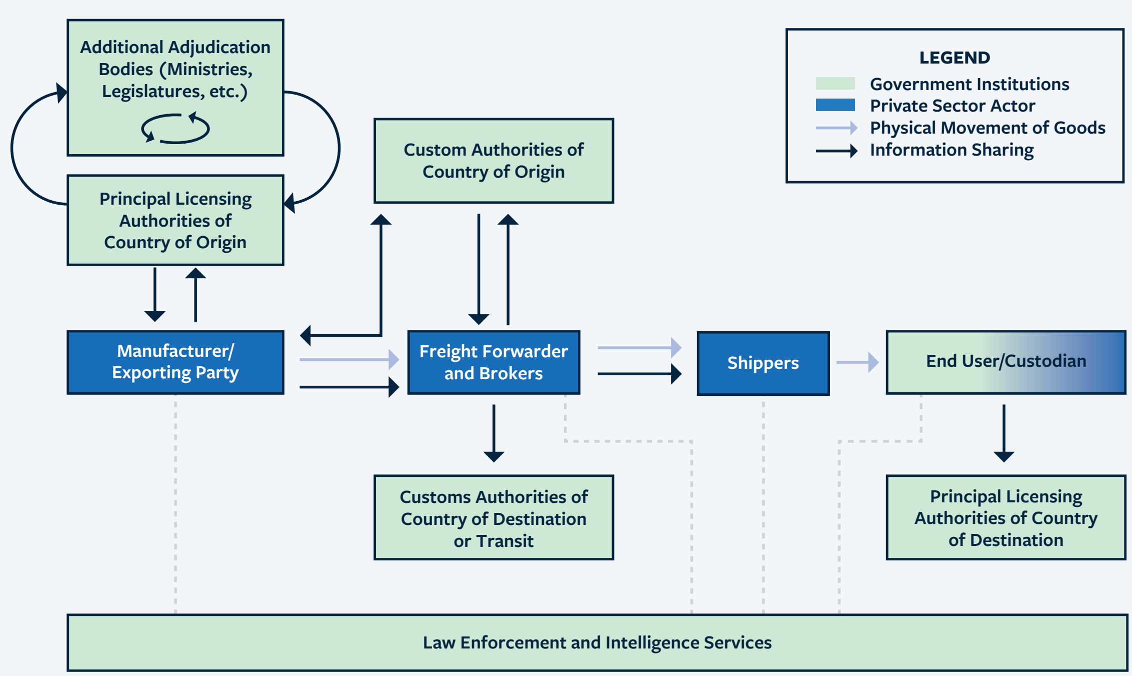


Figure 4 illustrates the sequenced nature of information sharing in the contemporary arms transfer context as well as the important "nodes" that might be incorporated into a DLT ecosystem. In most cases, communication among these nodes is not automated, and therefore requires manual inputting of data. Information access and sharing may also be irregular, as is often the case for law enforcement and intelligence services. Moreover, visibility among nodes not in direct communication is minimal, thus requiring duplicative efforts to ensure the necessary data is available to multiple stakeholders across the supply chain.

Challenges and Opportunities in Current Arms Transfer Control Architecture

Contemporary arms transfer ecosystems are growing in scale and complexity, reflecting broad evolutions in global trade aimed at enabling greater volume and speed alongside more intensive national and multilateral efforts to enhance control measures.[15] Processes and procedures in increasingly intricate arms transfer supply and information exchange chains present certain features that are notable in relation to the potential known benefits of DLT systems.

NUMEROUS, MULTI-SECTOR STAKEHOLDERS

International arms transfers involve numerous stakeholders across sectors and geographies. Within each of those sectors lie additional networks of institutions and individuals involved in developing, managing, overseeing, and executing these complex transactions. Each of these stakeholders maintain various overlapping, parallel, or isolated information ecosystems that must, to some degree, connect with each other for a transfer to eventually move from the point of manufacture to the point of delivery.

LARGE VOLUMES OF SENSITIVE DATA

International arms transfers generate an enormous amount of data and information, both as a matter of commercial necessity as well as regulatory compliance. The information spans a range of subjects and can include sensitive information, be that trade secrets, regulatory information, or information related to national security. That data reflects the imperatives, remits, and information architectures of the various stakeholders engaged in the enterprise, with varying degrees of cross-sectoral relevance. This information is vital to developing, evaluating, and executing an international arms transfer, but given the scale of the information generated and the specificity of the information required, parsing through information, organizing it, and ensuring its accessibility without sacrificing security is an ongoing a challenge. Moreover, ensuring that data remains error-free and protected against tampering or mismanagement is essential to preventing commercially costly errors or arms diversions.

