BTI Institute
Borders • Trade • Immigration
A Department of Homeland Security Center of Excellence

Transforming Trade and Ensuring Global Supply Chain Security with Blockchain and Smart Contracts

Released March 2020

The Borders, Trade, and Immigration Institute

A Department of Homeland Security Center of Excellence
Led by the University of Houston

Thank You

This product, along with everything we do, is dedicated to the men and women of the United States Department of Homeland Security. We thank them for their tireless efforts to secure our Nation and safeguard our economic prosperity by facilitating lawful travel and trade.

Specifically, we want to thank the team with U.S. Customs and Border Protection Business Transformation & Innovation Division for championing this project.

Contact
Email: bti@uh.edu
Website: www.uh.edu/bti/
Twitter: @bti_uh
LinkedIn: Borders, Trade, and Immigration

Project Report

Transforming Trade and Ensuring Global Supply Chain Security with Blockchain and Smart Contracts

December, 2019

Project Report

Transforming Trade and Ensuring Global Supply Chain Security with Blockchain and Smart Contracts

Prepared for the Border, Trade, and Immigration Institute at the University of Houston - A Center of Excellence Sponsored by the Science & Technology Directorate, Department of Homeland Security.

Project Period	2018 - 2019.

Project team

Larry (Weidong) Shi, Ph.D.	University of Houston
Lefteris Iakovou, Ph.D.	Texas A & M University
Mr. Vincent Iacopella	Licensed Customs Broker, Trade Co-Chair of the 14th COAC Committee

Project champion

Mr. Vincent Annunziato	Director, Office of Trade, U.S. Customs and Border Protection

Additional contributors

Ms. Dana Alsagheer
Mr. Keshav Kasichainula
Mr. Damon Spencer
Kelvin Gao, Ph.D.
Lin Chen, Ph.D.

Acknowledgments

This document was prepared as an account of work sponsored by the Office of University Programs (OUP), U.S. Department of Homeland Security (DHS) under Grant Award Number 2015-ST-061-BSH001 to the Borders, Trade, and Immigration (BTI) Institute: A DHS Center of Excellence led by the University of Houston. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

We would also thank OUP, the OUP program manager, the project champion, the BTI directors and administrators, staffs, as well as the partners and collaborators for their support and feedback of this project. Special thanks will extend to people and stakeholders who provided feedback to the study report, and contributed to the teleconference interviews.

Contents

1

Executive Summary

Blockchain is a technology capable of providing a global view of the supply chain for visibility without using a traditional centralized infrastructure. As such, it holds the potential to improve efficiency in the global supply chain, facilitate data sharing and data exchange among supply chain stakeholders including the regulatory authorities and Customs, ensure compliance with the trade laws, and facilitate legitimate cross-border commerce. Recent global supply chain digitalization initiatives attempt to demonstrate the value of blockchain for end-to-end (E2E) supply chain visibility, facilitating collaboration along the supply chain value chain, and allowing the stakeholders (e.g., suppliers, producers, logistics providers/3PLs, shippers, importers, exporters, Customs brokers, and regulatory agencies) to share and exchange information with improved effectiveness.

Realizing its potential to transform global trade, many global trade oriented international organizations have created blockchain related initiatives. The efforts may include setting up a team to identify use cases of blockchains to the global trade, develop future plans in terms of standardization and coordination, or create a framework for pilots and PoCs that may involve multiple stakeholders. According to the WCO, with support of blockchain technologies, Customs would be able to collect the necessary data in an accurate and timely manner (all data tied to the imported goods such as seller, buyer, price, quantity, carrier, finance, insurance, status and location of the commodity, product information, etc.).

Data conveyed by the blockchains could be integrated automatically into the Customs systems and validated against the data submitted by the traders and carriers. With incoming adoption of the blockchains by the global supply chain industries, functions of Customs could be more integrated with the digital platforms of global supply chains such as goods could be automatically cleared within the supply chain blockchains or distributed ledgers.

Despite significant advances in recent years applying electronic and digital based solutions for entry and declaration related process, the current system still faces some challenges that may be addressed using blockchains. These include: data fragmentation due to multiple views of the supply chain information (trade/commercial view, logistical view, financial view, and regulatory view); limited data sharing between the regulatory agencies and the private sectors; unstructured and uncorrelated data embedded in the trade documents; manual document processing and reconciliation of multiple databases that store the same information; and trustworthiness, timeliness, and quality of the data entered into the Single Window system.

Blockchains offer opportunities to tackle some of these challenges and pain points. Blockchain enabled supply chain visibility allows agencies to gain deeper integration of the entry process with the supply chain information flows Customs and partnering agencies can thus have a clear picture of the trade related information regarding the imported goods, facilitating collection and validation of entry data. As the entry processing becomes more information driven leveraging blockchain based supply chain data, correlation of entry data across support documents will become easier. It will also create new opportunities of automation, and reduce manual work required for entry declaration. The improved data quality and efficiency would allow Customs to prioritize their resources with more accurate risk based assessment, and therefore be able to focus on the high risk imports. As a result, it will create many benefits to help Customs accomplish its mission, and address high priority trade related issues.

Blockchains may enable uniform access to all the four business areas of data views in the global supply chains and trade (commercial, financial, logistical, and regulatory), which could significantly enhance the capabilities of Customs and regulatory agencies for accomplishing their missions and facilitating legitimate flows of goods [1].

Specifically, blockchains may enable:

- Early and advance sharing of commercial and trade data between the trade actors and the regulatory authorities in pre-export commercial phase for purpose of trade facilitation and improved Customs control. The trade view involves discovery of products by potential buyers, identification of business partners, establishment of agreements for purchasing goods, and activities dealing with the fulfillment of the purchase order. The trade view reflects the services sought by the trade actors, such as buyers, sellers and manufacturers of the goods.

- Data cooperation between the supply chain actors, which can enable supply chain visibility, and a holistic view and connectivity of data from all the four process areas (trade/commercial, logistical, regulatory, and financial).

- Information driven data exchange between the supply chain actors over distributed ledgers that eliminates data duplication, error prone manual processing of data; facilitates timely sharing of supply chain data between the stakeholders; assures data quality and integrity; improves trust between the supply chain actors; enhances supply chain predictability by improving information flow; and reduces administrative cost.

[1] Despite the differences, in this report, to simplify discussion, we use blockchain and distributed ledger somewhat interchangeably.

- Enhanced automation by integrating distributed ledgers with the entry process.

Advance information sharing with the Customs and the regulatory authorities during the trade phase may provide many benefits to both sides in terms of trade facilitation. These include:

- Facilitating risk management by establishing patterns of commercial data, and risk profiles.
- Demonstrating evidence of reasonable care and compliance during supply sourcing and procurement stage of trade.
- Reducing delays at port of entries, expediting clearance and release upon arrival due to decreased risk perceived by the authorities.
- Decreasing supply chain uncertainty, disruption, and risk by integrating distributed ledger with the trade process.

Distributed ledgers may enable the possibilities of global scale distributed identity management for traders, economic actors, manufacturers, and products. Based on more accurate information of identities of economic actors, manufacturers, and imported products, regulatory authorities can increase targeting efficiency with the existing resources by focusing on the high risk entries.

Many partnering agencies have third party testing and certification programs, the process may be facilitated with distributed ledgers. Through a holistic product life-cycle data management, the community of producers, laboratories, accredited bodies, regulators, and consumers may work together to create a cooperative distributed ledger based environment, for sharing product testing outcome, compliance and product quality certification, licensing, and others with all the relevant actors having access to the related information.

Data sharing through “permissioned” or private ledgers in a secure and cooperative manner between the supply chain actors can lead to end-to-end “data pipelines” such that accurate supply chain information can be shared between the involved actors in real-time.

With necessary information lodged in the ledgers, blockchains provide benefits to the trader and broker side because workload can be reduced to accurately assemble the required information for declaration. The process to prepare declaration could be partially or completely automated. On the Customs side, with access to the ledgers, blockchains reduce manual verification and resources required to validate the data contained in the declarations. This would result in better data quality, faster entry processing, and reduced end-to-end lead time.

Distributed ledgers may help post release compliance verification, detection of red flags for mitigating risk of AD/CVD evasion, mis-invoicing, and bond insufficiency, and improvement of audit decisions. Under the new process, distributed ledgers will be used to promote transparency of supply chain information, sharing of risk profiles related to illicit financial flows, and data cooperation environment between trade finance, insurance, surety, and Customs. This would potentially help address issues of mis-invoicing, illicit financial flows, mis-declaration, revenue risks, and etc.

There are different data cooperation dimensions including G2G (Government to Government), B2B (Business to Business), B2G (Business to Government), G2B (Government to Business), and A2A (Agency to Agency). B2B ledgers are often driven by digitalization and data cooperation needs by the global supply chain industry to improve supply chain efficiency, visibility, and transparency. Business process can be automated and integrated with shared ledgers. There could be multiple ledgers (vertical or horizontal) led by different supply chain sectors such as trade finance, freight forwarding, retail, pharmaceutical supply, and manufacture industry.

Cooperation between different government agencies on trade facilitation may be realized via shared ledgers by the government agencies such that supply chain related information can be exchanged and disseminated in real-time between the agencies for trade facilitation, advanced targeting, risk management, and etc. This approach allows resources to be shared between the agencies and may reduce cost for maintaining and managing ICT infrastructure by using a common distributed data platform.

Distributed ledgers can contribute to the overall big data oriented vision for Customs. Information pulled from the supply chain ledgers can be integrated and combined with other sources of data to assist risk assessment and decisions to entry declarations.

Today, there exist many different blockchain and distributed ledger projects, often led through a consortium or trade organization focusing on developing supply chain ecosystems by leveraging the blockchain and distributed ledger technologies. In addition, each ledger system may attempt to create an ecosystem around its users, and integrate the supply chain actors horizontally, vertically, or both along the value chains.

To support interoperability of different supply chain ledgers, it is plausible to implement a common inter-chain ledger, which can verify cross chain transactions on behalf of the users. This common inter-chain ledger hides heterogeneity ledger design, infrastructure, operation, and governance model of the multiple connected supply chain ledgers. It offers a unified interface to the supply chain stakeholders to validate transactions or claims made by an actor. The verification can be done irrespective of which ledgers the inputs are originally created and stored.

The early public blockchains that adopt Proof-of-Work consensus mechanism sometimes can only support probabilistic transaction finality. Fortunately, not all the consensus processes rely on the same principle. Most permissioned or private distributed ledgers use more efficient consensus protocols based on well-established theories in distributed computing. These consensus protocols don't have the same transaction finality issue that the PoW based systems have, which perhaps make them better options for the supply chain industries or cross-border trade use cases.

In a public ledger or blockchain, each new “block” of transactions is verified and then appended immutably to the end of the “chain” of prior transactions, so it can’t be altered. All the information about every transaction is made public. This understandably raises concerns from the supply chain stakeholders and makes them resistant to such kind of public disclosure.

There have been significant efforts to enable strong privacy and confidentiality assurance over distributed ledgers. Although it is still an area of active research, privacy may be preserved using different approaches below:

- Side-chain or off-chain transactions: where private transactions between the supply chain stakeholders can be conducted off-chain or using side-chain transactions. The results can be merged later back to the main chain.
- Decentralized access control: For data sharing, it is possible to implement fine grained data access control using distributed ledger and mature secret sharing technologies. Decentralized access control can significantly improve protection of data confidentiality and support auditable history of data accesses.
- Private transaction protocols using zero-knowledge proofs: Zero-knowledge proofs are cryptographic schemes where a prover is able to convince a verifier that a transaction statement is true, without disclosing any more information than that the statement is true. It can be applied to implement auditable blockchain transactions with data confidentiality and privacy preserved.
- Secure hardware execution environment and enclave: Data confidentiality of blockchain transactions can be assured using secure hardware execution environments, a feature offered in products by most modern computer hardware vendors. An advantage of such approach is that it allows confidential general purpose computation over distributed ledgers, for instance, machine learning and data mining of private blockchain data in a network of multiple stakeholders.
- Secure multi-party computation integrated with the blockchains: Data privacy could be alternatively protected under the classic multi-party computation framework where transaction validation, audit, and compliance can be verified by third parties meanwhile satisfying data confidentiality constraints.

Due to adoption of privacy oriented public blockchain projects, zero-knowledge based protocols are gaining support and popularity in blockchain projects where privacy and data confidentiality are mandatory requirements for the projects to gain adoption. Zero-knowledge based protocols could be applied to support the following use case scenarios:

- Enable private transactions: Zero-knowledge protocols allow blockchain transaction details to be kept private by the involved supply chain parties; and at the same time, the transactions can be verified and audited by the blockchain participating nodes.

- Hide transaction flows and avoid data mining by other blockchain nodes/participants: Besides privacy of transaction data itself, supply chain business actors may wish to eliminate any chance that leaks confidential information to other participants of a common ledger such as business relations, supply chain patterns, and statistical data through flows of transactions. With zero-knowledge protocols, it is plausible to achieve that all the supply chain transactions lodged in a ledger are both verifiable and indistinguishable from one another (mean that they all appear the same to the validators and no statistical information of any kind can be extracted based on the transaction history lodged in a shared ledger by a supply chain actor).

- Support data migration across private chains with different governance policies: Zero-knowledge protocol may facilitate data migration and portability when information is exported from a private ledger and imported by another ledger with different governance rules and operation models.

- Enable private access to data lodged in blockchains: Zero-knowledge protocols may enable confidential access to blockchain transactions where both flexible access management and privacy of data requester can be guaranteed. This protects regulatory agencies and supply chain entities from accidentally disclosing data of interest through history of data accesses and requests.

- Privacy preserving digital identities: Zero-knowledge protocols allow privacy-preserving querying of digital credentials and licenses.

A consortium blockchain refers to a blockchain where several supply chain related entities work together to form an alliance and participate in its management. It is one of the favored approaches for creating enterprise grade blockchain platforms. Members of the consortium may collaborate to determine how the blockchain is implemented and operated. Each entity may run one or multiple nodes.

A major challenge with the consortium model is potential fragmentation of standards and blockchain platforms because there exist many competing blockchain consortia targeting supply chain stakeholders, and engaging in activities to develop their own standards. One implication of the environment comprising multiple supply chain and logistics blockchain consortia to future entry process and integration of Customs functions with these blockchain systems is that data collection has to be planned and designed under a multi-sector and muti-chain context. Information collected from the multiple chains needs to be correlated and linked. This suggests the importance of open standards. The various supply chain consortia, organized by the industry members, may not always necessarily put adoption of open standards as its priority.

Regulatory authorities could play a constructive role in the process to promote adoption of uniform standards and avoid isolated blockchain ecosystems.

As the blockchain based systems gain traction in the global supply chains, it will encounter the same challenges as the prior and other existing efforts in paperless trade and supply chain document digitization. For instance, uncertainty over the legal status of the electronic transferable records such as electronic letters of credit, electronic bills of lading in the context of different jurisdictions, has been identified as one of the obstacles that hinder wide adoption of electronic trade documents and other related instruments.

Potential policy barriers of blockchain adoption also stem from the inherent nature that global trade is inter-jurisdictional. When talking about flow of electronic trade documents and information, a blockchain based trade infrastructure has to satisfy regulatory obligations within different jurisdictions.

Harmonizing legal status of electronic trade information and blockchains may take significant amount of time before it is approved and enacted by different jurisdictions. Meanwhile, global trade and supply chain industries may leverage blockchain consortium for creating governance policies and playbooks for permissioned supply chain ledgers.

As blockchain consortia often are led by private sector entities, there are questions how regulatory authorities and border related agencies coordinate and interact with these blockchain consortia to make sure that the developed approaches cater to the regulators' needs, fit with the government's agenda regarding emerging technologies, and the deployed systems could work with the regulators' operational environments so that the benefits of new technologies can be realized.

This could be achieved through private-public dialogue. There are different ways that regulatory agencies could work with the industry led blockchain consortia. A more efficient and practical approach is to leverage the existing private and public channel such as the COAC to facilitate dialogue between the private sectors and the regulatory authorities regarding emerging technologies. This would avoid repeated efforts dealing with each blockchain consortium separately for discussing the same issue of concerns by the regulatory authorities.

At present, a number of efforts exist to advance interoperable and open standard based approaches for distributed ledgers. These include efforts by the UN/CEFACT, the WCO, the W3C, ISO, etc.

Regardless the policies and best practices developed, technological neutrality perhaps is one of the most essential principles for guiding policy makers regarding new technologies. This means that the regulatory requirements and laws should neither exclude, nor require and assume the use of a particular technology. In a rapidly changing digital and technology environment, the principle should also ensure that future and emerging technologies can be accommodated.

Preliminary discussion with the trade stakeholders suggests that the trade community is open to changes such as an entry process integrated with the blockchains. For such a new system, protection of data confidentiality in distributed ledger environment needs to be considered as a top priority. With increased amounts of data pulled from the blockchains, tools are required to map, filter, link, and process the data. The process needs to be transparent to the filers and brokers so that they will be able to assist and certify the information.

2

Introduction

The overarching goal of this project was to: (i) explore innovation opportunities provided by the blockchains and other relevant technologies for transforming the entry data collection process in order to facilitate timely analysis of supply chain risks, and to ensure trade compliance; (ii) conduct feasibility evaluations of simplifying entry data collection by integrating and leveraging commercial blockchain based end-to-end supply chain ecosystems; (iv) identify values and use case scenarios of alternative and new technologies for entry data collection; and (iii) provide assessment (technical, business flow, and operational aspect) of the viability of blockchains and related innovations to Customs and partnering agencies.

2.1. Purpose and Scope

The international supply chains are characterized by flows of goods and related data. These are aligned with the movement of associated funds which reflect the transaction nature of supply chains. Combined together, they constitute, flows of goods, documents, information, and finance. Typically, these flows are linked to specific events in the supply chains. Goods flow from the exporter to the importer in return for funds that flow in the reverse direction. The flow of goods and funds is supported by a bidirectional flow of data such as purchase orders, invoices, shipping notices, bills of lading, letters of credits, certificates of origin, and import/export declarations lodged with the regulatory authorities. Entry declarations of imported goods are submitted to Customs electronically through a unified portal of Single Window implementation. The entry data are routed to the relevant partnering agencies who regulate the imported goods. Each year, CBP processes over 30M entries and collects around $44 billion revenue (duties, fees, and tariffs).

Global supply chain is a sophisticated ecosystem with many stakeholders, e.g., exporters, importers, origin/destination agents, Customs bonded warehouses, financial intermediaries, ports, shipping lines, insurance companies, brokers, Customs, and border related regulatory agencies. The complexity results in enormous challenges in maintaining the flow of the supply chain information, data, and documents, severe problems in terms of supply chain efficiency, visibility and transparency. The existing document centric process for exchanging supply data between the supply chain stakeholders still needs improvement regarding data quality, process automation, data integrity, data validation, efficiency, human labor and administrative cost, etc.

The global supply chain business operations and regulatory authorities demand new capabilities of efficient supply chain data sharing infrastructures to tackle these challenges in order to facilitate legitimate flow of goods without jeopardizing security of the homeland and assuring compliance with the trade laws. Many of the described challenges potentially might be tackled with a globally centralized database where all the global supply chain stakeholders would use for sharing supply chain data and documents. However, because the number of parties involved is large and they are geographically distributed over multiple jurisdictions, it is impossible to have such a centralized service that connects all of them and stores every piece of information in one place. Even if such a centralized system could be set up, security of the information stored in such centralized system becomes a major concern (e.g., the records could be modified, removed, or added illegally by malicious cyber actors or insiders).

Blockchain is a technology capable of providing a global view of the supply chain and visibility without using a traditional centralized infrastructure. As such, it holds the potential to improve efficiency in the global supply chain, facilitate data sharing and exchange among the stakeholders including regulatory authorities and Customs, ensure global trade compliance, and facilitate legitimate cross-border commerce. Recent global supply chain digitalization initiatives attempt to demonstrate the value of blockchain for achieving end-to-end (E2E) supply chain visibility, facilitating collaboration along the supply chain value chain, and allowing stakeholders (e.g., suppliers, producers, logistics providers/3PLs, shippers, importers, exporters, Customs brokers, and regulatory agencies) to share and exchange information with improved effectiveness.

According to the WCO [75], with support of blockchain technologies, Customs would be able to collect the necessary data in an accurate and timely manner (all data tied to the imported goods such as seller, buyer, price, quantity, carrier, finance, insurance, status and location of the commodity, product information, etc.).

Data conveyed by the blockchain could be integrated automatically into the Customs systems and checked against the data submitted by the traders and transporters. With incoming adoption of blockchains by the global supply chain industries, functions of Customs could be more integrated with the digital platforms of global supply chains such as goods could be automatically cleared within the supply chain blockchains or distributed ledgers.

To investigate the potential of blockchains for transforming entry process and facilitating legitimate global trade, the team conducted this study with the following scope:

- Conduct feasibility investigation of pulling out new sources of trade and supply chain data from the supply chain blockchains, and transforming the process of entry data collection process by the Customs and regulatory agencies to enhance capability of risk-based analysis, and visibility of global supply chain security.

- Brainstorm opportunities and new approaches for entry re-engineering by leveraging advances of new technologies such as blockchains, and distributed ledgers.
- Work closely with industry stakeholders, subject matter experts, and the project champion to evaluate these new approaches.
- Understand incentives, economic models, and benefits to the industry stakeholders and the regulatory agencies regarding adoption of blockchain based end-to-end supply chain and trade platforms, often led by a consortium of supply chain, finance, logistics and trade stakeholders.
- Identify use cases, and data collection process for the proposed technologies.
- Analyze potential issues such as governance models, policies, regulatory changes, interoperability, as well as incentives for sharing and exchanging supply chain information lodged in the supply chain blockchains by the industry stakeholders with the Customs and regulatory authorities.

2.2. Research questions

The goal of the project is to work closely with the private sector and government stakeholders and leverage new technologies around blockchains for improving the mission of Customs in facilitating global trade and ensuring compliance with the trade laws and regulations. This can be achieved by taking advantage of the unique characteristics of blockchains (e.g., consensus driven, data exchange in decentralized/distributed IT environment, immutability of history, strong protection of data integrity, cyber-attack resilience, built-in support of auditability), to streamline and harmonize the exchange of global supply chain information, improve data quality, support the timely analysis of supply chain risks, and contribute to more efficient entry processes between the Customs and the global supply chain stakeholders.

Some of the research questions include:

- How the Customs and the regulatory agencies leverage end-to-end supply chain ecosystem for efficient sharing and tracking of trade related documents, data, and information to enhance their missions (trade facilitation, import security, and trade enforcement)?
- What are the benefits for the Customs and the regulatory agencies to tap into the blockchain based end-to-end supply chain and trade ecosystems, often led by a consortium of supply chain and trade stakeholders? How could such efforts streamline and enhance the current entry process to collect global supply chain data?

- How should potential new sources of trade and supply chain data (e.g., purchase orders, invoices, shipping data, manufacturer data) be pulled from the global supply chain blockchain ecosystem, and be integrated, harmonized or linked to data collected by CBP (pre-entry, entry, post-entry) for enhancing capability of risk based analysis and management?

- What are the operation and governance models if the Customs and regulatory authorities attempt to participate in the network of digital supply chains over the blockchains?

- What are the potential issues, opportunities, policies, obstacles, as well as benefits for sharing and exchanging supply chain data (lodged in the supply chain blockchains) by the industry stakeholders with the Customs and government stakeholders?

- What are the options and recommendations for a path forward where interoperability and standardization can be achieved?

2.3. Methodology

We organized project efforts by applying the DSR methodology (Design Science Research), which is an established and proven practice for re-designing business process. According to the DSR, efforts can be divided into phases below: understanding the problem (entry data collection and business process), brainstorm for suggestions and ideas, process redesign, evaluation through engagement with the stakeholders, and report.

To achieve the project goals, the research team conducted literature survey, in depth analysis; brainstorming sessions; gathering of pilot experiences/lessons learned; teleconference meetings and discussions with the private industry stakeholders, COAC consultants, and government side subject matter experts. Applying A/B tests, the endeavor was to develop objective assessment of both viability and benefits for the Customs and the global supply chain stakeholders regarding use cases of blockchain for improving data quality and harmonization, business process automation, enhancement of global supply chain data alignment and correlation for the goal of increased efficiency and supply chain visibility in cross border trade.

2.4. Summary of project efforts and activities

Working closely with the project champion and subject matter experts, the project team:

- Carried out investigation to document and map AS-IS landscape of entry business process. This was achieved using publicly available entry related documents and business process guidelines published by CBP (e.g., [4, 5, 7, 8, 42, 43]); insights and comments from the project champion, consultant, and subject matter experts; as well as relevant literature (e.g., academic research papers [81], WCO reports [75], WTO reports [61] and documents, GAO reports [12–15]).

- Conducted comprehensive literature survey on entry process modernization driven by new technologies such as digitalization, advanced data sharing platforms, IoTs, and AI, in particular potential application of blockchains to global supply chain management and its impact/opportunities to Customs entry process. The surveyed literature include: reports of CBP blockchain related pilots; reports from the international bodies such as the WCO, the WTO (focus on data sharing, and blockchain), the UN/CEFACT [22], the ISO [19], the WEF [41, 59]; reports/whitepapers focusing on application of blockchain to global supply chain management [2, 9, 10, 22], trade finance [31], and logistics; blockchain use case studies focusing on cross border trade; workshops/presentations/ keynotes focusing on blockchain application scenarios relevant to the missions of Customs and entry process; reports on application use cases of blockchain for detecting fraud in entry process (e.g., VAT fraud, trade based money laundering).

- Based on the results of the steps above, conducted brainstorms to create ideas and suggestions for entry process re-design.

- Analyzed the AS-IS flow of data attributes and documents for entry process and conducted ontology map at entry data element level.

- Summarized the analysis and brainstorm outcome as new processes.

- Conducted Before/After analysis in terms of benefits such as gains achieved and pains reduced.

- Conducted surveys and interviews of stakeholders on adoption of blockchain as data sharing solution for entry process.

- Engaged with the stakeholders (e.g., brokers, importers, logistics providers) relevant to the project mission though the project consultant, and the project champion.

2.5. Outline of the rest of the report

The rest of the report is organized as the following:

Chapter 3 provides brief background information of blockchains and distributed ledgers; describes some emerging trends of blockchain technologies; summarizes relevant efforts by the WCO, UN/CEFACT, WEF, and etc.; and discusses the overall opportunities of leveraging blockchains for entry process.

Chapter 4 is one of the main parts of the report. It summarizes the efforts and results applying DSR. After briefly describing the methodology, it describes the AS-IS business process for entry processing, followed by analysis. Then it provides suggestions to improve the process, and analysis of the changes.

Chapter 5 focuses on technology feasibility evaluations. It covers several sub topics including, support for inter-ledger operations, standardization, data collection from multiple supply chain ledgers, consensus finality related issues, assurance of supply chain data privacy and confidentiality lodged in common supply chain ledgers, scalability and performance of blockchains, and etc.

Chapter 6 summarizes results of the stakeholder interviews.

Chapter 7 and Chapter 8 discusses non technical related issues such as supply chain blockchain governance, policies, private-public relations, and etc.

Chapter 9 concludes the report.

Additional materials in the appendices include:

Appendix A: List of brainstorm ideas and suggestions.

Appendix B: Additional Figures including activity and process diagrams.

Appendix C: Additional Tables.

Appendix D: Guided interview questions.

3

Blockchain Opportunities

Blockchain is the technology that can enable a shared, trusted, public ledger of transactions, that everyone can inspect but which no single user controls. Since it was introduced, first applied to implement cryptocurrencies, private institutions started to realize that they could use the core idea of blockchain as a distributed ledger technology (DLT), and create a permissioned blockchain (private or federated), where the validator of blockchain transactions is a member of a consortium or separate legal entities of the same organization.

3.1. Type of blockchain systems

In summary, there are three types of blockchain technologies:

- State-of-the-art public blockchain protocols based on Proof-of- Work (PoW) or Proof-of-Stake (PoS) consensus algorithms are open source and not permissioned, which means that everyone can be part of the public chain and act as a full node for validating transactions.
- Federated blockchains operate under the leadership of a group. As opposed to the public blockchains, they don't allow any person with an Internet connection to participate in the verification of transactions process. Federated blockchains are faster, more scalable; and provide additional transaction privacy. Consortium blockchains are mostly used in finance and global trade sectors. The consensus process is controlled by a pre-selected set of nodes; for example, one might imagine a consortium of thirty institutions, each of which operates a node and of which twenty must sign every transaction in order for it to be valid. The right to read the blockchain may be public, or restricted to the participating nodes only.
- Private blockchains take advantage of the blockchain technology by setting up groups and participants who can verify the transactions internally. Private blockchains have

their use cases, especially when it comes to scalability and state compliance of data privacy rules and other regulatory issues. They have certain security advantages, and other security disadvantages, such as risks of security breaches.

Both the federated blockchain and the private blockchain can be treated as permissioned blockchain, as they do not open to the public.

3.2. Characteristics of blockchains

Blockchains offer a potentially new paradigm for data management, data sharing and exchange, based on the principle of automated transactions and decentralization. Some of the main characteristics include:

- Transparency: All the data lodged in a blockchain is available to the other nodes of the system; and transactions can be validated by the participating nodes of the system. After accepted by the nodes, transactions and records cannot be arbitrarily tampered with.
- Immutability: Changing records lodged in a blockchain is prohibitively difficult and requires consensus provided in accordance with the protocol (e.g., by the majority of the blockchain nodes). Thus, integrity of records is ensured by intrinsic properties of the underlying code rather than from the identities of system operators.
- Auditability: All the transactions can be audited by a network of validators or auditors using the immutable blockchain log which is append only. Blockchains support build-in auditability where transactions can be audited in real-time before they are added to the chain.
- Redundancy: Each node of the blockchain solution may hold a copy of the data, thus it cannot be easily taken offline due to a system malfunction or malicious actions of third parties. This avoids potential single point of failures.
- Dis-intermediation: The removal of intermediaries from transactions decreases transaction costs and risks associated with presence of such intermediaries.

3.3. Emerging trends of blockchains

Both blockchain/distributed ledger technologies, and their application to the global supply chains are active areas of research and under intense development. Although there have been many pilots and PoCs by the global trade communities since 2017, the technologies are still evolving. There are few technical trends that may have impact how distributed ledgers will be adopted for satisfying the needs of trade and supply chain communities.

3.3.1. Transaction privacy and confidentiality

There have been major advances to protect and assure data privacy in blockchain transactions by applying advanced cryptographic technologies. There are different research directions to enable stronger privacy guarantees without losing the principles of distributed ledgers and blockchains. These could be categorized in the following areas:

- Applying side-chain, satellite chain, or off-chain transactions to safeguard data privacy where accesses to the transactions are based on permissions (need to know basis) and only available to the participants who are involved in the transactions. The results can be later merged back into the main chain or common ledger.
- Assuring data privacy through multi-party computation (MPC) based technologies [54, 83]. MPC and its applications for privacy respecting computation have been studied for decades. The MPC model could find many applications in distributed ledgers where transactions can be updated and computed by multiple participants where each participant doesn't need to disclose its own private information used as inputs to the transactions. MPC when combined with practical homomorphic encryption schemes also allows blockchain nodes to validate transactions based on consensus mechanisms without direct access to the original data.
- Avoiding any potential leakage of information to other parties with zero-knowledge proof based protocols [80]. Zero-knowledge proofs have been applied to implement privacy driven cryptocurrencies and smart contracts [58]. The tools can be applied to guarantee privacy in many use cases not related to the cryptocurrencies. A main advantage of zero-knowledge proof is that it could prevent any potential information leakage from blockchain transactions beyond simple confidentiality protection of transaction content. With zero-knowledge proof based protocols, it is possible to make all the transactions lodged in a ledger indistinguishable from one another, which prevents disclosure of any statistical patterns or possibilities of de-anonymization.
- Protecting data privacy with full support of distributed ledgers using trusted execution environment or enclaves. Recent hardware based designs provide trusted software execution environment (TEE) at runtime where data privacy can be safeguarded using hardware based insulation, which prevents tampering by the local users. The main advantages of TEE based approach include: higher performance than the other approaches, and full support for general purpose computing. It is possible to enable big data analysis, machine learning, and artificial intelligence based tasks without compromising privacy constraints. This may be extremely useful in multi-agency environment where data analytics can be conducted even of each agency doesn't disclose data to the others.

3.3.2. Identity management

There have been significant efforts to leverage blockchains for implementing self- sovereign identity management (SSI). SSI attempts to give users control over their own digital identity. It removes the need for a central trusted authority. Users can store their identity data on local devices and provide the required information to those who need it for validation purposes. Therefore, SSI not only facilitates interoperability across multiple platforms but also enables control by the users over their own identities. DLT seems to be promising for SSI since it does not require any central authority for transactions validation. Encouraged by such promise, recently, a number of projects have been created to leverage DLT for implementing SSI, for instance Uport [23], EverID [78], Sovrin [21], LifeID [36], SelfKey [32], and etc.

3.3.3. Cross chain operations

In recent years, the blockchain communities have focused on developing support for interledger operations. Transactions in a ledger can be linked or correlated with transactions in other ledgers or external events. Information from multiple ledgers can be collected and stored in structured formats that allow arbitrary queries. Transactions across multiple ledgers can be configured and supported. An example of such a use case is atomic swap that includes correlated transactions that must occur in different ledgers. Advances in this area could help distributed ledgers manage supply chain documents and information flows in the context of multiple ledgers.

3.3.4. Blockchains as a service

Vendors have started to offer blockchain based infrastructures and APIs as a service (BaaS). For instance, Oracle, Microsoft, IBM, and Amazon are some of the cloud computing service providers who offer BaaS. The integration of blockchains with the cloud computing framework open opportunities for new innovations, business process automations, and cost reduction for adopting distributed ledgers. BaaS could facilitate a multi-cloud or hybrid cloud environment as the ICT infrastructure for global supply chains.

3.3.5. Scalability and performance

The initial generations of blockchains suffer from various performance related limitations such as low throughput and long latencies. Part of the reasons for low performance is due to the consensus mechanisms used for these blockchain systems. Most public blockchains, for instance Bitcoin and Ethereum, adopt Proof-of-Work (PoW) for reaching consensus. PoW is often the bottleneck that causes low performance. For permissioned and private ledgers, a different type of consensus protocol based on the Byzantine Fault Tolerant design (BFT) has been developed for achieving better performance than the PoW based blockchains, for instance, Hyperledger Fabric as an example.

The classic BFT protocol is known to have scalability limitation when the network size increases. To address this issue, various types of BFT protocols are developed to improve performance and reduce complexity [53, 65, 71, 82], which increases scalability and transaction throughput significantly.

There have been two active research fronts regarding throughput and performance. One is to design and develop scalable BFTs that can scale to a large number of nodes using efficient communication mechanisms and cryptographic signing schemes, for instance short signatures [50]. Comparing with the classic BFT consensus protocols, these new designs could achieve performance of a few thousands transactions per second under relatively large network size (hundreds of nodes) compared to classic BFT. On the second front, the concept is to apply divide and conquer strategy to execute transactions [46, 67, 84]. Both ledger states and transactions can be partitioned and executed in parallel. In ideal situation, the total throughput of the system would be the throughput of each partition multiplies the number of partitions. With this kind of optimization, in near future, it is plausible that new systems could achieve hundreds of thousands of transactions per second.

3.3.6. Integration with IoTs

Another highly active area of blockchain research is integration of blockchains with Internet of Things (IoTs) and Cyber-Physical Systems (CPSs). Intensive research has been conducted in this area in the last couple of years. Blockchains can be applied for managing IoT devices, and data. One topic area has attracted attention from the community as a research direction, is to integrate blockchains, IoTs, and cloud under one unified framework that will facilitate applications such as smart cities, large scale data analytics of IoT data, Industry 4.0 use cases, smart and data driven logistics, etc.

3.4. Landscape of cross border trade related blockchain efforts

Realizing its potential to transform global trade, many global trade oriented international organizations have created blockchain related initiatives. The efforts may include setting up a team to identify use cases of blockchains to the global trade, develop future plans in terms of standardization and coordination, or create a framework for pilots and PoCs that may involve multiple stakeholders. For most such initiatives, the work is still ongoing. Here we provide a high level overview to summarize these efforts.

3.4.1. WCO

The WCO has initiated work to identify possible case studies and uses of blockchain for Customs and other border agencies with a view to improve compliance, trade facilitation, and fraud detection, while touching on associated adjustments in the legal and regulatory frameworks. The efforts have been led by the WCO Research Unit. Some of the findings and suggestions by the WCO regarding the potential of blockchains have been included in this report.

The WCO concludes that the power of blockchain could have a great impact on the Customs' day-to-day operations, and be an important technology piece for the future Customs. It represents a step forward for Customs and the trade, both of which desire greater efficiency in their business operations. These impacts include:

- Customs will become more data driven
- Customs may become part of the blockchain and become more embedded within the trade processes
- Blockchain can enhance revenue compliance and cooperation between Tax and customs authorities
- Blockchain can help Customs better combat financial crimes

3.4.2. UN/CEFACT

Aligned with the UN/CEFACT's mission to improve the ability of business, trade and administrative organizations, through focusing on the simplification and harmonization of processes, procedures and information flows, the UN/CEFACT has created initiatives to identify the potential of blockchains to improve supply chain efficiency and integrity, as well as strategies for the UN/CEFACT to leverage its role in making supply chain and trade standards. The research resulted in a list of suggestions that may extend the UN/CEFACT's existing models to this new technology. These include:

- Investigating the development of a reference architecture so that all specifications and new technologies can be understood as constituent parts of a consistent whole
- Reviewing the UN/CEFACT process models to allow integration of blockchain based transactions and events driven updates of supply chain states facilitated by the blockchain based transaction models
- Performing a gap analysis to define what is needed to have an inter-ledger interoperability framework for supply chains in the face of the inevitability of a plethora of blockchain platforms
- Performing a gap analysis to define what is needed to provide supply chains with a standard way to discover and consume data regardless of which platform hosts information about a resource
- Relying on a semantic framework that releases new value from the existing UN/CEFACT work products such as the Core Components Library (CCL). There are opportunities offered by the blockchains and related technologies, and the ongoing work of the UN/CEFACT is to deliver new technical specifications that will release new value by supporting supply chain inter-operability, efficiency and integrity

A high level diagram of integrating the UN/CEFACT standards with the blockchain based trade framework can be found in Appendix B.

3.4.3. WEF

Consistent with the World Economic Forum's mission of applying a multi-stakeholder approach to address issues of global impact, the WEF has been investigating blockchains in a range of trade related areas such as finance, identity management, and Single Window implementations. The studies included experts across various industry sectors, government agencies, intergovernmental organizations and academic institutions. The early result is to create a framework that can pave the way for blockchain pilots around the world. For instance, the WEF and the Inter-American Development Bank will be working to implement proofs of concept with a subset of LAC governments to pilot blockchain use cases, use the guidelines developed by the WEF and build LAC governments' capacity to understand and apply new technologies on border clearance while sharing the lessons learned.

3.4.4. ISO

ISO/TC 307/WG 1 is the working group tasked with producing recommendations related to the foundational elements of blockchain and distributed ledger technologies. The current ISO working group focuses on the following areas: terminology, reference architecture, taxonomy and ontology, discovery issues related to interoperability, and study on data flows and data taxonomy [19].

Most of the efforts are still works in progress. In particular, the discovery issues related to interoperability are relevant to supply chains. At this moment, the documents as result of this work seem to be at high level and early stage.

3.4.5. W3C

Other efforts include work by the W3C and ISO. The W3C has been developing standards to enable decentralized identifiers and verifiable credentials.

3.5. Opportunities for entry process re-engineering

As revealed by the reports and studies, there are pain points associated with the existing declaration and entry processes. Some of the persistent challenges are:

Data fragmentation and limited interoperability. Global trade in nature includes stakeholders in multiple jurisdictions. However, data coordination across jurisdictions and global supply chain stakeholders is limited. There exist many silos of trade related information.

The fragmented environment is often due to disparate databases managed under different jurisdictions and supply chain actors, lack of platforms for efficient exchange of data, heterogeneous regulations, and different document formats.

Sharing of data among governments and the private sector is still limited, impeding agencies' ability to trace goods to their origins, verify certificates, recognize anomalous patterns and manage import risks, ultimately resulting in potential hazards to end users of the shipped products.

Unstructured and uncorrelated data embedded in the trade documents. It is not easy to align entry data with the trade documents in ways to support more advanced and automated analysis. Structures and formats of data are not always harmonized. The involvement of manual processing is not only error prone but also ties valuable human resources of regulatory authorities, which makes it less efficiency and optimal in terms of focusing on high risk cargo and goods.

Manual document processing and reconciliation of databases. The same data may be reentered manually multiple times into new documents and databases, a process prone to error. Even in more digitized settings, updates to agencies' databases can require manual interventions, which wastes staff time, increases the odds of error and stops agencies from allocating resources to more value adding work such as focusing on high risk import activities and priority trade issues.

Limited trustworthiness of data entered into the system. Border agencies and traders' processes involving the re-entry of the same data multiple times while reconciling different agencies' databases undermine the trustworthiness of data in Single Windows. Data trustworthiness diminishes if data provided by the agencies and trader differ.

As covered in the following sections, the blockchains offer opportunities to tackle these challenges and pain points. Blockchain enabled supply chain visibility allows agencies to gain deeper integration of the entry process with the supply chain information flows so that Customs and partnering agencies can have a clear picture of trade related information regarding the imported goods. This will facilitate collection and validation of entry data. As entry processing becomes more information driven leveraging blockchain based supply chain data, correlation of entry data across support documents will become easier. It will also create new opportunities of automation and reduce manual work required for entry declaration. The improved data quality and efficiency would allow Customs to prioritize their resources with more accurate risk based assessment, and therefore be able to focus on high risk imports. As a result, it will create many benefits to help Customs accomplish its missions and address high priority trade related issues.

4

Can Blockchain Transform Entry Process?

4.1. Methodology

To fulfill the research goals, the team analyzed the business process of cross border trade and Customs entry processing. The outcomes are models and artifacts for designs of re-engineering entry process.

4.1.1. Research Framework

The research steps are divided into phases, shown in Figure 4.1. First, through literature studies, interactions, and engagements with the stakeholders, the team maped cross-border trade and entry process. Second, the team analyzed the process, gains additional insights of the operational context, and identifies opportunities and pain points where emerging technologies could be applied to improve efficiency and operation effectiveness. Following the aforementioned steps, the team conducted brainstorm sessions to identify new ideas and suggestions to improve and enhance the process.

The brainstorm ideas are aimed to address the earlier identified opportunities and pain points by integrating distributed ledger based technologies. Then, the team proposed re-designed business process according to the ideas and suggestions. After that, the business process was analyzed and evaluated including comparison with the status quo. Additionally, through focused interview sessions, the team collects feedback from the stakeholders. The inputs helped the team to identify barriers, and assess potential to have the new process adopted eventually by the stakeholders. At the end, the team summarized the findings, reached proper conclusions based on the research, and developed suggestions for the future work.

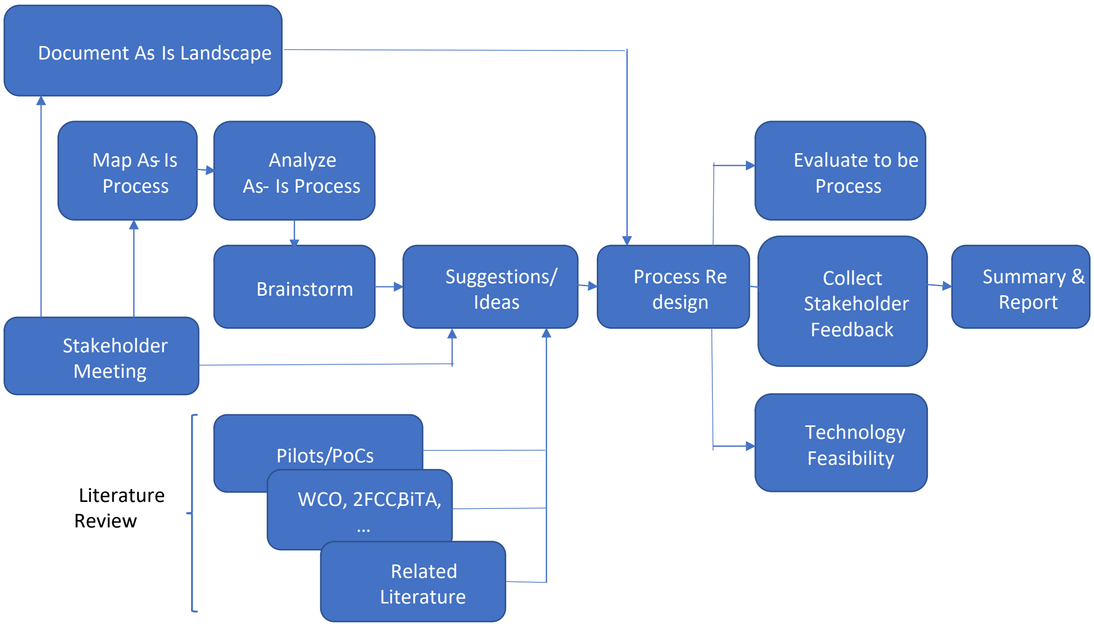


Figure 4.1: Research methodology used in this study.

4.1.2. Data Collection

In order to map the existing process, the team relied on the following main information sources: publicly available information describing the existing entry process and procedures (including entry business process documents released to the public by Office of Trade, CBP); reports and standards created by the international associations relevant to the project, for instance, the WCO, the UN/CEFACT, the WEF and other global organizations developing standards and data models for cross-border business process; relevant reports from Office of Inspector General (GAO), Congressional Research Service (CRS), Government Accountability Office (OIG), and COAC (Commercial Customs Operations Advisory Committee); knowledge from the subject matter experts. Specifically, the team relied on cross border supply chain business process model developed by the UN/CEFACT, and the WCO data models.

4.2. Mapping the as-is business process

This subsection briefly summarizes the efforts on mapping the as-is business process.

4.2.1. BSP supply chain model

The International Supply Chain Reference Model (ISCRM) [3] describes the processes following the recognition of need by a customer for a product until the fulfillment of an order by an international supplier and the resulting financial settlement. In addition, the model also covers the logistics processes and the regulatory activities that are required by the intermediaries and authorities. The main activities are defined as:

- Identify potential trading partner: The buyer looks for potential sellers and the seller looks for potential buyers.
- Establish business agreement: A buyer issues a request for quotation to sellers for a product or service. Sellers respond or send quotes to a potential buyer. The buyer negotiates with the selected sellers to agree with the terms for a contract agreement.
- Order: The buyer recognizes a need for a product and places an order under a contract agreement. The seller receives the order and responds.
- Manufacture: The seller places an order for the manufacturing of that product to a manufacturer, to meet customer's order. The manufacturer confirms the planned delivery date, when the product is available for shipping.
- Ship: The seller dispatches the products according to the terms of trade specified. All transport arrangements are made and executed. The requirements laid down by the relevant authorities are met. Invoice (demand for payment) is raised. The buyer receives the product.
- Pay: A demand for payment is received. The payer makes the payment and the payee receives the payment according to the terms of trade agreed.

The ISCRM maps business processes in four main interrelated business areas, namely the; (i) commercial, (ii) logistical, (iii) regulatory and (iv) financial, including procedures as illustrated in Figure 4.2. The four areas include, commercial trade, transport and logistics, regulatory and border clearance processes together with the corresponding information used both within each business area and which passes between them. The same areas are also captured by the BUY/SHIP/PAY model of the UN/CEFACT, see a diagram of the BUY/SHP/PAY model in Appendix B.

4.2.2. Entry declarations

From the Customs and the CBP perspective, the regulatory view of cross border trade is divided into three phases, pre-entry, entry, and post entry.

Pre-entry. Before goods leave their country of origin and prior to goods arriving at a U.S. port of entry, importers and carriers file paperwork and provide required advance electronic information for the CBP to review.

At entry. Importers or brokers file entry documents when the goods reach a U.S. port of entry. At the ports, the CBP and other agencies with regulatory responsibilities review documents, and may examine the goods for import security and trade enforcement purposes. In

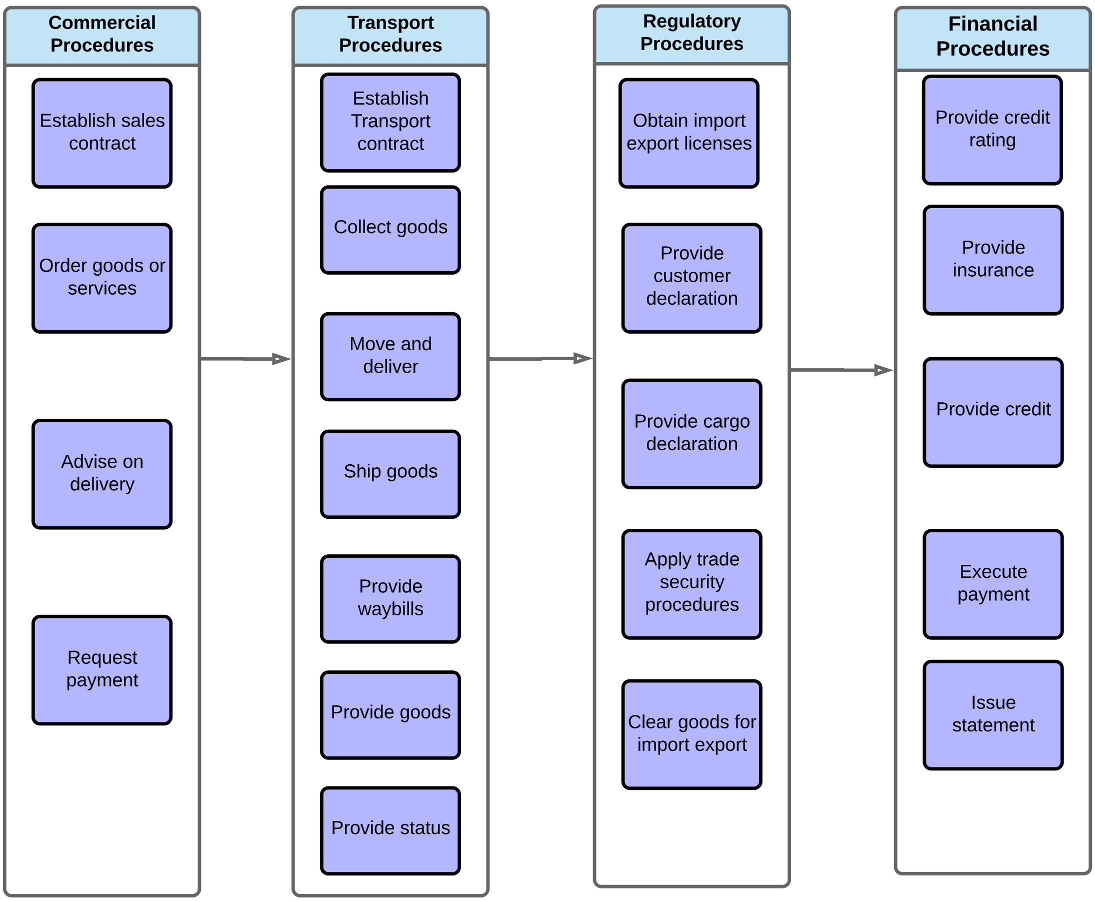


Figure 4.2: Business process within the four business areas as defined in SCRM.

some cases, the CBP and partner agencies (PGAs) may target cargo for examination based on a risk assessment. Cargo that is scanned or inspected may be deemed as non-admissible because of trade law violations, among other things. If the CBP finds such violations, it may seize the cargo and issue penalties and/or fines. If the goods pose a risk of nonpayment of duties, and the shipment meets certain risk assessment criteria, CBP may require additional bond coverage (e.g., single transaction bond). Admissible goods are released from the port and enter into the U.S. commerce.

Post-entry. During the post release entry liquidation phase, importers or brokers file additional entry summary documents that the CBP reviews to ensure trade compliance. CBP verifies the importer's cargo classifications and calculation of customs duties, taxes, and fees owed, taking action when needed. For instance, the CBP may determine that an importer mis-classified goods in an attempt to pay lower duty rates, such that the agency issues the importer a bill for a greater amount based on the proper classification and possibly applies a penalty. To mitigate risks of nonpayment and importer default, if CBP identifies that importer's bond is insufficient, it may request supplement bond from the importer. In case of AD/CVD import, CBP may suspend entry liquidation until a final AD/CVD rate is determined. During post entry liquidation, CBP continues to review and process trade information provided by the importer. For instance, CBP may conduct audits, review and validate information provided by the importer to check for importer compliance.

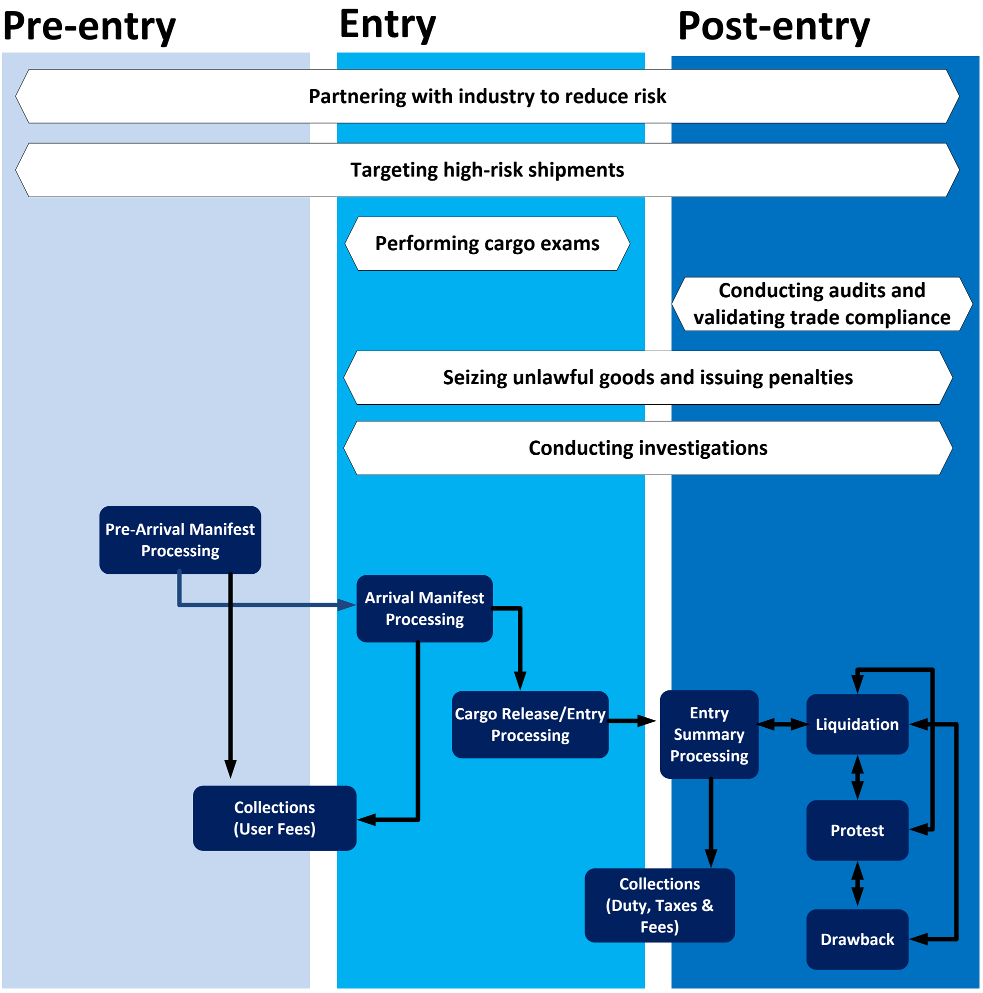

Pre-entry
Entry
Post-entry
Partnering with industry to reduce risk
Targeting high-risk shipments
Performing cargo exams
Conducting audits and validating trade compliance
Seizing unlawful goods and issuing penalties
Conducting investigations
Pre-Arrival Manifest Processing
Arrival Manifest Processing
Cargo Release/Entry Processing
Entry Summary Processing
Liquidation
Protest
Drawback
Collections (User Fees)
Collections (Duty, Taxes & Fees)

Figure 4.3: Customs declaration and entry process (pre-entry, at-entry, and post-entry).

CBP collects entry data on behalf of all the partner agencies that CBP identified as bearing responsibility for clearing the imported goods. Some of the agencies are listed in Appendix B. The protocol may work as follows. CBP and each agency work together to specify data that the partner agency may access in accordance with its responsibilities and as allowed by statute. Agencies may obtain these data elements through the CBP's electronic entry data and support document submission system (ACE). Agencies may access these data directly through ACE or may establish web linkages between ACE and their own data processing systems that will allow their systems to receive automatic transmissions of data.

Several federal laws enable regulatory agencies to rely on third parties to assess compliance with mandatory standards [73]. For example, the FDA and the EPA [11, 29, 35], have programs that rely on third parties that serve the function of certification bodies. Different regulatory agencies may have used a variety of names for these third parties, such as Third-Party Auditors, Accredited Persons, or Certification Bodies. These programs share similar certification process, as shown in Figure 4.4. Regulated entities contract with a third-party certification body to assess and certify whether they are in conformity with an applicable regulatory standard. The certification bodies are generally private entities that have been accredited to perform this task by an accreditation body that has been approved or recognized by the regulatory agency.

For imported goods, mandatory standards must be complied with in order for a regulated entity to legally operate or sell a regulated product. For instance, in two programs, imported food programs administered by the Food & Drug Administration's (FDA) and children's product safety rules administered by the Consumer Product Safety Commission's (CPSC), the third party certifier is an obligatory part of the compliance process: the regulated company is required to contract with the third party for compliance assessment. In FDA's programs for medical devices, in contrast, the use of a third party is optional: companies have the choice of hiring a third party or having the agency conduct the review or inspection instead. For additional details of agencies' third party programs, please refer to Figure B.3in Appendix B. It lists several agencies and compliance programs that allow accredited third parties to provide test and certification.

A benefit of third-party programs designed for the regulatory purposes is that it can enable more frequent inspections and more complete data about compliance. Accredited laboratories are subject to either an on-site surveillance or a full reassessment periodically to ensure that they maintain their standards of independence, accreditation, performance, and technical expertise.

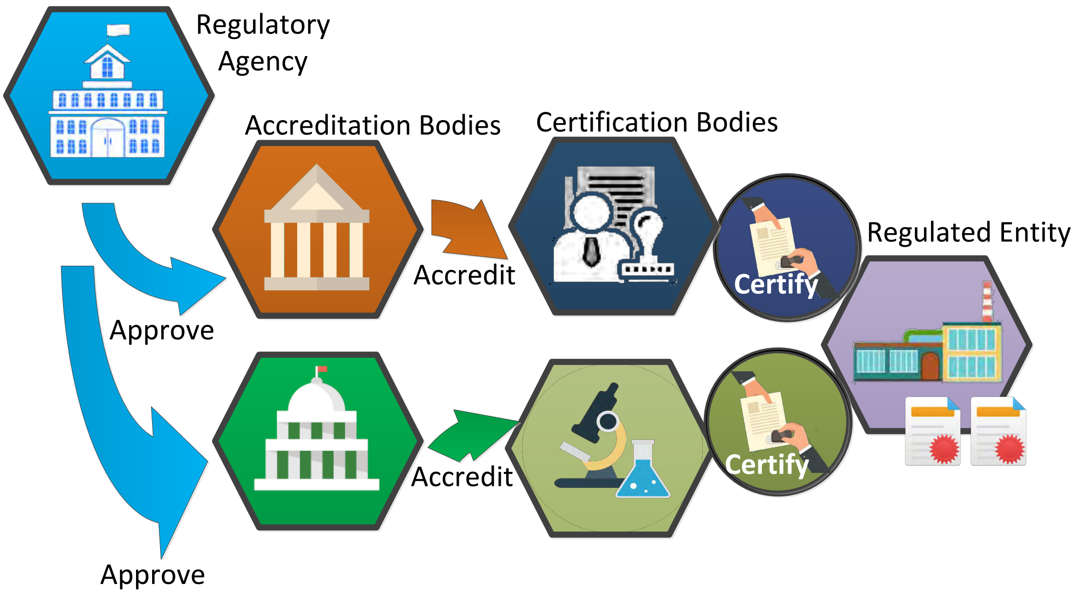


Figure 4.4: Third party accreditation process.

4.2.3. Different views of global supply chains

To summarize, there are different views of cross-border supply chain events during the BUY/SHIP/PAY process by the involved actors.

The trade view involves discovery of products by the potential buyers, identification of business partners, the establishment of agreements for purchasing goods, and the activities dealing with the fulfillment of the purchase order. Supply chain events, such as order confirmation, dispatch and delivery, are relevant to this view. The trade view reflects the services sought by trade actors, such as the buyers, the sellers and the manufacturers of goods.

The transport view includes processes linked to the physical carriage of goods on a means of transport. These processes are linked to the booking of space, packages of transport equipment, loading and unloading of goods, and the delivery of goods to the ultimate consignee.

The regulatory view deals with regulatory reporting to the authorities along the entire supply chain. In this view, actors are entities that fulfill regulatory formalities with authorities at import, export and transit. The regulatory view maintains the focus on the exchanges between the regulatory authorities and the regulated business entities. This view helps understand supply chain events in terms of events involving regulatory controls.

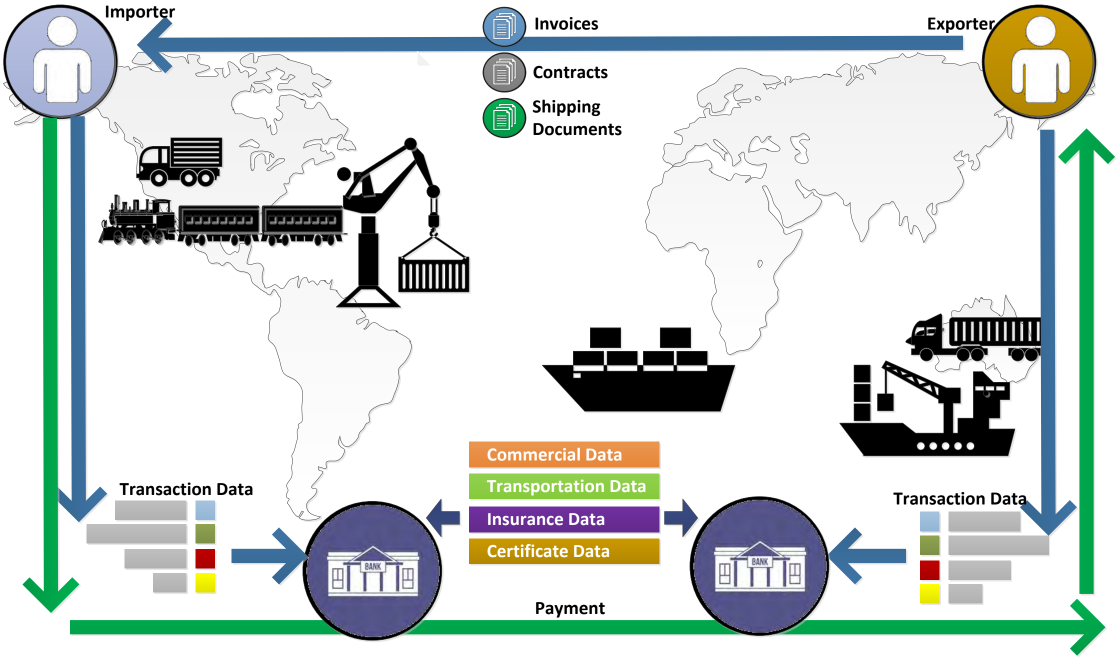


Figure 4.5: A high level diagram of trade finance and stakeholders.

The finance view includes the process related to credit, insurance, payment, settlement, etc. The process may involve issuing of letter of credit from a customer to the supplier. For purpose of trade finance, importer, supplier, and their corresponding banks (financial institutions) may exchange documents such as commercial data (e.g., invoice, purchase order, contract term, payment term), transportation data (e.g., bill of lading), insurance data, and certificate data (e.g., COO, PGAs required certificates for import).

4.3. Analyzing the as-is business process

Literature survey and analysis of the as-is business process suggests the following characteristics of the current cross-border supply chain information flow that directly or indirectly affects the entry process by the regulatory agencies.

Regulatory visibility to commercial data that already exists and is available in the global supply chain information flow before export and shipping process starts. According to the current business process model, the regulatory view is separated from the other business procedures, and data exchange with the regulatory agencies starts after the commercial procedures. Based on the model, the regulatory review does not cover these trade processes such as supplier discovery, establishing sales contracts, ordering goods, ordering to produce, etc.

Although the regulatory view can be divided to include, "pre-export", "export", "international transport", "international transit", "import" and "post-clearance" phases, it is often the case that import authorities don't have visibility regarding the commercial and trade information prior to the events such as booking of shipment, completion of production of the ordered goods.

Lack of visibility and advance data during trade process, may limit the authorities' capability to perform accurate and targeted risk assessment. As DLT can be potentially applied to each process and every phase of the global supply chain (e.g., procurement, purchase, order, manufacture, booking, transportation, entry declaration), there is an opportunity to advance the data collection timeline to the trade and commercial phase. Doing so may create benefits to both the trade community and the regulatory agencies in terms of trade facilitation, Customs risk management, and targeted enforcement.

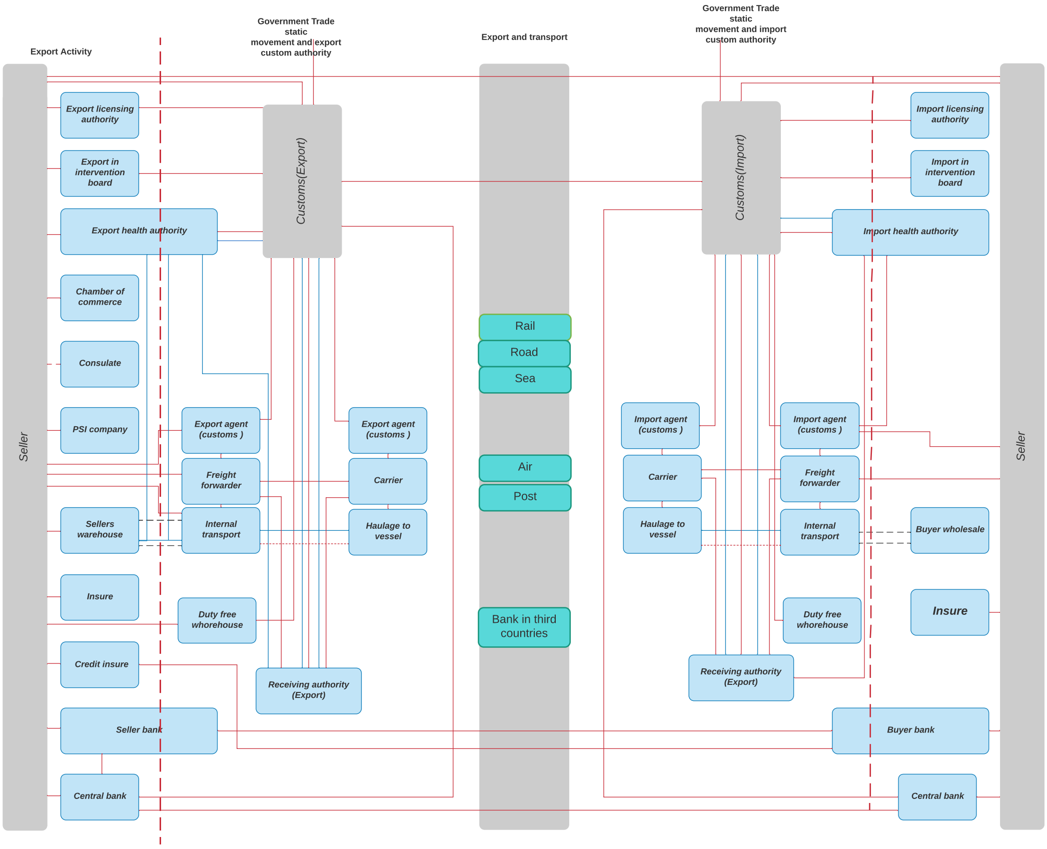


Figure 4.6: Information flow in the international supply chain - dominated by numerous peer to peer data exchanges between two entities, which limits supply chain visibility. The diagram shows more than forty actors involving in the data flow.

Segregated views of both business processes and supply chain information flows. The current view model (commercial, logistical, regulatory, and financial) that covers the four process areas is a best fit for data exchange technologies prior to availability of distributed ledgers. For instance, data communications between economic actors rely on peer to peer exchange of electronic messages, which creates segregated flows of supply chain information between the supply chain actors. The situation is perhaps best demonstrated by the information flow diagram in Figure 4.6.

The existing model based on peer to peer messages, with unintended consequences, creates many information silos among the supply chains actors. For cross border supply chain, one import transaction from the beginning to the end may involve more than thirty actors, as demonstrated in Figure 4.6. Each actor may maintain its own database for storing, processing, and communicating supply chain data to the other actors with whom it exchanges information. The same piece of data may be re-entered, converted, copied, and translated many times before it is received by a data consumer including the regulatory agencies. In case that the data is updated, there is no assurance that the update can be disseminated in a timely manner to all the actors who need a copy of the update.

Through distributed ledgers and cooperation between the supply chain stakeholders, information flow can be streamlined and consolidated, which avoids manual data duplication, automatic synchronization of data updates, and timely sharing of supply chain data. If DLT delivers its potential and promise for achieving supply chain transparency and promoting data sharing cooperation among the supply chain actors, the segregated environment of the four different views (trade/commercial, logistical, regulatory, and financial) can be dismantled. A unified view that covers all the four business process areas could be realized by applying distributed ledger technologies.

As pointed out also by a whitepaper released by the WEF, the existing process is heavily “document-driven” instead of “information-driven”. Data exchanged in electronic messages is organized in line with the corresponding documents such as invoice, bill of lading, Customs declaration and so on. These documents represent different views of the information stored in the supply chain stakeholders’ databases.

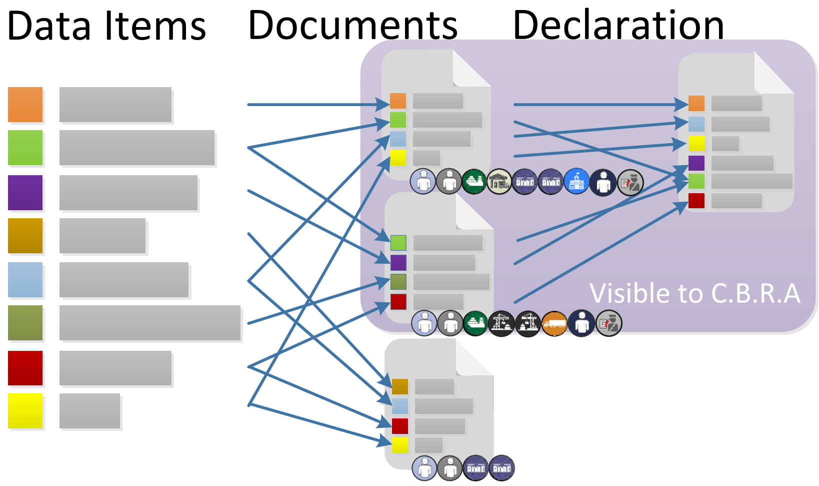


Figure 4.7: Document driven process. Document, which represents a view of the data attributes behind, instead of the original information is received by the Customs and C.B.R.A. In addition, reference links between the data attributes are often not preserved when data is exported as views, which creates challenge to correlate them by the regulatory authorities who only have access to the views.

In order to produce reviews (documents shared within the global supply chain), data objects stored in the tables of these databases are queried, and exported as the document views. Such process often discards relations among the data objects because access keys that connect the data objects may not be preserved in the created view and exported. After the views (paper documents or electronic equivalents) are communicated, supply chain stakeholders and regulatory authorities will re-enter the data to their own databases. For instance, the Customs will populate its own Single Window database based on the data from the views (declarations and support documents).

As most documents (views of information) are part of a chain of information exchanges, a good deal of information tends to be repeated at each step and to be reflected in another document view. It is not surprising that authorities may sometimes find it a challenging task to link and connect data objects among the different views regarding the same piece of information. Figure 4.7 illustrates the nature of document driven information sharing, where each document or electronic equivalent represents different views of the same set of information.

This process is not optimal nor efficient in preserving the relationships between the supply chain data. Furthermore, with such process, the different views shared with the different supply chain stakeholders and the regulatory authorities are not necessarily the same or aligned with each other, which creates the potential for fraud. The problem is demonstrated in Figure 4.8. False description can show up in certain support documents and Customs declarations. The document views by different stakeholders are not aligned or consistent.

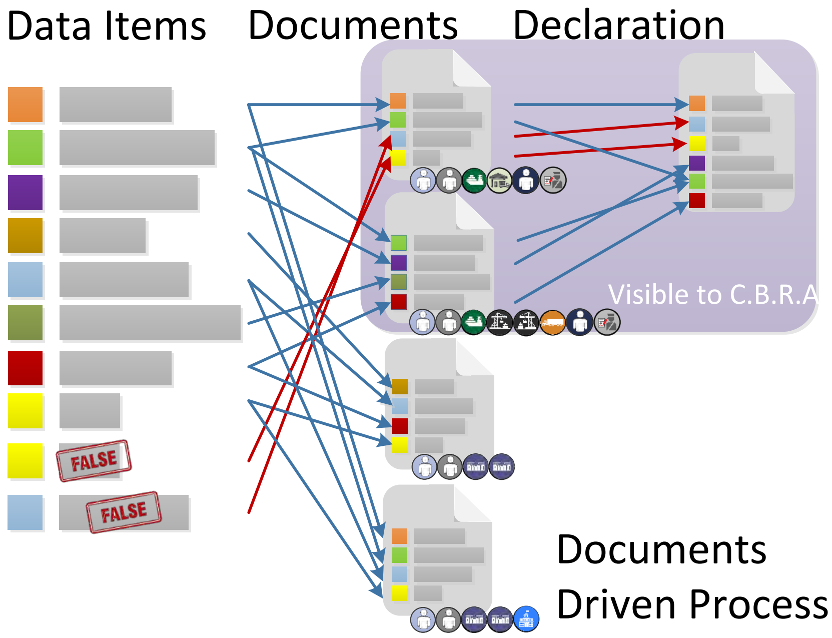


Figure 4.8: Example to show why document driven process is prone to fraud and false data in declaration. Different views of the same supply chain activity may not be aligned or matched. Distributed ledgers facilitate sharing of data attributes instead of document views.

An information driven process may solve this problem by mapping data models and processes of different domains to a universal distributed ledger model of supply chain information. Information needs to be stored in the distributed ledger only once (either off chain or on-chain), and will be shared automatically among the involved stakeholders. After an event of supply chain has happened (e.g., sales term agreed, order confirmed, good manufactured, shipment booked, cargo packed, cargo loaded), only one update to the information is enough because every stakeholder's database including the Customs' database is synchronized to the same source of information provided by a distributed ledger.

This perhaps moves forward the concept of Single Window to globally single view of information, which will significantly increase visibility of global supply chain and improve transparency. Such vision to provide an information driven and holistic view of supply chain data to all the stakeholders is aligned with the efforts that aim to create harmonized data models that can connect data models designed for different process areas (commercial, logistical, regulatory, and financial).

4.4. Ideas and brainstorm results for a new process

This section summarizes the ideas as results of literature review and brainstorm. Analysis of the existing process suggests the following areas or opportunities for optimization and re-engineering under the context of distributed ledgers at high level.

- Early and advance sharing of commercial and trade data between the trade actors and the regulatory authorities in the pre-export phase for purpose of trade facilitation and improved Customs control.
- Data cooperation between the supply chain actors that can enable supply chain visibility, and a holistic view and connectivity of data from all the four process areas (commercial, logistic, regulatory, and financial).
- Information driven data exchange among the supply chain actors over the distributed ledgers in order to eliminate data duplication, error prone manual process of data; facilitate timely sharing of supply chain data among the stakeholders; assure data quality and integrity; improves trust among the supply chain actors; enhances supply chain predictability by improving information flow; and reduces administrative cost.
- Enhanced automation by integrating distributed ledgers with the entry and declaration process.

The following subsections elaborate some of the key ideas. Appendix A documents the list of re-engineering ideas from the brainstorm session.

4.4.1. Early and advance sharing of commercial data

According to the process diagram of ISCRM, authorities don't interact with the commercial process until the shipping phase. If distributed ledgers are adopted by the supply chain actors for e-procurement, e-contract negotiation, e-purchase, e-invoice, and etc., it opens new opportunity of trade facilitation. In the new process, after information is lodged in the distributed ledgers, authorities may collect early data whenever the trade phase starts, which may include, process for discovering trade partners, establishing business agreement, ordering, and manufacturing – blue lines in Figure 4.9.

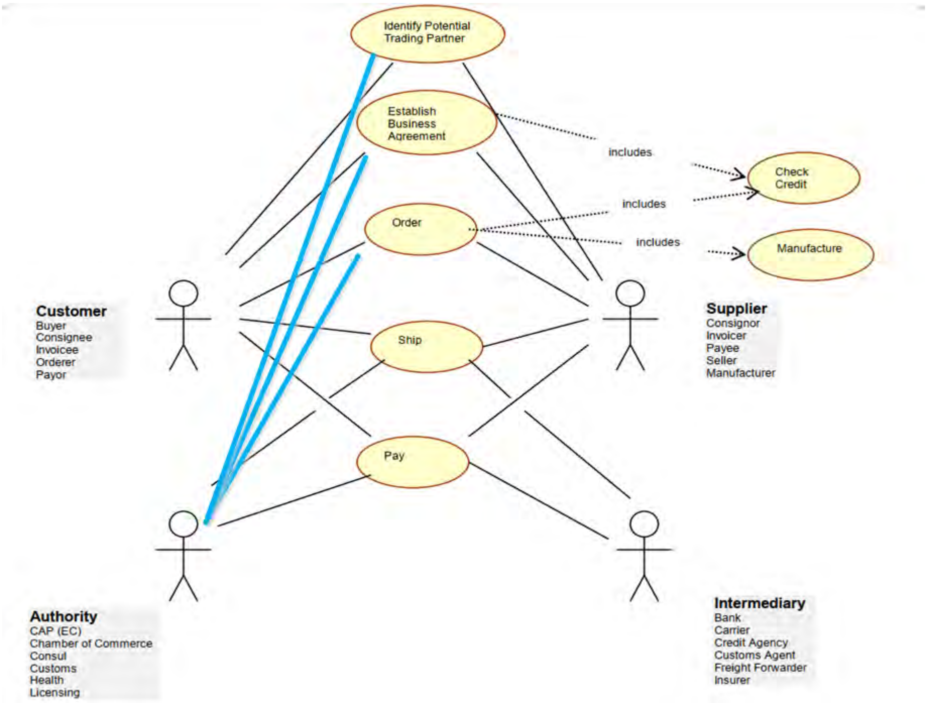


Figure 4.9: Revised actor diagram with advance data sharing in the commercial/trade stage between the actors and the regulatory authorities (blue lines).

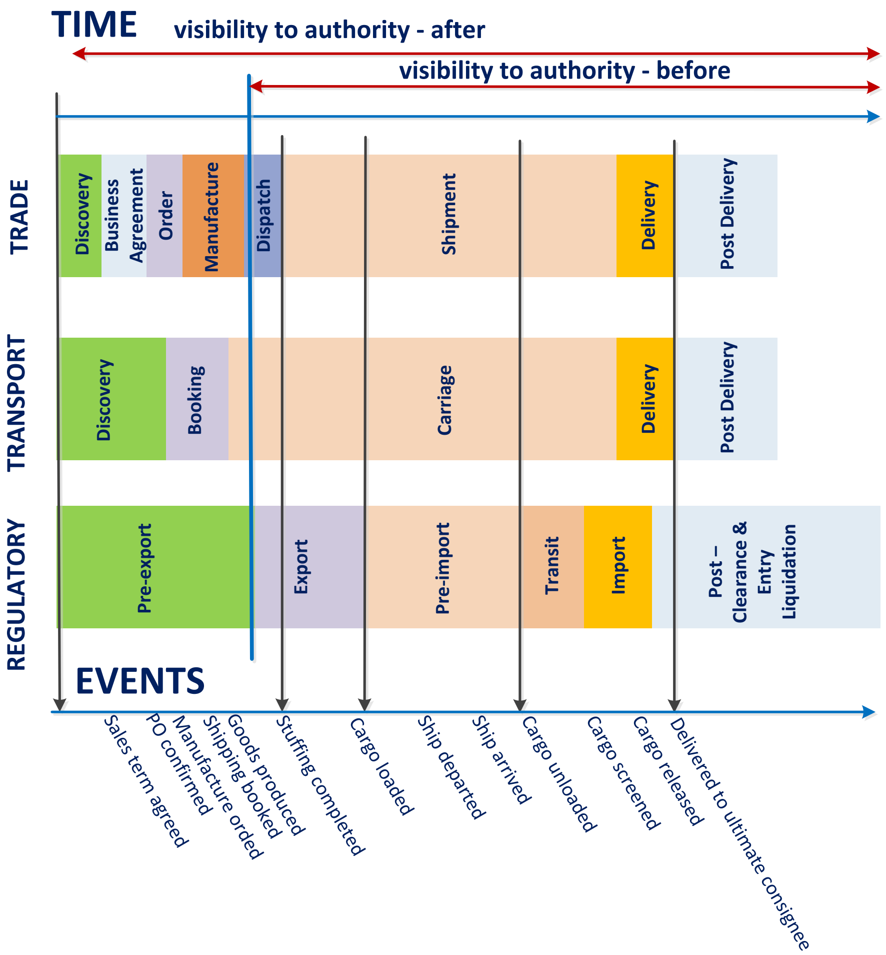


Figure 4.10: Comparison of timeline of regulatory access to the cross-border trade information (before and after).

Advance information lodging and sharing with the regulatory authorities during the trade phase may provide many benefits to both the trade community and the authorities in terms of trade facilitation. These include:

- Facilitating risk management by establishing patterns of commercial data, and risk profiles;
- Demonstrating evidence of reasonable care and compliance during supply sourcing and procedure stage of trade;
- Reducing delays at the port of entry points, expediting clearance and release upon arrival due to decreased risk perceived by the authorities;
- Decreasing supply chain uncertainty, disruption, and risk by integrating distributed ledgers with the trade process.

4.4.2. Information driven process of entry data collection and cooperation

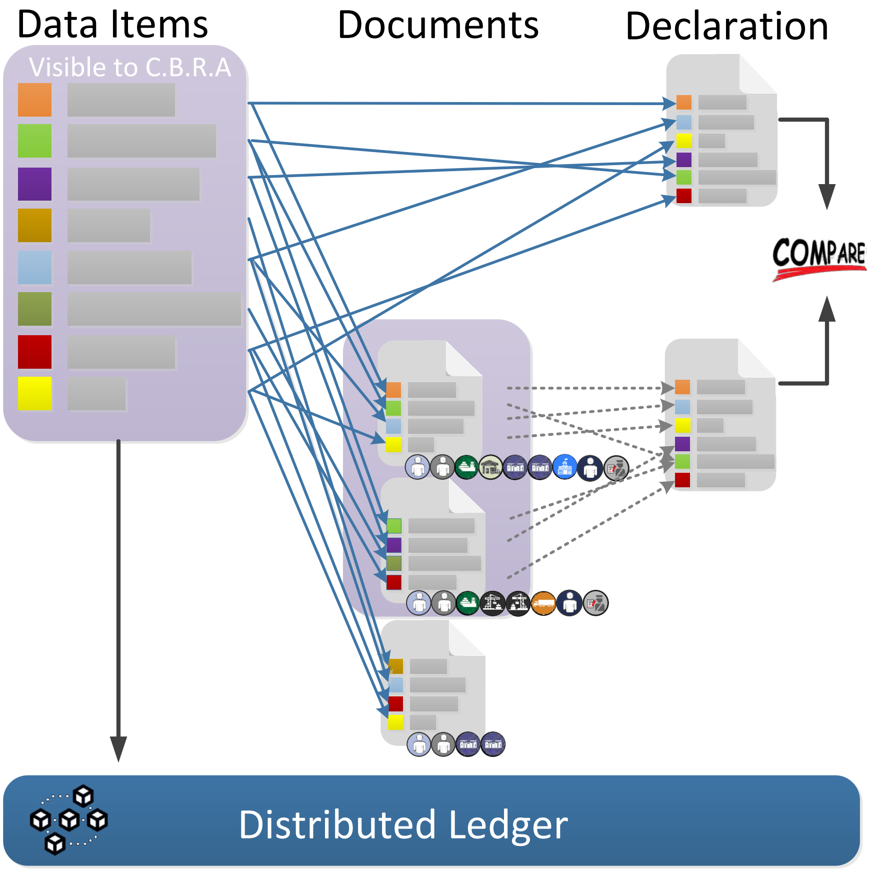


Figure 4.11: Information driven sharing of data items.

Figure 4.11 illustrates a process that allows collaboration between supplier, customer, broker, carrier, financial institution, and authority. Actors involved in cross border trade can lodge information to distributed ledgers. Data exchange between the supply chain actors is implemented at the data item and the attribute level, instead of the document level. The data set required for declarations can be gradually built up based on the supply chain events.

Information is allowed to be incrementally added, updated, and accessed in a collaborative environment, with the progression of the status of the import transaction.

The actors involved in the transaction have access to the information secured by the distributed ledgers that cover all the four process areas of trade. With consent from the data owners, the system could allow the regulatory authorities to access each data item required for declaration and risk assessment in a timely manner when it is added to the system based on the supply chain and business events. The system promotes data sharing in real-time, and access to the relevant information by all the actors with concern.

In the past, such a process is envisioned to be implemented using a centralized service. Since economic actors are often not willing to give up control and management of the data, distributed ledgers offer another more feasible alternative to the centralized service concept for managing flow of information between the supply chain actors and the regulatory authorities. The process minimizes the efforts for collecting data, preparing entry declaration, and validating the data as all the actors have access to the same sets of information in real-time.

The new system enables an evolution based approach that the supply chain actors can maintain their own internal ERP based databases, which are automatically synchronized with one another using the distributed ledgers. This possibly allows gradual transition from the currently isolated systems to a data cooperation based operational environment.

The information driven process resolves an issue that appears in the current entry processing, where data arriving to the Customs by both the supply chain and the transportation related sources are not consolidated and are not always aligned with each other. This often makes it a challenge or labor based task to cross-relate descriptions concerning the same data item.

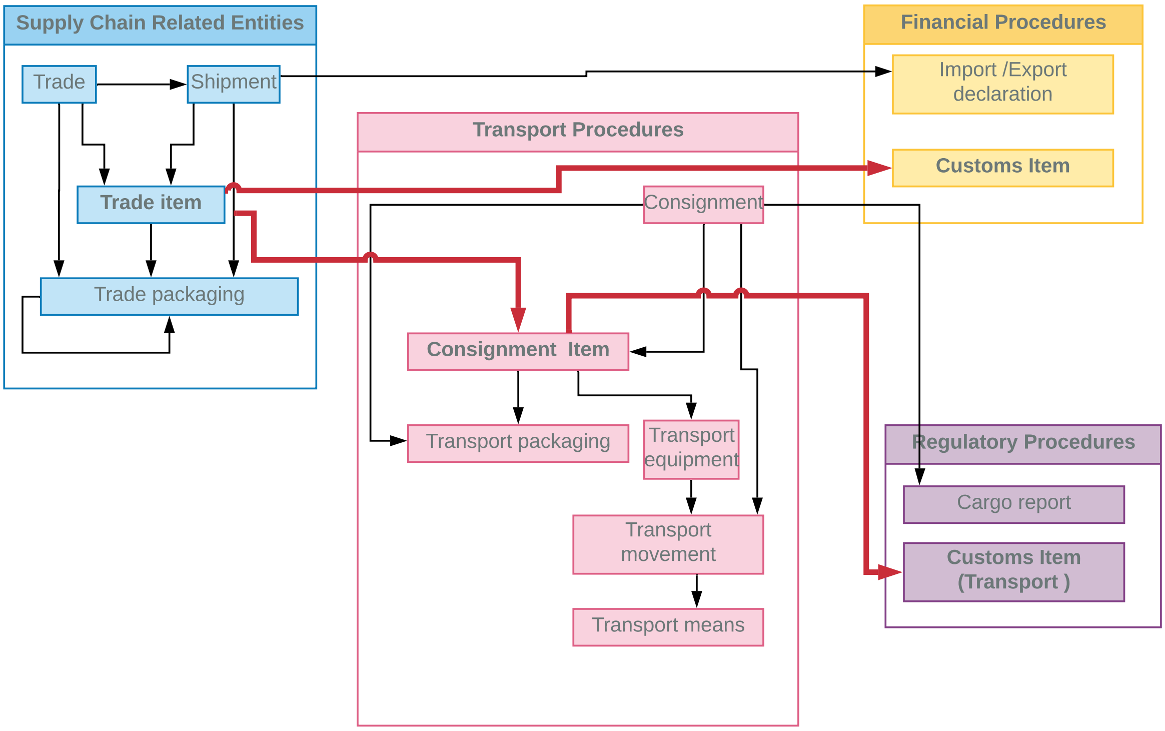


Figure 4.12: Unifying data models for different views. The same information such as traded product exists in all the four areas (trade. logistics, finance, and entry declaration). The data items in the four business areas can be correlated and unified under a uniform model.

Distributed ledgers offer an opportunity to unify the different views (trade, logistics, declaration, and finance) and data models in order to synchronize and correlate data items with identical meanings. The concept is illustrated in Figure 4.12, where information of the same origin belonging to the four business process areas is mapped and correlated, use trade item as example.

4.4.3. Managing identities of AEOs and issuing of LPCO over distributed ledgers

Distributed ledgers can be applied to support self-governing digital identity management, which provides several advantages over the centralized and federated identity management approaches [68], as highlighted by many recent studies and reports.

Distributed ledgers could eliminate the need for an intermediary to certify the identities of business entities or AEOs, which may offer a pivotal technology to realize the WCO's vision of globally recognized unique identity for AEO and trader [39].

In a federated environment with multiple identity providers, distributed ledgersa may provide a unification layer that interconnects a network of identity providers (e.g., authorities, private organizations, and C.B.R.A. in different countries who certify economic actors) to enable globally unique and attestable identities for entities, economic actors, and traders. The identities could be recognized and verified across the whole government-business ecosystem.

As described earlier, there are increasing requirements by the partner agencies for product certification in order to meet the concerns of product safety and quality. Various licenses, permits, certificates, and other authorizations (LPCO) may be required for Customs clearance depending on the nature of goods and related national regulatory requirements.

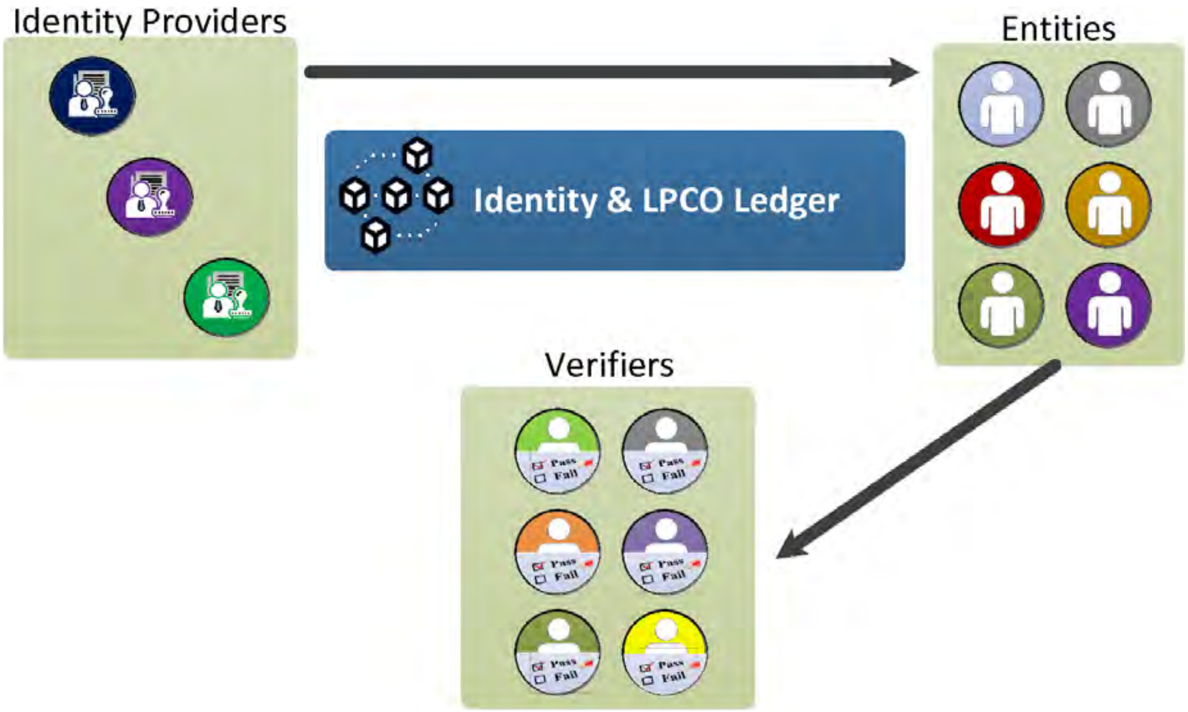


Figure 4.13: Actors in self-sovereign identity management.

In case of the third-party certification process by accredited stakeholders such as certification bodies and testing laboratories, the results and process need to be shared with the public, customers, consumers, and the regulatory agencies. Distributed ledgers could provide a holistic product life-cycle data management. The community of producers, manufacturers, laboratories, certification bodies, regulators, and consumers can work together for realizing a shared data environment to facilitate data provenance, licensing, testing, and product certification with all the relevant actors having access to all the related information. Electronic provenance of LPCOs (e.g., e-Phyto certificate, e-Certificate of Origin) can be maintained and secured by distributed ledgers. Distributed ledgers could ensure that a certificate is appropriately issued, and properly and digitally signed by a valid regulatory/issuing agency, and at the same time could also prevent any alteration/manipulation of the content or misuse of an e-certificate by a third party.

4.5. Development of a new entry process

This section describes business processes as activity diagrams. Activity diagrams can be used to specify business processes or re-engineered business processes. Applying business modeling tools such as the standard modeling language (e.g., UML diagrams) to describe business processes and data models is a well established practice utilized by the international trade related organizations including the WCO and the UN/CEFACT. The models developed can form a basis for business process standardization activities between the trade

Table 4.1: Five major groups of Single Window business process and re-engineering opportunities provided by the blockchains and distributed ledgers.