COMPLEX INFORMATION FLOWS

In general, across the range of stakeholders involved in international arms transfers, there are countervailing imperatives around limiting access to information while at the same time ensuring information can move efficiently as regulatory or commercial needs dictate. Indeed, information flows — both within and among governments and private sector actors — are essential to the enterprise but face significant practical and normative hurdles. Disparate information ecosystems must be linked in some capacity, including within and across stakeholder sectors. In many cases, these linkages are not automated and depend on manual inputs for intra-sectoral and cross-sectoral information sharing. Moreover, despite the value of ensuring stakeholders across the enterprise have access to relevant data, stovepiped infrastructures as well as sensitivities around information security often act as inhibitors of efficient information flows.

PHYSICAL MOVEMENT OF HIGH-RISK, SENSITIVE GOODS

At their core, international arms transfers concern the physical movement of defense articles across national boundaries, carrying with them certain risks not associated with other commercial goods. National control regimes are intended to mitigate those risks and ensure those transfers align with national interests and other strategic concerns. Although a significant portion of those processes concern assessments of the parameters and actors of an associated transaction prior to the physical movement of materiel, fewer investments have been made in tracking those defense items geographically after the first point of departure. Visibility and awareness surrounding the location and intermediary exchanges of arms in transit is minimal, particularly for regulatory and enforcement actors.

COMPLEX OVERLAPPING CONTROL REGIMES

Because of the unique risks associated with international arms transfers, national governments and multilateral institutions have sought to impose risk-mitigating control regimes. Accordingly, compliance is an important aspect of the arms transfer enterprise. However, control regimes can be enormously complex, requiring significant resources and time from both private sector and state institutions to implement. Verifying alignment with these regimes represents significant elements of the private-public engagement on international arms transfers, involving complex information flows and, in many cases, arcane digital or even physical paperwork processes. For states that participate in multilateral control instruments or voluntary confidence-building mechanisms, including the Arms Trade Treaty or the UN Register of Conventional Arms, these represent additional ecosystems of reporting and compliance necessitating amalgamation and synthesis of transfer-related information. These national and supranational regimes and mechanisms are rarely harmonized, creating an additional hurdle for commercial actors and governments to ensure that transfers do not run afoul of national or international control systems and standards.

Potential Benefits and Applications of DLT for Arms Control and Management

International arms transfers present several regulatory, reporting, information-sharing, and structural complexities that can exacerbate risks of mismanagement, loss, theft, or misappropriation of legally exported conventional arms. Ensuring regulatory compliance, efficient information sharing, and effective tracking are all important factors in mitigating these risks as well as making certain that transfers can proceed with sufficient efficiency to meet foreign policy and national security objectives. But meeting these imperatives can place a significant burden on both governments and private sector actors engaged in the enterprise and create new barriers to safe, efficient, and responsible transfer processes.

Sharing information on international arms transfers requires both the discrete and efficient transfer of data — imperatives that, under current modalities, can often be at odds. Yet, the ready availability of information, tailored to the unique needs of various stakeholders, is both instrumental in mitigating arms transfers risks and enabling the efficiency of a given transaction, as well as informing future transfer decisions. Given the number of actors engaged in the enterprise — all of whom require information for legal, regulatory, or commercial reasons — DLT can provide an integrated platform from which industrial, commercial, and government entities can transact information in near-real time, thereby decreasing the regulatory burden, simplifying reporting processes, and ultimately creating greater efficiency along the information supply chain. Lessening the burden and complexity of information inputs and sharing for industry may incentivize compliance with government and international regulations and reduce the risk of error and discrepancies in reporting. Similarly, more efficient information flows could aid the internal communication processes for national authorities, including for pre-transfer assessments, which may require input from various government bodies.

More easily accessible information, safeguarded by agreed-upon permissions for various actors, is especially valuable as items begin their physical transit from exporting to importing country, and where customs officials, commercial transporting actors, and importing authorities all require efficient access to data to effectively vet, monitor, and transact shipments according to various regulations and control regimes.

Moreover, a DLT-enabled information-sharing platform could improve the security of sensitive data as well as ensure critical data is visible only to those permissioned to access it. Such a system could be constructed to ensure each user is granted access only to their own inventory of information, and any information willingly shared by other participants.

Additionally, DLT platforms can integrate other technologies to facilitate even greater visibility and integrity in arms transfer supply chains. For example, data from unique identifiers, such as QR codes, could be captured in a DLT platform and used to track the physical movement of goods from manufacturer to final end user, and from the point of export and import in all countries involved in a transfer. Customs agencies could also use the same blockchain platform to quickly access information relevant to a particular transfer stored in the QR code or other associated identifier, reducing the risk of reporting inaccuracies and potentially minimizing the time required to process transfers.