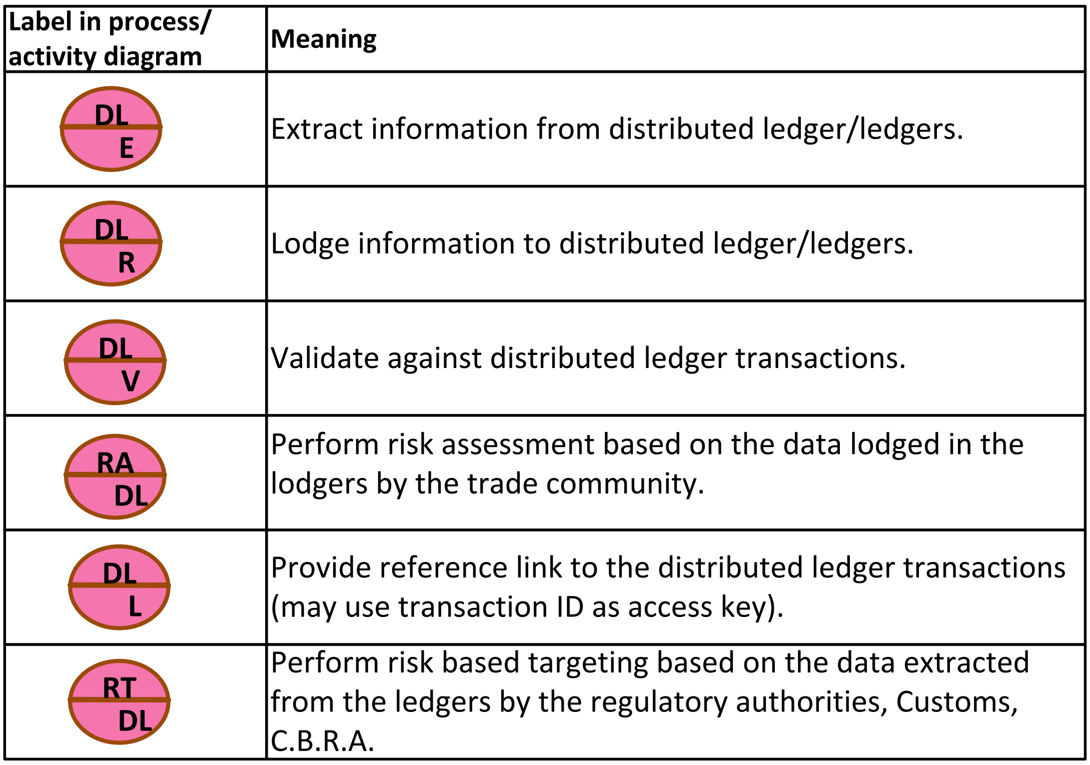
	Business process group	Opportunities
I	Registration/regulatory authorization	Distributed ledge enabled identity management (decentralized).
II	Application/issue of licenses, permits, certificates, other (LPCO)	Issuing, managing, and validating LPCO using distributed ledgers.
III	Advance information	Exchange of cross-border supply chain data over distributed ledgers; and unified data flows between all the four business areas.
IV	Goods declaration/cargo reports	Automation of Customs declaration and filing process, improved risk management and targeting capability (e.g., admissibility, import safety).
V	Post-release compliance verification and entry liquidation	Risk based assessment and detection of red flags (e.g., risk based bonding, mis-invoicing, warning signals for audit).

and the regulatory authorities, and to aid in the facilitation and simplification of the Customs declaration and entry related procedures.

During development of the process diagrams included in this section, the team has referenced the business process diagrams from the WCO data models, international supply chain business models released by the UN/CEFACT, entry processing diagrams made publicly available by CBP, and entry related knowledge gathered from literature review and subject matter experts.

The business processes are further divided into five groups in Table 4.1, which roughly follows the WCO categorization of business process of Customs declaration and Single Window.

The activity and process diagrams shown in this section mark places where there are data interactions with distributed ledgers, Figure 4.14 lists the meanings of these labels.



Label in process/ activity diagram	Meaning
DL E	Extract information from distributed ledger/ledgers.
DL R	Lodge information to distributed ledger/ledgers.
DL V	Validate against distributed ledger transactions.
RA DL	Perform risk assessment based on the data lodged in the lodgers by the trade community.
DL L	Provide reference link to the distributed ledger transactions (may use transaction ID as access key).
RT DL	Perform risk based targeting based on the data extracted from the ledgers by the regulatory authorities, Customs, C.B.R.A.

Figure 4.14: Explanation for the labels in the activity/process diagram.

4.5.1. Registration/authorization of AEOs

According to the WCO, mutual recognition of controls is the recognition by a Customs authority of a control process performed on an economic operator by another Customs administration. It eliminates or reduces the potential duplication of the control process, and consequently enhances trade facilitation. This includes mutual recognition of AEOs (Authorized Economic Operators). An identifier for an economic operator can be issued to provide a unique identity to that economic operator, which can be used as a reference key to access a larger set of information relating to the economic operator. The set of information may cover legal status, structure of the entity, contact details, director/partners, etc.

Distributed ledgers offer the opportunity to facilitate “Customs-to-Customs cooperation” and “government-to-government cooperation” without having a centralized intermediary storing identities of all the AEOs that engage in international trade. The technology can be a vital enabling component for a network of interconnected Customs authorities, and strengthen trade facilitation through mutual recognition and access to information of AEOs.

Digital identities of AEOs, after issued, can be stored and/or protected using distributed ledgers. The interconnected ledgers can potentially enable globally unique identities for the AEOs, and global recognition of the AEOs by the international trade community. It simplifies authorization process of the economic actors, and reduces possibility that the AEOs are misidentified, or non AEOs are incorrectly recognized as the AEOs.

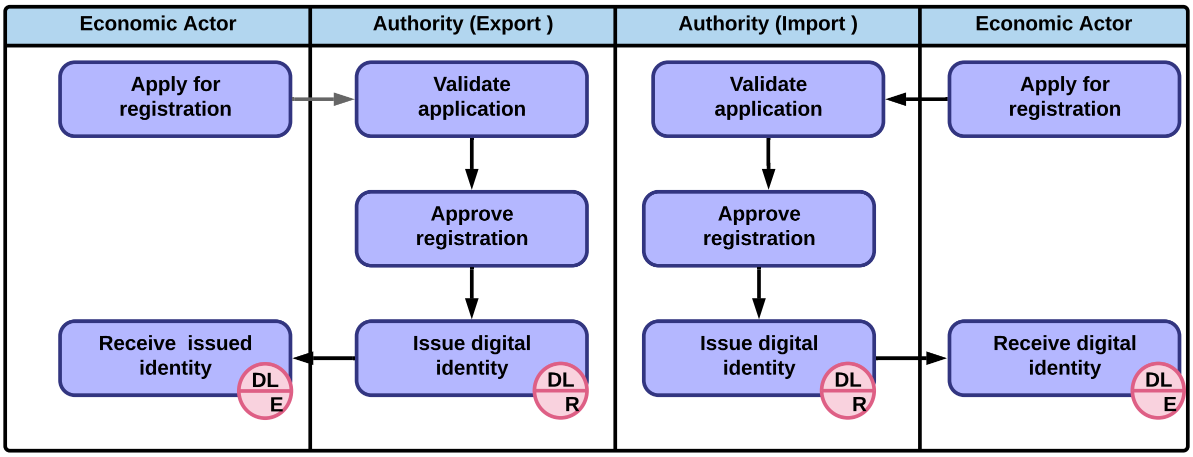


Figure 4.15: Process to authorize economic actors.

Figure 4.15 is a simple process diagram that describes AEO registration process by the export or import Customs administration. After the digital identities are lodged in the distributed ledger, it will be recognized by all the global participants including both business actors and regulatory authorities.

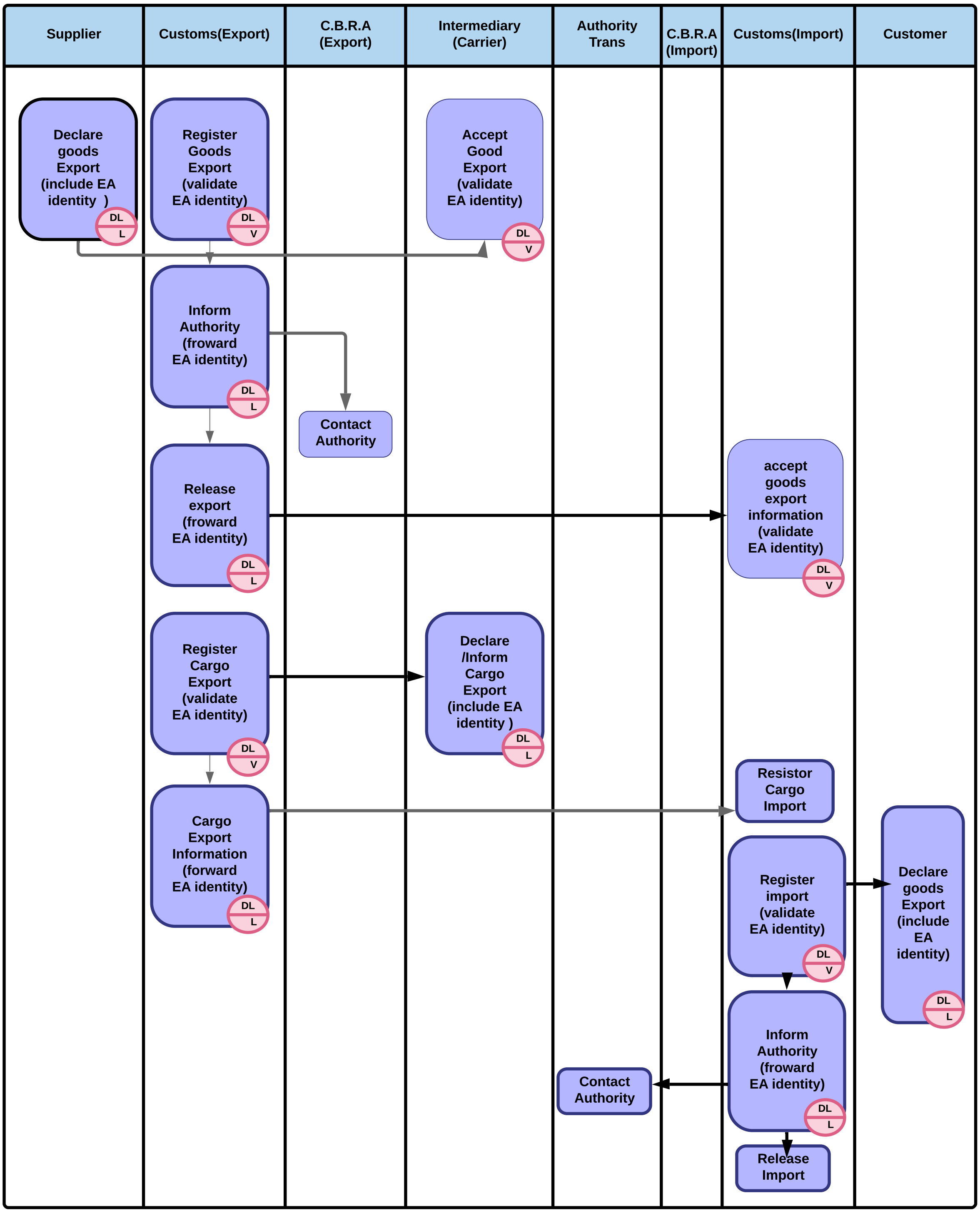

Supplier
Customs(Export)
C.B.R.A (Export)
Intermediary (Carrier)
Authority Trans
C.B.R.A (Import)
Customs(Import)
Customer
Declare goods Export (include EA identity)
DL L
Register Goods Export (validate EA identity)
DL V
Accept Good Export (validate EA identity)
DL V
Inform Authority (froward EA identity)
DL L
Contact Authority
Release export (froward EA identity)
DL L
accept goods export information (validate EA identity)
DL V
Register Cargo Export (validate EA identity)
DL V
Declare /Inform Cargo Export (include EA identity)
DL L
Resistor Cargo Import
Cargo Export Information (forward EA identity)
DL L
Register import (validate EA identity)
DL V
Declare goods Export (include EA identity)
DL L
Inform Authority (froward EA identity)
DL L
Contact Authority
Release Import

Figure 4.16: Process how AEO identities are shared and validated under the WCO cross-border regulatory global model (activity diagram).

Access and usage of AEO identities during the cross-border process are depicted in the process diagram in Figure 4.16. The actors include, AEOs in the exporting country, Customs in the exporting country, AEOs in the importing country, intermediaries, and Customs in the importing country.

For export, AEOs in the export country include access key to their digital identities in the export declaration. The Customs and export country C.B.R.A can validate the submitted identities. When information regarding the export goods is forwarded to the import Customs, access key to the AEO digital identity can be forwarded together with the export information, which allows the import Customs and C.B.R.A to validate the AEO's identity based on the distributed ledger data that they have access.

Furthermore, access keys to the digital identities of the intermediaries can be included in the transportation manifests, and validated by the export and import Customs. Import declarations can include access keys to the involved AEO identities. The import Customs and C.B.R.A can validate authenticity and validity of the provided identities against the shared ledger.

A common and shared ledger facilitates globally unique identities of AEOs and mutual recognition of Customs control, enhanceing the efficiency of the clearance process by reducing the efforts needed to validate the AEOs and time required for Customs control. It improves visibility and transparency of the international supply chains.

4.5.2. Process for managing accreditation and issuing product certification

Many partner agencies have third party certification programs. The accreditation and certification process include both business-to-government (B2G) and business-to-business (B2B) scenarios. In these scenarios, regulated entities contract with a third-party certification body (e.g., a testing laboratory) to assess and certify whether they are in conformity with an applicable regulatory standard for import.

Accreditation bodies are approved or recognized by the regulatory agencies to perform accreditation. They determine whether testing, inspection and certification bodies are operating in accordance with the international standards (e.g., ISO/IEC standards) that apply to them. Accreditation bodies may be public or private entities. It is common to have multiple private accreditation bodies in a country instead of a national accreditation body.

Accreditation bodies, in turn, are often members of either the International Accreditation Forum (IAF) or the International Laboratory Accreditation Cooperation (ILAC), which require adherence to the international standards for accreditation bodies and use a system of peer evaluation to assess accreditation bodies for membership [26].

The certification bodies are generally private or non-government entities that have been accredited to perform certification and compliance testing task by an accreditation body. The accredited third party entities or laboratories are often subject to either an on-site surveillance or a full reassessment after certain period of time (depending on the specific

Table 4.2: ISO standards for conformity assessment activities

Conformity Assessment Activity	Relevant International Standards
Supplier's Declaration of Conformity (SDoC)	ISO/IEC 17050, Conformity assessment - Supplier's declaration of conformity.
Testing	ISO/IEC 17025, General requirements for the competence of testing and calibration laboratories.
Inspection	ISO/IEC 17020, Conformity assessment – Requirements for the operation of various types of bodies performing inspection.
Certification	ISO/IEC 17065, Conformity assessment – Requirements for bodies certifying products, processes and services.
Accreditation	ISO/IEC 17011, General requirements for accreditation bodies accrediting conformity assessment bodies.

regulatory requirement) to ensure that they maintain their standards of independence and technical expertise.

The process integrated with distributed ledgers is illustrated in Figure 4.17. Different regulatory agencies (e.g., EPA, FDA) often have their own accreditation programs. Process diagram in Figure 4.17 is general enough to capture the basic procedure as these program often share the same basic structure.

With support of distributed ledgers, the chain of accreditation and certification events can be captured and protected with blockchains. Figure 4.17 shows interaction of each step with a distributed ledger.

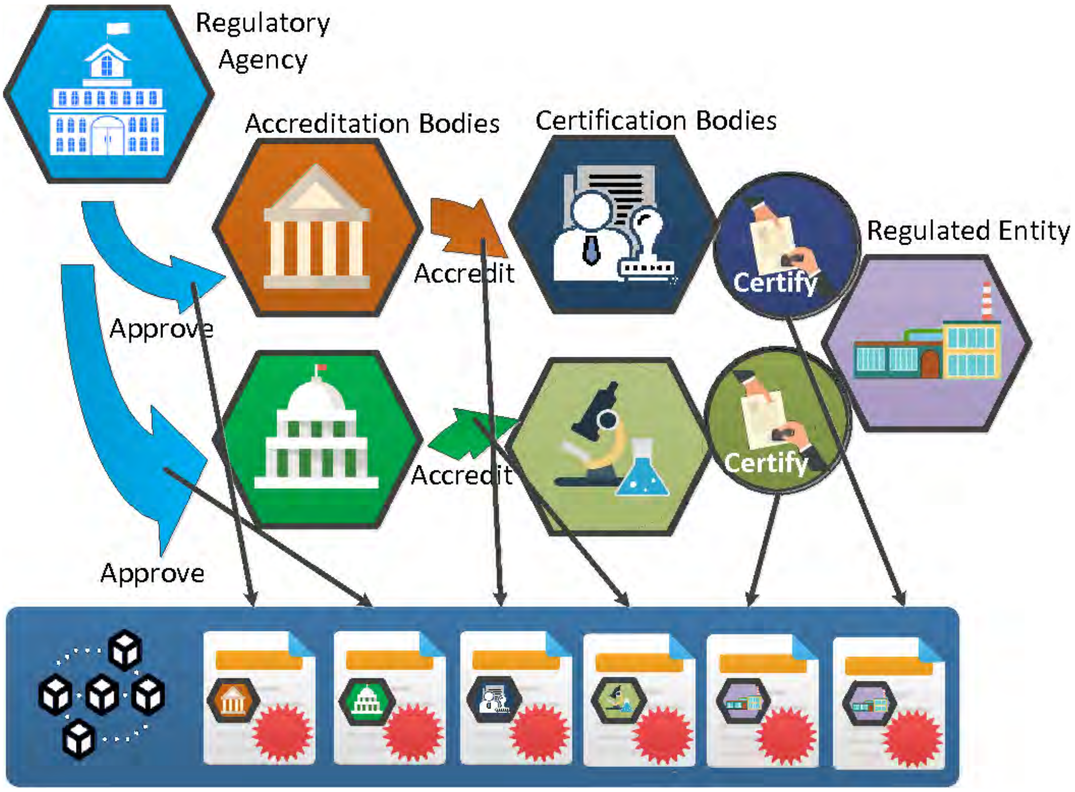


Figure 4.17: Leveraging blockchain and distributed ledger for accreditation and certification.

Distributed ledgers can enable the implementation of electronic certification and accreditation in a more efficient, secure and trusted manner. It could ensure openness and integrity of the process such that certificate is appropriately issued; properly and digitally signed by a valid accredited certification issuing body.

Meanwhile, blockchains also provide security protection to prevent any alteration of the content or misuse of the issued certificate by a third party. The cooperative environment facilitated by distributed ledgers can help fulfill the mutual recognition vision of accreditation and certification by the IAF and the ILAC, "tested or certified once - accepted everywhere". This can significantly reduce the burden of importers and exporters, streamline the certification process, and facilitate trade [26].

Once the information is lodged to distributed ledgers, the regulatory authorities, customers, and consumers may have access to the information. The information can be accessed and used for validation during procurement, trade agreement, and declaration. PGAs can use the information to assess risk of import safety, and determine if goods can be admitted to the commerce, or require further examination before release. With respect to product quality, consumers may prefer independent assurance of quality and conformity by the accredited testing bodies.

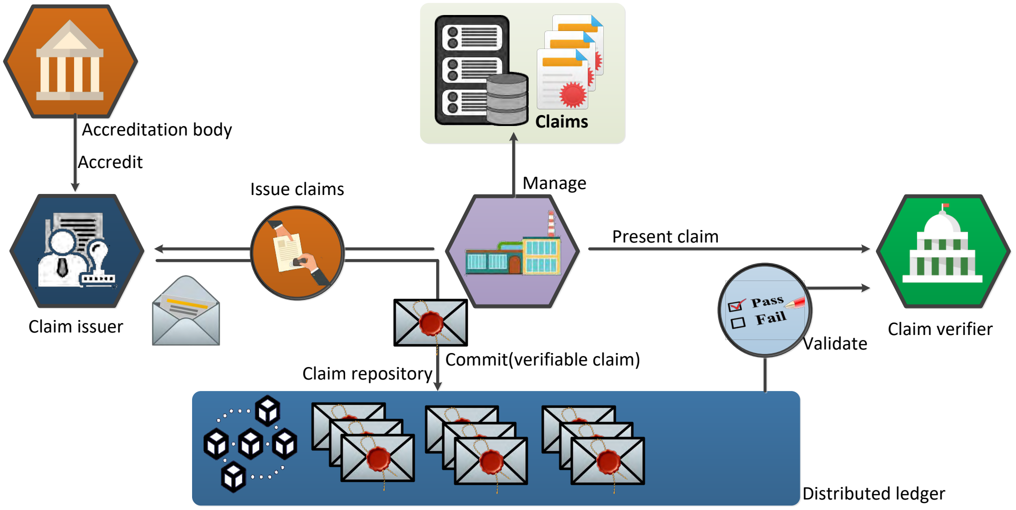


Figure 4.18: Process for issuing, managing, and verifying claims under the blockchain model.

Distributed ledgers allow supply chain actors to manage various claims such that products meet compliance requirements, quality criteria, environment and sustainability standards without a centralized intermediary. The process is illustrated in Figure 4.18.

Certification can be issued in the form of verifiable claims. Contents of the claims are managed by the economic actors. This avoids trade secret and confidential business information from being disclosed to the public, for instance, business relations between the accredited certification body and the regulated economic actors. With necessary information lodged to a distributed ledger, an economic actor can present claims to the customers, consumers, and regulatory authorities. These claims can be validated against information lodged in the distributed ledger.

4.5.3. Map of distributed ledger data sources and data collection

Considering the likely scenario of adoption of distributed ledgers to support international supply chain management that covers all the major business process areas (commercial, logistical, financial, and regulatory), vast amounts of supply chain information will be accessible from the distributed ledgers and protected by the blockchain technology. The integrated data environment allows the regulatory authorities (Customs, C.B.R.A) to collect accurate and high quality supply chain data from the distributed ledgers, which can be applied for trade facilitation, risk assessment, and Customs control.

The process needs to be formalized because for the global supply chains, there will be a plethora of distributed ledgers (both vertical and horizontal) and consortia behind these ledgers. For a distributed ledger that connects with multiple supply chain stakeholders across the value chain, there should be a unified view of data model that allows data exchange and communication over the distributed ledgers. This unified view bridges the gaps between different views of supply chain models (trade, transportation, regulatory declaration, and finance). It helps integration of distributed ledger with the private ERP systems maintained and administrated by each respective stakeholder.

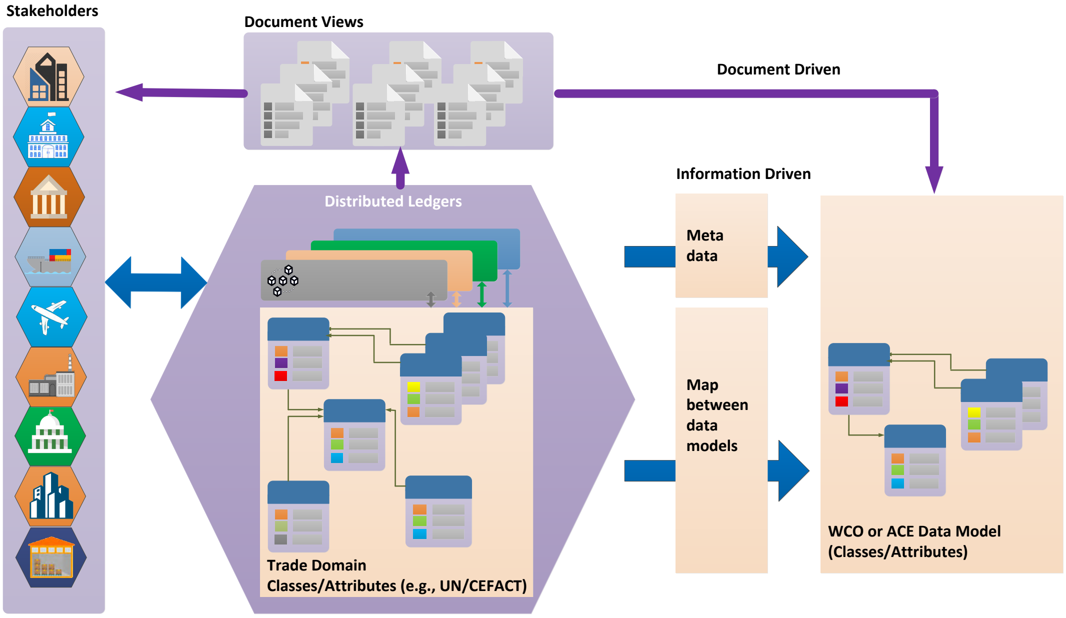


Figure 4.19: Map data items of different views.

For mapping different views in the commercial sides, the international standard organizations such as the UN/CEFACT, ISO, and blockchain/distributed ledger consortia often could take the leading roles. The responsibility to map distributed ledger data sources to the regulatory view is likely with the WCO and Customs. Figure 4.19 depicts a high level diagram, where information stored in the supply chain distributed ledger domain can be mapped to the Customs data model. The information driven process allows direct map between the unified view and the Customs data model, which facilitates correlation of the same data between different views.

At high level, the process to map distributed ledger data sources to the Customs data model can be the one depicted in Figure 4.19.

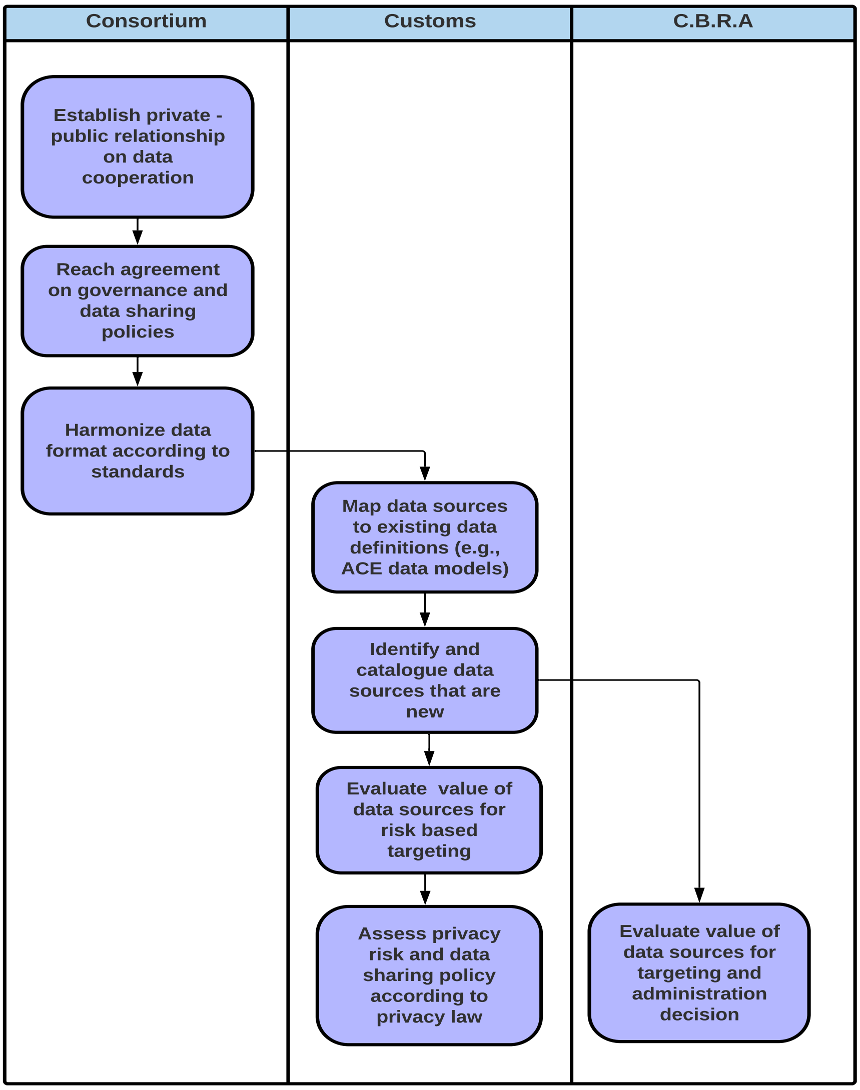

Consortium
Customs
C.B.R.A
Establish private - public relationship on data cooperation
Reach agreement on governance and data sharing policies
Harmonize data format according to standards
Map data sources to existing data definitions (e.g., ACE data models)
Identify and catalogue data sources that are new
Evaluate value of data sources for risk based targeting
Assess privacy risk and data sharing policy according to privacy law
Evaluate value of data sources for targeting and administration decision

Figure 4.20: Process to map blockchain data source.

The process involves the steps described in Table 4.3.

During cross border trade, economic actors will lodge supply chain data in the distributed ledger (e.g., private or permissioned). A simple model describing the data collection process is shown in Figure 4.21.

Table 4.3: Process to map blockchain data to the Single Window data model for data collection.

Establish private-government relationship	Distributed ledgers and blockchain projects are often led by industry initiated consortia. The consortia play the role for setting standards, managing operation environment, and creating governance policies of the distributed ledgers. Members of a consortium include private industry supply chain actors. For data collection and cooperation between the regulatory authorities and a private distributed ledger environment, a formal relation between the involved cross-border supply chain consortium and the regulatory authority is the first step of data sharing.
Reach agreement on data sharing	After a formal partnership is established, the regulatory authority can reach an agreement with the consortium and its members regarding data sharing policies, and governance principles. There is no one-size-fit-all approach. Likely an agreement tailored for the specific distributed ledger under concern is needed.
Harmonize data structure and view	To facilitate a unified view and map between the data available on a distributed ledger to the Customs data model, data structures and formats need to be harmonized. This ensures to some degree that information accessible by the regulatory authority is compatible with the terminology, semantics, and standards used by the authority.
Map data sources	This step correlates the collectible data available on the distributed ledger to the data definitions used by the regulatory authority.
Identify new data sources	During the previous step, the regulatory authority may discover and identify collectible data sources that are new. These new sources of data need to be cataloged with descriptions such as who produces the data, who accesses the data during trade, format of the data, and data semantics.
Evaluate data sources	Potential contributions of the data sources for risk assessment, Customs control, and trade facilitation can be evaluated. The assessment may help the regulatory authority to prioritize data collection efforts focusing on data with the most value.
Assess privacy risk	The regulatory authority assesses privacy risk of data collection and compliance in accordance with the privacy laws and data confidentiality regulations that the government needs to follow.

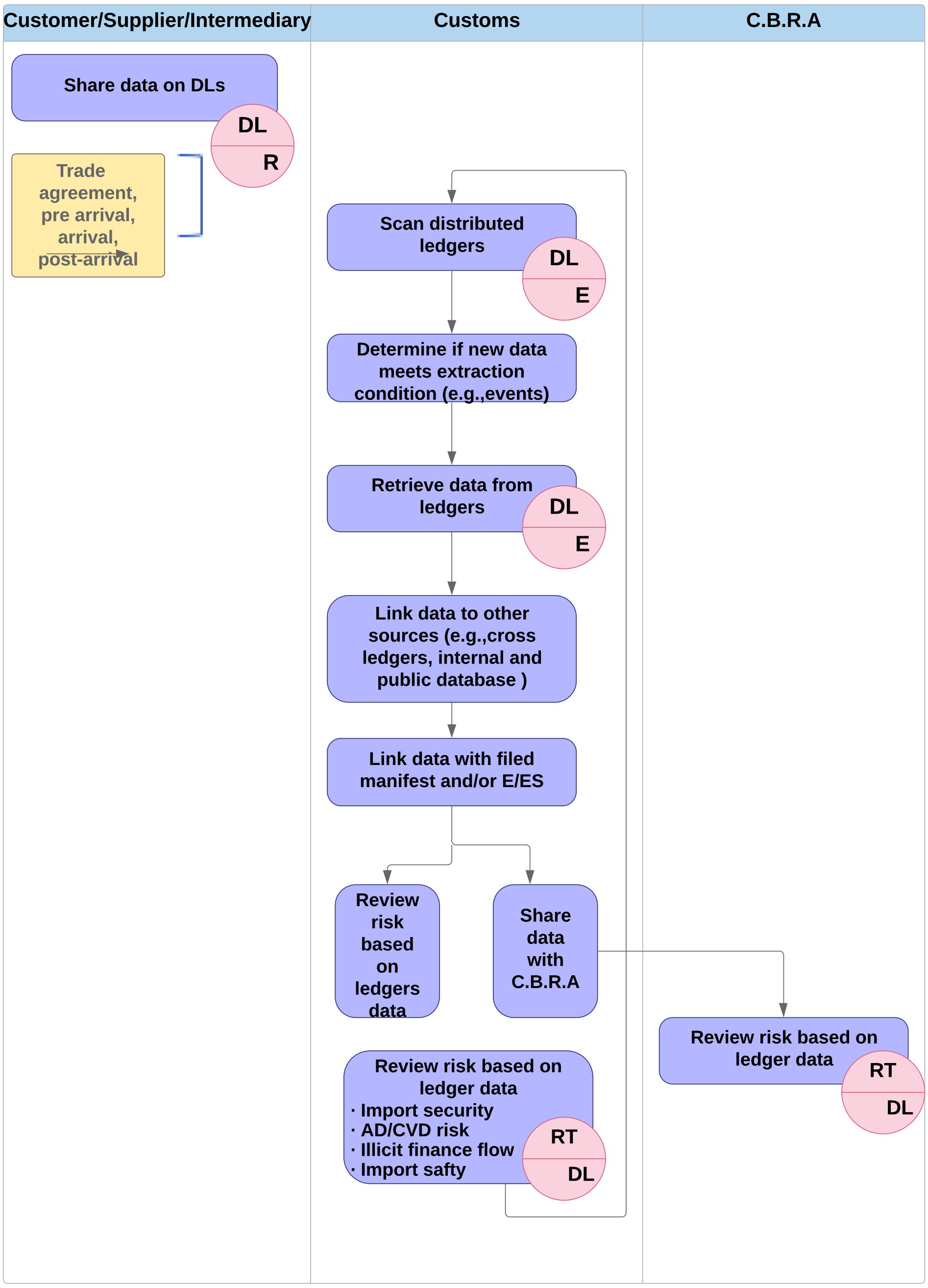

Customer/Supplier/Intermediary
Customs
C.B.R.A
Share data on DLs
DL
R
Trade agreement, pre arrival, arrival, post-arrival
Scan distributed ledgers
DL
E
Determine if new data meets extraction condition (e.g.,events)
Retrieve data from ledgers
DL
E
Link data to other sources (e.g.,cross ledgers, internal and public database)
Link data with filed manifest and/or E/ES
Review risk based on ledgers data
Share data with C.B.R.A
Review risk based on ledger data
· Import security
· AD/CVD risk
· Illicit finance flow
· Import safty
RT
DL
Review risk based on ledger data
RT
DL

Figure 4.21: Process to extract data from a supply chain ledger.

The process involves the steps in Table 4.4.

Figure 4.22 depicts two approaches for sharing data with the partner agencies. In the first approach, partner agencies reach out to the relevant distributed ledgers and establish independent data pipes for collecting data from the targeted ledgers. For example, regulatory partner agencies responsible for food safety, pharmaceutical product imports can create

Table 4.4: Process for data collection from shared supply chain ledgers.

Lodge data to a distributed ledger	Cross-border trade actors lodge supply chain data to a distributed ledger during trade process.
Scan the ledger	Regulatory authority scans the distributed ledger for available and relevant supply chain data.
Determine data extraction	Regulatory authority determines whether the new data lodged to the ledger meets extraction conditions (e.g., supply chain events).
Retrieve data	Regulatory authority retrieves data from the ledger, and applies pre-processing to clean the data.
Correlate data	Regulatory authority correlates the retrieved data with the prior data collected from the same ledger, or related data retrieved from other ledgers. The data is also correlated with the data collected from other sources such as public databases, Internet, and etc.
Correlate with declarations and manifests	Regulatory authority correlates the data with the Customs declaration data or manifests.
Review risk	If conditions are met to trigger a review (e.g., significant mismatch of data attributes, red flags), regulatory authority reviews the information for risk assessment.
Share data with C.B.R.A	Regulatory authority shares relevant data with the partner agencies.
Review risk by C.B.R.A	Partner agencies conduct risk assessment of the imported goods.

data cooperation agreements with the consortia focusing on the agriculture and food supply chains, or pharmaceutical product supply chains. Agencies such as the EPA may create separate data pipes with the consortia focusing on testing and certifying compliance of environment laws.

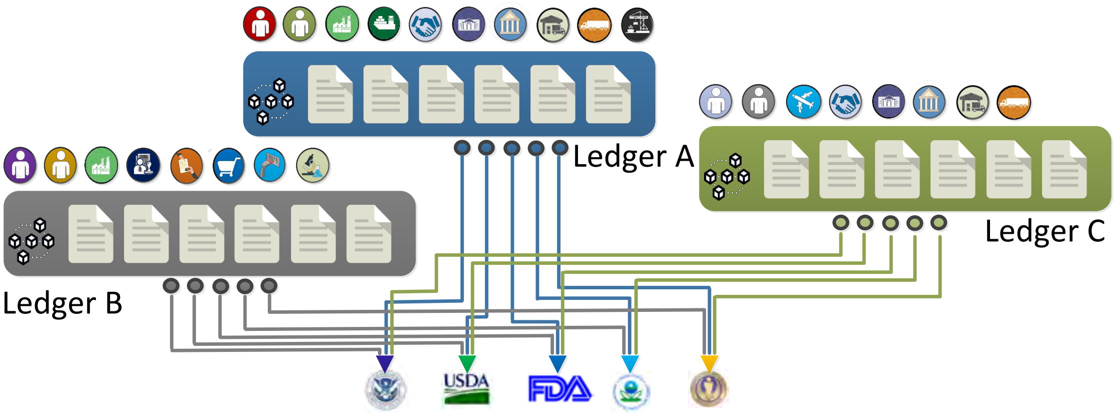


Figure 4.22: Data collection process by the partnering agencies - data pulled by the agencies from the ledgers.

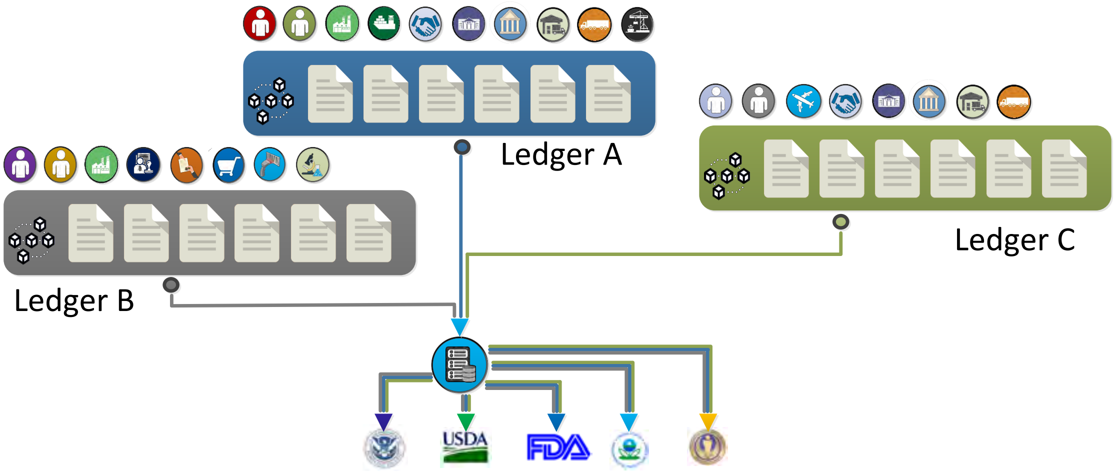


Figure 4.23: Data collection process by the partnering agencies through the Customs where the ledger data is pulled by the Customs on behalf of the partnering agencies.

The second approach is to have a single Customs agency who will reach data exchange agreements with the various cross-border supply chain consortia or private ledgers for data collection. This simplifies engagement between the regulatory authorities and distributed ledger operators. After necessary processing to clean the collected data, it can be further routed to the relevant partner agencies.

4.5.4. Advance commercial data sharing

According to supply chain research, there are benefits for cross-border supply chain trade to apply distributed ledgers at the commercial phase of trade agreement.

The process usually starts with the buyer recognizing the need for a product and preparing the certifications. Market sourcing, through the selection or tendering the process, assists identification of a suitable product and supplier. Thereafter, the buyer and the seller negotiate the terms and conditions of sale for the goods being purchased. Once agreement is reached, the buyer issues a purchase order, an accepted pro forma invoice. The buyer may place this against a framework agreement already established with the pre-selected suppliers.

The process results in an extensive flow of information between the buyers and the sellers, and any intermediaries involved in the transaction. With the ERP systems designed to enable e-purchasing, e-invoicing for payment, and electronic support for sourcing the market, the information could be lodged in a distributed ledger. Such information can be made only available to the members with properly designed access control enforcement.

Integration of ERP systems with the distributed ledgers can reduce dispute over sales agreement, invoices, and purchases. It can bring in transparency, and reduce cost of tracking and reporting. Figure 4.24 illustrates a simple procurement process assisted by the distributed ledgers. Qualified suppliers (e.g., identities of manufacturers, identities of suppliers), product lists, and product information (e.g., classification, certificates, unique product identifiers) can be managed in a transparent way between the suppliers and the buyers, and constantly updated.

In addition, framework agreements for long-term partnerships between the buyer and the seller, which set out the arrangements and conditions for trade and the technical details under which the buyer may place repeated orders (e.g., blanket purchase agreements, master ordering agreements), can be lodged in the distributed ledger. This improves the trust and helps resolving dispute when it occurs.

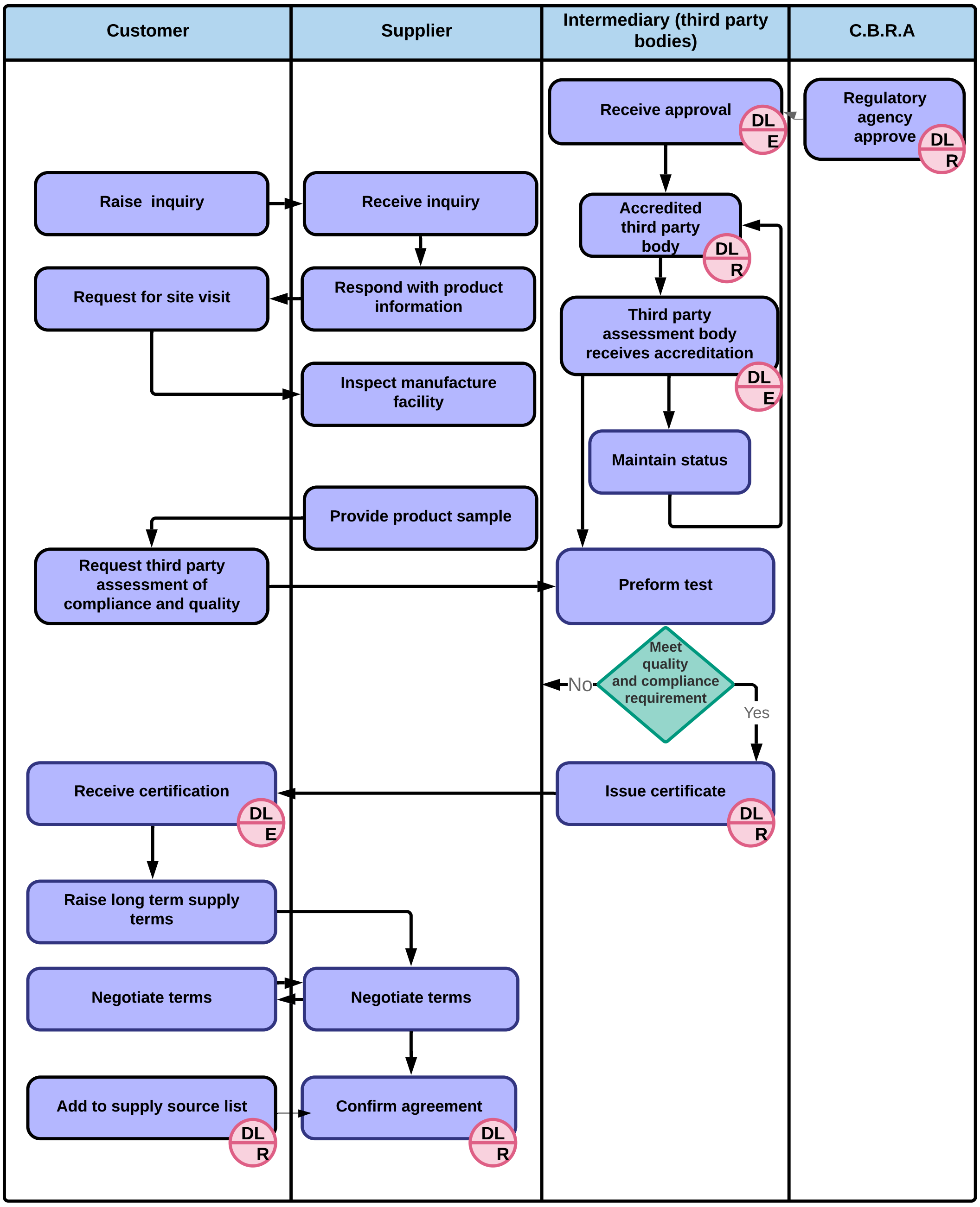

Customer
Supplier
Intermediary (third party bodies)
C.B.R.A
Receive approval
DL
E
Regulatory agency approve
DL
R
Raise inquiry
Receive inquiry
Accredited third party body
DL
R
Request for site visit
Respond with product information
Third party assessment body receives accreditation
DL
E
Inspect manufacture facility
Maintain status
Provide product sample
Request third party assessment of compliance and quality
Preform test
Meet quality and compliance requirement
No
Yes
Receive certification
DL
E
Issue certificate
DL
R
Raise long term supply terms
Negotiate terms
Negotiate terms
Add to supply source list
DL
R
Confirm agreement
DL
R

Figure 4.24: A simple process integrated with the blockchain for discovering and sourcing suppliers.

Figure 4.25 shows ordering process enhanced with distributed ledgers.

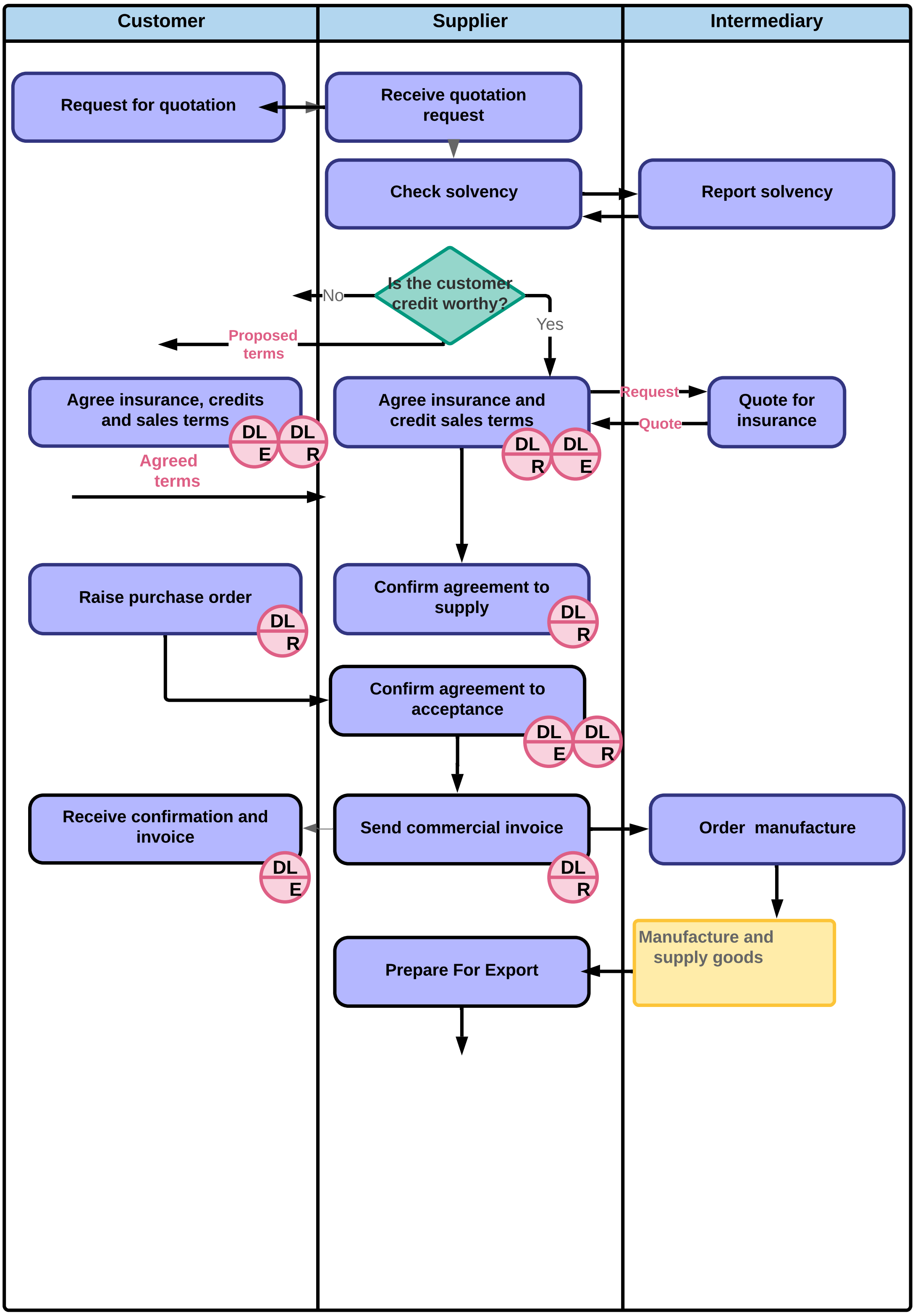


Figure 4.25: A simple process integrated with the blockchain for trade agreement.