Ultimately, the harmonization of information flows among different industry, commercial, and government parties involved in international arms transfers could increase the efficiency and transparency of national and international regulatory and reporting processes while also contributing to overall compliance and the ability of authorities to better track and account for the movement of conventional arms and components. Increased levels of compliance and the reduction of reporting inaccuracies could contribute significantly to minimizing the risk of missing and potentially misappropriated arms.

Barriers and Challenges to the Application of DLT for Arms Transfer Management and Controls

Though DLT may present notable benefits for arms transfer management and controls, adopting the technology and adapting contemporary architectures to effectively leverage its efficiencies presents several practical and normative challenges.

At the technical level, a DLT-enabled ecosystem requires participants to capture and store data digitally. Though many governments and private sector actors have adopted electronic databases to manage various components of arms transfer transactions, others continue to rely on paper records or other legacy systems. The use of physical recordkeeping for processes such as licenses, transfer tracking, and customs documents can reflect technical and financial constraints as well as cultural preferences of different institutions. For example, some licensing and customs authorities may prefer or be legally required to maintain and use hard copy paperwork to validate the authenticity and provenance of documentation.

Uneven adoption of DLT based on a lack of digitized recordkeeping could also exacerbate existing technical disparities and inequities in the arms transfer ecosystems between wealthy and developing countries. For countries that do not digitize records because of technical or financial constraints, adoption of a DLT platform would, ironically, require higher startup costs, presenting a serious barrier to implementation. However, DLT is well suited for adoptability, interoperability, and scalability once a digital database is established, meaning that the financial and technical burden is reduced once data is stored digitally. For countries that have made the investment to digitize records, application programming interfaces (APIs) would allow different databases to make “calls” into a shared DLT system, even if those databases themselves were nonstandardized. This would allow organizations to utilize “blockchain as a service” by software providers instead of having to build their own DLT platform from scratch.

In addition, concerns around security and confidentiality are a significant barrier to DLT adoption. Among various stakeholder communities, the notion of engaging in a shared digital ecosystem with external actors draws serious skepticism. This is especially true for governments, which may feel uneasy about participating in a digital platform with non-government actors, and for private sector stakeholders concerned about intellectual property or sensitive commercial data. In practice, data captured by a DLT platform is "hashed" or encrypted by a unique algorithm, which is extremely difficult to reverse-engineer. The hash is used to authenticate data that exists in a participant's unique database, or that is shared between participants, ensuring that any substantive information remains accessible only to those permissioned to view or engage with it. For industry stakeholders, the information that would be captured on a DLT platform is much the same as data already shared with regulators through existing channels. Transacting that information through a DLT system would simply make those information flows more secure and less susceptible to tampering or administrative errors.

Nevertheless, sentiments about DLT systems may not reflect nuances of how these platforms manage information; thus despite the practical security and safeguards offered by DLT, misunderstandings about the technology, especially pertaining to confidentiality and security will continue to be a barrier to adoption. Indeed, misgivings about DLT as an enterprise management tool frequently reflect popular myths about the technology that would need to be dispelled to encourage key stakeholders to consider the tool for arms transfer applications. Some of these myths are discussed below.

Debunking Popular Blockchain Myths

BLOCKCHAIN ≠ CRYPTOCURRENCY

Despite its relatively recent emergence into the public consciousness, blockchain technology is not new. Rather, DLT represents the innovative adaptation of existing technologies to provide new solutions to current technological challenges, such as streamlining information flows within complex, multi-stakeholder ecosystems.[16] The recent popularization or "hype" surrounding cryptocurrencies like Bitcoin and Ethereum, which represent just one possible application of DLT, has propelled blockchain to wider public attention — so much so that the term "blockchain" is sometimes used interchangeably with terms like "crypto" in many publications. Estonian company Guardtime's KSI blockchain timestamping service, for example, was already being developed for the government of Estonia when Bitcoin's foundational white paper was published in 2008.[17] In reality, distributed ledger technologies like blockchain have a wide variety of different applications, as also evidenced by the examples of recent commercial and government initiatives above.

Blockchain Enhances (Rather than Undermines) Confidentiality

Another of the many misconceptions surrounding DLT is that the distributed and decentralized nature of the technology does not allow for data confidentiality between a platform's different participants. Within permissioned systems, strict access controls can be established to govern how the different participants share information and what actions they can perform. The flexibility and potential interoperability of blockchain technology is such that each stakeholder can continue to maintain their own separate databases while a blockchain network provides an immutable record of past transactions among participants and validates the authenticity of shared records. In addition, rather than storing sensitive data or records on the blockchain network itself, hashes may contain only certain timestamped metadata that can still be used to validate the authenticity of any data or records transacted between participants.

Blockchain Can Be Environmentally Friendly

As many cryptocurrency and nonfungible token trading platforms recently grew in popularity, blockchain also became increasingly associated with the negative environmental impact of large public blockchains.[18] Bitcoin, for example, requires public volunteers to "mine" or contribute computational power to the wider blockchain network in order to solve the algorithms used to verify transactions. The computational power needed to sustain these large public networks is significant, and if the energy miners consume is not sustainably sourced, the environmental impact is equally significant. However, tokenization and open public access are common features of blockchain fintech applications, whereas blockchain solutions designed to address supply-chain management or regulatory reporting, such as in the examples provided by IBM's Food Trust and the De Beers Tracr platform, are more likely to be permissioned to a select number of participants, with fewer nodes and less demand for computational power. Stakeholders may also choose to implement newer, more energy-efficient cryptographic algorithms used to validate transactions (i.e., Proof of Stake versus Proof of Work).[19]


Hapag-Lloyd
APL
CMA CGM
STOP
STOP

Conclusion

As the global trade in conventional arms continues to grow, so too will the complexities of managing, tracking, and regulating the enterprise. At a time when global tensions are high and armed conflict is proliferating, ensuring that arms transfers are evaluated, tracked, and conducted responsibly and within robust control and regulatory ecosystems becomes all the more important. To meet the moment, governments and private sector stakeholders are already adopting new technologies to improve the efficiency, integrity, and efficacy of arms transfer management ecosystems.

DLT offers benefits that, if appropriately implemented, can enhance and improve key information and management processes essential to the international arms transfer enterprise. In so doing, national authorities stand to enjoy greater interagency visibility into arms transfers, efficiency in their internal and external communications, and greater speed in meeting demands of international partners. Such an ecosystem could also improve the robustness of arms transfer decision-making, ensuring information pertaining to pre-transfer evaluations and risk assessments is readily available to key government stakeholders without sacrificing efficiency or timeliness.

Private sector actors could enjoy greater visibility into and clarity of control processes, reduced regulatory burdens by virtue of more efficient communications with national authorities, and greater visibility into their own supply chains.

Compared to other technologies, DLT is unique in providing the highest level of information integrity, confidentiality, and consensus-based information sharing among a variety of stakeholders. Unlike other conventional database systems, which have inherent vulnerabilities including single points of failure and susceptibility to data manipulation, DLT cross-references and validates hashed data across all nodes, ensuring information is accurate and highly-tamper resistant. The more expansive the DLT platform, and the more nodes it incorporates, the greater the benefits.

Nevertheless, practical and normative barriers still present a challenge to DLT's adoption and application. Any DLT ecosystem would require digitization of records among participants, something that may be both financially and technically burdensome for lower income countries, as well as a breach of cultural preferences for paper records as a means of validation and provenance. Additionally, institutional conservatism around the adoption of new technologies, especially technology that would allow data transactions across multiple participants, touches on understandable concerns around security and confidentiality, especially among national governments. Because government actors are, generally, cautious about engaging in digital ecosystems that include nongovernment or foreign government entities, advancing DLT as a tool for arms control and management would require educating key stakeholders about the safeguards and technical modalities of DLT-enabled platforms. This might include the development of a prototype DLT platform that could facilitate hypothetical arms transfer decisions and illustrate to relevant stakeholders in a highly concrete manner the technical contours of the technology's real-world applications. Such research could build on the initial findings of this brief as well as on one of the proposed scenarios below.

Annex: Hypothetical DLT Ecosystems

To support this scoping exercise and to illustrate the modalities of a potential DLT ecosystem, this section offers three distinct and hypothetical DLT-enabled ecosystems for arms control and management.