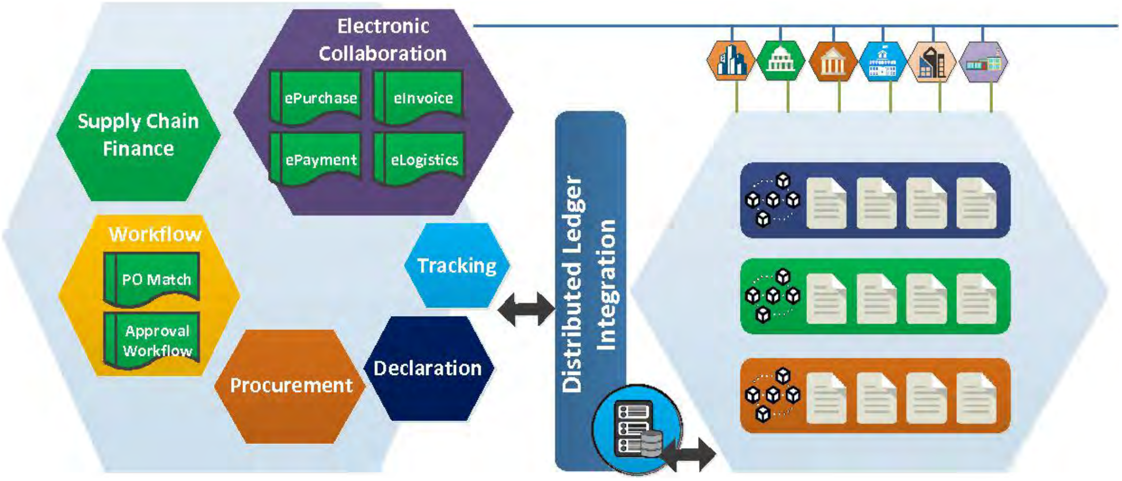


Figure 4.26: Integration of distributed ledgers with the existing enterprise system.

Regarding implementation, it is plausible to integrate blockchains with the existing ERP systems that have been developed to support digital trade such as e-purchase, e-procurement, e-sourcing, and e-invoicing. This allows companies to take advantages of blockchain technology without giving up their currently deployed systems. Figure 4.26 shows a diagram of integrated ICT design.

In case EDI messages are transferred across the involved supply chain actors with the confidential data protected by the distributed ledgers. The messages can include access key to the information lodged in the distributed ledgers. The data includes sales orders, purchase orders, agreements, or certificates. The message itself no longer needs to include such data except the references to the data secured by the blockchain.

After goods are ordered by a buyer, supplier can issue order to have the goods produced. As illustrated by Figure 4.27, the process can be enhanced with distributed ledgers where the production process can be monitored; and real-time data recording the manufacture process can be logged for purpose of audit and certification by a third accredited body. IoT sensors can provide a continuous flow of information, and link between the physical production and information flow. Data can be linked to the materials and products on the stages of the manufacturing process. It provides a trail of historical events, and automated mechanism to validate process that a product goes through. Based on the data, accredited third parties can certify that the products manufactured meet compliance and product quality requirements, which is recorded by a distributed ledger [47, 49, 60].

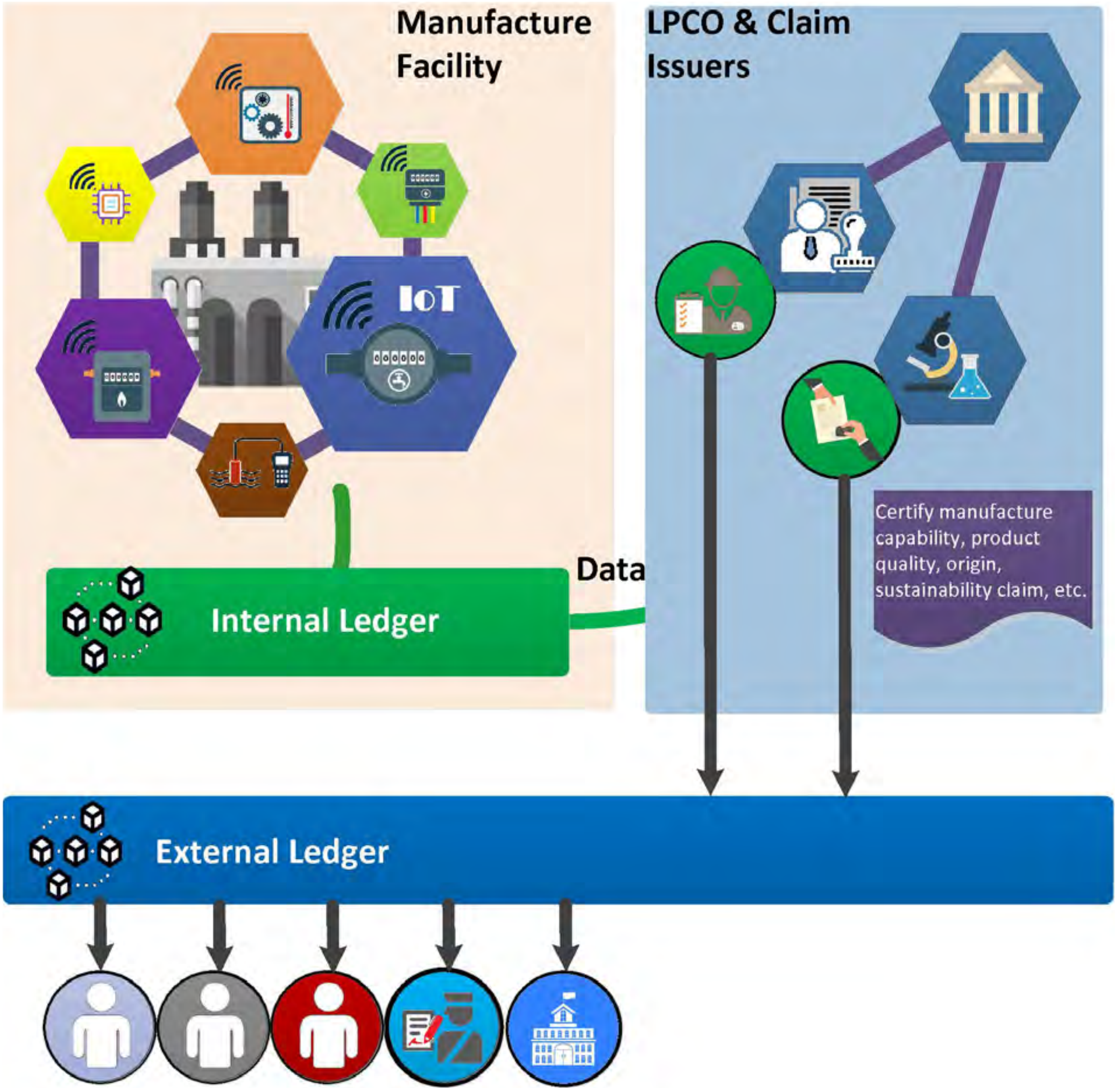

Manufacture Facility
IoT
Internal Ledger
Data
LPCO & Claim Issuers
Certify manufacture capability, product quality, origin, sustainability claim, etc.
External Ledger

Figure 4.27: Process to produce ordered goods with blockchain based certification.

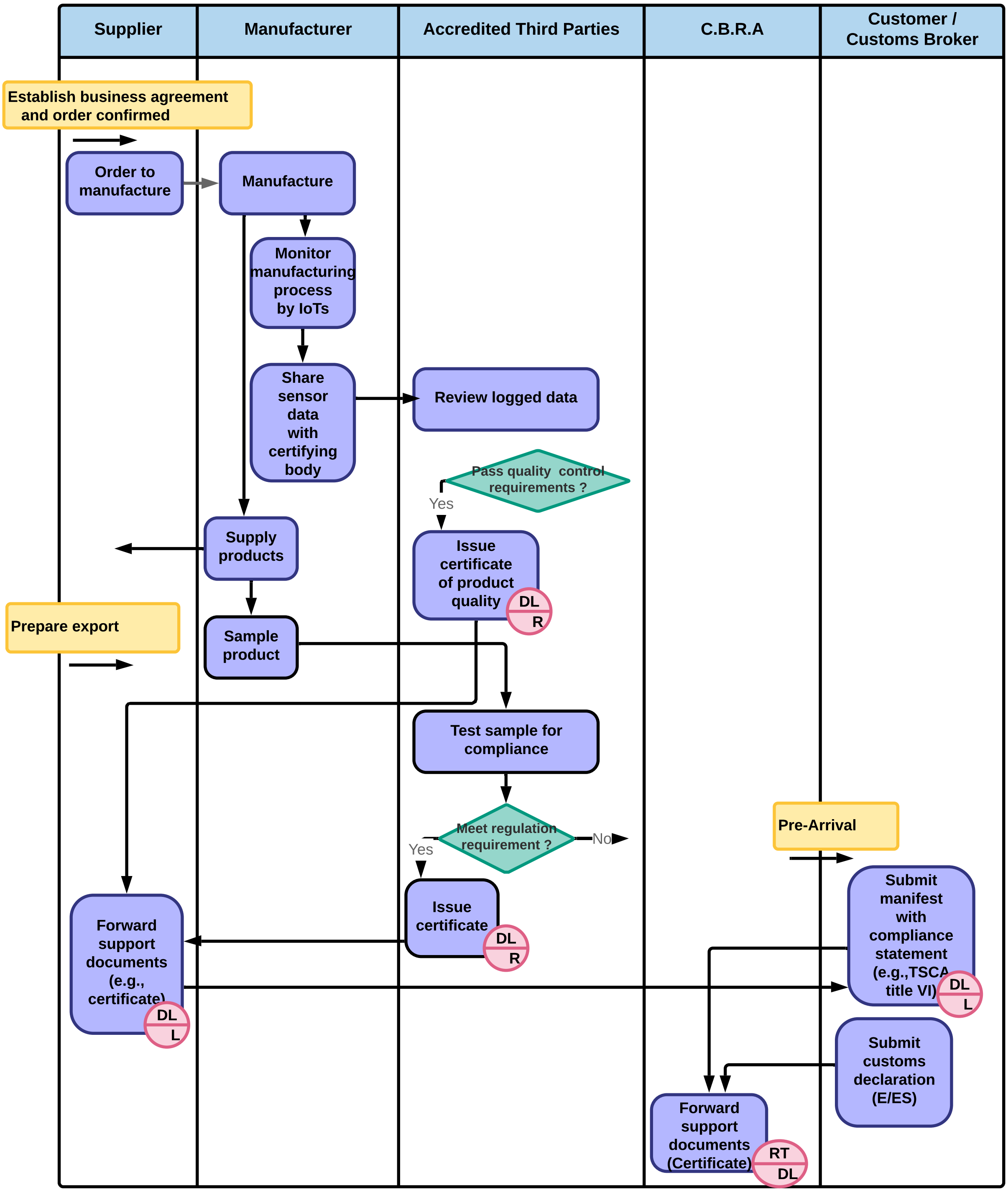

Supplier
Manufacturer
Accredited Third Parties
C.B.R.A
Customer / Customs Broker
Establish business agreement and order confirmed
Order to manufacture
Manufacture
Monitor manufacturing process by IoTs
Share sensor data with certifying body
Review logged data
Pass quality control requirements ?
Yes
Issue certificate of product quality
DL
R
Supply products
Prepare export
Sample product
Test sample for compliance
Meet regulation requirement ?
Yes
No
Issue certificate
DL
R
Forward support documents (e.g., certificate)
DL
L
Pre-Arrival
Submit manifest with compliance statement (e.g.,TSCA title VI)
DL
L
Submit customs declaration (E/ES)
Forward support documents (Certificate)
RT
DL

Figure 4.28: Process to certify manufactured goods and share the result using blockchain.

4.5.5. Automated declaration process

With supply chain information lodged in distributed ledgers, declaration process can be streamlined and simplified. This can result in more automated declaration process, reduction in errors, less manual work, and smoother data exchange with the regulatory authorities.

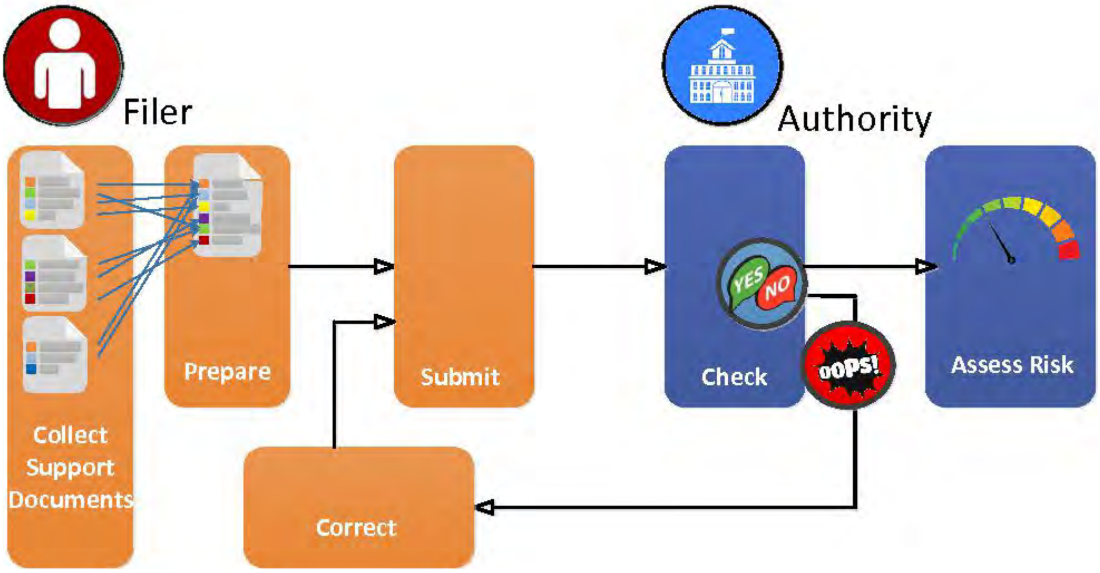


Figure 4.29: A simple diagram showing the declaration process.

Figure 4.29 shows a simplified diagram of the existing declaration process, where Customs broker and filer need to collect support documents, filter the information manually, and re-enter the data in accordance with the entry declaration requirements. With the supply chain information already lodged in the ledgers, this process can be streamlined and automated as illustrated in Figure 4.30.

View of entry declaration can be automatically created based on the supply chain events. Reference keys can be provided that link the submitted information to the transactions recorded by the corresponding ledgers (e.g., transaction IDs). Brokers who have access to the ledgers can validate the information, certify its accuracy, and endorse the declaration.

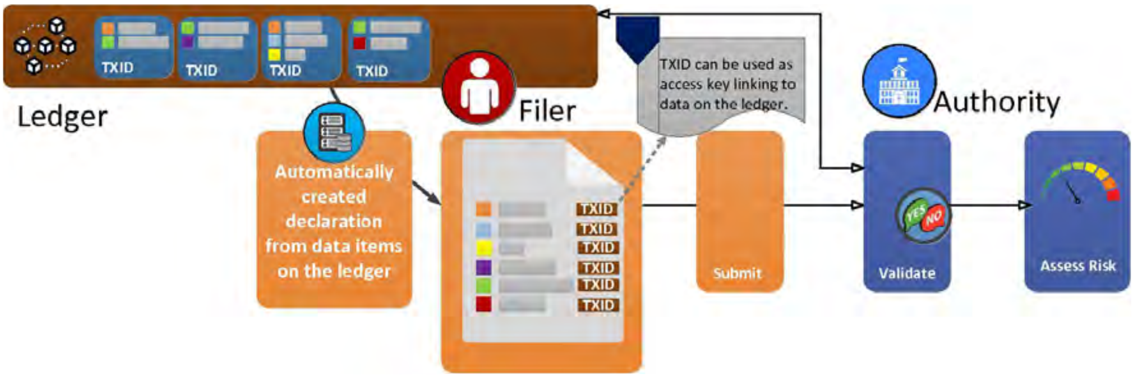

TXID
TXID
TXID
TXID
Ledger
Filer
TXID can be used as access key linking to data on the ledger.
Authority
Automatically created declaration from data items on the ledger
TXID
TXID
TXID
TXID
TXID
TXID
Submit
YES
NO
Validate
Assess Risk

Figure 4.30: A simple diagram showing the declaration process integrated with supply chain blockchains.

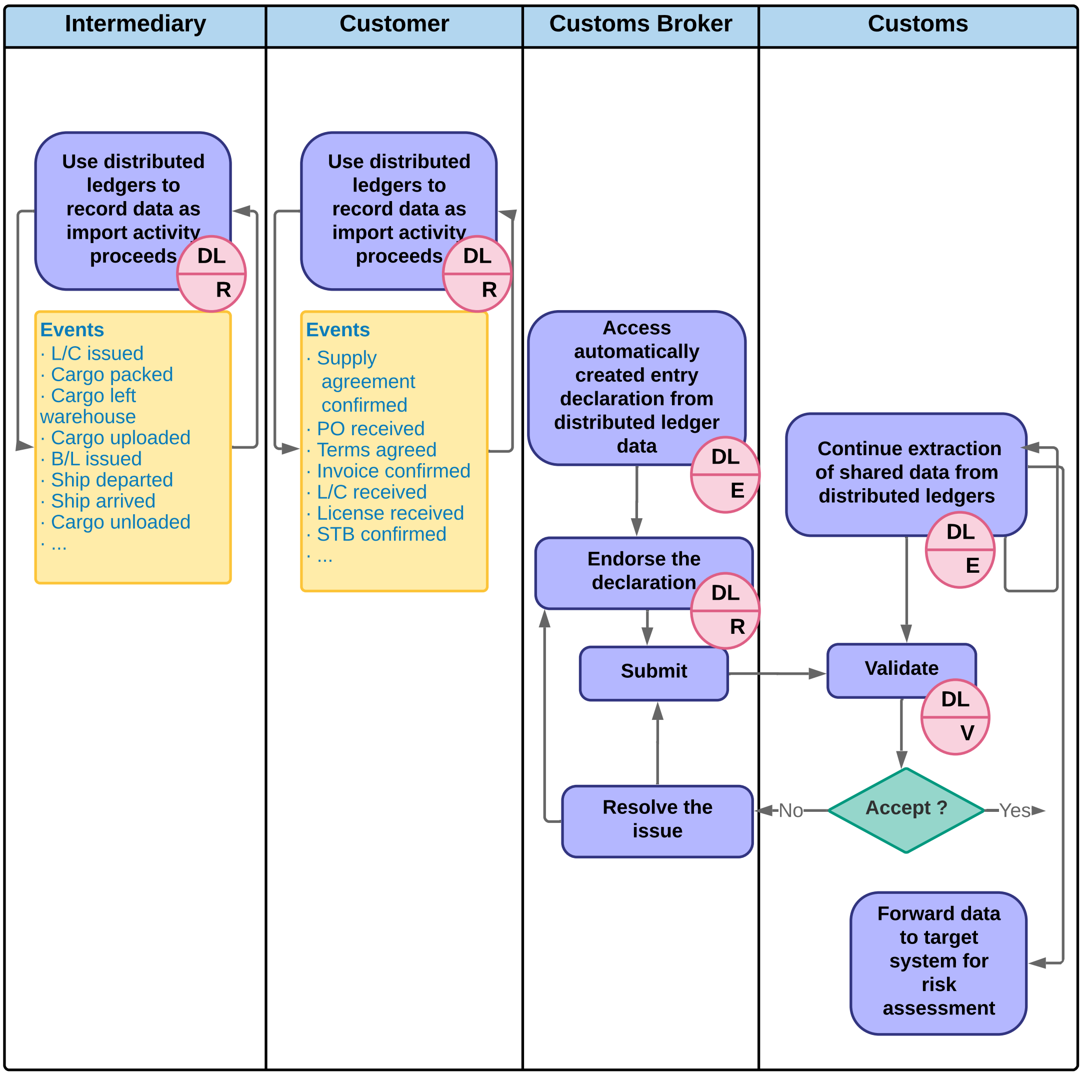


Figure 4.31: A simple process diagram on blockchain facilitated filing process.

Figure 4.31 provides a simple process diagram for illustrating the declaration process after it is automated by integrating with the distributed ledgers. Since the regulatory authorities can have access to the same ledgers that the brokers use as the data sources for declaration, the submitted information can be easily validated (assume that reference keys are provided). With built-in data quality assurance by the distributed ledgers, the submitted information will be less error prone. This reduces the number of times that brokers need to have the data corrected.

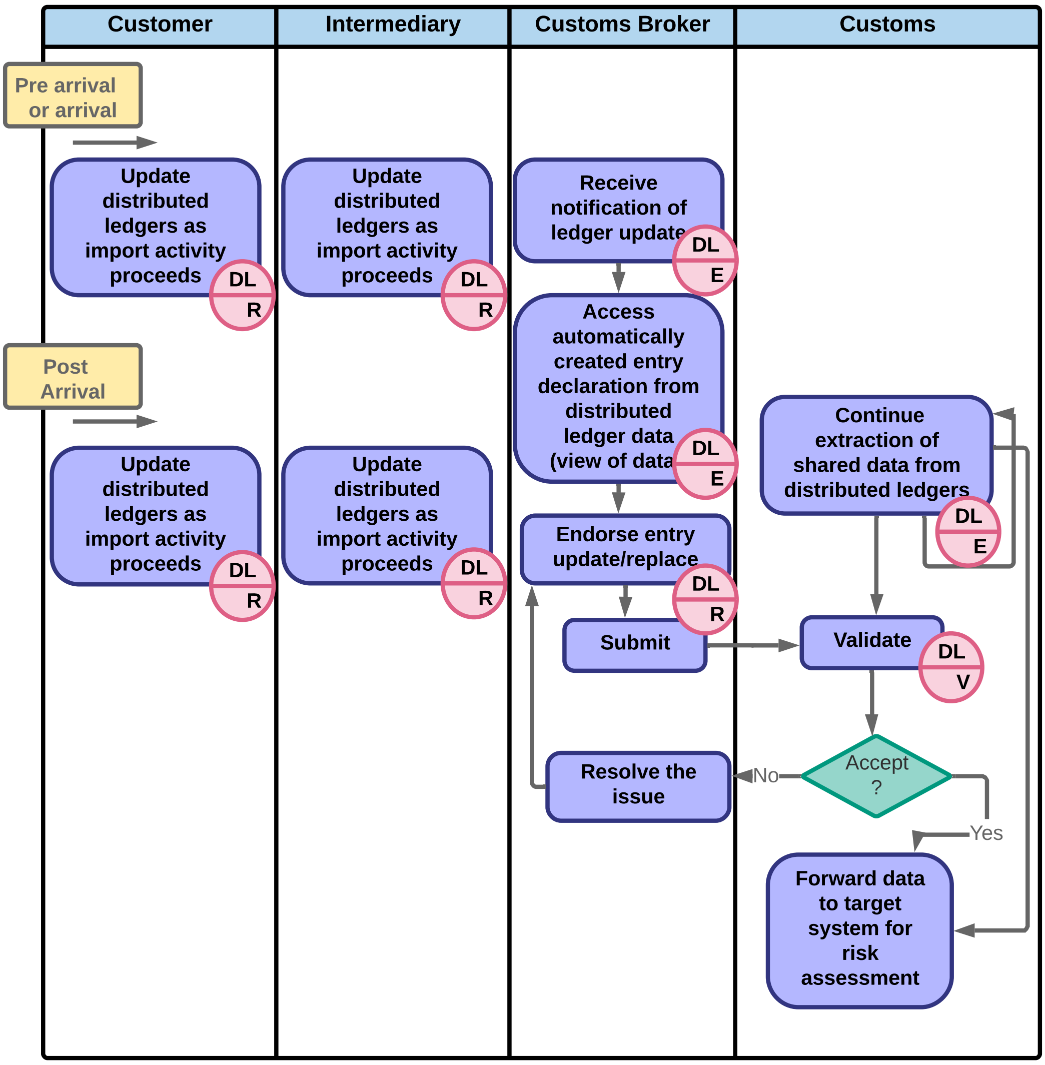

Customer
Intermediary
Customs Broker
Customs
Pre arrival or arrival
Update distributed ledgers as import activity proceeds
DL R
Update distributed ledgers as import activity proceeds
DL R
Receive notification of ledger update
DL E
Access automatically created entry declaration from distributed ledger data (view of data
DL E
Post Arrival
Update distributed ledgers as import activity proceeds
DL R
Update distributed ledgers as import activity proceeds
DL R
Endorse entry update/replace
DL R
Submit
Continue extraction of shared data from distributed ledgers
DL E
Validate
DL V
Accept ?
No
Yes
Resolve the issue
Forward data to target system for risk assessment

Figure 4.32: A simple process diagram on blockchain facilitated filing process when update of entry is needed.

Whenever changes are made to the supply chain information recorded by the distributed ledgers, for instance update according to the supply chain events, brokers can be notified and a declaration update can be generated. Figure 4.32 depicts the process for updating entry declaration after the initial version is submitted.

4.5.6. Post-release compliance verification and risk assessment

Distributed ledgers can facilitate information cooperation between the supply chain stakeholders, which will increase the regulatory authorities' capabilities in post release compliance verification and risk based assessment of issues such as non-payment risk, illicit finance flow, mis-invoicing, and etc. Correlating information collected from the distributed ledgers with the Customs declarations, the regulatory authorities may be able to identify high risk entries, and conduct holistic audit using the enriched risk profiles and signals.

4.5.6.1. Illicit finance flow

The use of distributed ledgers can reduce compliance errors and remove the duplicated effort involved in validation of illicit finance flow and trade based money laundering risk.

Data pooling of distributed ledgers, particularly including data from trade finance and freight forwarding ledgers, can assist in detecting invoicing anomalies, spotting financial flow irregularities, and identifying entities attempting to create fraudulent histories.

Risk information sharing across public-private sectors is vital to identifying trends and patterns of illicit finance flows [52, 66]. Distributed ledgers provide opportunities for a digital cooperative environment between the regulatory authorities and the trade finance intermediaries to increase trade transparency. Figure 4.33 depicts the process where trade finance related information and risk profiles can be lodged to distributed ledgers. Data sharing is protected with approaches to safeguard privacy.

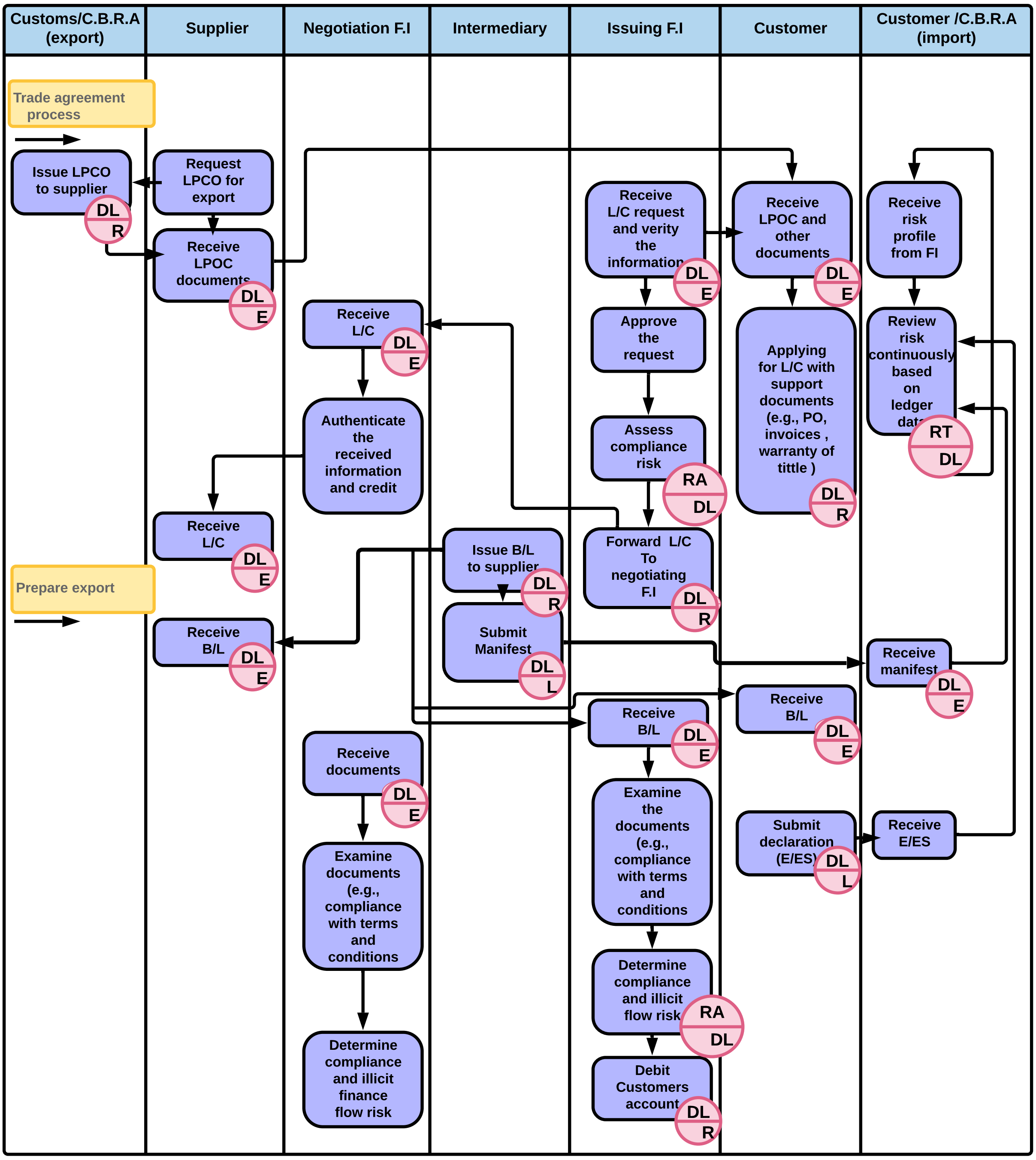

Customs/C.B.R.A (export)
Supplier
Negotiation F.I
Intermediary
Issuing F.I
Customer
Customer /C.B.R.A (import)
Trade agreement process
Issue LPCO to supplier
Request LPCO for export
Receive LPOC documents
Receive L/C request and verity the information
Receive LPOC and other documents
Receive risk profile from FI
Approve the request
Applying for L/C with support documents (e.g., PO, invoices , warranty of tittle)
Review risk continuously based on ledger data
Receive L/C
Authenticate the received information and credit
Assess compliance risk
Receive L/C
Prepare export
Issue B/L to supplier
Forward L/C To negotiating F.I
Submit Manifest
Receive B/L
Receive manifest
Receive B/L
Receive B/L
Receive documents
Examine the documents (e.g., compliance with terms and conditions
Submit declaration (E/ES)
Receive E/ES
Examine documents (e.g., compliance with terms and conditions
Determine compliance and illicit flow risk
Determine compliance and illicit finance flow risk
Debit Customers account
DL
R
E
L
RA
RT

Figure 4.33: Process for sharing trade finance information over blockchains.

4.5.6.2. Risk based bonding

Lack of transparency along the supply chain causes various concerns, including that the prices paid might be an inaccurate reflection of the true value which has implication on Customs revenue. The issue of AD/CVD duty evasion, mis-invoicing, and mis-declaration could potentially be tackled in a more transparent manner if distributed ledgers are adopted for transactions of trade finance and Customs bonds. To reduce non-payment risk, Customs leverages bonds provided by the surety. The process of surety is depicted in Figure 4.34.

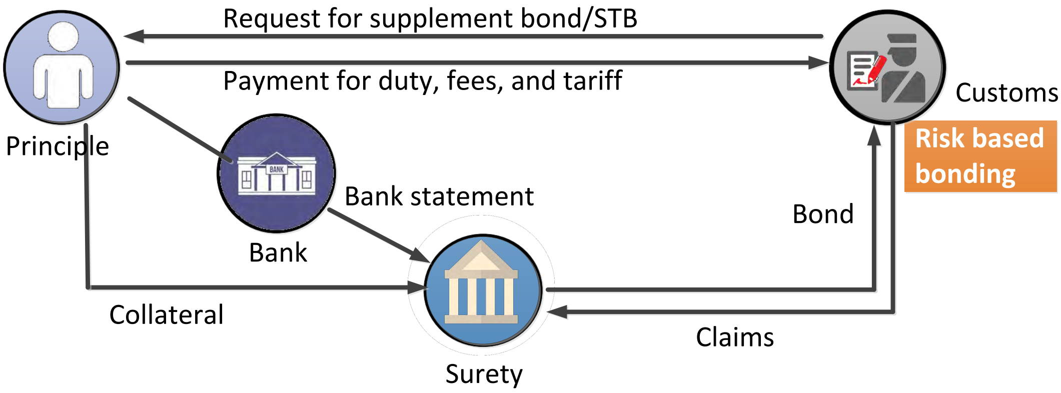


Figure 4.34: Process of Customs bond and duty collection.

Customs allows importers to provide two types of basic importation and entry Customs bonds: a continuous entry bond, and a single transaction bond to secure the duties, taxes, and fees associated with the import of goods. Continuous entry bonds are used to secure financial obligations for one or more entries for a period of up to 365 days. Single transaction bonds are used to secure financial obligations related to a specific entry. If an importer fails to pay the full amount owed on a final duty bill for an AD/CV duty entry, CBP will attempt to collect payment from the surety that underwrites the bond for the entry. The amount CBP may be able to collect from the surety depends on how much the bond covers.

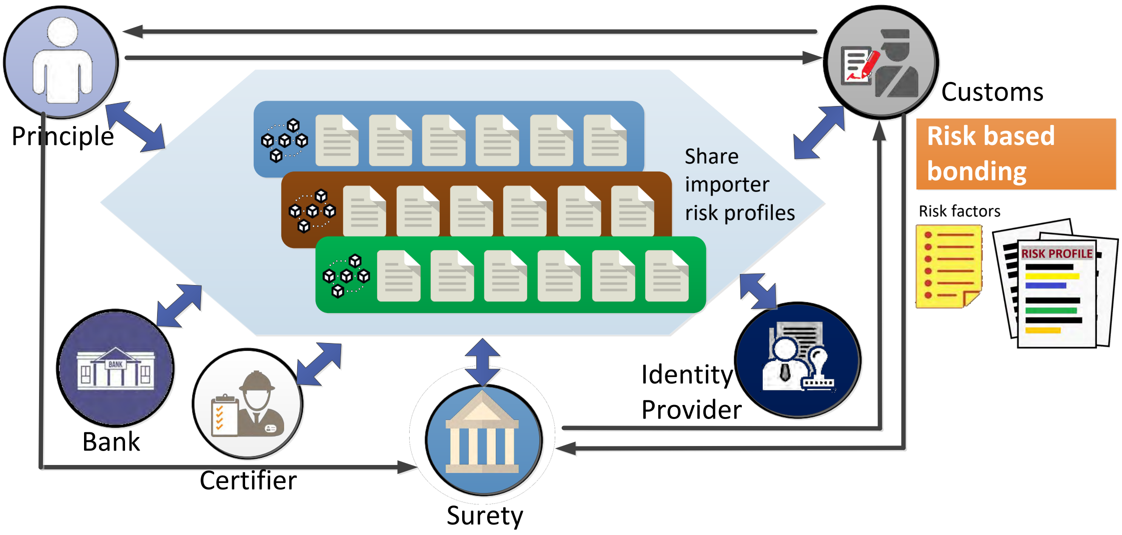


Figure 4.35: Data cooperation between surety providers and Customs bond stakeholders over blockchains.

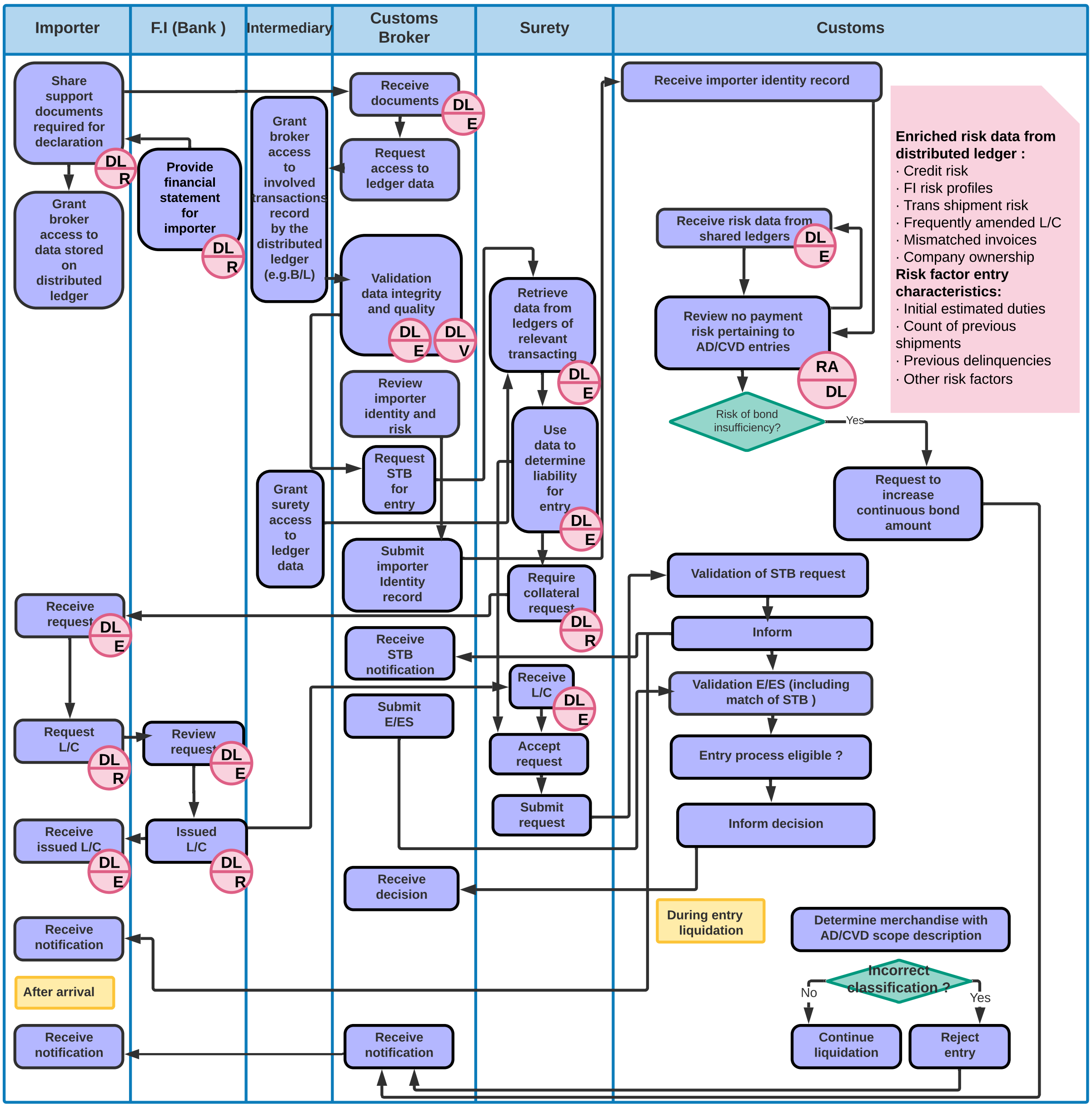

Importer
F.I (Bank)
Intermediary
Customs Broker
Surety
Customs
Share support documents required for declaration
DL R
Grant broker access to data stored on distributed ledger
Provide financial statement for importer
DL R
Grant broker access to involved transactions record by the distributed ledger (e.g.B/L)
Receive documents
DL E
Request access to ledger data
Validation data integrity and quality
DL E
DL V
Review importer identity and risk
Request STB for entry
Submit importer Identity record
Grant surety access to ledger data
Retrieve data from ledgers of relevant transacting
DL E
Use data to determine liability for entry
DL E
Require collateral request
DL R
Receive importer identity record
Receive risk data from shared ledgers
DL E
Review no payment risk pertaining to AD/CVD entries
RA DL
Risk of bond insufficiency?
Yes
Request to increase continuous bond amount
Enriched risk data from distributed ledger :
· Credit risk
· FI risk profiles
· Trans shipment risk
· Frequently amended L/C
· Mismatched invoices
· Company ownership
Risk factor entry characteristics:
· Initial estimated duties
· Count of previous shipments
· Previous delinquencies
· Other risk factors
Receive request
DL E
Receive STB notification
Validation of STB request
Inform
Submit E/ES
Receive L/C
DL E
Validation E/ES (including match of STB)
Request L/C
DL R
Review request
DL E
Accept request
Entry process eligible ?
Submit request
Receive issued L/C
DL E
Issued L/C
DL R
Inform decision
Receive decision
During entry liquidation
Determine merchandise with AD/CVD scope description
Incorrect classification ?
No
Yes
Continue liquidation
Reject entry
Receive notification
After arrival
Receive notification
Receive notification

Figure 4.36: Process for detecting non-payment risk with blockchain based data sharing of financial related risk indicators.

Leveraging data cooperation, distributed ledgers facilitate the use of systematic data analysis techniques to reduce risk of AD/CV duty evasion. Information lodged in distributed ledgers can enrich risk factors for evaluating bond insufficiency risk. Data pooling between the stakeholders allows more effective assessment of risk exposure using an enriched set of red flags and risk factors [33, 44, 45]. Figure 4.35 illustrates the environment.

A process diagram is shown in Figure 4.36. Information collected from the distributed ledgers setup for trade finance and bonds can enhance Customs' risk based bonding capability. It may increase ability to assess ongoing aggregate risk posed by specific importers, and identify entries that need review by officials.

4.6. Analysis of the new process

This section first provides an overall analysis, and then it is followed by detailed analysis of benefits for each re-engineering area.

4.6.1. Overall analysis

Taking advantages of the distributed ledgers as information sharing infrastructure, global supply chain information can be shared under a unified framework for achieving information flow cooperation between financial intermediaries, suppliers, importers, brokers, accredited bodies, government agencies, Customs, regulatory authorities, etc. There are different data cooperation dimensions including G2G (government to government), B2B, B2G, G2B, and A2A (agency to agency). A high level architecture is depicted in Figure 4.37.

B2B (business-to-business) ledgers are often driven by digitalization and data cooperation needs by the global supply chain industry to improve supply chain efficiency, visibility, and transparency. Business process can be automated and integrated with the shared ledgers. There could be multiple ledgers (vertical or horizontal) led by different supply chain sectors such as trade finance, freight forwarding, retail, pharmaceutical supply chain, and manufacture sector. Ledger gateways can be developed to facilitate data pipelines between the industry led ledgers and the regulatory authorities (business to government). For managing authorized economic actors, official licenses, permits, risk profiles, advance ruling, etc., government may interact with the supply chain ledgers as validation sources, or act as claim issuers/digital identity providers (government to business).

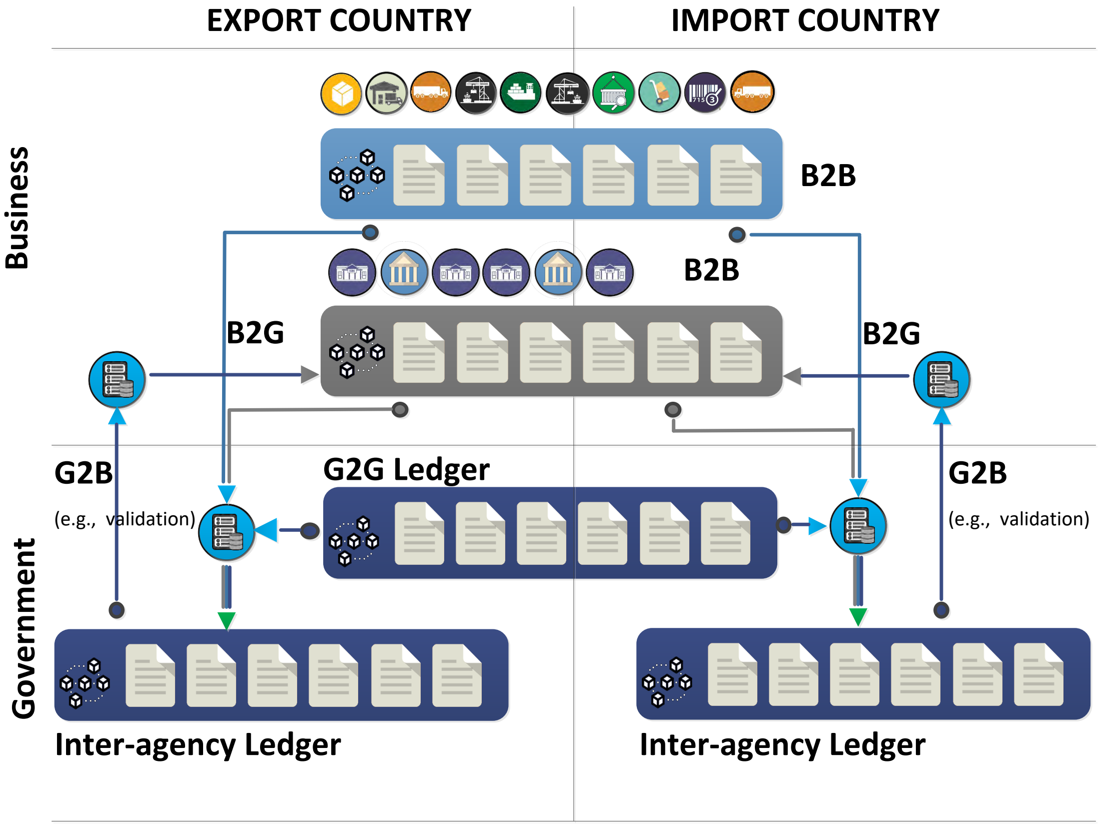


Figure 4.37: Likely environment of multiple ledgers that cover B2B, B2G, G2G, A2A, and G2B.

Cooperation between different government agencies may be realized via shared ledgers by the government agencies such that supply chain related information can be exchanged and disseminated in real-time between the agencies for trade facilitation, advanced targeting, risk management, and etc.

Comparing with the traditional approach, distributed ledger based ICT infrastructure may provide assurance of data quality, higher protection of data integrity, automatic synchronization of data update, and improved transparency. As a result, different government agencies can cooperate more effectively. This approach allows resources to be shared between agencies and may reduce cost for maintaining and managing ICT infrastructure by using a common distributed technical platform.