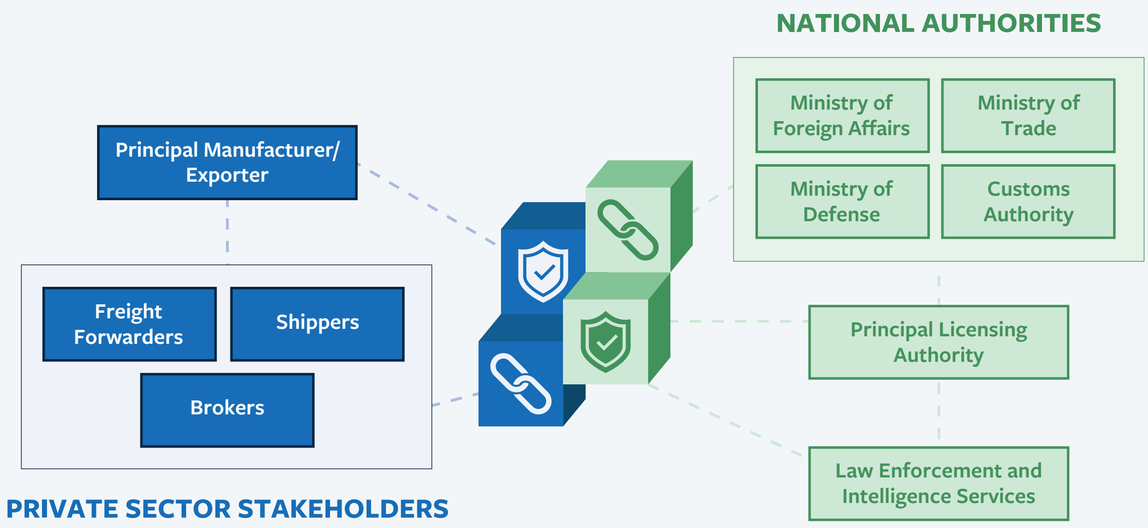
Developing these hypothetical scenarios illustrates the importance of considering which stages, stakeholders, and transactions would be encompassed in a DLT-enabled ecosystem. Given DLT's broad utility, the scope of its implementation will depend largely on the preference, equities, and comfort of the interested stakeholders. The scenarios below consider hypothetical ecosystems on three different scales — as a tool for managing and transacting information for domestic licensing and compliance purposes, a platform to manage and verify transactions bilaterally between two state participants, and a multi-state ecosystem involving numerous countries as well as multilateral institutions.

Scenario 1 – Single Country, Industry Licensing, and Compliance Ecosystem

Scenario 1 imagines a DLT-enabled environment for the purposes of facilitating and managing domestic licensing and pre-export compliance between national authorities and private sector stakeholders. The principal forms of data and tracking pertain to compliance paperwork, including licensing and customs documents.

The participants, or "nodes" within this digital ecosystem (see Figure 5 below) include manufacturers/principal exporting parties, government licensing and adjudication authorities, customs and compliance entities, and transfer facilitators including freight forwarders and shipping entities.

Figure 5: Scenario 1 — DLT Nodes



These participants use a DLT platform to transact information in conformity with confidentiality agreements and while maintaining full ownership of their individual databases and proprietary information systems. All information transacted is voluntarily shared among the participants.

Transactions begin with the manufacturer's/principal exporting party's submission of a license application into the ledger, triggering notifications to the relevant licensing authority and, based on the individual requirements of the country's control system, other stakeholders in the national adjudication process.

Participants using this DLT platform may only access and transact data according to certain permissions established to ensure data confidentiality. Potential licensees, for example, would be able to see, in real time, the status of their applications within the digital chain of custody, allowing greater transparency within the broader ecosystem for both public and government actors. Similarly, upon final approval, all the necessary stakeholders may view and verify the issuance of an adjudicated license, including relevant customs and private sector stakeholders.