Distributed ledgers can be setup to facilitate a network of Customs agencies (G2G) for exchanging and validating data such as licenses, permits, certificates or other authorizations.

Distributed ledgers also offer a unique opportunity to achieve information driven data exchange between the global supply chain actors instead of the current process that relies on isolated communication channels for sharing of documents.

It potentially harmonizes different views of supply chain (trade, finance, logistics, and declaration) with data items to be pulled directly from the common ledgers by the involved stakeholders. Such a platform can improve data quality, reduce delay and friction of information flow, prevent tampering of the data along the path of information flow, eliminate manual duplication of data, etc. Consequently, regulatory authorities can be certain that the information received in declaration is consistent with all the other views seen by the supply chain stakeholders, which reduces cost and resources needed to validate declaration and entry data. This potentially would increase the Customs and the regulatory authorities' capability to focus on the high risk cargo and imports.

Figure 4.38 summarizes the infrastructure. MSME can connect to supply chain ledgers via service providers. This removes the need for them to operate computing facility as full node of the ledgers, which reduces adoption cost. Under the new process, ledger gateways can be deployed to integrate supply chain ledgers with the Single Window environment. Data can be pulled out from the ledgers and correlated with the declaration data for purpose of validation and automation.

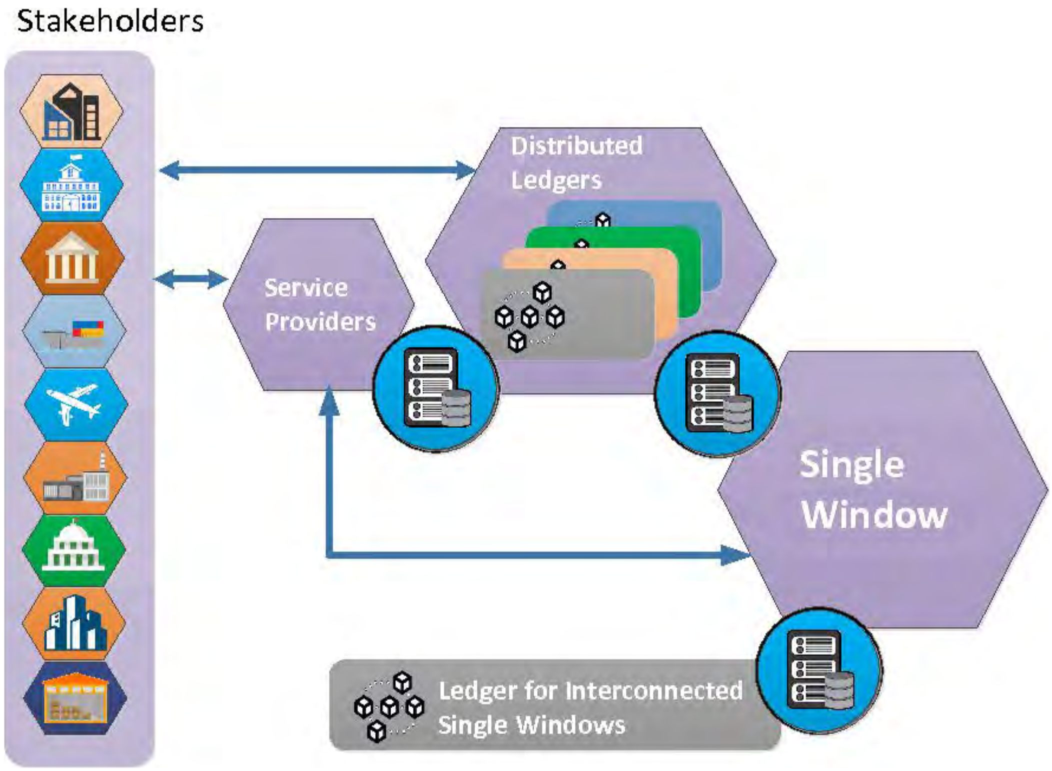


Figure 4.38: Integration of distributed ledgers with the Single Window.

As the new process suggests that distributed ledgers can enable advance supply chain data sharing between the importers and the regulatory authorities at trade/commercial phase, which extends the Customs view of supply chain information in time dimension. Supply chain information can be shared soon after it is created in accordance with progress of the commercial activities and supply chain events. Such advance information sharing may have many advantages. It helps the regulatory authorities early vet legitimate transactions, and allow quicker release of the imported goods and reduce delay at the port of entry. Further, the improved transparency can reduce supply chain risk, improve predictability, and result in increased trust between the involved actors (financial intermediaries, surety providers, insurance companies, and customers) because they can see that the goods are cleared ahead of time.

Distributed ledgers can contribute to the overall big data oriented vision by Customs [24]. Information pulled from the supply chain ledgers can be integrated and combined with other sources of data to assist risk assessment and decisions regarding entry declaration. Figure 4.39 shows distributed ledgers as sources of information to help Customs control, risk management, and tackle high priority trade issues (see Appendix B for a list of high priority trade issues).

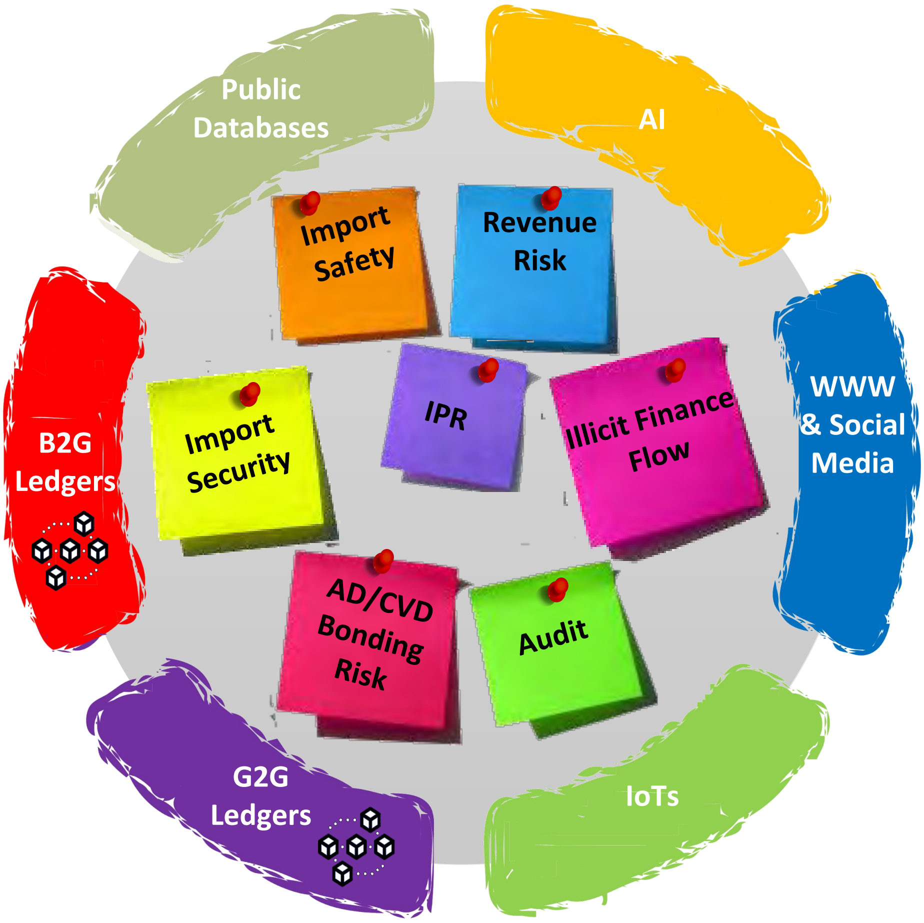


Figure 4.39: Apply blockchains as data sources for improving Customs control.

In addition, distributed ledgers potentially allow multiple supply chain BUY/SHIP/PAY cycles to be chained. Figure 4.40 depicts such scenario, from export to import to production, and to another cycle of export to import. Such ability to trace supply chain transactions can improve trust between the suppliers and buyers/importers. To safeguard privacy and trade secret, verifiable claims can be shared for information that crosses multiple rounds of supply chain cycles. For instance, a manufacturer can make a verifiable claim about all its materials that pass compliance requirements and quality testing, without disclosing to the downstream actors who are the suppliers of the materials. The claim can be validated by the receiving party using data lodged in the supply chain ledger.

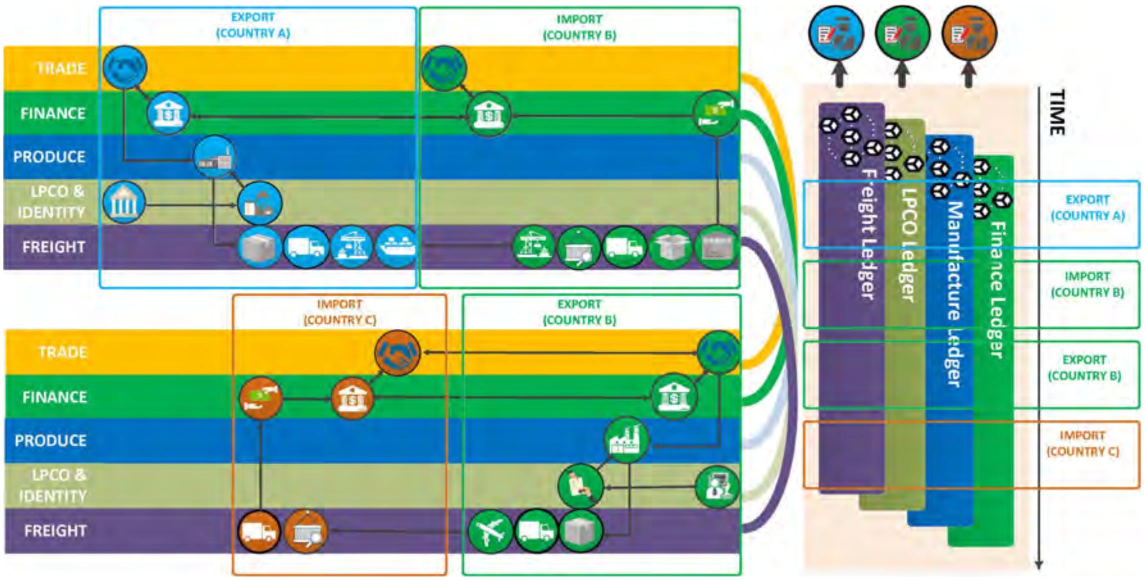


Figure 4.40: Supply chain visibility of multiple cross-border BSP (Buy-Ship-Pay) cycles.

4.6.2. Detailed Analysis

This subsection provides analysis of potential benefits for each business area. It analyzes potential benefits from both the perspective of trade side as well as the regulatory authorities and Customs.

4.6.2.1. Registration/authorization

As discussed in the previous sections, distributed ledgers may enable the possibilities of global scale distributed identity management for traders, supply chain economic actors, manufacturers, and products.

For legal entities such as suppliers, manufacturers, traders, freight-forwarders participating in the global supply chains, globally unique identity can be created. Such service allows any business interactions in the global supply chains and enables any supply-chain partner to dynamically validate the trustworthiness of a legal entity with which it is about to engage in a business interaction. Such vision may be achievable with distributed ledgers as one of the enabling technologies.

Table 4.5: Benefits to the trade and Customs due to the new process.

	Trade	Customs	Gains derived from
Faster Processing	✓	✓	Sharing data early, and improved risk-based targeting.
Enhanced data reliability and quality	✓	✓	Elimination of data duplication and built-in cross validation of data accuracy by the stakeholders during data creation.
Improved revenue collection		✓	Automated payment collection (self-execution of chain code), richer financial data (detecting mis-invoicing, trade-based money laundering, AD/CVD non-payment risk, and etc.).
More effective use of governmental resources		✓	Due to improved data reliability, quality, and timeliness.
Improved timeliness of communication	✓	✓	Applying blockchain for messaging and ordered transactions (e.g., producing a globally ordered records of actions - everybody sees events in the same order).
More effective inter-agency data management		✓	Blockchain-based data sharing and messaging support.
Effective cost sharing	✓	✓	Consortium-based development model and jointly maintained ICT infrastructure.

Distributed ledgers, as an approach to implement automatically synchronized and tamper proof distributed databases that are managed by independent supply chain organizations or regulatory entities, can potentially solve some of the long standing identity and registration related issues that the global supply chain is facing.

Although the vision to have a single global network that allows entities engaging in the global supply chain to look up, identify, and verify basic information of the economic actors, manufactures, physical locations, products, or shipments, all based on globally unique identifiers is not new. There has been a lack of enabling technology and infrastructure to deliver such vision.

Distributed ledgers may offer the kind of infrastructure to support such vision, for instance, GEPIR (Global Electronic Party Information Registry) as an example. GEPIR is internet-based service that gives access to basic contact information for companies that are members of GS1. GEPIR comprises a network of local GS1 servers, see Appendix B for a diagram of the GEPIR architecture. The network may benefit from the distributed ledger technology to enhance its service and solves some of the data quality and completeness that the end users seem to face.

Another example is Manufacturer ID or MID, designed to identify foreign suppliers. The existing MID scheme, due to its nature of two-sided trade data, is likely susceptible to issues related to the uniqueness and consistency of the foreign supplier identification data.

The problem is summarized in a study report [64] that cross checks foreign supplier data from different databases. Using the World Bank's public-use Exporter Dynamics Database (EDD) that contains destination specific information on exporting firms from 43 countries. The authors of the report identify 91,841 exporters from the EDD vs. 114,888 firms compared to the result using the U.S. import data. Further study shows varying degree of correlation of the data under different HTS categories. Having globally unique identifiers for authorized economic actors, manufacturers, and products can provide many benefits to the global supply chain such as trade facilitation, risk management, Customs control, and etc.

Based on more accurate information of identities of economic actors, manufacturers, and imported products, regulatory authorities can increase targeting efficiency with the existing resources by focusing on high risk entries. For instance, product examinations could be reduced significantly by issuing unique product codes, which may save mid-size importers a significant amount of money annually.

Table 4.8 compares properties of different identity management schemes.

Distributed ledgers could enable the governments and the business entities to have one self-managed digital identity throughout global supply chains for the authorized economic actors, manufacturers, and products [57, 68, 76]:

- Self-managed: Each government and business can fully manage its own identity in-

Table 4.6: Comparison of different identity management approaches.

	Centralized	Federated	Decentralized
Definition	A single organization establishes and manages a point to point trust relationship with each economic actor and adds tailored credentials.	Multiple standalone systems, each with their own trust anchor, establish domain to domain trust. Credentials are standardized within the domain.	Economic actors manage their own digital identities. Multiple identity providers contribute to economic actor's credentials.
Identity providers	Authorities, standard bodies, certified identity providers, trade associations, private entities.	Authorities, standard bodies, certified identity providers, trade associations, private entities.	Authorities, standard bodies, certified identity providers, trade associations, private entities.
Number of individual identities	New digital identity required for each identity provider. Multiple credentials created by each identity provider.	New digital identity for each domain. Credentials recognized within each domain.	Globally recognized identity for each economic actor. Decentralized verifiable credentials.
Direct interaction in peer to peer business transactions	Reliance on centralized intermediary to verify identity.	Reliance on centralized intermediary to verify identity.	Identity can be verified in P2P fashion without intermediary.
Managing and controlling identity	Economic actors have low control of their identities (controlled by the identity providers).	Economic actors have low control of their identities (controlled by the identity providers).	Facilitate self-management of digital credentials by the economic actors.

formation. This may facilitate micro, small and medium-sized enterprises, to more effectively participate in the international trade and enhance their competitiveness.

- Market participant neutral: It is neutral to supply chain market participants and doesn't give a competitive advantage to any one organization.
- Registered once, globally verifiable: It avoids duplicated registration. After registered, any government and business should be able to verify information of the economic actor, and imported product.
- Support for multiple jurisdictions: The digital identifiers can be recognized by multiple jurisdictions. Each jurisdiction may decide to acceptance level of the identities recorded by the distributed ledgers.
- Cost-effective for MSME: The service may be cost effective for MSME than some of the existing processes that often require high cost registration fees.
- No vendor lock-in: Leveraging standard based approach, it may avoid lock-in to any specific vendor's solution of identity management.

4.6.2.2. Process for managing accreditation, certification and others

As reported by the U.S. General Accountability Office (GAO), domestic high-risk supply chain facilities receive inspections once every three years and medium-risk facilities only once every five years. While the law does not impose an inspection frequency for foreign manufacturers, those that are high-risk are reportedly inspected only once every six years and medium-risk only once every 27 years. Testing and certification by the third-party programs can enable more frequent inspections and potentially improve import safety.

With the new process, third party programs may be facilitated with distributed ledgers. Through a holistic product life-cycle data management, the community of producers, laboratories, accredited bodies, regulators, and consumers could work together to create a cooperative distributed ledger based environment, for sharing data provenance, testing outcome, certification, licensing, and others with the relevant actors.

Decisions of advance ruling can be lodged to the distributed ledgers, which can be applied for process automation.

According to a study by OECD, measures to streamline procedures and advance rulings are identified as the greatest contributors, in achieving the most significant reductions in trade costs, with the former reducing trade costs by 5.4% and the latter by 3.7% [27].

Advance rulings enhance certainty and predictability of cross-border trade transactions [40]. Disputes at the actual moment of release or clearance with the Customs authority on tariff classifications, origin, i.e. eligibility to preferential treatment, are reduced and consequently delays can be avoided. Sales and purchase contracts can be concluded based on the information of the advance ruling. There are many benefits applying distributed ledgers for such purposes.

- Certificates, accreditation, and claims, once appropriately issued, digitally signed by a valid regulatory/issuing agency/accredited body, and lodged to the ledgers, the content could not be tampered and altered, which prevents fraud and misuse of the information.

- Cost to manage the process and lodged information may be reduced.

- Possibility to harmonize standards and assessments procedures such that third-party tests would be able to satisfy the regulatory requirements of multiple jurisdictions in which a manufacturer operates or sells products, where the results can be made available in the involved distributed ledgers.

- Once lodged in the ledgers, claims about product quality, compliance status, product related claims can be made available to the relevant supply chain actors and the consumers under a unified access interface (instead of connecting with various organizations and parties with diverse application interfaces).

The regulatory authorities can verify claims of compliance against the secure and tamper resistant information kept by the ledgers.

4.6.2.3. Supply chain data collection and exchange

Distributed ledgers facilitate cooperation of efficient information flow between the supply chain actors. The technology can help overcome some of the data quality, delay, and information visibility related challenges. Data sharing through “permissioned” or private ledgers in a secure and cooperative manner between the supply chain actors can lead to end-to-end “data pipelines” to deliver accurate supply chain information that can be shared between the involved actors in real-time.

With unification of different views (trade, finance, logistics, and declaration), the Customs and partner government agencies can pull accurate supply chain data, right from the source after it is lodged to the ledgers.

This potentially improves the efficiency of Customs and the partner agencies for conducing risk assessment, making decisions (e.g., clearance, release, screen, admissibility, need of further review by official). Information obtained from the importer declarations and other sources can be cross validated with the transactions lodged in the distributed ledgers.

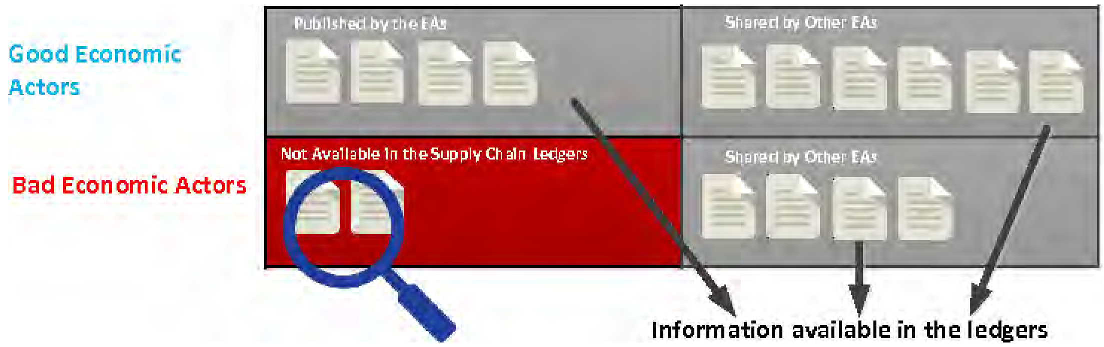


Figure 4.41: Improving target efficiency with entry data validated by the blockchains.

In a cooperative environment where legitimate actors lodge supply chain information and related transactions using distributed ledgers, entry data from bad actors, for instance, these attempt to circumvent Customs control, violate trade law, evade detection of importing non-admissible goods, will be more likely to be scrutinized. This increases Customs capability to target high risk entries.

The capability to have the transactions validated, audited and endorsed by the involved supply chain stakeholders before they are accepted and added to the distributed ledgers, can simplify regulatory authorities' job with respect to risk management. The benefits are illustrated in Figure 4.42. Leveraging supply chain distributed ledgers as data sources, Customs and regulatory authorities can

- More effectively validate data received from the importers.
- Improve visibility and transparency of supply chains.
- Increase accuracy of risk based targeting.
- More efficient use of Customs' resources to and focus on high risk cargo.
- Reduce release time and waiting time at the port of entry.

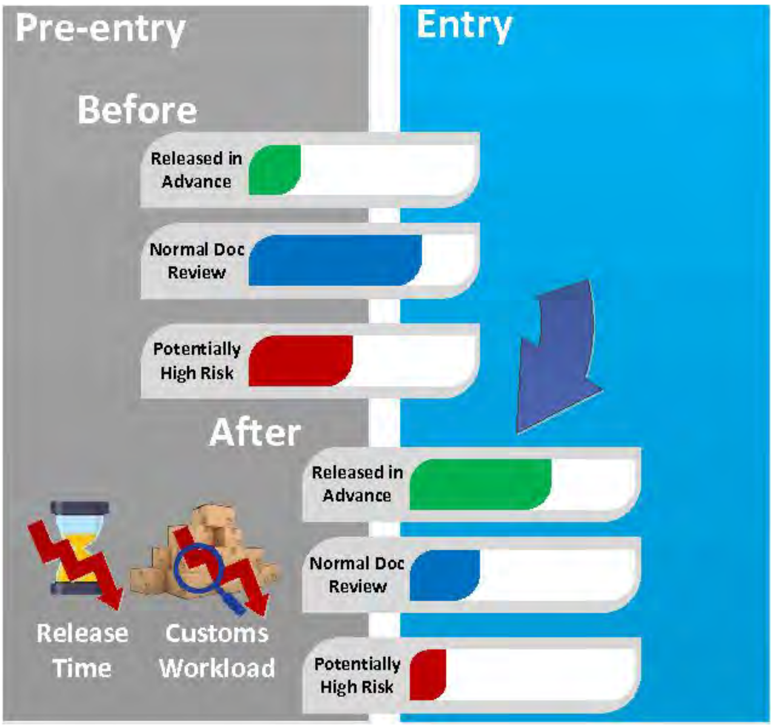


Figure 4.42: Trade facilitation due to improved data sharing and cooperation.

4.6.2.4. Advance commercial data sharing

There are many benefits for importers and suppliers to adopt distributed ledgers as the approach for managing procurement electronically, trade negotiation, purchasing and invoicing processes. Applying a common ledger to collect all the required information from sourcing, contracting, ordering, preparing and shipping the products, can improve trust between the importers and the suppliers, reduce potential disputes regarding sales agreements and invoices. According to statistics, at any given moment, there are about $100M invoices with disputes in the global supply chain. Most these disputes can be avoided and resolved with shared ledger for managing trade.

Extending the Customs and regulatory authorities' visibility to the trade phase and beyond, may contribute positively to both trade facilitation and risk management by the Customs and the partner government agencies. If the information is already lodged to a common supply chain ledger shared between the importers and the suppliers, making the data available to the Customs would be easy. The extra benefits sharing advance trade information during the trade phase include:

- Decreased perception of risk by regulatory authorities as advance sharing of trade data shows evidence of reasonable care, compliance (e.g., sourcing of suppliers meeting the regulatory requirements and standards), and internal control.
- Potential expedition of clearance and release process as result of sharing data early.

- Faster processing and validation of entry information because the information can be matched with the information lodged in the ledger and traced back to the beginning of the transactions as illustrated in Figure 4.43.
- Reduced perception of risk by the supply chain partners such as finance institutions who provide trade finance, insurance companies, surety, and downstream customers.

With advance lodging and sharing of information in a common ledger that can ensure data quality, it may allow for a release with little or no delay upon arrival. During this process, trust between the trade community and the regulatory authorities to safeguard privacy and confidentiality of the information, and a friendly policy environment to encourage advance data sharing may be critical for such a process to succeed. Therefore, it is important to establish a positive atmosphere of mutual access and respect between the Customs and the traders.

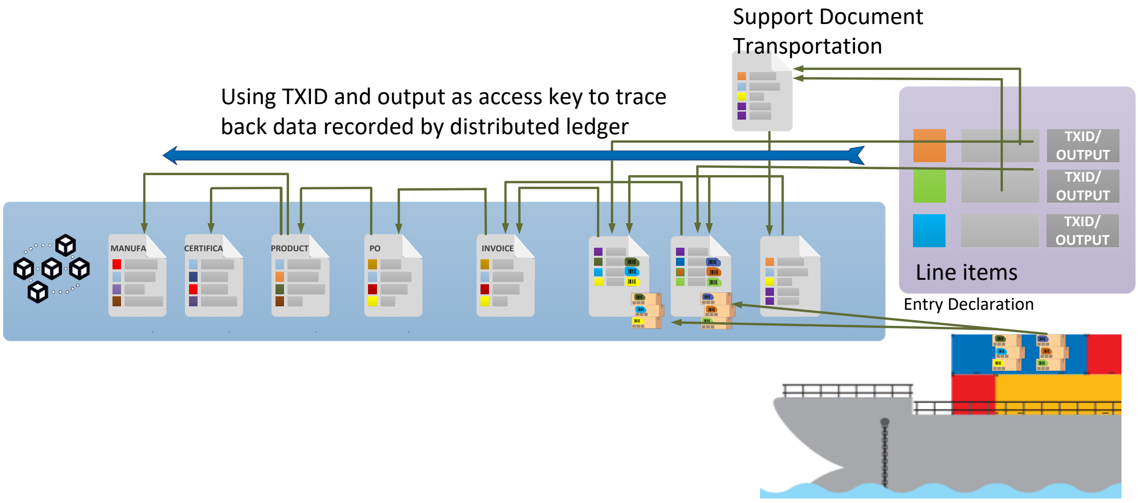
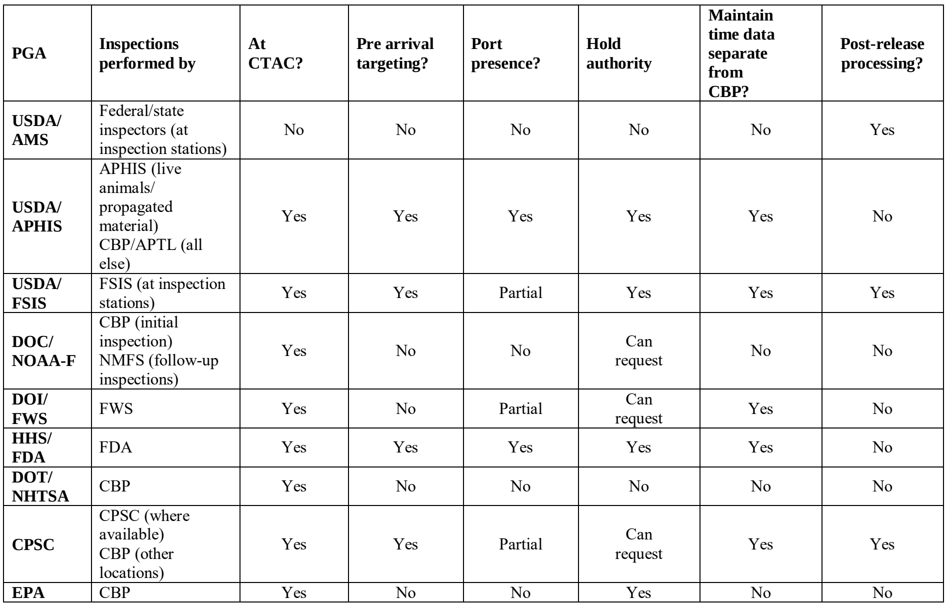


Figure 4.43: Blockchain enables traceability of transactions so that data items can be correlated based on access keys to the blockchain transactions. Each transaction has a unique transaction ID. Transactions are linked through inputs and outputs.

Such advance data sharing may potentially bring benefits to the trade involving partner government agencies due to increased transparency, data quality, and supply chain visibility. Figure 4.44 lists partnering agencies and their authorities regarding release of imported goods.

4.6.2.5. Automated declaration process

Each year, Customs processes approximately 32 million import entries, while collecting more than $44 billion in duties, taxes, and other fees. Creation of Customs declaration documents is a very complex task, involving multifarious activities. There are challenges in collating (often achieved manually) correct information from various documents and



PGA	Inspections performed by	At CTAC?	Pre arrival targeting?	Port presence?	Hold authority	Maintain time data separate from CBP?	Post-release processing?
USDA/ AMS	Federal/state inspectors (at inspection stations)	No	No	No	No	No	Yes
USDA/ APHIS	APHIS (live animals/ propagated material) CBP/APTL (all else)	Yes	Yes	Yes	Yes	Yes	No
USDA/ FSIS	FSIS (at inspection stations)	Yes	Yes	Partial	Yes	Yes	Yes
DOC/ NOAA-F	CBP (initial inspection) NMFS (follow-up inspections)	Yes	No	No	Can request	No	No
DOI/ FWS	FWS	Yes	No	Partial	Can request	Yes	No
HHS/ FDA	FDA	Yes	Yes	Yes	Yes	Yes	No
DOT/ NHTSA	CBP	Yes	No	No	No	No	No
CPSC	CPSC (where available) CBP (other locations)	Yes	Yes	Partial	Can request	Yes	Yes
EPA	CBP	Yes	No	No	Yes	No	No

Figure 4.44: Partnering agencies with hold authorities. (Source: CBP)

Table 4.7: Benefits to trade and partnering agencies due to the new process.

	Trade	PGAs
Faster process of admissible goods by the PGAs	✓	✓
Reduced uncertainty	✓	
Efficient use of resources		✓
Improved data cooperation	✓	✓
Improved risk assessment using advance commercial information, third party certification program, and procurement data		✓

Table 4.8: Automation of preparation for entry filing leveraging blockchains.

	Access to Cross-Border Supply Chain Blockchain Data to Assist Entry Filing	Fully Automated Entry Filing Process
Copy of data	Avoided to some degree	Avoided
Data consistency and quality	Guaranteed	Guaranteed
Manual mistakes	Avoided partially	Eliminated (most if not all of them)
Automation	Somewhat automated	Automatically created, automatically synchronized
Declaration preparation cost	Reduced	Minimal preparation cost due to automation
Data validation cost	Reduced	Reduced

various stakeholders, such as sales data, product information, manufacturing details, as well as logistics information. Because of outsourced services and distributed data sources, this process is cumbersome and runs with a potential risk of non-compliance. In many cases, traders involve third party providers to handle the Customs declaration process.

There are several challenges in receiving accurate data on time for preparing declaration. There could be issues with data quality; data not being submitted on time; and potential inadvertent or deliberate mistakes in data due to its changing multiple hands. Additionally, delays generated due to filer errors (e.g., for late or incomplete support documents) also contribute to delay in clearance and release of goods [30].

With necessary information lodged in the ledgers, it provides benefits on the trader and broker side because workload to accurately assemble the required information for declaration, can be reduced. The process could be completely automated as the new process shows. On the Customs side, with access to the ledgers, it reduces manual verification and resources required to validate the declarations. This would result in better data quality, faster Customs declaration processing, and reduced end to end lead time.

4.6.2.6. Post-release compliance verification

Distributed ledgers may help post release compliance verification, detection of red flags for detecting evasion of AD/CVD, mis-invoicing, bond insufficiency, improvement of audit decisions, etc.

Under the new process, distributed ledgers will be used to promote transparency of supply chain information, sharing of risk profiles related to illicit financial flows, and data cooperation environment between trade finance, insurance, surety, and the Customs. This would potentially help address issues of mis-invoicing, illicit financial flows, mis-declaration, rev-

Table 4.9: Estimated total values of mis-invoices for U.S. imports.

	Total import	Amount over priced	Amount under priced
2012	$1,906B	$221B	$284B
2013	$1,884B	$217B	$306B
2014	$1,939B	$216B	$321B
2015	$1,812B	$216B	$333B
2016	$1,747B	$215B	$332B

enue risks, and etc.

Global money laundering transactions are estimated to account for 2-5% of Global GDP. Only <1% of global illicit financial flows are currently seized by the authorities. Global Financial Integrity (GFI) has suggested that perhaps more than 80% of illicit financial flows (IFFs) are accompanied through trade mis-invoicing. One study results of under and over invoice are listed in Table 4.9.

Table 4.9 summarizes the aggregate gross overpriced export amount and underpriced export amount for the 5-year period (imported goods by the U.S). The total import amount includes only records with quantity defined. Non-quantified records are excluded from the mispricing estimation.

Another risk area is collecting payments for AD/CVD duties. In FY 2017, there were imports of approximately $2.39 trillion in goods into the U.S., and receipts of approximately $34.6B in duties. Of the $2.39 trillion in goods imported in FY 2017, approximately $13.3 billion (0.55 percent) were subject to an AD/CVD order [4]. There are many challenges to calculate and collect AD/CVD duties. Importers may intentionally misclassify imported goods to evade duties, perform transshipment to conceal country of origins, under-value the imported goods, mis-describe the goods, and etc.

Many of these issues share similar patterns, for instance, mis-invoicing, or red flags regarding detection [28]. With data cooperation environment enabled by the distributed ledgers, risk factors and profiles could be shared between the trade side and the Customs, such as detection of illicit financial flows, evasion of AD/CVD duties, and prevention of nonpayment risks could be more effectively addressed.

There are incentives for the supply chain and trade finance community to adopt distributed ledgers for benefits. Recent pilot studies suggests potential advantages of distributed ledgers including, significantly decreased delay applying trade finance credits, reduced errors in trade finance or insurance applications, improved automation, etc. For instance, industry estimates, 4 out 5 L/C documents first version contain inaccuracies, errors, and discrepancies. As high as 70% of L/C documents are rejected on the first presentation, which increases cost and effort to L/C amendments. With distributed ledger support, the time could be reduced from 7-10 days to 2.5 hours (BBVA blockchain pilot study). It helps all the stakeholders discover mistakes, errors and discrepancies early and reduce L/C amendment cost.

In addition, there are significant benefits to integrate trade finance and physical supply chains, and correlate financial flow with the movement of the goods. The traditional approach lacks transparency and visibility to the physical supply chains, which increases transaction costs in terms of administration and monitoring. With integration of trade finance with the physical movement of the goods under distributed ledgers, risk information can be shared in real-time, which reduces trade finance cost. The concept is illustrated in Figure 4.45 depicting the elements that a bank uses to determine the fee based on the expected risk profile of the physical supply chains. The solid line shows that a more competitive fee can be charged if the bank has more information available to adjust its risk profile as the physical supply chain evolves. Similar benefits in cost could be obtained if the regulatory agencies share risk data with the financial intermediaries.

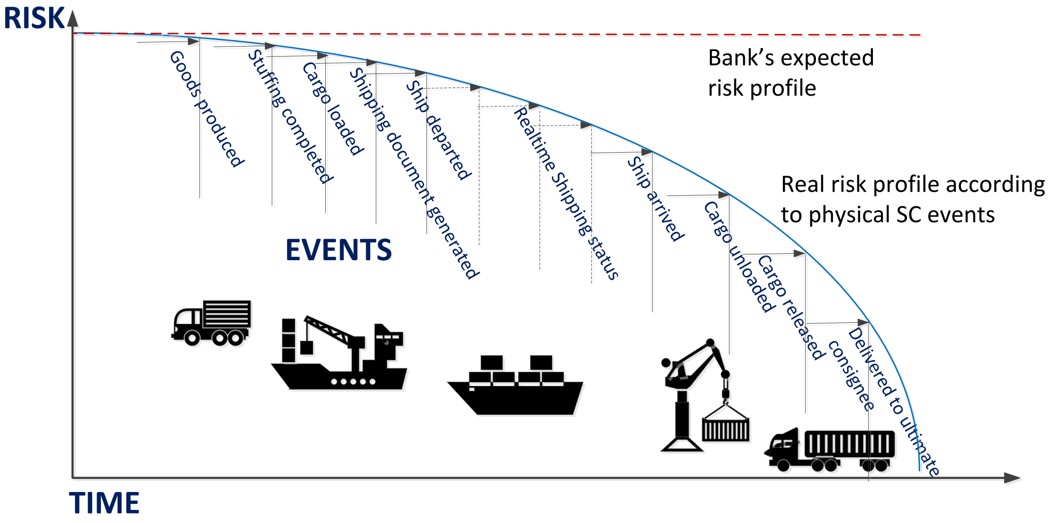

RISK
Bank's expected risk profile
Goods produced
Stuffing completed
Cargo loaded
Shipping document generated
Ship departed
Realtime Shipping status
Ship arrived
Cargo unloaded
Cargo released
Delivered to ultimate consignee
Real risk profile according to physical SC events
EVENTS
TIME

Figure 4.45: Connection between trade finance and physical supply chain to reduce cost and improve risk assessment of import activities with real-time information.

Detection of mis-invoicing and illicit flows In general, trade based illicit finance flows may involve [52, 74]:

- Over or under invoicing: Misrepresenting the price of the goods.
- Multiple invoicing: Invoicing one shipment several times.
- Short or over shipping: Shipping more or less goods than invoiced.
- Obfuscation: Shipping something other than what is invoiced.

- Phantom shipping: Shipping nothing at all with false invoices.

Distributed ledgers may easily detect frauds involving multiple invoicing, for instance fraudulent duplicate discounting of receivables. In a some real case, companies were alleged to have used warehouse receipts for the same metals stockpiles several times to commit hundreds of millions of dollars of fraud. A proof of concept run by banks in Singapore demonstrated that distributed ledger technology was able to mitigate the multiple invoicing fraud problem. For the technology to be effective, more financial institutions need to join the common ledger and collaborate on fraud detection.

In trade mis-invoicing [38], either the importer and exporter or both may manipulate the value (e.g. price, quantity, or quality) of trading goods in their Customs declarations. The motives governing such trade mis-invoicing range from evading tariff or tax, avoiding trade regulations, exploiting trade incentives, or disguising capital flight (see Table 4.10 for different mis-invoicing cases). When an attempt is made at disguising IFFs via a trade transaction, financial records reported to relevant financial institutions (the amount actually paid/received) may not correspond with the true or correct value of the goods, but rather with the manipulated invoices.

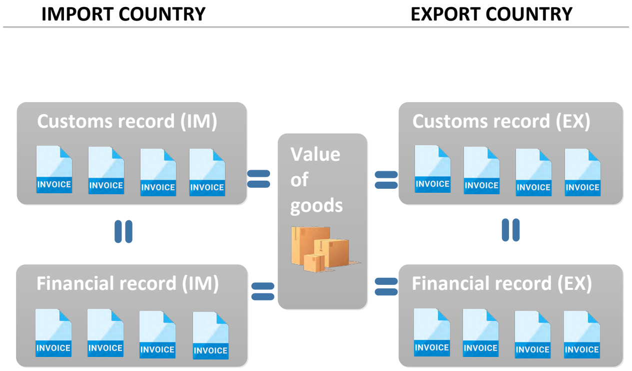


Figure 4.46: A simple diagram that illustrates mis-invoicing.

Table 4.10 summarizes different cases of mis-invoicing.

With data cooperation with trade finance and logistics for sharing risk profiles and transaction anomaly information, most of the mis-invoicing scenarios could be potentially detected. Figure 4.46 shows data flow paths enabled by distributed ledgers to detect mis-invoicing.

Table 4.10: Different scenarios of illicit financial flows and mis-invoiving (according to the WCO).

	Explanation	Illicit motives	Collusion
A	Importer submitted under-valued invoice in the import declaration	Tariff and tax evasion: The importer exploited tax exemption scheme for low value goods.	Exporter issued false invoices for the importers.
B	Importer submitted over valued invoice in the import declaration	Importer evaded domestic financial controls.	Importer and financial intermediary.
C	Over invoicing export.	Exporter made a fake export declaration without actual export of goods.	Tax evasion.
D	Over invoicing export. Exporter submitted over valued invoice in the export declaration.	Exporter enjoyed unauthorized receipt of duty drawback of export goods, and brought back illicit proceeds into the own country.	Exporter and financial intermediary.
E	Over invoicing import and export. Importer and exporter in collusion submitted over-valued invoice respectively in import and export declarations.	Tariff evasion. Importer evaded the price differential duty, which is imposed to protect domestic industry.	Both involved bogus companies to use fabricated invoices.
F	Importer and exporter in collusion submitted over valued invoices respectively in import and export declarations.	Importer evaded domestic financial controls.	Exporter is a subsidiary shell company of the importer.

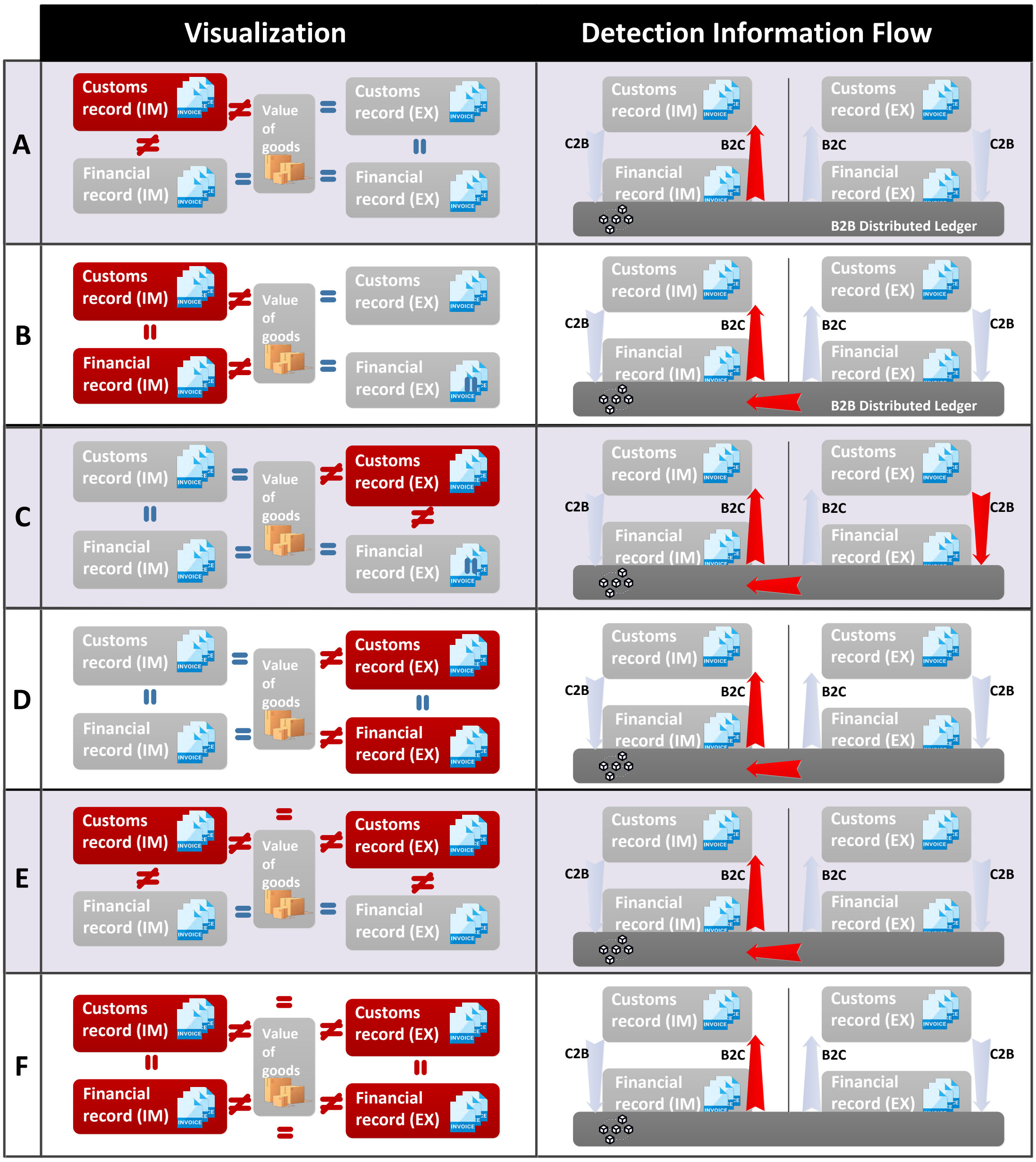


Figure 4.47: Mis-invoicing risk sharing over blockchains and how it could be applied to detect different mis-invoicing scenarios.

Table 4.11 summarizes the benefits from both trade finance and compliance perspectives.

Risk assessment of AD/CVD duties The Customs have the responsibility to administer AD/CVD entries, collect AD/CVD duties, and enforce AD/CVD orders [6, 15, 37]. There are many challenges to collect AD/CVD duties. Importers may evade AD/CVD duties through incorrectly filed entries, mis-declaration, mis-classification of the goods, transshipping [69], and etc. In addition, it may take several years to determine the final amount of AD/CVD due. Importers may be unwilling or unable to pay the actual duties, and some are no longer

Table 4.11: Benefits of the new process on financial data sharing and cooperation (B2B, B2G, and G2B).

	Before	After
	Compliance	
Data pooling and sharing	Lack of sufficient collaboration among stakeholders including financial intermediaries, authorities, freight forwarders).	Improving data pooling and exchange of risk profiles between the stakeholders.
Manual checking	Manual detection of anomalies an red flags.	Automating anomaly detection and reducing manual based inspection.
Lack of SC visibility	In non-document trade, only payment transactions visible to the financial intermediary, not enough physical supply chain information.	Improving visibility to and access to physical movement of the goods.
Timely information	Anomaly often detected after trade and import.	Assessing risk early.
High false positive rate	Lack of quality information and data sharing environment resulted in high false positive rate.	Reducing false positive due to data sharing, access to the physical supply chain, movement of goods, and exchange of risk profiles.
	Finance	
Delay	Time delay for approving credits.	Reducing delay (according to pilot study).
Human mistakes	High error rate in the submitted documents to financial intermediaries.	Reducing or eliminating errors due to manual duplication of data.
Risk assessment	Risk assessment not considering events in the physical supply chain.	Timely risk assessment due to better information of the physical supply chain.

Table 4.12: Benefits of the new process to the stakeholders in Customs bonds.

Surety	Customer	Broker	Customs
Improving assessment of risks; reducing risk exposure; improving cooperation with stakeholders (e.g., financial intermediaries).	Reducing supply chain risk; reducing risk exposure; reducing manual check and verification of the suppliers.	Reducing cost for risk verification; reducing risk exposure.	Increasing capability to determine risk liability Increasing dataset of risk factors (data cooperation of risk profiles with the stakeholders); improving non payment risk assessment; improving detection of AD/CVD evasion due to sharing of risk profiles.

in business when the Customs issues a bill, leading to uncollected AD/CVD duties. Some importers, often in the form of shell companies or foreign nonresident importers, never intend to pay the final duties, and may simply disappear as soon as there is any indication that the final duties may increase. All of them add challenges to collect AD/CVD duties.

Data cooperation between financial intermediaries, surety, brokers, and freight forwarders, by applying distributed ledgers as demonstrated in the new process may potentially tackle some of these challenges.

A transparent environment for sharing risk profiles, validation by stakeholders of financial status and statements, and consistency between the transactions viewed by the financial intermediaries, carriers, freight-forwarders, surety providers may be able to detect AD/CVD evasion risks and anomalies. Information pulled from the distributed ledgers may be used to validate accuracy of risk factor related data collected from the declaration process, and potentially add new dataset to the risk factors. This would increase Customs capability to conduct risk based assessment of AD/CVD evasion, and bond sufficiency. The process can be automated. When the assessed risk reaches certain level or criteria, it may trigger official review to determine if there is a need to take actions, for instance entry liquidation suspense, rejection of the entry, request of additional bond coverage, and audit.

Table 4.12 lists benefits to each involved stakeholders.

5

Technology Capability Studies

This chapter focuses on technology feasibility evaluations. It covers several sub topics including, support for inter-ledger operations, standardization, data collection from multiple supply chain ledgers, consensus finality related issues, assurance of supply chain data privacy and confidentiality lodged in common supply chain ledgers, scalability and performance of blockchains, etc.

5.1. Inter-ledger interoperability and standardization

Today, there exist many different blockchain and distributed ledger projects, often led through a consortium or trade organization focusing on developing supply chain ecosystems by leveraging the distributed ledger technologies. A distributed ledger platform may focus on a particular industry sector, for instance, freight forwarding, trade finance, payment, pharmaceutical supply chain, ocean shipping, smart manufacture, Industry 4.0, or attempt to provide end-to-end supply chain management with the capability to support tracking and traceability. With alliance of the private sector stakeholders, a distributed ledger project may be setup to address a specific regulatory requirement or concerns from the consumers, such as food safety. In the future, it is likely that more blockchain and distributed ledger related projects will be created targeting different use cases of the global supply chains.

It is possible that for a single import transaction, from the beginning to the end, it may involve data exchange and interaction with multiple ledgers or blockchains. For instance, the importer and the exporter may use a trade finance ledger with banks as it members for financial transactions. They may exchange and verify licenses, and product quality certificates using another distributed ledger. When products are manufactured, data collected from the IoT sensors could be lodged and processed with support of a third ledger system. Furthermore, product traceability could be provided by a separate ledger, for instance, with involvement of the retail industry. Insurance companies may choose to use their own permissioned or private ledger for data exchange. In addition, when goods are shipped, freight forwarders and carriers may operate their own common ledger for managing shipping related data and documents. It is likely air cargo and ocean shipping may as well have different ledgers. It is not difficult to imagine that some of these systems could even adopt a hybrid infrastructure, with varying degree, where private ledgers interact with the public ledgers.

In addition, each ledger system may attempt to create an ecosystem around its users, and integrate supply chain actors along the value chain either horizontally, or vertically, or both. In such environment, there will be increasing needs for verification of information obtained from different ledgers, exchange of data between different ledgers (private, permissioned, as well as public), and possibly implementation of transactions across multiple ledgers.

There are opportunities as well as significant challenges to support inter-ledger operations in a multi-ledger environment. For end-to-end supply chain transactions, information flow may well span multiple distributed ledgers with different governance mechanisms, which likely creates challenges for inter-operability. There are questions such as:

- How supply chain actors and distributed ledger consortia who design, develop, maintain, and participate in multiple ecosystems can adopt a strategy to avoid expensive cost in terms of integration?
- How information flow should be managed in such environment of multiple ledgers so that promised benefits of blockchains including traceability, transparency, auditability, informed compliance, can be still achieved?

The quest for interoperability across multiple distributed ledgers, is not unique to the case of global supply chain blockchains or ledgers. For public blockchains, there has been plenty research and efforts aimed to enable across chain operations. One well known example of across chain transactions is atomic swap – swap of assets maintained by two public ledgers. This could be implemented using hashed timelock transactions.

In such scenario, recipients of a transaction have to acknowledge payment by generating a cryptographic proof within a certain timeframe. Otherwise, the transaction does not take place. For example, consider the case that Alice wants to send an asset to Bob using hashed timelock transactions, in gratitude for taking money from Bob. Alice first generates random secret data s, called a secret, and produces hashlock h = H(s), where H is a cryptographic hash function. Next, Alice publishes the transaction to the ledger with hashlock h. After that, if Alice takes money form Bob, Alice reveals the secret s to Bob. When Bob sends the secret s to the distributed ledger, the ledger irrevocably transfers Alice's asset to Bob. Alice also sets timelock t so that her escrowed asset can be returned if Bob does not give money to Alice within the time. More complex operations across more than two public blockchains could be supported as well based on the similar concept. With advance of research, it is plausible to enable general purpose tasks, beyond simple swap, and complex across ledger transactions for both public chains and private chains.

To verify a transaction, input data of a transaction may come from the same ledger, for instance, data stored in the previous transactions recorded by the ledger, or come from external sources. The external sources include, other distributed ledgers (e.g., public, alliance, permissioned, private), public databases, physical supply chain events, the Internet, or company's internal databases such as ERP system. The data can be stored off-chain. The data itself can be kept in the clouds (e.g., cloud based databases), distributed file systems, or peer to peer storage network such as the Inter Planetary File System (IPFS) [18], which is an open, content addressable memory that uses standard Internet protocols, or any other systems that allow shared access to the supply chain stakeholders who are involved in a transaction.

Furthermore, private data can be applied as input to a transaction. It is plausible for a distributed ledger to validate and audit a transaction created with private input without revealing the private data itself to the validators.

With references to off-chain or cross chain or private data, it is possible for distributed ledger validators to know that some data exists, but to have their access to the data restricted depending on the data sharing policies. Appendix C compares types of the data vs. on-chain/off-chain storage.

It is easy for a full node of a distributed ledger to verify validity of a transaction based on the inputs from the same ledger. This is because each full node has a complete copy of the ledger. In case, a supply chain transaction includes information from multiple ledgers, it may not be always feasible for the supply chain actor who wants to verify legitimacy of the transaction, to have full node access to all the involved ledgers. Moreover, these ledgers may use diverse designs, and have different governance policies. For instance, some may be private ledgers, or permissioned ledgers open with restricted accesses only to certain users.

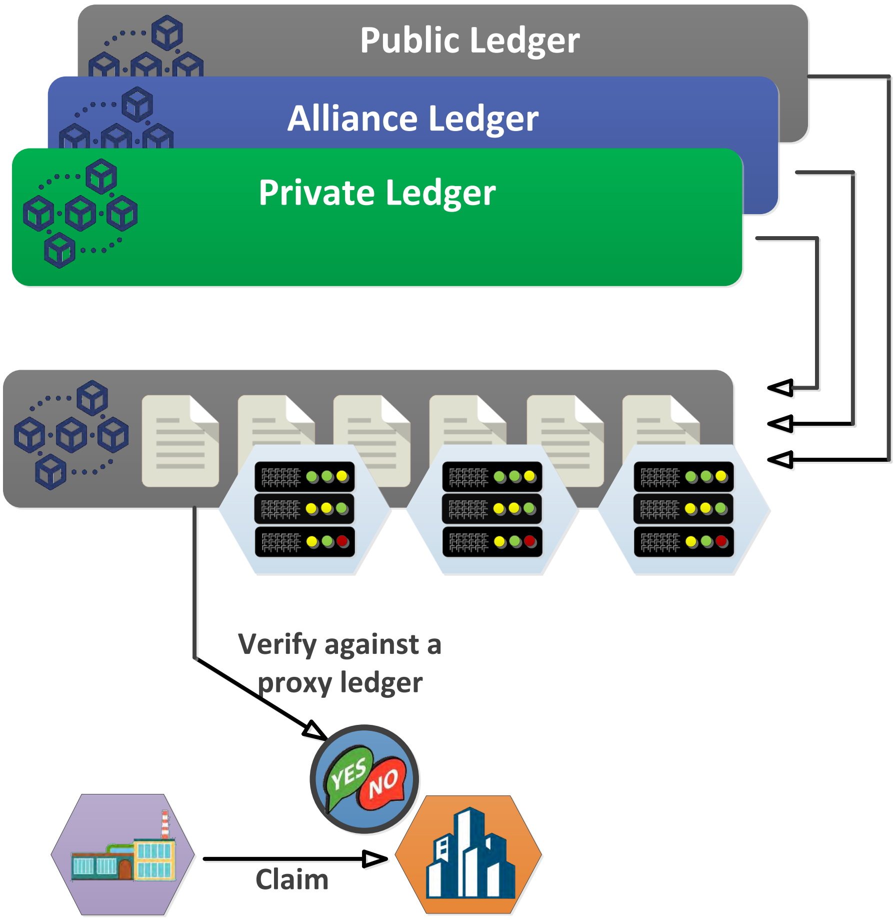


Figure 5.1: Verify claims in context of multiple blockhains.

The scenario is illustrated in Figure 5.1. In this case, a dedicated ledger designed to verify inter-ledger claims and transactions can be applied for validating transactions that touch input data from multiple ledgers. It is not necessary that each node of this cross chain ledger must have full node access to all the ledgers. Each node of the inter-chain ledger may have access to a subset of ledgers could be sufficient for validation purposes.

This common inter-chain ledger hides heterogeneity in terms of ledger design, infrastructure, operation, and governance of the multiple connected ledgers. It offers a unified interface to supply chain stakeholders to validate transactions or claims made by an actor. The verification can be done irrespective of which ledgers the inputs are originally created and stored.

Protecting trade secrets and proprietary information is vital for distributed ledgers to succeed in adoption by the supply chain industry. In case, a transaction or claim involves private information lodged by a ledger whose data is hidden from a verifier, it is still possible to have the transaction or claim validated by the verifier without access to the ledger or the private information.

One option to verify transactions with only partial or incomplete data in such context (restricted access to the ledgers with different governance policies, proprietary information stored in local databases), is to leverage zero knowledge proof. More explanation of zero knowledge proof is included in the succeeding sections of this Chapter.

At high level, a supply chain actor can present his/her claim or transaction with a digital proof to a verifier. If the verifier had access to all the information used for creating the transaction or claim, it could be easily verified. However, in case part of the information cannot be disclosed or hidden from the verifier, it can be still validated based on data that the verifier can obtain.

Figure 5.2 demonstrates the process. A major benefit of zero-knowledge proof [25] is that it allows transactions or claims to be validated against ledgers (permissioned ledgers or public ledgers) with only partial information available to the verifiers. The data accessible to the verifiers can be extremely concise, for instance, a cryptographic hash summary of an entire ledger. Depending on the design and level of protection, it is feasible to use zero-knowledge proof in such a way so that it is provable that no information what so ever is leaked to the verifier.

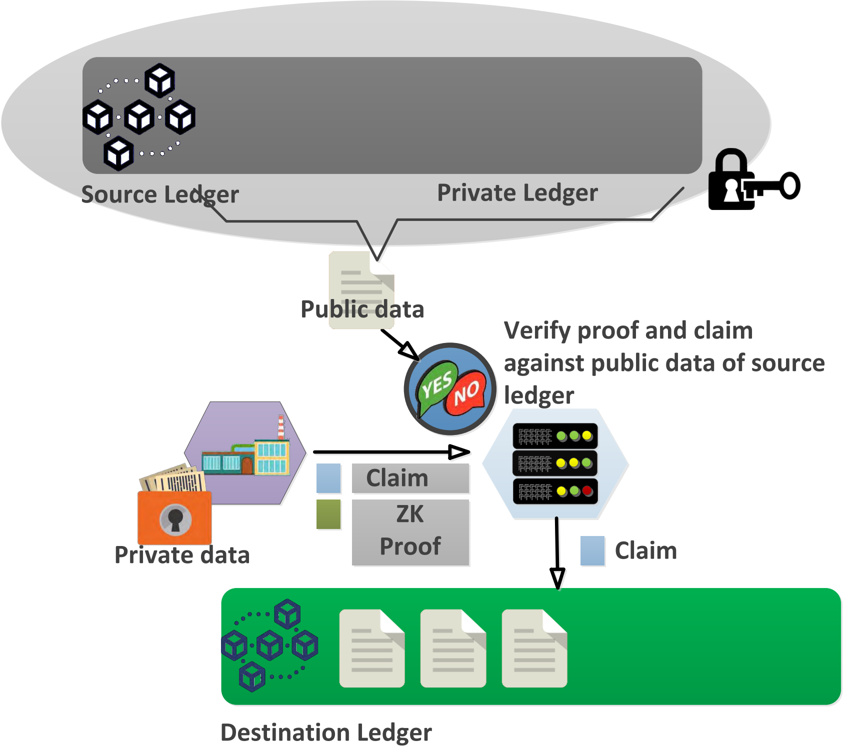


Figure 5.2: Port data items across chains/ledgers.

Another likely use case scenario of inter-ledger operation, is to verify accuracy of information by a supply chain stakeholder without disclosing it to the others [51]. For instance, a piece of information such as invoice may be lodged by two or more ledgers, say ledger

A and ledger B (ledger A could be a trade finance ledger and ledger B could be a logistics ledger). If a participant of ledger B wants to verify if information regarding the same invoice stored in ledger A matches with the counterpart in ledger B (e.g., price or quantity are the same, or within a threshold, or within a threshold after computing currency exchange rate), he/she could accomplish the task without access to the data in ledger A. In this case, neither ledger A nor ledger B discloses what it knows or its data to the other (price or quantity). The two ledgers can work together to verify a claim regarding the invoice based on the information lodged in its own ledger.

This is achieved by jointly computing a function by the two sides who only use information available to themselves. Figure 5.3 illustrates the use case at high level, where it shows the result computed jointly using each side's input data, without letting the other side know the information. Such operations can be implemented using well established multi-party computation (MPC) approaches [54, 83]. MPC based approaches may facilitate inter-ledger operations, in particular when the two private ledgers have different governance mechanisms and restrictions regarding data privacy. One example is G2G data exchange between two governments or between two different agencies.

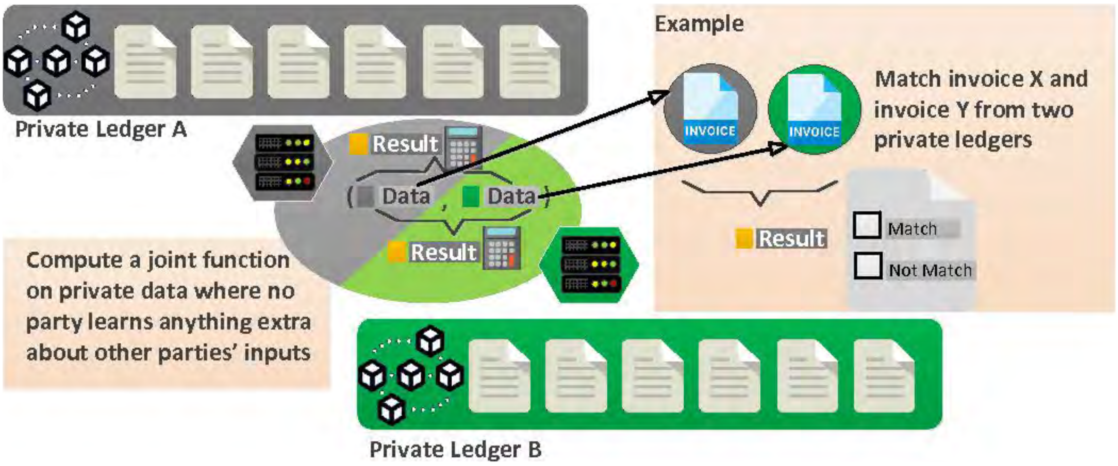

Private Ledger A
Result
Data
Data
Result
Compute a joint function on private data where no party learns anything extra about other parties' inputs
Example
INVOICE
INVOICE
Match invoice X and invoice Y from two private ledgers
Result
Match
Not Match
Private Ledger B

Figure 5.3: Cross chain computation with data confidentiality assurance where data belonging to each chain is not disclosed.

The use of common standards and semantics (i.e. data definitions) could simplify the task to integrate, correlate and interpret data from different sources. Both the WCO and the UN/CEFACT may provide enhanced data model for trade-related semantics which could be used for such purpose to facilitate information flow across ledgers. Semantics across different views (trade, finance, logistics, and entry declaration).

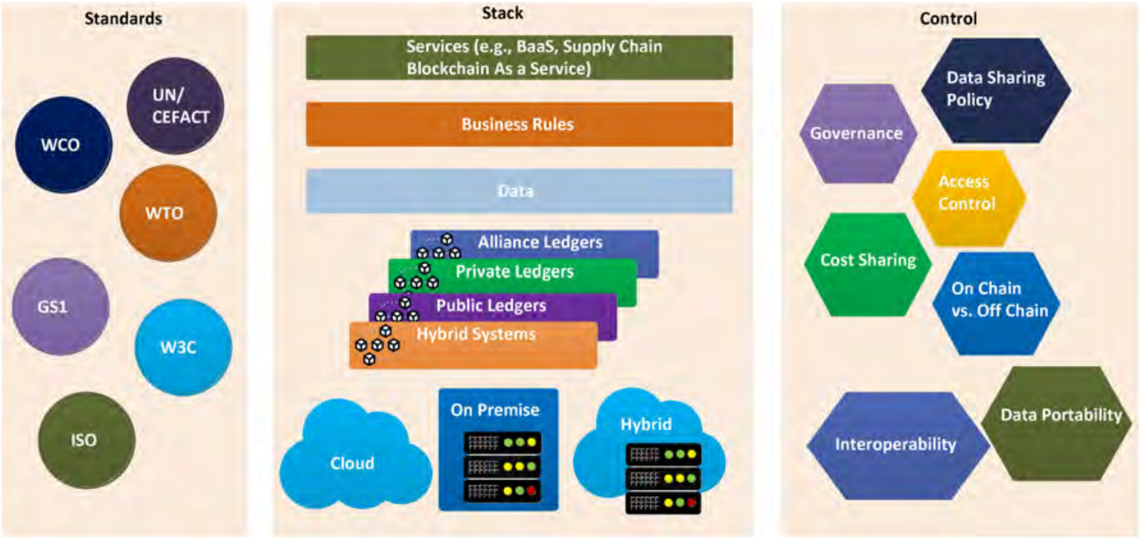


Figure 5.4: Three planes of distributed ledger framework: infrastructure stack, standards, and control.

Figure 5.4 shows three planes of distributed ledgers, infrastructure stack, standards, and control. The infrastructure plane deals with issues such as deployment of ledgers over IT infrastructure (cloud, on-premise, hybrid), data models and information flow over multiple ledgers, business rules and processes on top of the ledger data, and services to the supply chain customers. The control plane handles issues such as governance, interoperability, data sharing policies, off-chain data storage, data portability, and etc. The standard plane focuses standardization efforts, which may involve many standard bodies such as the WCO [1], the UN/CEFACT, the W3C [70], the GS1, the ISO, and etc.

To link data stored in multiple ledgers with the global standards, the W3C has been working on blockchain based identity management systems for realizing support of decentralized identifiers, and decentralized verifiable credentials.

Decentralized Identifiers (DIDs) [56] are identifiers whose purpose is to facilitate the creation of persistent encrypted private channels between entities without the need for any central registration mechanism. They can be used, for example, for credential exchanges and authentication. An entity can have multiple DIDs, even one or more per relationship with another entity. When an entity has one DID per relationship with other entities, it is called a pairwise pseudonymous DID. Ownership of a DID is established by demonstrating possession of the private key associated with the public key bound to the DID.

A distributed ledger can support the management of keys and identifiers by acting as a Decentralized Public Key Infrastructure (DPKI), which leads to a decentralized identifier system.

5.2. Collecting trade data from multiple ledgers

Transaction data from multiple blockchains can be collected and converted into structured data to support efficient queries. This has been successfully demonstrated for public blockchains. For instance, platforms were created to support data analytics on public chains (e.g., Bitcoin and Ethereum), reorganizing blockchain data in SQL or NoSQL databases. The data can be combined with external information to support queries.

Another example is the service that Google provides. It collects from the public blockchains and makes the data available on their cloud computing platform. The data is incrementally updated. The platform allows querying the blockchain data on Google's BigData infrastructure using traditional SQL language. Querying blockchain data from Google BigQuery platform is highly convenient from the data analytics standpoint.

Similar efforts could be performed on private and permissioned supply chain ledgers. In contrast with public chains, gathering data from private chains need to deal with the heterogeneous environment of governance and data access policies. In addition, there could be increasing need to discover where supply chain information is hosted, obtain access to appropriate data, and correlate data across different supply chain ledgers.

Development of standard based approaches such as efforts from the UN/CEFACT and the ISO could facilitate the process of resource and data discovery, so that the disparate platforms of multiple supply chain ledgers could act as one global source of information.

The UN/CEFACT has started to look into creation of specification that could bridge independent platforms to discover resource data regardless of where it is stored.

5.3. Consensus protocols and transaction finality

Early public blockchain projects mostly adopt Proof-of-Work (PoW) based consensus. Due to limitations of PoW, recent blockchains attempt to replace PoW consensus with variety of Proof-of-Stake (PoS) based designs, which includes voting based system (so called delegated PoS) such as EOS where block proposers are elected by voting rather than by an on-chain algorithmic process. Projects like IOTA replaced the chain-of-blocks data structure with a DAG (Directed Acyclic Graph) data structure, which breaks the limitation of sequential processing of transactions.

For permissioned ledgers or private blockchains, a popular design is to use an efficient version of BFT algorithm (Practical Byzantine Fault Tolerance) that can best suit the purpose and the intended environment of the distributed ledger. BFT as an academic research area of distributed computing has been studied intensively in the past decades. The classic BFT algorithm has performance and scalability issues in practice. Practical BFT (PBFT) attempts to address these issues with a more efficient design [53]. In PBFT, one node is elected as the "leader", while the rest of the nodes are "validators". Each round of PBFT con-

Table 5.1: Performance comparison of some consensus protocols for blockchains. PoA: Proof of Authority; DPoS: delegate Proof of Stake; PoET: Proof of Elasped Time; FBA: Federated BFT.

Consensus	Concept	Comm overhead	Comp overhead	Throughput	Scalability
PoS	amount of stake	low	medium	low	low
DPoS	nodes with stake taking turns to create transactions	low	medium	medium	low
PoA [48]	reputation	low	low	medium	low
PoET [55]	time based enforced by hardware	low	medium	medium	low
FBA [72]	leader selection based on quorum intersection	high	medium	low	low
IoTA [77]	non sequential distributed ledger	low	low	medium	medium
Harmony [46]	Sharding based on stake; fast BFT within each shard using short signature	low	low	high	medium

sensus involves two major phases: the prepare phase and the commit phase. In the prepare phase, the leader broadcasts its proposal to all of the validators, who in turn broadcast their votes on the proposal to everyone else.

Beside PBFT, there are many other formats of BFTs. These include, Fast BFT [71], Cheap BFT [65], Min BFT [82], etc. In FBFT, instead of asking all the validators to broadcast their votes, the leader runs a multi-signature signing process to collect the validators' votes and then broadcast it. So instead of receiving multiple signatures, each validator receives only one multi-signature, thus reducing the communication overhead.

Option of consensus protocols by a blockchain or distributed ledger platform may have different implications related to when and how the transactions are finalized. Meaning of so called transaction finality is often well supported by the legal and regulatory framework.

To support supply chain and finance operations, parties involved in a transaction and their intermediaries rely on the definition and timing of finality when they update their own internal ledgers. Depending on the type and design of consensus mechanism, in certain blockchain systems, multiple parties jointly work together to maintain and update a common ledger. Those parties must agree to a particular state of the ledger through a defined consensus process.

In case of PoW, which adopts a longest chain principle for consensus, the longer a transaction is considered settled by the system participants, the less likely this transaction will be challenged, rejected, canceled, or reversed eventually. Some other consensus mechanisms, for instance IOTA, adopt a similar concept where transaction finality is probabilistic.

This approach to finality contrasts with the traditional concept of finality that relies on approach of defining an unambiguous and transparent moment of finality. The probabilistic approach to finality may have implications. For instance, legal liability may be difficult to assign or be ambiguous in such a network due to the uncertainly of transaction finality.

Fortunately, not all consensus processes rely on the same longest chain principle. Most permissioned or private distributed ledgers adopt various BFT like mechanisms for reaching consensus. These consensus protocols based on the BFT protocols don't have the same transaction finality issue that PoW based systems have, which perhaps make them better options for certain industries or use cases when considering to adopt distributed ledgers.

Another issue related to transaction finality, is transaction automation. Blockchains automate recording, acceptance, and synchronization of transactions among a group of stakeholders. The question of transaction finality regarding blockchains and distributed ledgers, sometimes is likely a question on legal, contractual, and regulatory compatibility to have the transactions fully automated with minimal or no human intervention. Within the legal or contractual framework, as long as transactions can be automated, and the conditions to accept transactions can be verified by the permissioned participants of a system, it is plausible to achieve transaction finality by choosing an appropriate consensus protocol that matches with the operational requirements.

5.4. Safeguard of trade side proprietary data

In a public ledger or blockchain, each new "block" of transactions is verified, and then appended immutably to the end of the "chain" of prior transactions, so it can't be altered. All information about every transaction is made public. This understandably raises concerns from the supply chain stakeholders and makes them resistant to such kind of public disclosure.

In a permissioned or private ledger, only authorized nodes can maintain the system and manage the records using more efficient and scalable consensus protocols than the public ledgers. Records on the permissioned or private ledger are synchronized on all the nodes to ensure tamper resistance and immutability.

Although such system can keep some information from the public view, it still allows access to the data stored in the ledger by the permissioned nodes. In case of an alliance ledger, companies work together to manage the ledger as a distributed data system may be able to see each other's transaction information, which still worries the supply chain stakeholders. There is a potential issue related to Anti-Trust regarding certain data sharing using a consortium or alliance ledger, which is outside the scope of this report.

There are several approaches to address concerns of privacy, and protect proprietary information without scarifying the basic principles of a distributed ledger such as auditability and validation of transactions contained in a block by the peer nodes.

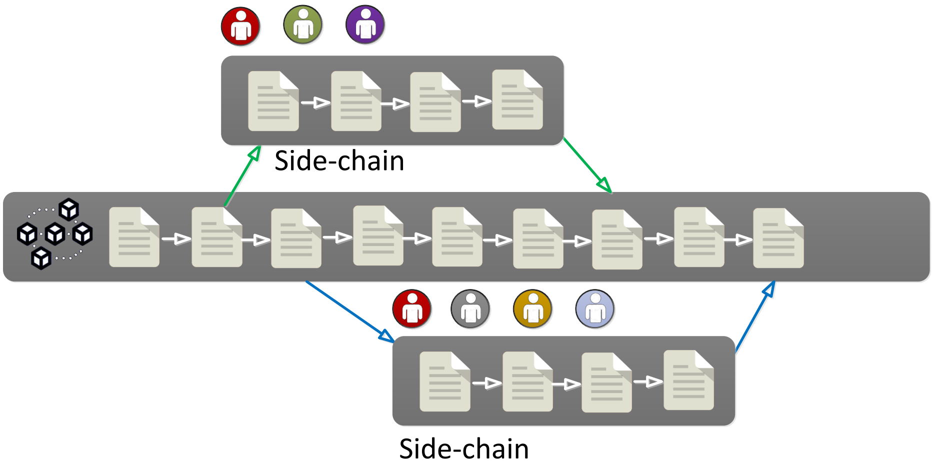


Figure 5.5: A simple diagram on side chain.

Privacy may be preserved using side-chain or off-chain transactions, see high level diagram in Figure 5.5. A subset of nodes can form a separate side-chain for conducting private transactions. Then the final state of the side-chain can be later merged back into the main chain or common ledger.

Payment channels or lightening networks in public blockchains are example of off-chain transactions. Side-chain protects data confidentiality because transaction information is only available to the nodes belonging to the side-chain instead of nodes on the main chain. The concept of channel in permissioned ledger such as Hyperledger is similar where each channel behaves like a sub ledger (see Appendix B for details).

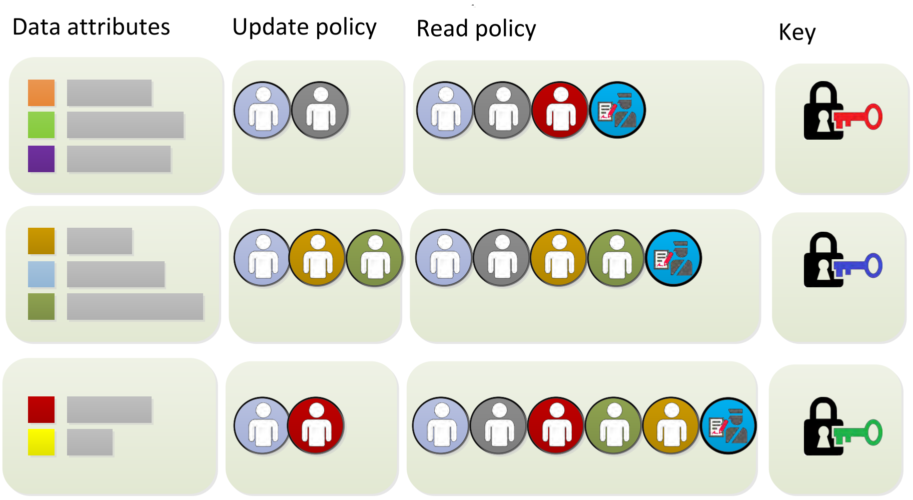


Figure 5.6: Data items and fine grained access policies.

Another option is to have transaction data encrypted, see Figure 5.6. The encrypted data can only be retrieved by the party/parties who is/are allowed to access the data.

For data sharing, it is possible to implement fine grained data access control using distributed ledger, named as decentralized access control management (DAM). Decentralized access control can significantly improve protection of data confidentiality and support an auditable history of data accesses. In contrast with centralized access management, decentralized access management does not store data access control policies such as ACL (Access Control List) in a centralized location. The approach allows access request to be verified in distributed manner based on blockchain consensus. It avoids storing ACL in a single location, and improves resilience against tampering and unauthorized modification of the ACL by insiders and bad cyber actors.

For each data item, data owner or creator can establish read and update policies that specify who can read or update the data, as well as under what conditions. Different cryptographic keys can be used for encrypting different data items, such as illustrated in Figure 5.7.

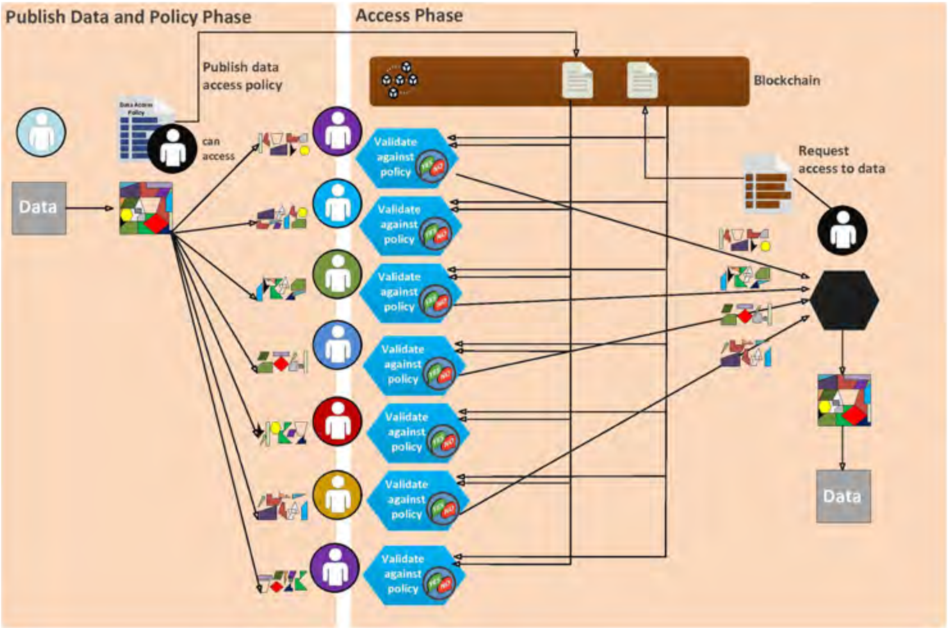


Figure 5.7: Decentralized access control using well established secret sharing approach. Storage of access rules and enforcement of data access control are both decentralized without possibility of single point of failure, or risk of unauthorized access through insiders or tampering.

For implementing decentralized access control, secret sharing scheme can be applied [63]. Secret sharing is a well established technology for managing data encryption/decryption keys in a distributed environment [79].

For protecting the cryptographic keys used to encrypt data items, a data owner applies secret sharing protocol to divide the keys into multiple pieces and distributes each piece to different peers of the system. Figure 5.8 illustrates the process. Specifically, data owner can select n nodes of the system and set a threshold k, divides a key to n sub-keys, according to the selected secret sharing scheme. The secret sharing scheme guarantees that when k or more selected nodes disclose their sub-keys to a validated data requester, the user can re-construct the key to decrypt the data.

When a data requester asks for access to a data item, each peer verifies whether the requester is authorized to access the data item based on published access policy for that data item, set by the data owner. If the requester has the permission, the peer encrypts its piece of encryption key and shares it with the data requester (for instance, encrypts its piece of the key with data requester's public key and submits to the ledger). Based on consensus of access control verification of a data access request, after the number of key pieces submitted to the system reaches the threshold set by the data owner, the data requester can recover the key used to encrypt the data item. Data owner can modify access policy such as adding a new user to the ACL.

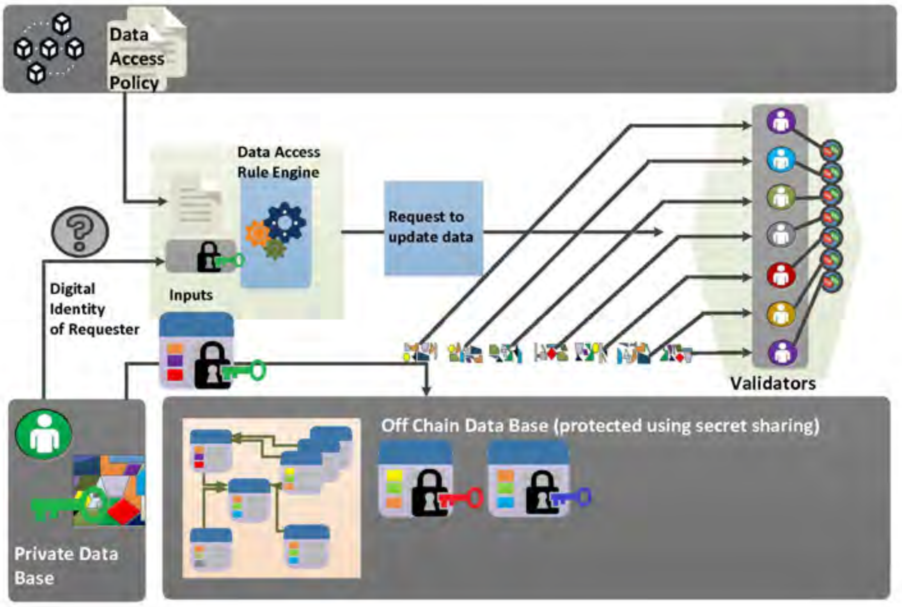


Figure 5.8: Update to data items with on-chain access policies.

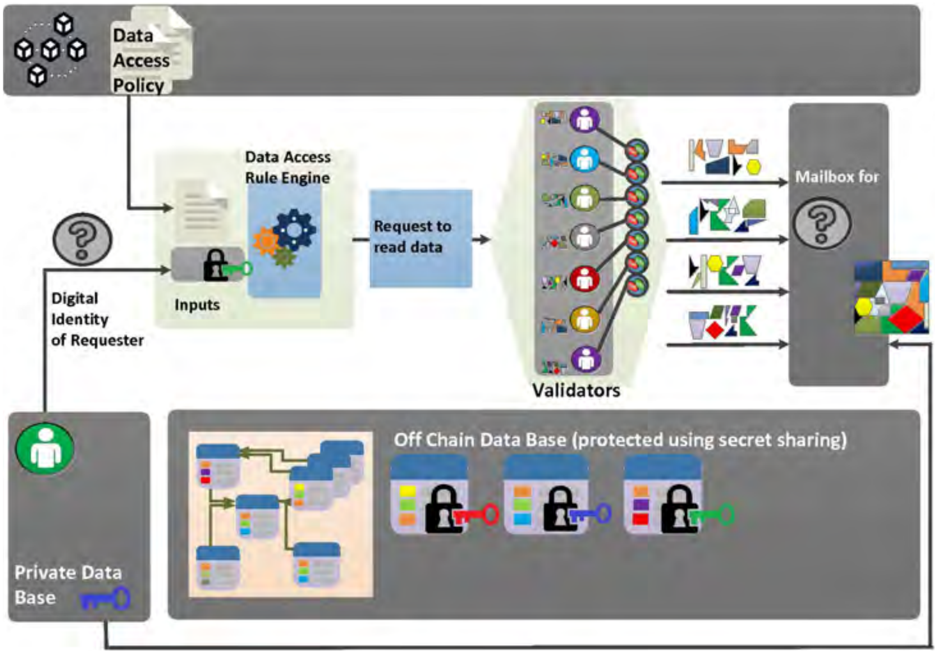


Figure 5.9: Request to retrieve data items with on-chain access policies.

5.5. Potential use case scenarios of zero knowledge proof protocol

Zero-knowledge proofs are cryptographic schemes where a prover is able to convince a verifier that a statement is true, without disclosing any more information than that the statement is true [25, 80].

Protocols using zero-knowledge (ZK) proofs can find application in various distributed ledger applications, which include identity management, transaction confidentiality, audit, etc. There are at least two parties in a ZK protocol: a prover and a verifier. The prover aims to convince the verifier that a statement is true without revealing any additional information.

There are two kinds of ZK protocols: interactive and non-interactive (NIZK). In an interactive ZK protocol, the prover and verifier engage in at least three rounds of communication exchange. Such protocols permit the verifier to submit challenges to the prover, whereby the prover replies with responses that reinforce the validity of the prover's original statement. There is no challenge response interaction in non-interactive ZK protocols. When a NIZK is a proof of knowledge, one can assume that there is a hypothetical extractor which can extract a witness satisfying the statement. Since there exists such an extractor, the verifier can be convinced that the prover must have known the witness. The witness information itself can be kept from the verifier. This way, NIZK can produce a proof of the truth of a statement without revealing any other information, in particular not revealing any information about the witness.

In a zero-knowledge protocol, the witness can be anything such as identity credential, price, quality, data access permissions, unique product identifier, supplier list, social security number, any kind of document, dataset, or even records of a complete database. Designing and implementing efficient zero-knowledge protocols for general purpose applications is an area of active research. There are joint academic and industry efforts to standardize the use of zero-knowledge proofs.

In case of global supply chain applications, zero-knowledge proofs can be applied for B2B transactions and audits where trade secrets and selected information can be kept private from being disclosed to the potential competitors while still allow transactions to be verified by the participating nodes of a permissioned or alliance ledger. This could be extremely useful when nodes that jointly maintain a supply chain ledger are both business partners and competitors, for instance, trade finance ledger managed by a group of banks, carrier ledger operated by a network of shippers, carriers, and freight forwarders.

Here we briefly describe certain use cases at high level.

5.5.1. Auditable transactions with data kept private

Zero-knowledge protocol allows blockchain transaction details to be kept private by the involved supply chain parties; and at the same time, the transactions can be verified and audited by the blockchain participating peer nodes (e.g., [58]). The verification can be on-chain instead of off-chain.

For instance, data attributes of an invoice, such as price, quantity, product code, can be validated against other documents on-chain by all the blockchain nodes without revealing the value of price, quantity amount, and content of the product code. Users can select and control the amount of information disclosed to the peer nodes of a distributed ledger. In this case, the data kept secret is the witness. A supply chain actor, also a prover, can prove to others that the transaction is valid and satisfies all the requirements without revealing the witness information.

As an example, assume that a buyer lodges a supplier list and products to a ledger. A cryptographic function can be applied to condense the list of products and suppliers as cryptographic commitments, for instance a hash value of the supplier list or product codes. The hash value instead of the original data is lodged to the ledger. In addition, the supplier can lodge cryptographic commitments computed from the product certificates, licenses, and etc. The supplier list itself is kept as trade secret by the buyer.

Later, when the buyer issues a purchase order to one of the suppliers for a specific product contained in the list, the buyer can generate a zero-knowledge proof that claims that the purchase order includes a product ordered from one of the suppliers in the list (previously lodged to the ledger). The purchase order can include references to the previously lodged certificates and licenses associated with the product. The supplier can claim that the purchase order contains product with valid licenses and certificates. In addition, the supplier can further make a claim that the price is within a certain range. Then the supplier can send the zero-knowledge proof to all the validators of the ledger associated with a new commitment computed using the purchase order as input. Without access to the original data including the supplier list, product list, certificates, and purchase order, a validator can verify whether all the claims are true or not based on the zero-knowledge proof. If the proof can be verified, the validator can accept the new commitment as record and have it lodged in the ledger.

Then if the supplier issues an invoice based on the purchase order, the supplier creates a new zero-knowledge proof for the invoice. The supplier can make claims such that the invoice matches with one of the previously lodged purchase orders regarding price, quantity, and product description. A cryptographic commitment can be computed with the invoice as input. The validators can verify all the claims using zero-knowledge proof without access both to the original purchase order and invoice. If the proof can be validated, the new commitment computed from the invoice will be accepted to the ledger.

With zero-knowledge protocol based support, a sequence of supply chain transactions can be validated by the peer nodes and lodged to the ledger. During this process, a main benefit of zero-knowledge protocol is that it allows transactions to be audited by the peers of a distributed ledger without disclosing any trade secret or information compromising confidentiality.

5.5.2. Protecting information flow and statistical information

Besides privacy of transaction data itself, supply chain business actors may wish to eliminate any chance that leaks confidential information such as business relations, supply chain patterns, or statistical data through flows of transactions. Although data itself is hidden from the validators, connections and references between transactions lodged in a ledger may be visible to the peer validators. This means that transactions could be traceable in the sense that a blockchain validator who is not part of a supply chain deal, may be able to see how different datasets are linked together in a sequence of supply chain transactions.

Although the datasets and their values are hidden, the links connecting them are not. For instance, a validator may be able to see a sequence of linked supply chain transactions, such as booking of carrier, shipping status, releasing of the goods. When correlating the data with publicly known information and records such as flight schedule, shipping schedule, and etc., it may be plausible to de-anonymize the parties involved in these transactions and further allow the peer nodes to gather metadata and statistical patterns, for instance, number of certificates or transactions issued from a supply chain entity. Such indirect disclosure of metadata, trading patterns, and statistical trends may as well worry supply chain entities. Fortunately, such information can be hidden from the validators as well using zero-knowledge proofs. For instance, a supply chain business actor can claim that an invoice matches with a specific purchase order lodged in a ledger without disclosing which one.

With zero-knowledge protocol, it is plausible that all the supply chain transactions lodged in a ledger are indistinguishable from one another (mean that they all appear the same to the validators). The links between these transactions can be completely hidden from the validators, which prevent the peer nodes from performing data mining or statistical analysis of the transaction data.

5.5.3. Data migration or import across ledgers

Zero-knowledge protocols may facilitate data migration and portability when information is exported from a private ledger and imported by another ledger with different governance rules and operation models.

It is often not feasible to have validator nodes in both ledgers to have the same access permissions to each other’s data. When data is exported from a source ledger that restricts access to its data by validators of the destination ledger, zero-knowledge based protocol can be applied to generate a proof claiming that the imported data matches with the data lodged in the source ledger. Truthfulness of the claim can be validated by the destination ledger using only information that the source ledger is allowed to share. At a minimum, such information can be just a cryptographic root hash of the source ledger. Different from the prior use case scenarios where zero-knowledge protocol is used for protecting confidential data contained in a transaction from the validators of the same ledger, data migration use case applies zero-knowledge to support validation by nodes of a different ledger when data is migrated from the original ledger. It allows nodes of the destination ledger who have no access to the source ledger to verify authenticity of the imported data.

5.5.4. Protecting confidentiality of data access policies and access history

When blockchain is applied to implement and enforce data access policies, the policies themselves may be stored in the ledger. Depending on the specific design, data management policies could leak business relations, and other proprietary information. For instance, ACL to data items if stored in cleartext could disclose information considered as confidential.

To protect confidentiality of access history of a data user, one can leverage zero-knowledge proof to hide data requester's identity and data management policies while still support enforcement of data access control. At high level, instead of directly storing allowed data users' identities in ACL in a ledger, the data owner derives something from information that is only available to the data users and commits data access policies and access control list using cryptographic commit.

When a user issues a request to access the data, the user can generate a zero-knowledge proof that every peer of the ledger can verify based on the proof that the user's identity is in the access control list without disclosing identity of the user and even the access control list itself. Furthermore, this proof can be re-randomized when the user submits a new request. So an adversary cannot learn the relationship between multiple requests from the same user by observing requests uploaded to the ledger. The process for both read and update requests is illustrated in Figure 5.10 and Figure 5.11. In both cases, the access policies are kept as confidential information off-chain.

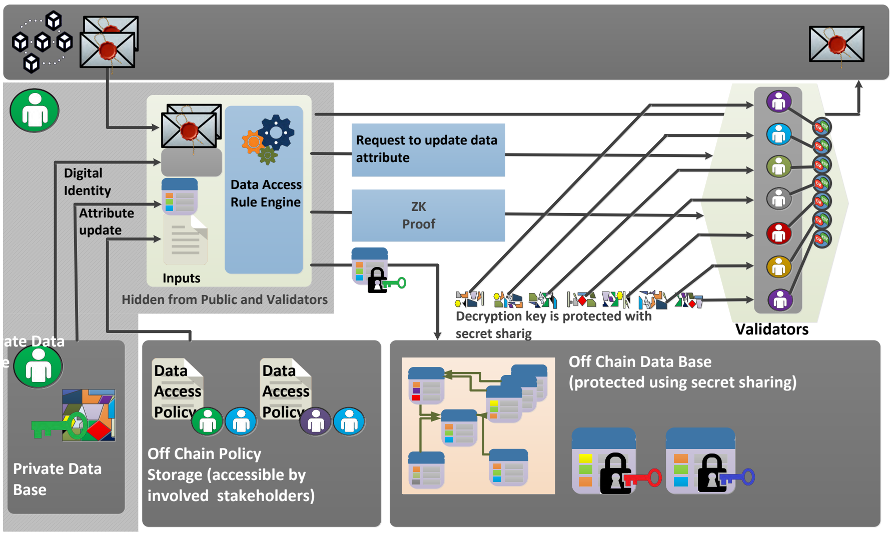


Figure 5.10: Blockchain verifiable request to update data items with private access policies (access policies stored offchain).

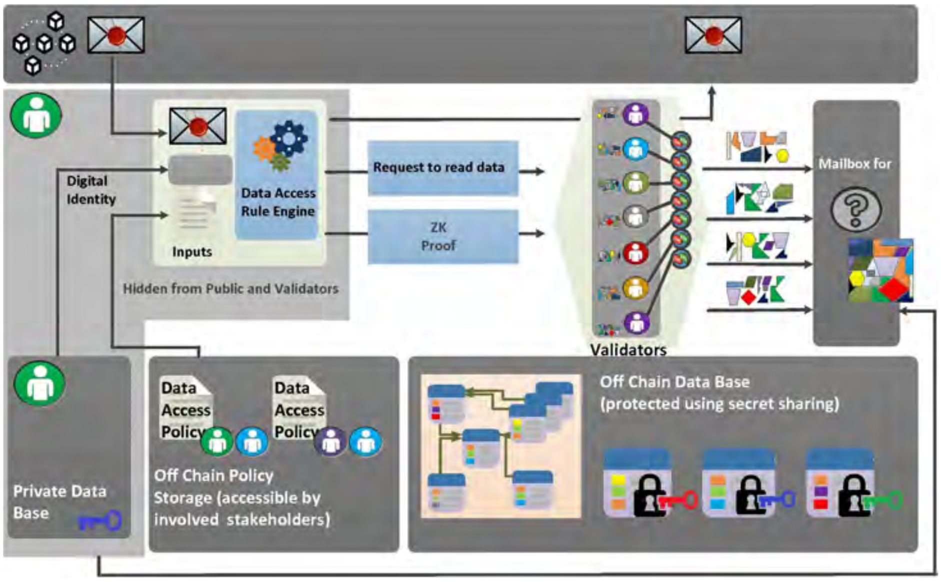


Figure 5.11: Blockchain verifiable request to read data items with private access policies (access policies stored offchain).