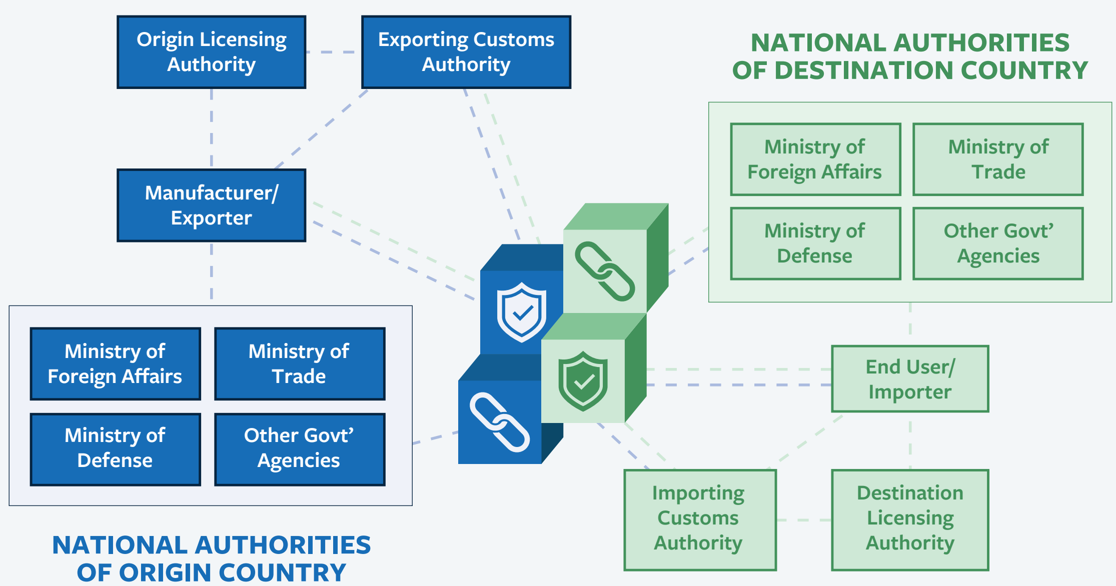
In this scenario, a DLT solution provides greater transparency for licenses and other export control-related documentation and enables all stakeholders to access relevant information in line with established permissions to streamline information sharing and expedite the final departure of defense articles. Such a system allows customs authorities to engage more readily with private sector stakeholders to verify compliance with pre-export control measures, as well as to ease the burden on manufacturers and freight forwarders. In addition, law enforcement and intelligence services are able to more easily access information within the DLT platform, facilitating more rapid investigation of possible compliance or regulatory violations.

Scenario 2 – Bilateral Transfer Tracking and Management Ecosystem

Scenario 2 imagines a management and control ecosystem between two countries for the purposes of both verifying, reconciling, and tracking bilateral arms transfers. This DLT ecosystem effectively records transfers between the two countries, maximizing transparency and reducing the likelihood of discrepancies in either data or actual trade.

The participants, or "nodes" within this digital ecosystem (see Figure 6 below) include manufacturers/principal exporting parties, government licensing and adjudication authorities from both the exporting and importing country, customs and compliance entities from both the exporting and importing country, and transfer facilitators including freight forwarders and shipping entities.

Figure 6: Scenario 2 — DLT Nodes



As with Scenario 1, all participants use a hypothetical DLT platform to transact information in-line with confidentiality agreements and while maintaining full ownership of their individual databases and proprietary information systems. All information transacted is voluntarily shared among the participants and would reflect agreements and consensus among the governments of both importing and exporting countries.

Much of the functions and processes described in Scenario 1 could, if desired, be contained within Scenario 2 and simply feed into the larger architecture. In this scenario, for example, an adjudicated license, once logged into the DLT system, could trigger an import form on the part of the recipient country, automatically populated with the category, number, and value of the weapon system/s to be exported.

These forms could, subsequently, either be made available or trigger customs-related documentation for customs authorities from both the exporting and importing country, allowing both to assess physical shipments against authorized import or export documents.

As with Scenario 1, participants of the Scenario 2 DLT platform may only access and transact data according to certain permissions established to ensure data confidentiality. For example, private sector actors may only be able to access information pertaining to their license, but not necessarily the export and import forms shared between national authorities of the importing and exporting country. Similarly, shippers and freight forwarders may have even narrower data access, related to the authorized transport and transit pathways for the physical movement of the defense articles. All such permissions would be developed by consensus among the various parties involved.