This use case may enable confidential access by the regulatory authorities to a shared ledger. With zero-knowledge support, access histories made by different supply chain stakeholders can be completely indistinguishable from one another. This means that all data access requests appear to be the same to the peer nodes of the ledger and validators. Zero-knowledge protocol can hide who are the data requesters, which data item is targeted by a request, and what is the data access control policy involved in a request.

Table 5.2: Confidentiality assurance under different schemes.

	Data encryption	Date encryption + credential privacy	Date encryption + credential privacy + ZK protocol based protection
Confidentiality of transaction data	Protected	Protected	Protected
Confidentiality of business relationship	No	Protected	Protected
Confidentiality of transaction flow	No	No	Protected
Confidentiality of statistical patterns	No	No	Protected

5.5.5. Identity credential with Privacy

Approach also exists where zero-knowledge protocols allow for privacy-preserving querying of credentials [62].

In an example use case, we consider an authorized economic actor that proves to a supply chain ledger that a submitted transaction meets all the requested requirements without disclosing confidential commercial details of the transaction.

This takes place through a system that enables the supply chain actors to build and disclose proofs derived from the licenses and certificates that they own. These can be: active status as an authorized economic actor, product certificates issued by the regulatory authorities or the third party certification bodies (showing that the product meets compliance requirements), and invoices. Rather than sharing the permits, licenses, certificates in their entirety to the ledger nodes, the presentation built by the system using zero-knowledge protocol allows the supply chain actor to combine the derived information from each licenses and certificates, and proves to the ledger nodes that the transaction is valid such that it has all the required licenses and certificates. Meanwhile, it hides what the product is, identity of the supplier, and what are in the certificates.

5.6. Scalability of blockchains: current and future trends

Public blockchains have been criticized for their performance. For instance, it takes minutes to complete a Bitcoin transaction. Approaches have been developed to tackle the performance challenge of distributed ledgers, with the goal to support high transaction throughput and scalability meanwhile preserving some of the basic characteristics of blockchains (e.g., distributed consensus, distributed book keeping, immutability, and auditability).

The scalability solution that preserves both security and decentralization is sharding [67, 84], which applies a strategy of divide-and-conquer. Sharding creates multiple groups (i.e. shards) of validators and lets them process transactions concurrently. As a result, the total transaction throughput increases linearly as the number of shards grows. Schemes such as side-chains or satellite chains may be considered broadly as approaches related to sharding to enhance performance and scalability.

Both states of a ledger and transactions can be sharded. Alternatively, nodes can be divided into groups and assigned to the transactions belonging to a shard.

In public blockchains with sharding support, scheduling of transactions or nodes can be done in a random and unpredictable manner. This could be achieved through a distributed randomness generation process which is unpredictable, fair, verifiable, and scalable. For permissioned ledgers, sharding decisions can be based on a different mechanism, for instance, amount of computing resources, physical locations of the nodes, identities of the nodes, and etc.

To reach consensus within each shard, an efficient algorithm based on certain flavor of BFT, can be applied. There are many options that allow customers to decide trade-offs between performance, scalability, resilience against disruptive events (e.g., DDoS attacks). Those include: PBFT, Cheap BFT, Fast BFT, Min BFT, and etc. It is plausible to achieve high performance through a linearly scalable BFT algorithm.

In addition, using efficient data communication and routing designs, transactions can be propagated quickly within shards. Efficient gossip protocols can be applied to support fast cross-shard transactions.

Recent experiment results show that with efficient implementation of sharding, a single shard may be able to support few thousand transactions per second. Performance such as hundreds of thousands of transactions per second could be achieved when there are multiple groups of nodes runnning transactions in parallel.

5.7. Complexity and limitations of smart contracts

Among technologies around blockchains and distributed ledgers, smart contract is one of the most easily confused concepts, among the legal and regulatory communities. Often the confusion stems from the terminology and its use of contract in the name. A different name, such as chain code, may better describe the behaviors of smart contracts and what it does at software program level. Discussions with the legal experts and law center faculty, suggest that the name of smart contract is a misnomer.

Nevertheless, this doesn't prevent the current lack of understanding of what smart contracts are from a legal perspective. Likely smart contract may be viewed as simply a piece of software which automates execution of some obligations by the involved parties and intermediaries. The extent, smart contract can be considered as self-sufficient binding agreements that exist in the form of computer code, which may have specific features in the contract law realm, remains to be debated. It is plausible that a legal binding contract may have smart contract codes and links included as references. The issue is how to apply traditional rules of contract law, relating to termination, amendment, and remedies for breach to smart contracts.

There are also questions such as how to define the liability of the parties in case that a smart contract does not work as expected due to flaws and bugs in the smart contract program, or cyberattacks to vulnerabilities of the consensus process and blockchain platform. There is well recognized need for the blockchain technology community and the legal community to develop common framework to improve understanding of smart contracts from both technical as well as appropriate legal perspective, specifically, on their compatibility and inter-operability with the legal regimes governing life cycles of contracts.

Apart from the issues related to legal interpretations of smart contracts, converting legally binding agreements between supply chain actors into self-executing software codes has many challenges. Complexities, limitations of the programming languages used for coding smart contracts, and flaws including software bugs embedded in the smart contracts themselves, are some of the major obstacles. The list is not intended to be comprehensive as there are many other issues and problems with the concept and implementation of smart contracts.

The idea to encode laws, regulations, and real world contracts as self-sufficient computer programs or state machines is not new. The idea has existed for many decades. The dis-intermediary nature of blockchains provides a new platform and landscape for such idea. However, complexity of real world contracts may very well make such task extremely difficult based on the technologies available today. This challenge is further amplified, sometimes, by limitations of the programming tools used for developing smart contracts, and quality of the software codes.

Unlike conventional software programs, smart contract codes may have significantly larger vulnerability surface and attack vectors. Since smart contracts need to be executed in a distributed manner, often by a large scale blockchain system, they often face complex operational environment and need to deal with sophisticated scenarios. During this process, there could be many places that things may go wrong. There is also a broad range of attack vectors that make them targets of cyberattacks. Some of the challenges are due to limitations of the underlying programming languages for coding smart contracts, or lack of tools to analyze or verify behaviors of smart contracts, or simply caused by bugs and deficiencies in the smart contract codes themselves.

Programming language limitation is often one of the prime reasons that prevent wider adoption of smart contracts. The current generations of smart contract programming languages are either too restrictive with constraints that make them suitable only for specific use case scenarios, or too general and low level that exhibit a large gap between the programming concepts that software developers use and are familiar with, and the concepts required by real-world business contracts. Designing better programming languages and execution environment for smart contracts that better serve the purposes of specific industry sectors is still a topic of ongoing research.

As long as software and codes are still written by humans, there will be bugs and mistakes in the codes. Smart contracts are extremely complex to verify and assure their properties and behaviors. Sometimes, bugs may be simply caused by the programmer's negligence. It is almost impossible to claim that a smart contract program is completely bug free. In addition, existing verification tools and research primarily focus on programming and software related bugs. There has been little research on verifying business process and legal aspect of a smart contract code. It is not difficult to imagine that a smart contract even in case without any programming bugs, may have major flaws when handling complex business scenarios.

6

Stakeholder Survey

6.1. Research questions

The following questions assume that an end-to-end (E2E), exchange to exchange, cross-border supply chain perspectives adopted by the supply chain stakeholders to maintain transactions, and that technology allows importers, suppliers, and brokers to share entry-related data way in advance. "In advance" in this case means much earlier than what is required today for declaration and entry submission. Indicatively, this new data sharing could begin even as early as the commercial stage when business agreements are concluded between the buyers and the sellers, or a purchase order is placed.

Areas for the stakeholder survey:

1. Non-technical barrier(s) for sharing entry data in advance with the CBP.
2. Accuracy, quality related to the data shared in advance with governmental time frames for data submission.
3. Time frames for data submission.
4. Benefits from the CBP side for advanced data submission; benefits for the private sector stakeholders.
5. Legal concerns related to data sharing in advance with the Customs.
6. Key ingredients for such advanced data sharing practices with the Customs to succeed providing proven benefits to the importers/filers.

A list of detailed questions are in Appendix D.

6.2. Methodology

This section describes the finding from the interviews that we did with selected people including brokers, importers, surety providers, and attorneys.

The purpose of the stakeholder interviews is to participate in a collaborative and constructive discussion initiative that would gather ideas, comments, benefits, and challenges associated with leveraging blockchains for entry processing and data collection. The findings of the interviews are divided into the following categories:

- Benefits for the importers;
- Attitudes towards changes of entry process;
- Non-technical barrier(s);
- Challenges need to be addressed.

6.3. Summary of the findings

6.3.0.1. Benefits of blockchains

Bassed on the interviews, a few importers acknowledged the advantages of blockchains, and confirmed that there are benefits of using blockchains based on their internal studies and pilots. Most of these beneficial outcomes such as supply chain traceability, process automation, and reducing administrative cost are in line with other recent reports and surveys that study the environment for adopting blockchains by the supply chain industry.

6.3.0.2. Embrace of changes and new technologies

Majority of the interview participants indicated they were amiable to changes. It was acknowledged that technologies have changed how they performed in their jobs in the past, and likely will continue to bring changes in the future. They indicated a receptiveness towards emerging technologies such as blockchains.

6.3.0.3. General comments

Majority of the interview participants agreed that commercial information such as ordering data is likely available to be shared early, assuming the importer is sophisticated so that data sharing with the CBP ahead of time will not have significant barriers. The earlier to push the timeline, more likely it will be the case that the data would not be complete. Some participants mentioned that they had experiences sharing incomplete entry data early with Customs.

Several interviewees commented that advance data sharing may lead to increased number of documents submitted to the CBP that more likely will be changed later, for instance amendments or cancellation of the orders. Often, data attributes such as price or quantity are not finalized until some later time. One suggestion is that with blockchain as an enabling technology, it might provide opportunity to implement account based system instead of relying on documents that often change over time.

Some interviewees commented that sharing data early may be a challenge for small companies, unsophisticated importers, or importers with few resources or limited expertise unless they have access to expertise and tools that could help them in some way.

Interviewees also commented that the blockchain concept could enable the government agency to gain visibility into the actual product itself such as who made it and who manufactured it, which could help the government decide early release.

Most of the participants acknowledged that the worst situation not only for the importers but also to the brokers is that when the goods for whatever reason cannot be released at the time of arrival because there is information that is lacking, and decisions cannot be made. So sharing data early for making the decision early would help the CBP and the importers.

Feedback from some participants on sharing data in advance related to concerns such as cost and how easy it is to change the information after the products are already shipped.

Also, they want to make sure about the benefits that the importers will get because CBP is not the only agency with authority to hold cargo. Getting a release from CBP is important but it's not the end of story. They seek for release from all the hold authority at the same time.

One of the interviewees provided comments regarding sharing data early: the immediate response would be like if it is going to cost money to do it. Second, brokers are already providing lots of information such as the importer security filing, so they want to make sure that the efforts would result in benefits without significant increase of burden.

6.3.0.4. Challenges need to be addressed:

A few challenges according to the interviews include:

Accuracy of the data: Although it was mentioned at the beginning that the quantity and price could change later on, some of them still have a concern about accuracy of data and they believe that the earlier one shares the data, the less accurate the data would be. For instance, sometimes, changes will be made in post purchase order due to the value or a country of origin in this case would the importer be held liable for this piece of data being not accurate.

Some interviewees brought up the issue that although early data is available, the data may contain noise and likely is not in a format to be consumed directly by CBP. It often requires manual work to filter and convert the data for entry process. It is not clear yet how blockchains could assist in such a process.

Connectivity with ACE: Another major question raised in the interview was support and connectivity to the ACE service interface by the supply chain blockchain systems. A question would be how data from the blockchains will be fed into the ACE using the ABI. There should be a place where the brokers and importers can control how blockchain information connects to the ACE. Importers and brokers should be able to edit the records even if they are on the blockchains. With ACE still being used, there should be integration and data pipe between these two environments so importers and brokers can manage the entry related reports and everything.

Therefore, they need to be more focused on the blockchain data going into the ABI in order to control what would be fed into the ACE system. The importers and brokers should be able to certify that they agree with the data and this whole process will help increase accuracy of the data.

Confidentiality and legal concern: Data confidentiality was a major concern for the participants especially with the competitors and foreign governments. They were not sure if the blockchains will satisfy this requirement.

Despite using a common ledger, the competitors may not be able to see what's in the invoice or the quantity or price. However, they may be able to gather some statistics like how many transactions and for this information to be hidden it often requires more sophisticated technology. They believe that even only showing the statistics such as a company has this number of transactions (not what in these transactions) will violate data confidentiality.

One of the interviewees had a concern because of the prior experience with the government. They wanted to know what information, if any, they provide to the government will be shared later by the government with other entities. For instance, Journal of Commerce could get data from the government which makes it very easy for an ocean carrier to know where every other exporter or importer is shipping to and from. With more information shared with the government through blockchains, there will be questions how government will manage the data for sharing with the public.

Similar concern was also raised by another interviewee, specifically on high level government policy governing early and advance data sharing through the blockchains. The comment was that it may come down to a paradigm shift where companies should be assured that by providing early and advance data in this process, it won't be used against them. It will be used to their advantages the way it should be happening.

One comment about confidentiality is that the common sense is that more folks who received your data and they receive it from different channels, then the higher risk it is to your confidentiality or proprietary information. They want to know how such concerns could be handled by the blockchains.

Another comment suggested blockchains used for data sharing may render the existing confidentiality provisions inadequate and outdated. The bottom line is that all of them agreed that blockchains should respect data confidentiality, and proper policies with respect to liability and data privacy should be in place regarding data sharing through the blockchains.

About legal concerns, some participant worries about the aspect of government to government data sharing that had been discussed previously will be considered in the blockchain scenario or not .

Cost: When it comes to cost, we may think in two different directions, i.e., the cost to adopt blockchain technology from both the private sector and the government perspective.

The interviewees mentioned that leveraging blockchains from the government side may lead to change of the structures of the government due to the mitigating risk that blockchains will provide. The government will have an access to end-to-end business process. As the result, the structure of the government for dealing with cross-border trade could be more efficient, which reduces the cost from the government side, and in return decreases the burden on the importers.

Cost to the private sector : Although they think that the quality and transparency of data will be better, the cost for adopting new technologies even to large companies is still high and may be sometimes difficult to swallow. Solving this problem, they think, will be by people who have motivation to learn and develop new skills.

Another interviewee mentioned a very good point about even if the cost is high, the company will do it if there is a reduction in the administrative cost for managing end-to-end supply chains. Some of the administrative cost, companies don't necessarily measure that today. Blockchains could bring many cost reduction benefits, especially from the administrative side, companies may not be able to see it unless they are measuring them.

7
Summary Of Cross Border Trade Related Blockchain Consortia

7.1. Research questions

A consortium blockchain refers to a blockchain where several supply chain related entities work together to form an alliance and participate in its management. It is one of the favored approaches for creating enterprise-grade blockchain platforms. Members of the consortium may collaborate to determine how the blockchain is implemented and operated. Each entity may run one or multiple nodes. Participants are authorized with known identities. The blockchain is often private; and only authorized users within the system can create, read, and update transactions.

Blockchain consortia are typically aimed to create standards and build shared platforms that address industry challenges, and bring benefits to the majority of its market participants.

7.2. Methodology

The methodology that we used is to collect data available in public. Unfortunately, there is only very limited information that we can find because almost all the consortia have little information disclosed to the public unless you are a member.

We studied several cross-border trade related consortia, mainly focusing on the consortium model, data sharing, and what the values that a consortium adds. More details on the consortia below are provided.

1. Global Shipping Business Network.

2. Komgo.
3. Marco Polo.

7.3. Summary of the findings

Comparing with the public blockchains, consortium blockchains could provide cost effective operation and maintenance. It also could achieve higher transaction performance, and better scalability. It potentially facilitates and supports many supply chain B2B use case scenarios. In addition, consortium blockchains may also support better and smoother integration with the existing ITC systems for supply chain management. For instance, supply chain data models can be mapped to a consortium chain through gateway nodes that connect to the consortium chains. Some examples of consortium blockchains include: R3 Corda, Hyperledger Fabric [16, 17], Enterprise Ethereum.

Success of consortium blockchains hinges on many factors. There will be multiple consortium blockchains segregated by the industry sectors, for instance, trade finance chains, freight forwarding chains, retail chains, manufacture chains, etc. A main challenge to the consortium model is to avoid fragmentation and final emerging of multiple rival blockchain platforms. For instance, there are multiple consortia focusing on trade finance. These include: Marco Polo, We.trade, Voltron, Komgo, and the others. Each has some number of financial intermediaries as members. For freight forwarding industry, there are, BiTA, GSBN (Global Shipping Business Network), and TradeLens.

A blockchain consortium always faces the challenge how to attract non-members to use the platform for transactions, and maximize adoption, in particular SME to participate in the efforts. This could be a challenge because currently members have to pay high membership fees each year. For example, according to the official website of the Hyperledger, premier members can get a seat on the board of the alliance with an annual fee of $250,000. Regular members are required to pay between $5,000 and $50,000, based on the size of the company.

The following will be a summary of the three consortia based on information available to the public.

Global Shipping Business Network: It is an open digital platform based on distributed ledger technology targeting shippers, forwarders, carriers and terminals to be involved which will lead to build a platform to collaborate in the industry. The software that will be provided by cargo smart based on the idea of digitization of the shipping industry and the development of innovative solutions based on the distributed ledger technology.

Regarding data sharing, according to their web site, the GSBN platform will create a single source of truth for the shipping industry with the following benefits based on the blockchain technology:

- Open and extensible: Cooperative network enables members to connect with the consortium networks which will increase the speed of data integration and improve business performance.
- Transparency and instant validation: Peer-to-peer networking allows data owners to share immutable records with other parties.

Komgo: Komgo is an open blockchain platform in partnership with ConsenSys and Kaleido. Its goal is to transform trade finance from a paper-based system to digitized and secure. Komgo has fifteen members including banks, trading companies, and oil companies. It will be built as an open platform on Enterprise Ethereum. Participants benefit from the end-to-end approach in which lowering the time and cost needed to manage data. In term of data sharing, Komgo is using kite document transfer system which allows documents to be exchanged between participants without Komgo seeing the information. KYC process leaves the data with the owners and allow only owners to select actors to see the data without using any central database. Data is shared using end-to-end encryption and the user of the data can verify the documents by inspecting cryptographic fingerprints of that data.

Marco Polo: The Marco Polo is an open and distributed enterprise software platform. It targets the market of banks, and corporates trade finance. Marco Polo partners are R3 and TradeIX. TradeIX is a technology company that created a trade finance platform with applications and licenses the platform to the banks who run it as their trade finance transactional solution. Marco Polo is a collaboration rather than a legal entity so banks work with TradeIX either by joining Marco Polo or working with TradeIX directly or in combination. Marco Polo promises security and confidentiality of the data.

Some challenges to study and gain insights of these consortia are: most of them still in early stage, and closed environment with very limited information disclosed to the public.

7.4. Implications of the findings to entry process

One implication of multiple consortium blockchains to future entry process and integration of Customs functions with supply chain blockchains is that data collection has to be planned and designed under multi-sector and muti-chain context. Information collected from multiple chains needs to be correlated and linked.

This suggests the importance of open standards. The various supply chain consortia may not necessarily put adoption of global standards as its priority. Regulatory authorities could play a constructive role in the process to promote adoption of uniform standards and avoid isolated blockchain ecosystems.

The blockchain consortia are often driven by private sector entities. How to support and integrate with the regulatory requirements remains a question. A suitable private-public relation customized for the blockchain consortium model is necessary to ensure that these developed platforms could take the needs of the Customs and cross-border regulatory agencies into consideration. Such efforts could lead to in depth integration of the Customs declaration and entry data flow with the supply chain information flows managed by these consortium chains.

8

Policy, Governance, And Operational Challenges

This chapter discusses various non-technical issues related to adoption of distributed ledgers by the global supply chain community. In particular, the focus would be in the areas of global coordination, governance, promotion of open standards, private public relations, and other related issues.

Distributed ledgers enable supply chain related electronic records to be transferred safely and securely by a wide range of supply chain participants including producers, traders, buyers, brokers, carriers, insurers, and financial intermediaries. By nature, the transactions will cross multiple jurisdictions. Success adoption of such technology depends on many factors. There are potential legal, governance, technology adoption, policy hurdles or challenges that have to overcome.

8.1. Uncertainty of legal status of electronic trade documents

As blockchain gains traction in the global supply chains, it will encounter the same challenges as the prior and other existing efforts in paperless trade and supply chain document digitization. For instance, uncertainty over the legal status of the electronic transferable records such as electronic letters of credit, electronic bills of lading in the context of different jurisdictions, has been identified as one of the obstacles that hinder wide adoption of electronic trade documents and other related instruments.

The concerns are mostly due to the lack of clarity, and predictability of the governing law. For instance, UNCTAD survey identified that one of the main barriers that potential users saw to embracing and incorporating eB/Ls into their operations by the logistics and supply chain industries was that the legal framework was not yet clear enough and not adequate. The laws often are written in such manner that are considered somewhat cryptic regarding online transferring of electronic records and documents. Some of the challenges faced, are related to the document of title function, one of the main functions served by the B/Ls. Being a document of title, it has effects in terms of both property as well as contract law.

To achieve equal treatment of eB/Ls and paper B/Ls under the law, it often requires amendment to the maritime code, which varies across countries and jurisdictions. Traditionally, UNCITRAL has played a critical role in developing Model Law [20] to facilitate equal treatment of electronic trade documents with paper documents, which covers: bills of lading, bills of exchange, consignment notes, checks, warehouse receipts, insurance certificates, etc.

A key question is that whether the existing works are general and flexible enough to accommodate potentially new issues brought up in the operational environment of blockchains and distributed ledgers. Some of the questions include whether a blockchain based ledger can act as a registry within the meaning of the Model Law.

Regarding trade finance, use of electronic versions of L/Cs is covered under Uniform Commercial Code (Article 5), where negotiable instruments including bills of exchange, are covered under UCC Article 3. Although UCC Article 5 deals with rights and duties in connection with an L/C, it does not address rights and duties in connection with an electronic bill of exchange even if the bill of exchange qualifies as a “document” under UCC Article 5 required to be presented for the beneficiary to draw under the L/C. To facilitate confidence and certainty to the financial intermediaries adopting distributed ledgers for digital trade, amendments to the related UCC articles may be required [34].

The question of legal and regulatory uncertainty may also arise regarding any new forms of data contained in a blockchain based ledger. As discussed in the previous sections, distributed ledgers move beyond the concept of digitizing the existing trade documents and forms. With introduction of the new technology, it likely also creates new forms of data that raises additional questions regarding legal status and regulatory compatibility.

8.2. Cross jurisdiction coordination

Potential policy barriers of blockchain adoption fundamentally stem from the inherent nature that global trade is inter-jurisdictional. When talking about flow of electronic trade documents and information, a blockchain based trade infrastructure has to satisfy regulatory obligations within different jurisdictions.

Different governments may have different requirements of how to comply with domestic regulations. Some of those requirements could cover the nature of how the information is recorded and provided. This may lead to significant friction around how governments recognize information stored in distributed ledgers and determine if it is sufficient to comply with the domestic regulations.

Without global coordination and orchestrated efforts to create a uniform regulatory framework, over time, the domestic regulations relevant to blockchains and use of blockchains for electronic supply chain documents and information, may diverge. Such divergent regulatory environments regarding blockchains between countries could create additional costs, in particular, for small and medium-sized enterprises (SMEs) to manage.

To mitigate this, it is imperative for the market participants to collaborate with the industry associations, international standard bodies, and regulators, to facilitate development of globally unified framework and principles for blockchains.

The efforts may facilitate creating uniform legal rules and environment across jurisdictions regarding emerging technologies such as decentralized identity management, global trade over distributed ledgers where these emerging technologies are applied in electronic exchanges across borders.

8.3. Interactions with legal realms

Supply chain ledgers can be permission based, or a hybrid that integrates private ledgers with public chains and ledgers.

There are specific governance issues related to the use of public blockchains in a distributed ledger setup for global supply chains. One of them is related to the immutability of public blockchains and governance of changes to correct prior incorrect transactions. There is a potential issue of dual realities that are not aligned with one another regarding supply chain information and titles. There is one version of reality recorded in the public blockchains. The second reality may be created in accordance with the officials and decisions of legal regimes. In case these two versions are misaligned, for instance, who owns the title of an electronic B/L protected by public chains, the question arises then how to align these realities in a way that would be acceptable for all the supply chain stakeholders.

Researchers have envisioned two possible approaches. One approach is to introduce regulators and government authorities as special users to the system, who can modify information stored in a distributed ledger under concern to reflect the decisions of legal and government authorities. This is achievable for private or permissioned ledgers where participants are known and authorized. This approach is difficult to implement for public chains. A plausible approach is to enforce decisions of authorities by pursuing the specific users and forcing them to include changes in the public chains themselves. Both approaches likely have their limitations. For instance, the second approach may cause concerns of deanonymization and jurisdictional issues, which may reduce its effectiveness.

8.4. Strategy for blockchain consortia and global cooperation

Harmonizing legal status of electronic trade information and blockchains may take significant amount of time before it is approved and enacted by different jurisdictions. Meanwhile, global trade and supply chain industries may leverage the blockchain consortium for creating governance policies and playbooks for permissioned supply chain ledgers.

Such playbooks would require any stakeholders admitted to the permissioned ledger to agree on a set of policies that govern any electronic trade information and any electronic documents of title held in connection with any trade transaction on the permissioned ledger. This likely will provide market participants certain guarantee of certainty over the use of electronic documents of title registered via distributed ledgers, and may facilitate adoption of the distributed ledger technology in global trade.

If properly managed, such strategy may help SME adopt emerging technologies for cross border trade and supply chain management because resources and costs could be shared in such a model. The industry consortium needs to focus on reducing adoption cost, for small and media enterprise instead of increasing the cost by paying high cost membership fees.

8.5. Public and private dialogue regarding emerging technologies

As electronic trade documents are often shared between private sector supply chain stakeholders and regulatory authorities, a constructive public-private partnership between policy makers and the private sector could facilitate to create frameworks that may harmonize the development and future adoption of emerging technologies.

There exist many blockchain alliances and consortia targeting supply chain market participants. These blockchain consortia often are led by private sector entities. In the majority cases, these consortia are sector specific. There are questions how the regulatory authorities and border related agencies coordinate and interact with these blockchain consortia to make sure that the developed solutions cater to the regulators' needs, fit with government's agenda regarding emerging technologies, and the deployed system could work with regulators' operational environments so that the benefits of new technologies can be realized to improve efficiency.

There could be different approaches for the private-public dialogue. Each may have its own pros and cons. In one approach, each major supply chain and trade finance related blockchain consortium could create a dedicated workgroup to tackle the needs and issues related to the regulatory authorities. For instance, a Customs and C.B.R.A workgroup could be setup in a blockchain consortium focusing on cross-border logistics and supply chains. A problem with this model is that there are so many blockchain related industry initiatives. Some financial intermediaries or supply chain entities are members of multiple such blockchain consortia or alliances.

A more efficient and practical approach could be to leverage existing private – public channel such as COAC to facilitate dialogue between the private sectors and the regulatory authorities regarding emerging technologies. This would avoid repeated efforts dealing with each blockchain consortium separately for discussing the same issue of concerns to the regulatory authorities.

However, different partnering agencies may have different engagement strategies. For instance, The FDA and USDA may have their own private – public channels to engage with the private sector distributed ledger initiatives on food safety, agriculture supply chains, and pharmaceutical products. It is an open question what would be the best model to address the need of agencies regarding this new technology, and optimize the cooperation efforts between the private sector stakeholders and the regulatory agencies.

8.6. Evolution vs. revolution

Prior efforts on trade facilitation using digital technologies suggest the benefits and success of evolutionary rather than revolutionary based approach. Often, blockchains are considered as transformative technology that can automate supply chain transactions in such a way that may constitute a revolution. A bold vision is to leverage this unique opportunity to switch from documents centered data collection by the regulatory authorities to more information driven or account based data collection model.

On the one hand, supply chain stakeholders are often driven by concerns related to productivity, operational needs, competitive pressure, or customer requirements. This would favor an evolutionary approach instead of rolling out an all-encompassing system. The emerging technologies will be set to be gradually adopted by the industries in order to realize their benefits. The private sector stakeholders and the regulatory authorities may work together to deploy evolutionary prototypes or perform pilot programs in multiple steps to identify adoption issues.

8.7. Technology neutrality

Regardless the policies and best practices developed, technological neutrality perhaps is one of the most essential principles for guiding policy makers regarding new technologies. This means that the regulatory requirements and laws should neither exclude, nor require and assume the use of a particular technology. In a rapidly changing digital and technology environment, the principle should also ensure that future and emerging technologies could be accommodated.

8.8. Development of open standards

At present, a number of efforts exist to advance interoperable and open standard based approaches for distributed ledgers. These include efforts by the UN/CEFACT, the WCO, the W3C, the ISO, the ICC, etc. On the other side, the existence of many sector specific industry consortia, with each one developing platform and technology specific standards for its members, may likely result in multiple isolated eco-systems of distributed ledgers.

To facilitate testing and development of open standard based blockchain solutions for supply chains, a high level governance body, for instance in form of a regional forum could be created. This body could address cross jurisdiction related adoption issues, focus on developing open standards, and facilitate regulatory recognition for the information governed on blockchain supply chains across multiple jurisdictions.

It may also assist coordination of pilot tests and trials of cross border supplies in a region with trade agreements. These pilots and proof-of-concept trials could help the supply chain stakeholders identify policies related issues.

8.9. Data privacy and cyber security laws

Last, but not the least, the aforementioned discussions are by no means comprehensive. There are other governance issues related to electronic signatures, cyber security laws, data privacy regulations (e.g, GDPR), legal liability around a decentralized network, and etc.

9

Conclusion

Global supply chain is a sophisticated ecosystem with many stakeholders and multi-stage transactions that occur in multiple jurisdictions. The complexity results in enormous challenges in maintaining the flow of the supply chain information, data, and documents, which causes severe problems in terms of supply chain efficiency, visibility and transparency.

The existing document centric process for exchanging the supply chain data between the supply chain stakeholders as well as between the importers with Customs and regulatory agencies can be improved regarding data quality, process automation, data integrity, data validation, efficiency, administrative cost, etc.

Blockchain is a technology capable of providing a global view of the supply chain without using a traditional centralized infrastructure. As such, it holds the potential to improve efficiency in the global supply chain, facilitate data sharing and data exchange among the stakeholders including regulatory authorities and Customs, ensure compliance with the trade laws, and facilitate legitimate cross-border commerce.

In this report, we studied the opportunities leveraging blockchains and related distributed ledger technologies for transforming the entry process.

At the highest level, blockchains when applied to the supply chain, logistics and trade finance industries, could lead to a unified framework for achieving information flow cooperation between financial intermediaries, suppliers, importers, brokers, accredited bodies, government agencies, Customs, regulatory authorities, etc. It could enable the entry process to be more integrated with the information flows of the international supply chains. With distributed ledgers as the enabling technologies, a data cooperative ecosystem where the four business areas including commercial, logistical, financial, and regulatory, could be harmonized to provide a uniform view of supply chain information, which could lead to trade facilitation and improved Customs control.

Entry related information could be shared right after it is created and lodged to a common supply chain ledger. The process will be more information driven instead of document driven in comparison to the existing process for declaration. The information lodged in the common ledger can be validated automatically and audited by the supply chain stakeholders. As such its quality and accuracy are assured. When combined with the tamper proof nature and record immutability provided by the blockchains, the result will enhance Customs capabilities in risk management and optimizing resources to focus on the high risk imports.

With supply chain information lodged in the common ledgers, it offers further opportunities to simplify and automate the entry process by integrating the Single Window environment with the supply chain blockchain ecosystem.

In this report, we analyzed how entry process could be affected or changed under the five major groups of Single Window business process including, registration of AEOs, managing LPCOs, data collection from the blockchains, advance sharing of commercial data, declaration/report, and post release compliance verification. There are opportunities to integrate with or apply blockchains at each phase of the entry data collection and processing.

The technology itself is still evolving. The landscape of enabling technologies for distributed ledgers could look very different in the next few years compared to today. Significant effort has been spent on addressing some of the identified challenges such as scalability, throughput limitation, assurance of data privacy protection, interoperability, standardization, etc. There is significant recent progress in these frontiers so hopefully in the near future, blockchain implementation will be able to deliver performance on a par with today's ICT infrastructures used for supply chain management at acceptable cost.

Very likely, blockchains and distributed ledgers will not replace the existing systems for managing supply chains. Instead, the technologies may be integrated with the existing operational environments in terms of both ICT infrastructure and business process. Blockchain assisted information flow of supply chain data could be integrated with the existing ERP systems, and the Single Window platform. The emerging Blockchain-as-a-Service model promises further integration of distributed ledgers with the successful cloud computing framework, and other rapidly growing areas such as IoTs and big data analytics.

Consortium has become a popular model for supporting industrial blockchain projects and developing blockchain ecosystems for the global trade. A blockchain consortium often targets a specific industry sector in the global supply chain, for instance, trade finance, freight forwarding, retail, or manufacturing. There are both opportunities and challenges for the consortium model to succeed. The risk lies in potential isolation and fragmentation where a small group of companies develop their own standards and processes for supply chains, which creates friction in supply chain information flows and hampers interoperability – jeopardizing the promises of blockchains to achieve supply chain visibility and transparency.

International organizations including the ISO, the WCO, the UN/CEFACT, the W3C, etc. may play crucial role to facilitate development of standards for the distributed ledgers in the context of global trade. Many organizations have initiated blockchain related programs towards achieving the goal to enable interoperability, resource discovery, and standards for distributed ledgers. Since majority of these programs were recently created, it will take some time before fruits of these efforts are made available to the global trade community.

In addition, government agencies could play a vital role to facilitate adoption of standards by the private sector blockchain initiatives because often it is of the best interests to the government stakeholders to use interoperable and standard based approaches for data sharing.

Successful adoption of the blockchain technologies by the global trade community depends on many factors including legal, governance, policy challenges that have to be overcome. Blockchains are facing some of the similar legal challenges that paperless trade and supply chain digitalization have experienced in the past. The regulations regarding legal status of electronic trade documents need to be harmonized and uniform in order to reduce uncertainty and improve confidence in the supply chain stakeholders so they are more willing to adopt emerging technologies that digitize and automate supply chain information flow. Cooperation across jurisdictions is critical to the development of uniform policies and regulations regarding trade and supply chain data over the blockchains.

To make sure that the developed blockchain supply chain platforms cater to the regulators' needs, and fit with government's agenda regarding emerging technologies, private sector and government stakeholders should work together to define how distributed ledger platforms for trade, developed under the private sector initiatives, can interact with the regulators' operational environment so that a seamless and smooth data pipeline for entry data can be implemented to realize the benefits of blockchains.

For such private and public dialogue, an efficient and practical approach is to leverage the existing private – public channel such as the COAC to facilitate interactions between the private sectors and the regulatory authorities regarding this technology. This would avoid repeated efforts dealing with each blockchain consortium separately for discussing the same issue of concerns.

The trade community is open to the changes such as entry process integrated with the blockchains. For such new system, protection of data confidentiality in distributed ledger environment needs to be considered as a top priority. With increased amount of data pulled from the blockchains, it requires new tools to map, filter, link, and process the data. The process needs to be transparent to the filers and brokers so that they will be able to assist and certify the information. Currently, there is missing link between the supply chain ledgers and the Single Window environment that could be addressed through the private – public relation regarding blockchain development and standardization.

Regarding possible future directions of research: some specific areas include but not limited to:

- Developing and testing a prototype implementation that could demonstrate the information driven entry process as described in this report.

- Implementing a prototype to demonstrate data collection from multiple heterogeneous supply chain ledgers and integration of the collected data with entry process.
- Modeling blockchain based information flow and business process for the PGAs.
- Extending the work to e-commerce use cases of blockchains for entry process.

Overall, blockchains as potentially transformative technology, provide both opportunities and challenges to further modernize the entry process and how Customs interacts with the global supply chain information flow in future. Success of applying such technology hinge on joint and collaborative efforts between the trade community, government stakeholders, regulators, policy makers, and academics.

Appendices

A

Appendix: List of Brainstorm Ideas

This appendix summarizes ideas from the brainstorming sessions.

The list below focuses enhancement of missions relevant to Customs, and regulatory agencies.

- Proactive collection of data (start from trade agreement process between importer and exporter including purchase orders).
- Applying blockchain for real-time sharing of GSM and 10+2 shipping data with customs.
- Data can be shared at element level (see Boston Consulting 2017 break down of data elements and documents for trade finance – apply similar ontology and data linage analysis to entry data) right after it is created during interactions between global supply chain stakeholders (over blockchain).
- Create a data matrix that maps entry data elements to stakeholders (buyer, seller, shipper, 3PL, bank, freight forwarder) and documents (purchase, invoices, B/L, packing list).
- Embed entry data collection process to blockchain based supply chain process (reduce direct interaction with customs, data available on the chain after each step of import activities).
- Targeting early (timeliness) as data elements of interests to customs are shared on the chain (within relevant stakeholders and with customs) – identify high risk import activity or shipping ahead of current submission time for entry.
- Using blockchain for ordering events and decisions (for instance, cancellation, hold decision by PGAs) – single order of certified actions or decisions (when, what and by whom).

- Applying blockchain as shared bulletin or message board (e.g., disseminating entry related messages to PGAs).
- Leveraging automated data synchronization capability of blockchain for interagency entry data management/sharing (also with Port of Entry?).
- Improving post entry audit with stakeholder data recorded on the chain (cannot be altered at later time), in particular financial transactions such as payments, transfer between importer bank and exporter bank, other related financial transactions.
- Possible benefits for detecting transfer price or profit shift when using blockchain as shared data platform – banks, customs, tax.
- Detecting trade money laundering fraud.
- Blockchain as an enabler for realizing continuous audit (a relatively new audit concept – automated audit process, possibly based on real-time data).
- Automatic collection of duty payment and fees (self-execution) – in particular for e-commerce.
- Fulfilling record keeping requirements.
- Possible application to valuation and detection of mis-invoices through data cooperation with trade finance blockchains.
- Recording advance ruling on blockchain (faster clearance).
- Using blockchain to manage certificates (from export customs to import customs) – different scenarios for inter-government blockchain data sharing.
- Integration with data produced by IoTs (sensors, scanners, smart phone apps).
- Integration with AI, many examples (AI used for classification, AI based risk assessment, AI use case for linking MIDs – export side and import side).
- Leveraging potential cost sharing model between trade and customs (include development cost – consortium based; operation cost – nodes maintained by trade; enhancement cost – adding new features).

The list below focuses impacts/implications to the trade side processes.

- Integration with existing ERP (mentioned in many studies).
- Decision to adopt and participate in environment that comprises competitors (Deloitte survey study).
- Already documented benefits of applying blockchain outside customs (time, administration cost, errors) - any change when adding customs to the equation (entry process)?
- Consolidation of databases, payment process (smart L/C), etc.

B

Appendix: Figures

Hyperledger Fabric applies a concept, called channel, to enable privacy among participants. The channel setup was complicated and they do not scale well at this moment. Using transactions between banks as a use case, below describes how Hyperledger channel is setup, see Figure B.1.

To enable privacy among participants, a channel is established, and network participants subscribe to the channel. In our model, if only "bank 1" and "bank 2" subscribe to a channel, only "bank 1" and "bank 2" have access to the transactions they are party to. However, even in our simple model, we observed that construction with three "banks" and a "supervisory node" required at least three channels for bilateral transactions, where the "supervisory node" is subscribed to each channel to "listen" to all transactions. In fact, any number of nodes can be subscribed to a channel with the understanding that all channel participants will receive the transaction details related to that channel. But this creates a problem.

In channel architecture, if three parties, let's call them "Alice," "Bob," and "Claire," are involved in a one-time transaction, a unique channel would need to be established. But if Alice and Bob continue to transact, and Claire is not involved any longer, Claire continues to have access to the transaction records of Alice and Bob, whether they pertain to her or not. To prevent this, another channel would need to be created between Alice and Bob only. Meanwhile, the original three-party channel would exist as a separate ledger until removed from the network or deleted.

When there are hundreds of entities on a given network, the number of potential channels multiplies exponentially, as does the effort to manage them. The considerable trade-offs that come with either including all transactions in one channel or creating separate channels for each group of transacting entities means that neither option may be desirable.

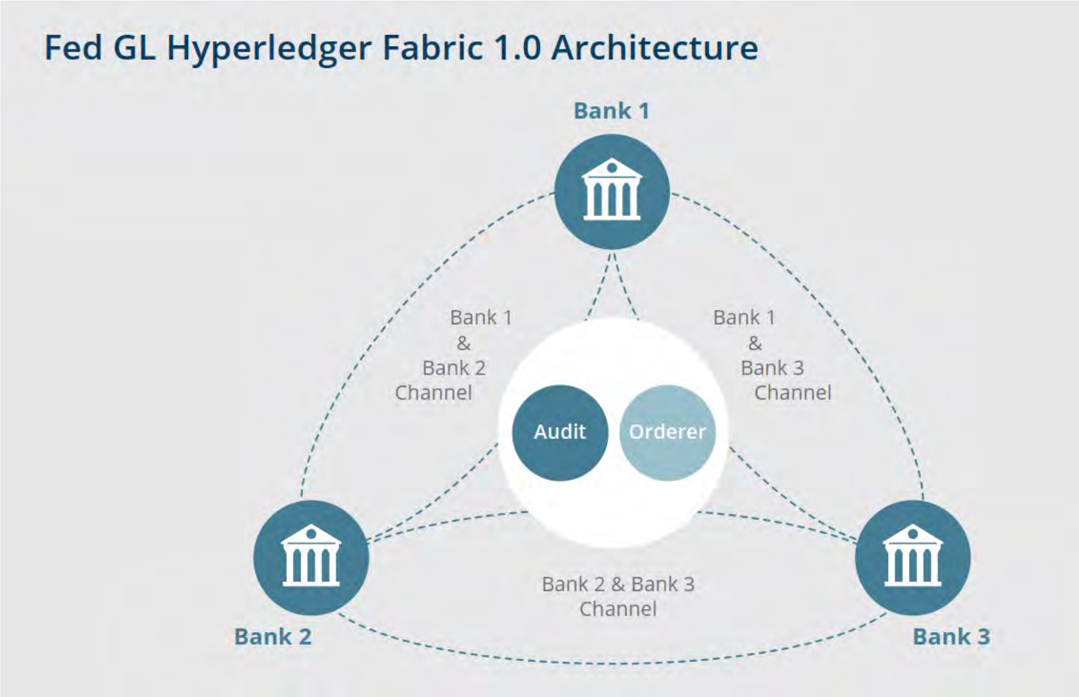


Figure B.1: Hyperledger channel.

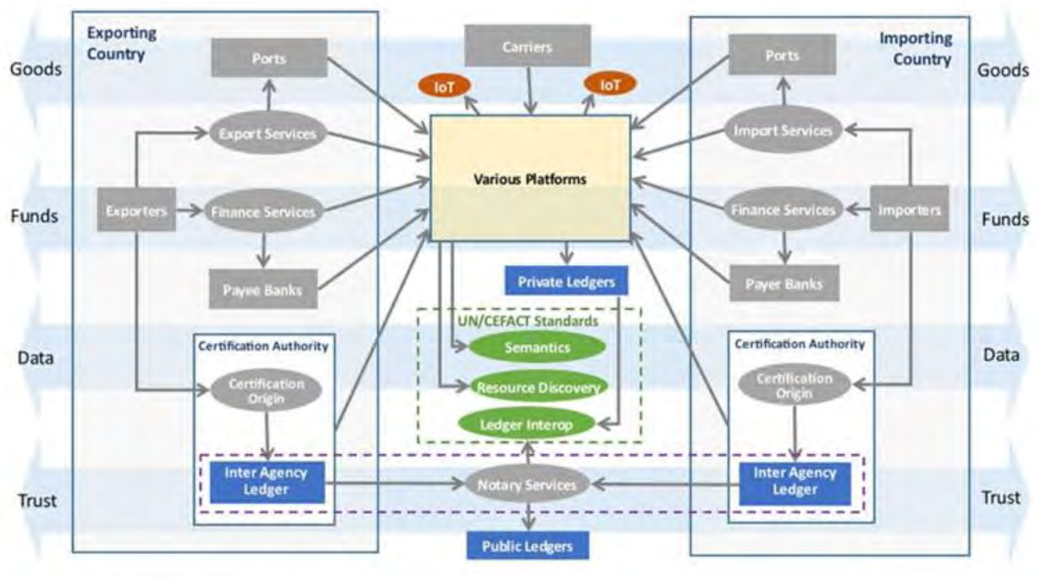
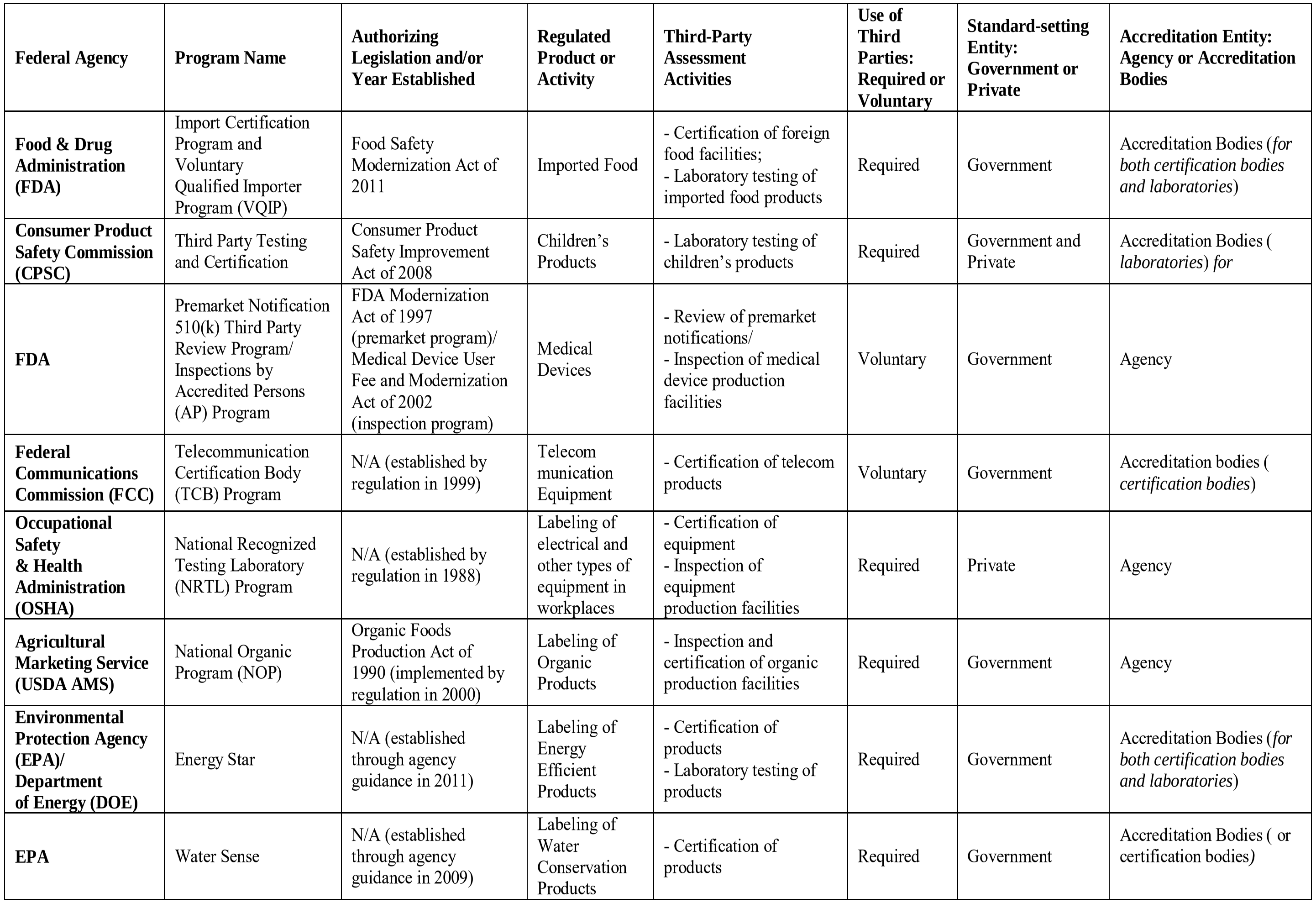


Figure B.2: The UN/CEFACT blockchain architecture diagram. It shows a high level view of integration with the UN/CEFACT standards.