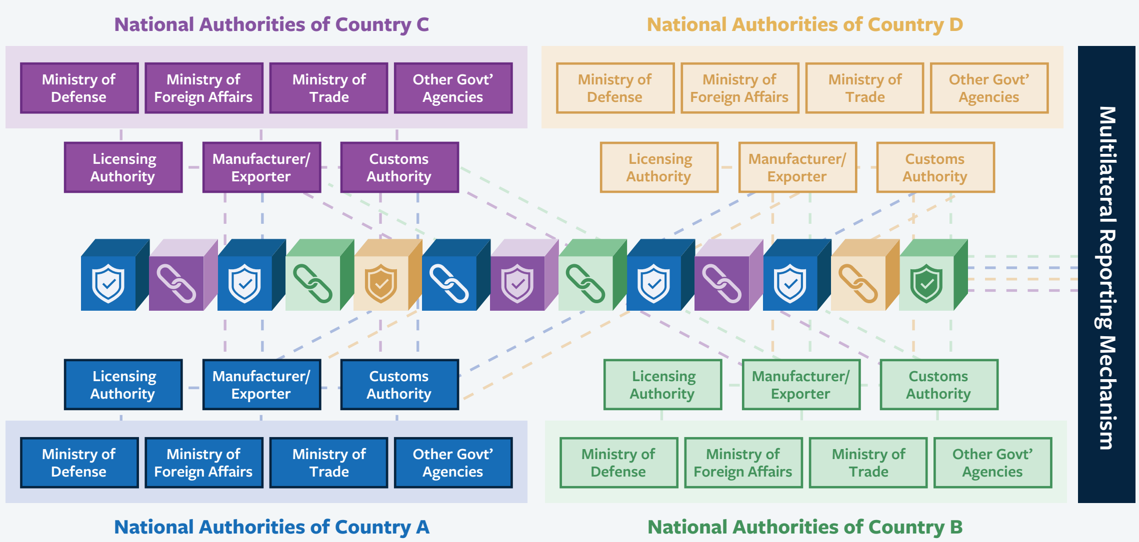
In this scenario, a DLT solution provides greater provenance over the chain of custody for export and import control-related documentation, enabling both countries to automatically verify and align exports and imports in a way that facilitates verification and compliance, while preventing trade discrepancies. Such an ecosystem can help mitigate diversion risks, while also reducing burdens on private sector stakeholders by automating key information sharing between compliance networks that would otherwise require manual data entry. This ecosystem could also incorporate physical tracking functions, whether through QR codes or other such features, to pair data to the physical movement of defense goods along the supply chain with license and customs documentation, providing all relevant parties with greater visibility and confidence in the supply chain.

Scenario 3 – Multi-Country Arms Transfer Tracking and Management System

Scenario 3 illustrates the most ambitious of the DLT-enabled environments. It imagines a multi-country ecosystem, composed of numerous governments and private sector stakeholders, as well as multilateral institutions concerned with the global arms trade. Such an ecosystem could facilitate tracking and data management for a significant portion of the global arms trade, acting as a permissioned register of arms transfer, automatically verifying import and export data across numerous nodes, flagging discrepancies, and facilitating multilateral reporting.

The participants, or "nodes" within this digital ecosystem (see Figure 7 below) include manufacturers/principal exporting parties, government licensing and adjudication authorities from both exporting and importing countries, customs and compliance entities from exporting and importing countries, and transfer facilitators including freight forwarders and shipping entities.

Figure 7: Scenario 3 – DLT Nodes



Scenario 3 mirrors many of the same functions as Scenario 2 but includes a wider network to incorporate multiple national control systems. As with the other scenarios, all information transacted is voluntarily shared among the participants and would reflect agreements and consensus among the governments of both importing and exporting countries. Each node within the platform could maintain its own unique databases that would be integrated into the platform using APIs. However, as with all the scenarios, digital recordkeeping and consensus about what data is captured would be a prerequisite, something that could prove challenging for such an expansive ecosystem.

Similar to Scenario 2, licensing and customs compliance processes for arms transfers could be captured in the DLT platform, allowing for simultaneous data verification between trading partners, leveraging automation and auto-population of documents. Transactions, at all stages of the transfer cycle for numerous nodes, could be logged and provide a tamper proof system of provenance across multiple countries. Similarly, import and export data, with the appropriate permissions and controls, could automatically be shared with multilateral bodies, aiding reporting requirements to instruments such as the Arms Trade Treaty or the UN Register of Conventional

Weapons. As with Scenario 2, participants of the Scenario 3 DLT platform may only access and transact data according to certain permissions established to ensure data confidentiality.

In this scenario, a DLT solution provides globally relevant provenance over the chain of custody for exports and imports of arms transfers, enabling numerous countries to automatically verify and match import and export data, facilitating trade compliance and, thereby, mitigating diversion risks. As with Scenario 2, this ecosystem could also incorporate physical tracking functions, whether through QR codes or other such features, to pair data related to the physical movement of defense goods along the supply chain with license and customs documentation, providing all relevant parties with greater visibility and confidence in the supply chain.

Summary of Hypothetical DLT Scenarios

Each of these scenarios leverages the unique technical advantages of DLT to address contemporary challenges or gaps in the arms transfer control and management systems, ranging from individual licensing transactions to global transfer chains. Each would require some degree of specialization for the platform, as well as consensus building among the nodes to develop appropriate permissions and to align data capture to reflect common measures and data points. The larger the ecosystem, the more important that consensus building becomes, particularly for the purposes of automation. Similarly, overcoming sensitivities around confidentiality and addressing legal questions around platform ownership and maintenance all become more severe as the ecosystem grows. Nevertheless, though expressed in very broad terms, these hypothetical scenarios illustrate the scale and scope of ecosystems that could be included in a DLT platform.

Endnotes

1. Hyperledger Foundation, "How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric," 2022, https://www.hyperledger.org/learn/publications/walmart-case-study.

2. Ibid.

3. IBM Blockchain, IBM Food Trust Solution Brief, June 2018, https://delaune.com/Awards/Delaune_Blockchain_Food_Trust_eBrochure.pdf.

4. Kate Vitasek, John Bayliss, Loudon Owen, and Neeraj Srivastava, "How Walmart Canada Uses Blockchain to Solve Supply-Chain Challenges," *Harvard Business Review,* January 2022, https://hbr.org/2022/01/how-walmart-canada-uses-blockchain-to-solve-supply-chain-challenges.

5. De Beers Group, "De Beers group introduces world's first blockchain-backed diamond source platform at scale," 5 May 2022, https://www.debeersgroup.com/media/company-news/2022/de-beers-group-introduces-worlds-first-blockchain-backed-diamond-source-platform-at-scale.

6. Mark Rakhmilevich, "Ensuring sustainability and ethical sourcing with Oracle Blockchain Platform," Oracle Blockchain Blog, February 2019, https://blogs.oracle.com/blockchain/post/ensuring-sustainability-and-ethical-sourcing-with-oracle-blockchain-platform.

7. Oracle, "Oracle Blockchain Platform for Verifying Diamonds," 3 May 2019, https://www.youtube.com/watch?v=zdwv4gpgDsM.

8. Tae Il Kang, "Korea pilots blockchain technology as it prepares for the future," World Customs Organization News, 22 February 2019, https://mag.wcoomd.org/magazine/wco-news-88/korea-pilots-blockchain-technology-as-it-prepares-for-the-future/.

9. Korea Customs Service, "Block Chain e-C/O – Industry 4.0: Customs Innovation," Korea Customs Service. 30 January 2019, accessible from: https://www.customs.go.kr/english/na/ntt/selectNttList.do?mi=8025&bbsId=1746.

10. Korean Customs Service, "New Technologies in Customs Innovation," 17 March, 2022. https://www.youtube.com/watch?v=Ocu-7qfWkMI&t=212s.

11. Cindy Vestergaard, Gabrielle Green, Edward G Obbard, Edward Yu, Guntur Dharma Putra, *SLAFKA: Demonstrating the Potential for Distributed Ledger Technology for Nuclear Safeguards Information Management,* The Henry L. Stimson Center, 17 November 2020. https://www.stimson.org/2020/slafka/.

12. Cindy Vestergaard, "SLAFKA: One Year On," European Safeguards Research & Development Association (ESARDA), *Connector,* Issue 4., 21 June 2021, accessible from: https://esarda.jrc.ec.europa.eu/publications/connector-n4_en.

13. The Henry L. Stimson Center, MATCH Prototype, 2022, https://www.stimson.org/project/match/.

14. The typologies identified here draw heavily from the Flemish Peace Institute's 2022 report on regulatory frameworks and control measures for the transit and transshipment of military goods: Diederik Cops, Kathleen Vanheuverswyn, "Under the Radar: Transit of Military Goods from Licensing to Control," Flemish Peace Institute, April 2022, 15, 17-18; Interviews with government regulators and commercial actors engaged in licensing and compliance.

15. Pieter D. Wezeman, Justine Gadon and Siemon T. Wezeman, "Trends in International Arms Transfers," Stockholm International Peace Research Institute, March 2023, 1.

16. 15 Chris Jaikaran, "Blockchain: Background and Policy Issues," Congressional Research Service, 28 February 2018, 1, accessible from: https://crsreports.congress.gov/product/details?prodcode=R45116.

17. Guardtime, "GDPR Compliance using KSI® Blockchain," Guardtime Whitepaper on VOLTA, its KSI® blockchain-based solution for GDPR, 2017, 5, https://m.guardtime.com/files/Guardtime-whitepaper-Volta.pdf.

18. The White House Office of Science and Technology (OSTP), "FACT SHEET: Climate and Energy Implications of Crypto-Assets in the United States," White House Press Release, 8 September 2022, https://www.whitehouse.gov/ostp/news-updates/2022/09/08/fact-sheet-climate-and-energy-implications-of-crypto-assets-in-the-united-states/.

19. Marc Blinder, "Making Cryptocurrency More Environmentally Sustainable," *Harvard Business Review,* 27 November 2018, https://hbr.org/2018/11/making-cryptocurrency-more-environmentally-sustainable.

The Stimson Center promotes international security and shared prosperity through applied research and independent analysis, global engagement, and policy innovation.

STIMSON.ORG

STIMSON

INNOVATIVE IDEAS CHANGING THE WORLD