Federal Agency	Program Name	Authorizing Legislation and/or Year Established	Regulated Product or Activity	Third-Party Assessment Activities	Use of Third Parties: Required or Voluntary	Standard-setting Entity: Government or Private	Accreditation Entity: Agency or Accreditation Bodies
Food & Drug Administration (FDA)	Import Certification Program and Voluntary Qualified Importer Program (VQIP)	Food Safety Modernization Act of 2011	Imported Food	- Certification of foreign food facilities; - Laboratory testing of imported food products	Required	Government	Accreditation Bodies (*for both certification bodies and laboratories*)
Consumer Product Safety Commission (CPSC)	Third Party Testing and Certification	Consumer Product Safety Improvement Act of 2008	Children's Products	- Laboratory testing of children's products	Required	Government and Private	Accreditation Bodies (*laboratories*) *for*
FDA	Premarket Notification 510(k) Third Party Review Program/ Inspections by Accredited Persons (AP) Program	FDA Modernization Act of 1997 (premarket program)/ Medical Device User Fee and Modernization Act of 2002 (inspection program)	Medical Devices	- Review of premarket notifications/ - Inspection of medical device production facilities	Voluntary	Government	Agency
Federal Communications Commission (FCC)	Telecommunication Certification Body (TCB) Program	N/A (established by regulation in 1999)	Telecom munication Equipment	- Certification of telecom products	Voluntary	Government	Accreditation bodies (*certification bodies*)
Occupational Safety & Health Administration (OSHA)	National Recognized Testing Laboratory (NRTL) Program	N/A (established by regulation in 1988)	Labeling of electrical and other types of equipment in workplaces	- Certification of equipment - Inspection of equipment production facilities	Required	Private	Agency
Agricultural Marketing Service (USDA AMS)	National Organic Program (NOP)	Organic Foods Production Act of 1990 (implemented by regulation in 2000)	Labeling of Organic Products	- Inspection and certification of organic production facilities	Required	Government	Agency
Environmental Protection Agency (EPA)/ Department of Energy (DOE)	Energy Star	N/A (established through agency guidance in 2011)	Labeling of Energy Efficient Products	- Certification of products - Laboratory testing of products	Required	Government	Accreditation Bodies (*for both certification bodies and laboratories*)
EPA	Water Sense	N/A (established through agency guidance in 2009)	Labeling of Water Conservation Products	- Certification of products	Required	Government	Accreditation Bodies (or certification bodies*)*

Figure B.3: A list agencies and third party programs.

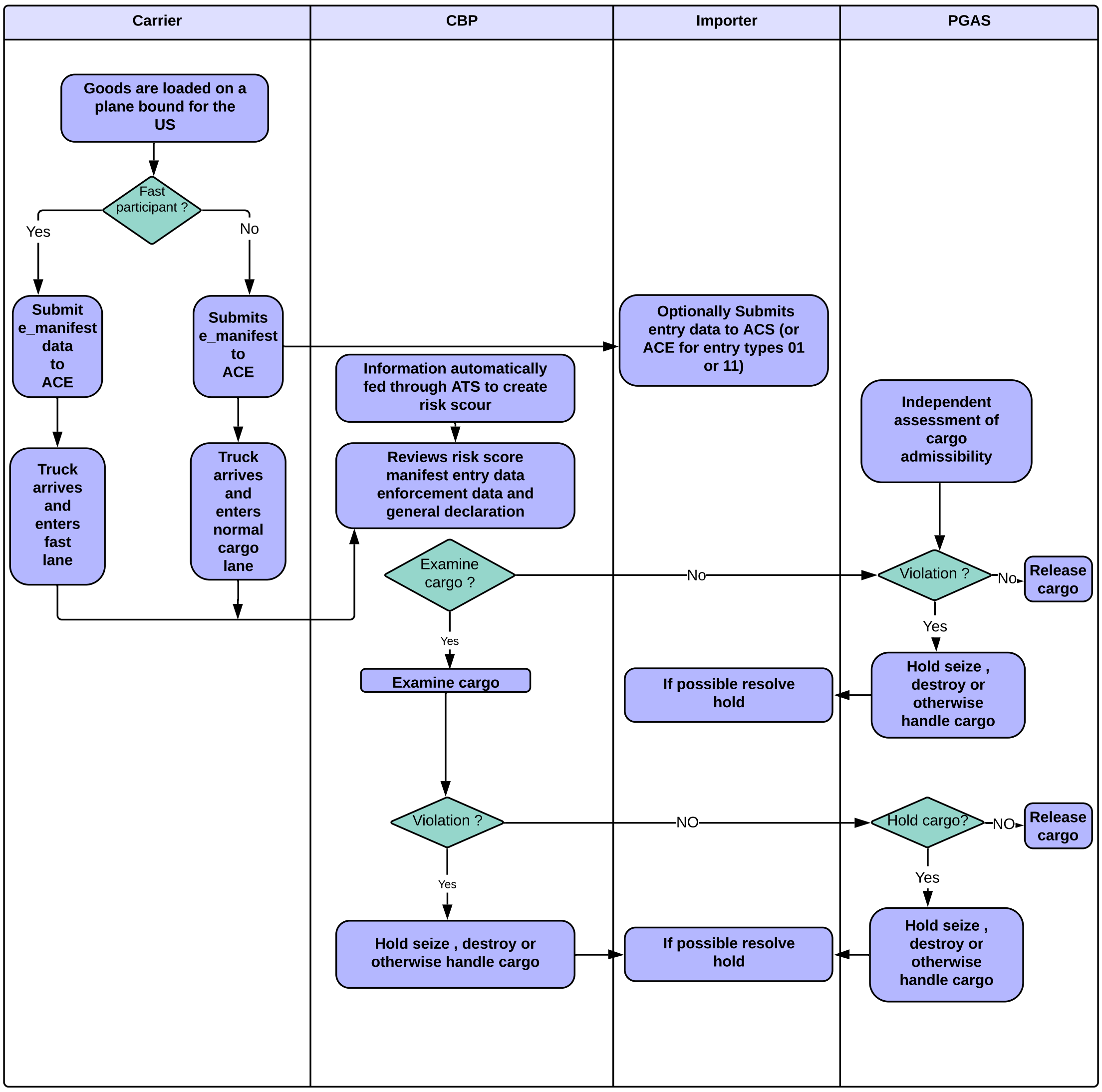

Carrier
CBP
Importer
PGAS
Goods are loaded on a plane bound for the US
Fast participant ?
Yes
No
Submit e_manifest data to ACE
Submits e_manifest to ACE
Truck arrives and enters fast lane
Truck arrives and enters normal cargo lane
Information automatically fed through ATS to create risk scour
Reviews risk score manifest entry data enforcement data and general declaration
Optionally Submits entry data to ACS (or ACE for entry types 01 or 11)
Independent assessment of cargo admissibility
Examine cargo ?
No
Violation ?
No
Release cargo
Yes
Yes
Examine cargo
If possible resolve hold
Hold seize , destroy or otherwise handle cargo
Violation ?
NO
Hold cargo?
NO
Release cargo
Yes
Yes
Hold seize , destroy or otherwise handle cargo
If possible resolve hold
Hold seize , destroy or otherwise handle cargo

Figure B.4: Cargo release process diagram: Land. (Source: CBP)

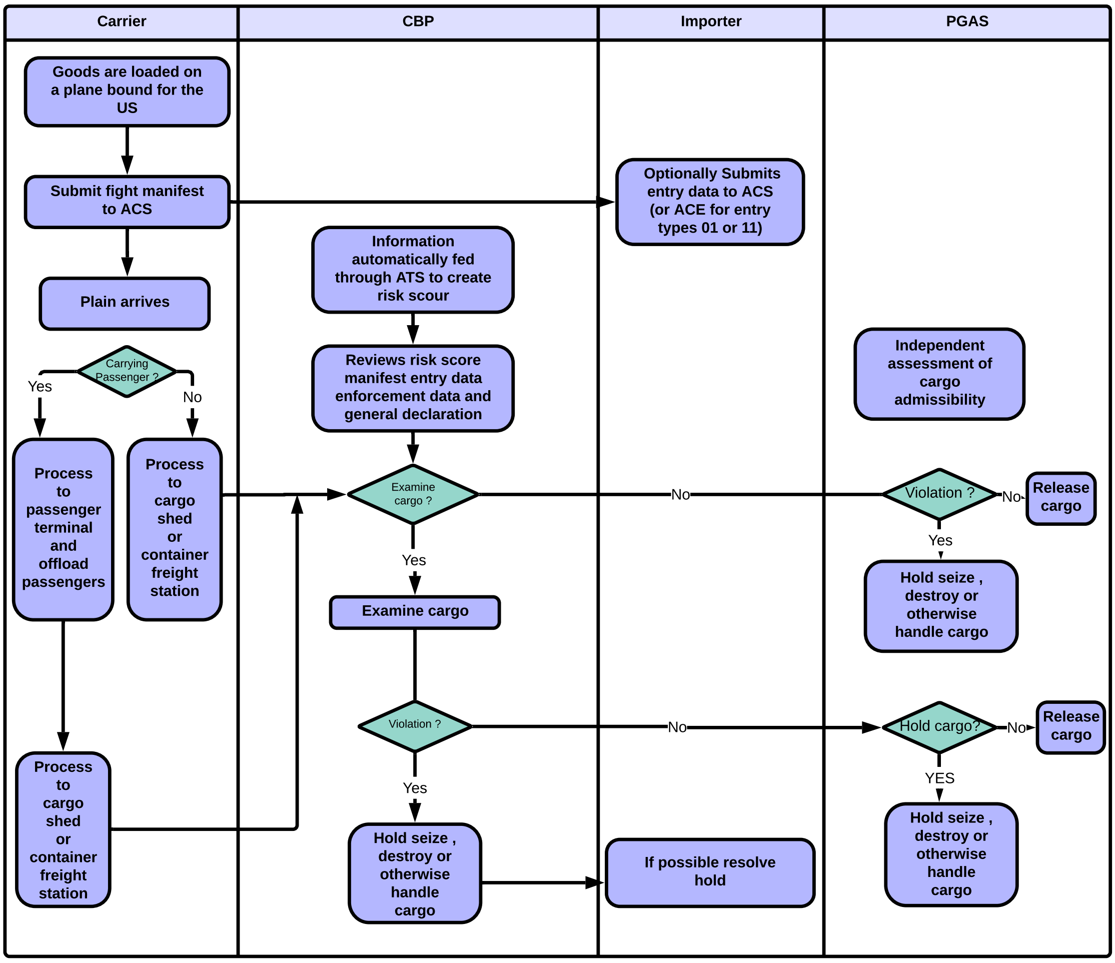

Carrier
CBP
Importer
PGAS
Goods are loaded on a plane bound for the US
Submit fight manifest to ACS
Plain arrives
Carrying Passenger ?
Yes
No
Process to passenger terminal and offload passengers
Process to cargo shed or container freight station
Process to cargo shed or container freight station
Optionally Submits entry data to ACS (or ACE for entry types 01 or 11)
Information automatically fed through ATS to create risk scour
Reviews risk score manifest entry data enforcement data and general declaration
Examine cargo ?
No
Yes
Examine cargo
Violation ?
No
Yes
Hold seize , destroy or otherwise handle cargo
If possible resolve hold
Independent assessment of cargo admissibility
Violation ?
No
Release cargo
Yes
Hold seize , destroy or otherwise handle cargo
Hold cargo?
No
Release cargo
YES
Hold seize , destroy or otherwise handle cargo

Figure B.5: Cargo release process diagram: Air cargo. (Source: CBP)

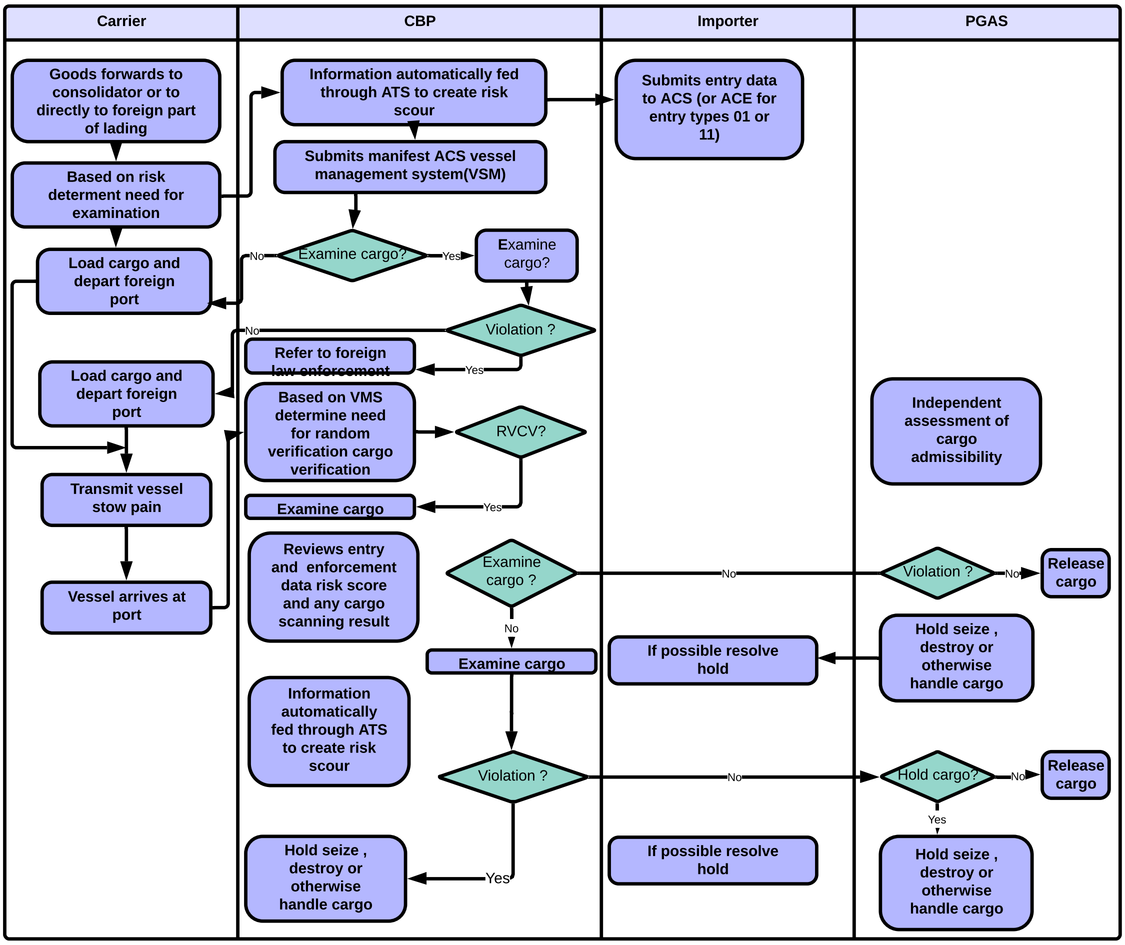

Carrier
CBP
Importer
PGAS
Goods forwards to consolidator or to directly to foreign part of lading
Based on risk determent need for examination
Load cargo and depart foreign port
Load cargo and depart foreign port
Transmit vessel stow pain
Vessel arrives at port
Information automatically fed through ATS to create risk scour
Submits manifest ACS vessel management system(VSM)
Examine cargo?
No
Yes
Examine cargo?
Violation ?
No
Refer to foreign law enforcement
Yes
Based on VMS determine need for random verification cargo verification
RVCV?
Examine cargo
Yes
Reviews entry and enforcement data risk score and any cargo scanning result
Examine cargo ?
No
Examine cargo
Information automatically fed through ATS to create risk scour
Violation ?
Yes
Hold seize , destroy or otherwise handle cargo
Submits entry data to ACS (or ACE for entry types 01 or 11)
No
If possible resolve hold
No
If possible resolve hold
Independent assessment of cargo admissibility
Violation ?
No
Release cargo
Hold seize , destroy or otherwise handle cargo
Hold cargo?
No
Release cargo
Yes
Hold seize , destroy or otherwise handle cargo

Figure B.6: Cargo release process diagram: Ocean. (Source: CBP)

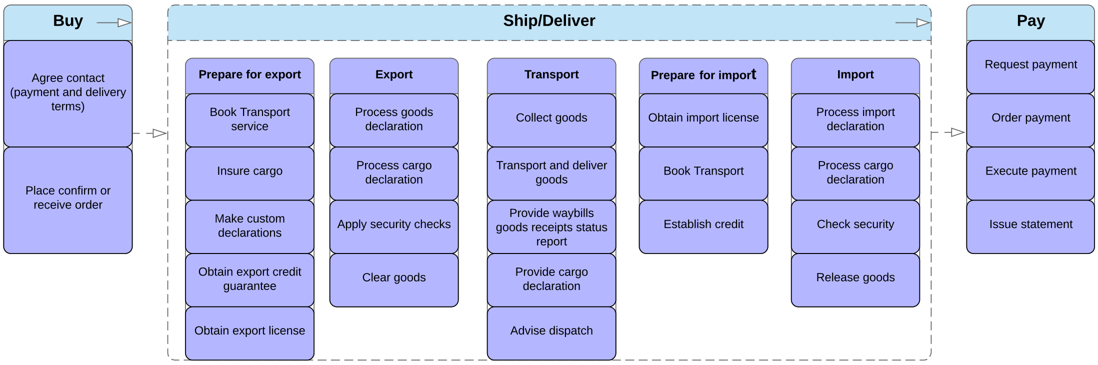


Figure B.7: The Buy-Ship-Pay model for modeling trade.

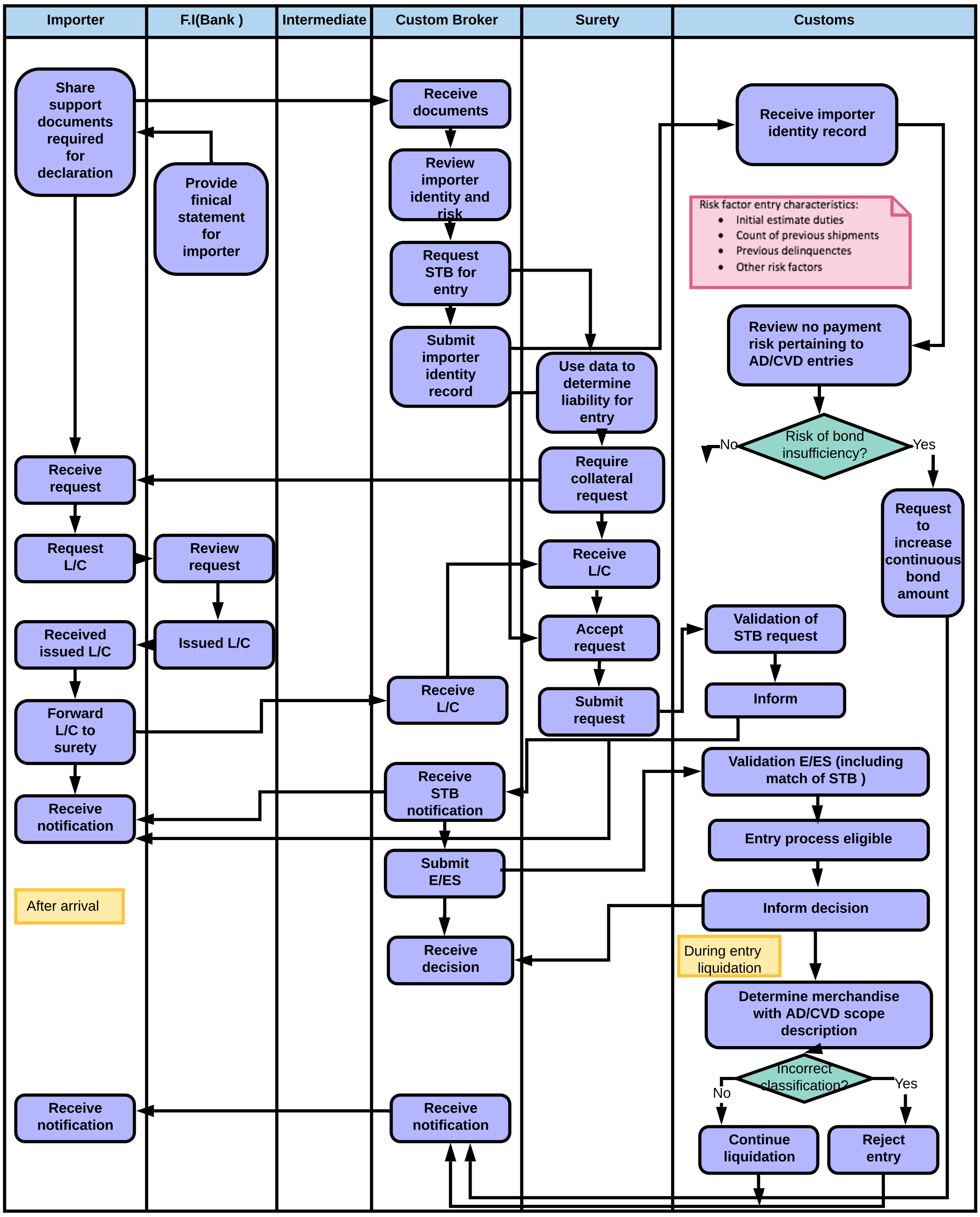

Importer
F.I(Bank)
Intermediate
Custom Broker
Surety
Customs
Share support documents required for declaration
Provide finical statement for importer
Receive documents
Review importer identity and risk
Request STB for entry
Submit importer identity record
Receive importer identity record
Risk factor entry characteristics:
Initial estimate duties
Count of previous shipments
Previous delinquenctes
Other risk factors
Review no payment risk pertaining to AD/CVD entries
Use data to determine liability for entry
Risk of bond insufficiency?
No
Yes
Require collateral request
Request to increase continuous bond amount
Receive request
Request L/C
Review request
Receive L/C
Accept request
Validation of STB request
Received issued L/C
Issued L/C
Receive L/C
Submit request
Inform
Forward L/C to surety
Receive STB notification
Validation E/ES (including match of STB)
Receive notification
Entry process eligible
Submit E/ES
After arrival
Inform decision
Receive decision
During entry liquidation
Determine merchandise with AD/CVD scope description
Incorrect classification?
No
Yes
Receive notification
Receive notification
Continue liquidation
Reject entry

Figure B.8: A simple process diagram on bonding and AD/CVD risk assessment.

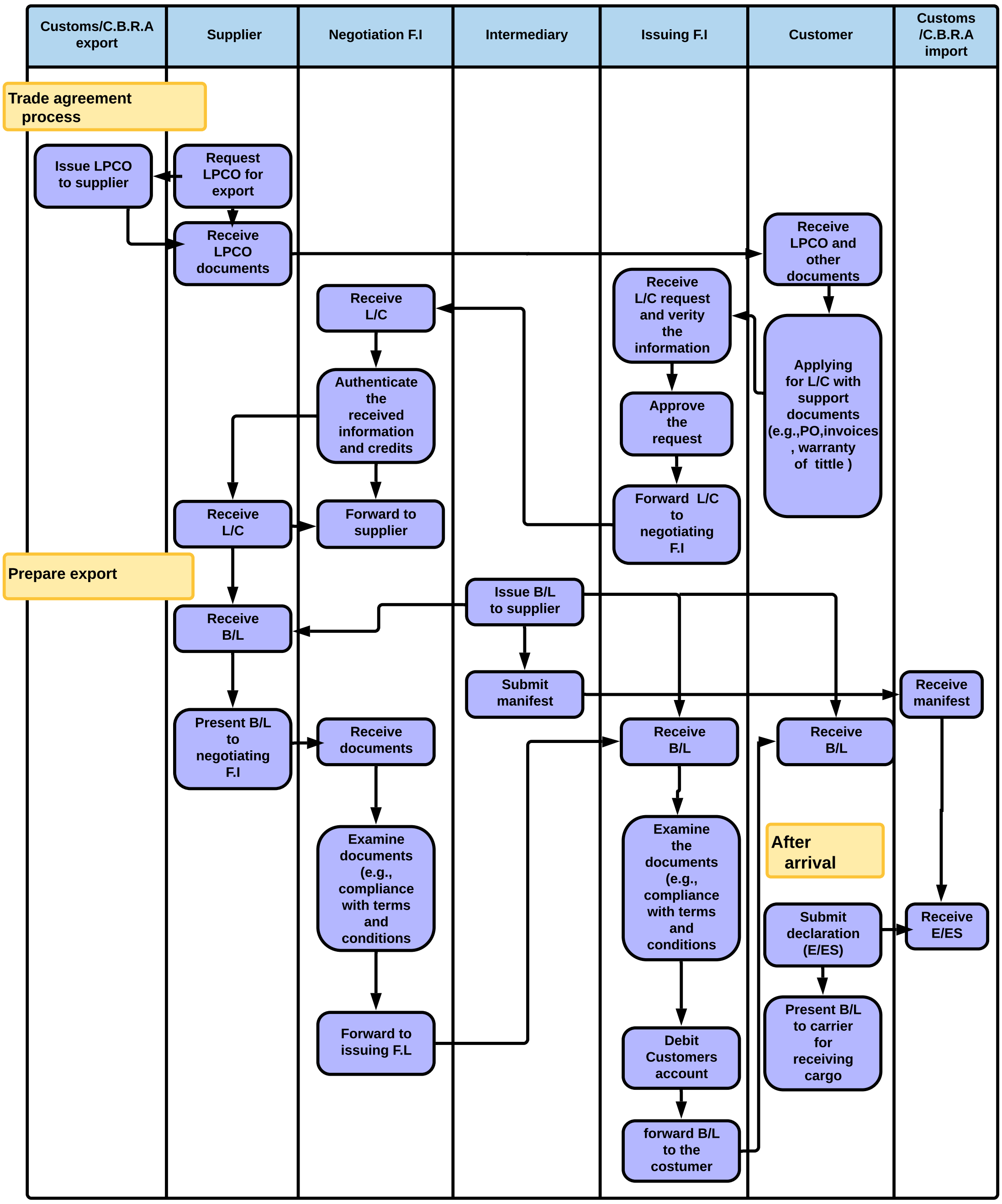

Customs/C.B.R.A export
Supplier
Negotiation F.I
Intermediary
Issuing F.I
Customer
Customs /C.B.R.A import
Trade agreement process
Issue LPCO to supplier
Request LPCO for export
Receive LPCO documents
Receive LPCO and other documents
Receive L/C
Receive L/C request and verity the information
Applying for L/C with support documents (e.g.,PO,invoices , warranty of tittle)
Authenticate the received information and credits
Approve the request
Receive L/C
Forward to supplier
Forward L/C to negotiating F.I
Prepare export
Issue B/L to supplier
Receive B/L
Submit manifest
Receive manifest
Present B/L to negotiating F.I
Receive documents
Receive B/L
Receive B/L
Examine documents (e.g., compliance with terms and conditions
Examine the documents (e.g., compliance with terms and conditions
After arrival
Submit declaration (E/ES)
Receive E/ES
Forward to issuing F.L
Debit Customers account
Present B/L to carrier for receiving cargo
forward B/L to the costumer

Figure B.9: A simple process diagram for document based trade finance.

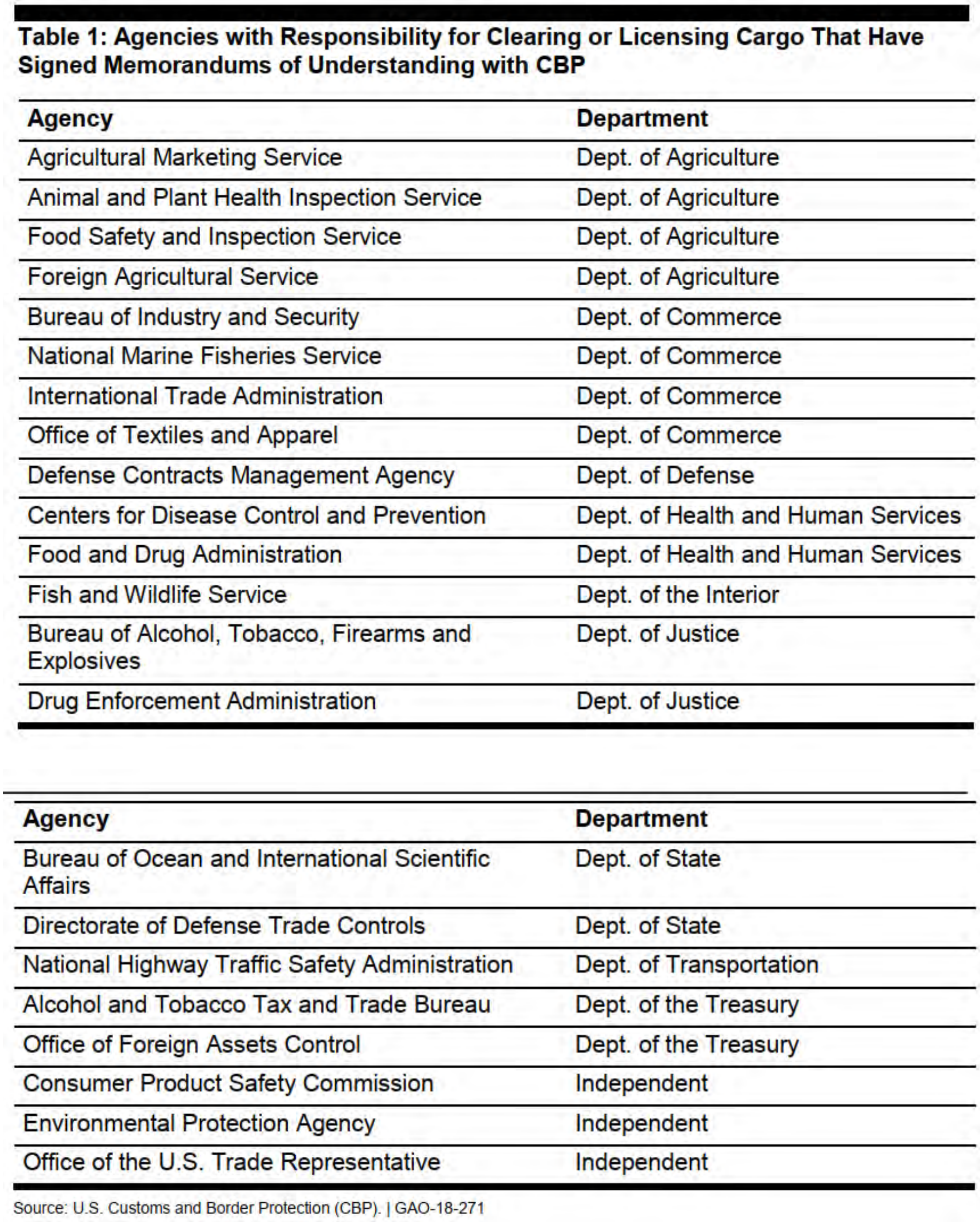


Table 1: Agencies with Responsibility for Clearing or Licensing Cargo That Have Signed Memorandums of Understanding with CBP

Agency	Department
Agricultural Marketing Service	Dept. of Agriculture
Animal and Plant Health Inspection Service	Dept. of Agriculture
Food Safety and Inspection Service	Dept. of Agriculture
Foreign Agricultural Service	Dept. of Agriculture
Bureau of Industry and Security	Dept. of Commerce
National Marine Fisheries Service	Dept. of Commerce
International Trade Administration	Dept. of Commerce
Office of Textiles and Apparel	Dept. of Commerce
Defense Contracts Management Agency	Dept. of Defense
Centers for Disease Control and Prevention	Dept. of Health and Human Services
Food and Drug Administration	Dept. of Health and Human Services
Fish and Wildlife Service	Dept. of the Interior
Bureau of Alcohol, Tobacco, Firearms and Explosives	Dept. of Justice
Drug Enforcement Administration	Dept. of Justice
Bureau of Ocean and International Scientific Affairs	Dept. of State
Directorate of Defense Trade Controls	Dept. of State
National Highway Traffic Safety Administration	Dept. of Transportation
Alcohol and Tobacco Tax and Trade Bureau	Dept. of the Treasury
Office of Foreign Assets Control	Dept. of the Treasury
Consumer Product Safety Commission	Independent
Environmental Protection Agency	Independent
Office of the U.S. Trade Representative	Independent

Source: U.S. Customs and Border Protection (CBP). | GAO-18-271

Figure B.10: Partnering agency list. (Source: GAO)

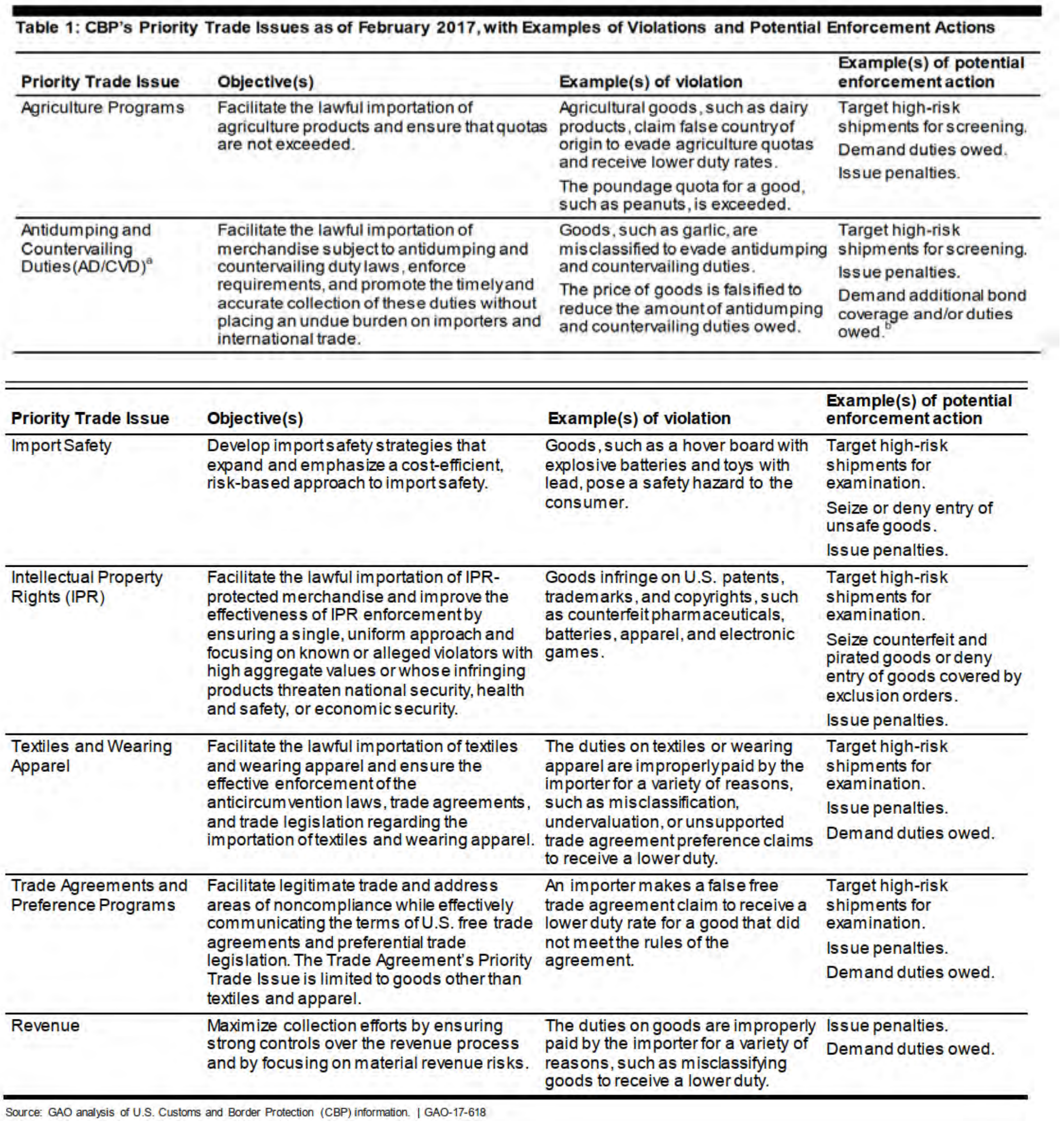


Table 1: CBP's Priority Trade Issues as of February 2017, with Examples of Violations and Potential Enforcement Actions

Priority Trade Issue	Objective(s)	Example(s) of violation	Example(s) of potential enforcement action
Agriculture Programs	Facilitate the lawful importation of agriculture products and ensure that quotas are not exceeded.	Agricultural goods, such as dairy products, claim false country of origin to evade agriculture quotas and receive lower duty rates. The poundage quota for a good, such as peanuts, is exceeded.	Target high-risk shipments for screening. Demand duties owed. Issue penalties.
Antidumping and Countervailing Duties (AD/CVD)[a]	Facilitate the lawful importation of merchandise subject to antidumping and countervailing duty laws, enforce requirements, and promote the timely and accurate collection of these duties without placing an undue burden on importers and international trade.	Goods, such as garlic, are misclassified to evade antidumping and countervailing duties. The price of goods is falsified to reduce the amount of antidumping and countervailing duties owed.	Target high-risk shipments for screening. Issue penalties. Demand additional bond coverage and/or duties owed.[b]
Import Safety	Develop import safety strategies that expand and emphasize a cost-efficient, risk-based approach to import safety.	Goods, such as a hover board with explosive batteries and toys with lead, pose a safety hazard to the consumer.	Target high-risk shipments for examination. Seize or deny entry of unsafe goods. Issue penalties.
Intellectual Property Rights (IPR)	Facilitate the lawful importation of IPR-protected merchandise and improve the effectiveness of IPR enforcement by ensuring a single, uniform approach and focusing on known or alleged violators with high aggregate values or whose infringing products threaten national security, health and safety, or economic security.	Goods infringe on U.S. patents, trademarks, and copyrights, such as counterfeit pharmaceuticals, batteries, apparel, and electronic games.	Target high-risk shipments for examination. Seize counterfeit and pirated goods or deny entry of goods covered by exclusion orders. Issue penalties.
Textiles and Wearing Apparel	Facilitate the lawful importation of textiles and wearing apparel and ensure the effective enforcement of the anticircumvention laws, trade agreements, and trade legislation regarding the importation of textiles and wearing apparel.	The duties on textiles or wearing apparel are improperly paid by the importer for a variety of reasons, such as misclassification, undervaluation, or unsupported trade agreement preference claims to receive a lower duty.	Target high-risk shipments for examination. Issue penalties. Demand duties owed.
Trade Agreements and Preference Programs	Facilitate legitimate trade and address areas of noncompliance while effectively communicating the terms of U.S. free trade agreements and preferential trade legislation. The Trade Agreement's Priority Trade Issue is limited to goods other than textiles and apparel.	An importer makes a false free trade agreement claim to receive a lower duty rate for a good that did not meet the rules of the agreement.	Target high-risk shipments for examination. Issue penalties. Demand duties owed.
Revenue	Maximize collection efforts by ensuring strong controls over the revenue process and by focusing on material revenue risks.	The duties on goods are improperly paid by the importer for a variety of reasons, such as misclassifying goods to receive a lower duty.	Issue penalties. Demand duties owed.

Source: GAO analysis of U.S. Customs and Border Protection (CBP) information. | GAO-17-618

Figure B.11: CBP priority trade issues. (Source: CBP and GAO)

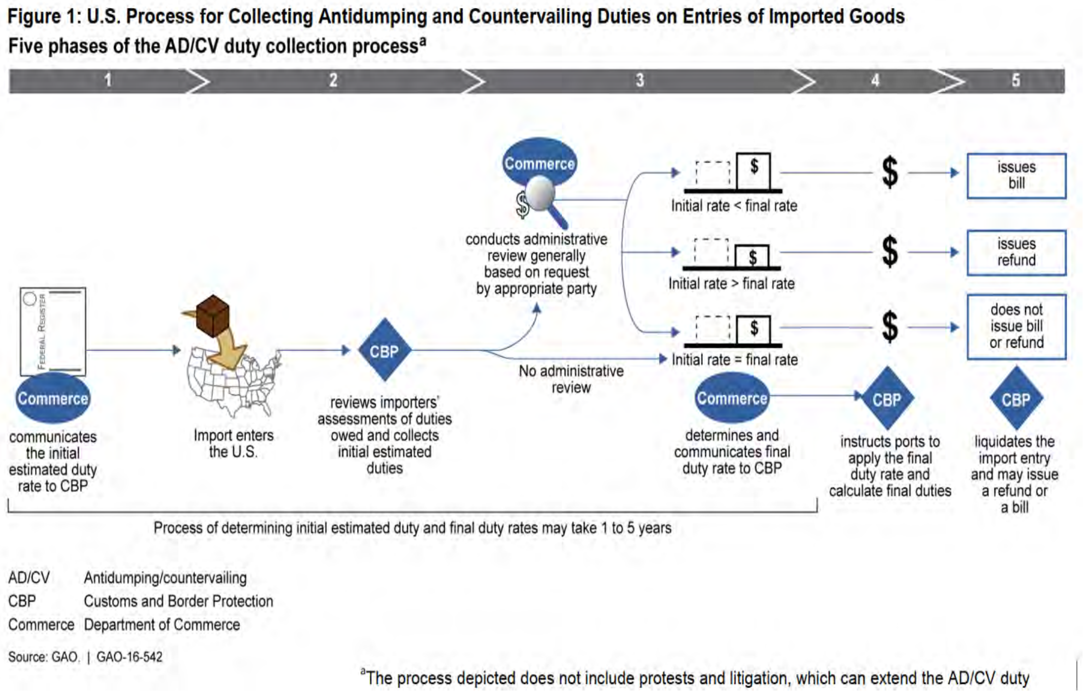


Figure 1: U.S. Process for Collecting Antidumping and Countervailing Duties on Entries of Imported Goods
Five phases of the AD/CV duty collection process^a
1
2
3
4
5
Federal Register
Commerce
communicates the initial estimated duty rate to CBP
Import enters the U.S.
CBP
reviews importers' assessments of duties owed and collects initial estimated duties
Commerce
conducts administrative review generally based on request by appropriate party
No administrative review
$
Initial rate < final rate
Initial rate > final rate
Initial rate = final rate
issues bill
issues refund
does not issue bill or refund
Commerce
determines and communicates final duty rate to CBP
CBP
instructs ports to apply the final duty rate and calculate final duties
CBP
liquidates the import entry and may issue a refund or a bill
Process of determining initial estimated duty and final duty rates may take 1 to 5 years
AD/CV Antidumping/countervailing
CBP Customs and Border Protection
Commerce Department of Commerce
Source: GAO. | GAO-16-542
^{a}The process depicted does not include protests and litigation, which can extend the AD/CV duty

Figure B.12: Process for collecting AD/CVD on entries of imported goods. (Source: GAO)

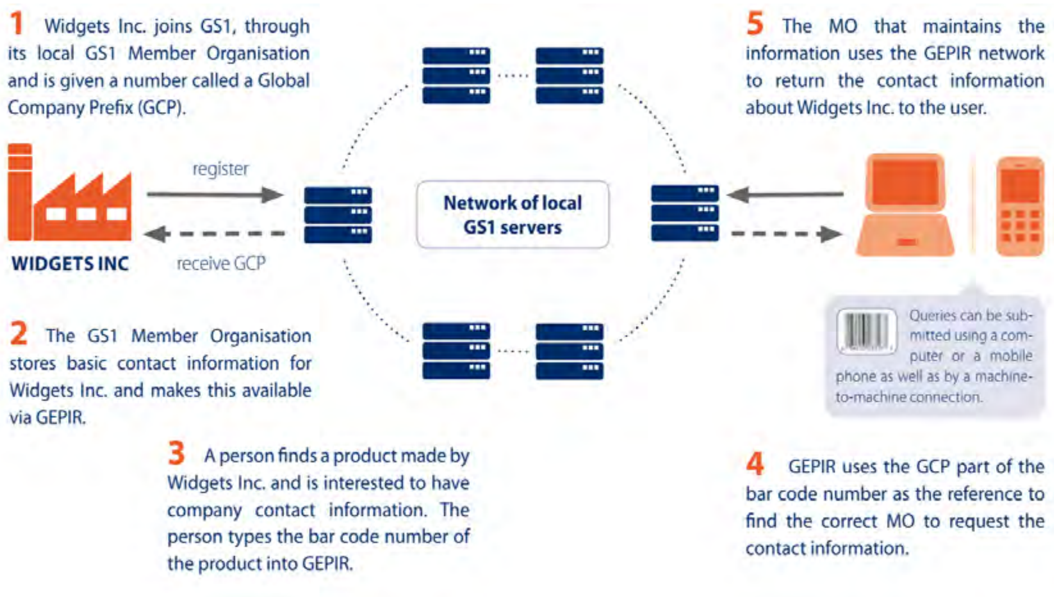

1 Widgets Inc. joins GS1, through its local GS1 Member Organisation and is given a number called a Global Company Prefix (GCP).
WIDGETS INC
register
receive GCP
Network of local GS1 servers
2 The GS1 Member Organisation stores basic contact information for Widgets Inc. and makes this available via GEPIR.
3 A person finds a product made by Widgets Inc. and is interested to have company contact information. The person types the bar code number of the product into GEPIR.
4 GEPIR uses the GCP part of the bar code number as the reference to find the correct MO to request the contact information.
5 The MO that maintains the information uses the GEPIR network to return the contact information about Widgets Inc. to the user.
Queries can be submitted using a computer or a mobile phone as well as by a machine-to-machine connection.

Figure B.13: The existing GEPIR infrastructure based on a network of distributed servers. Its services or other similar registration and lookup services of commercial entities and products could benefit from the distributed ledger technology for creating, maintaining, and querying unique identifiers of traders, products, manufacturers, and locations. (Source: GS1)

C

Appendix: Tables

Table C.1: Comparison of onchain vs. offchain storage for different types of trade data.

	Example	Onchain	Offchain
Data	Sales terms, price and currency, quantity, consignment contact, delivery date, L/C issuing bank, packing list, etc.	• Incurring significant performance overhead if stored on chain; • Data needs to be encrypted;	• Can be stored offchain in distributed data stores (e.g., IPFS, DHT, Cloud); • Data is encrypted; • Access to data can be protected with decentralized access control and management; • Data decryption key can be protected with secret sharing.
Data Model	Definitions of classes and attributes, data model schema (e.g., UN/CEFACT data model).	• If stored on chain, may help cross ledger interoperation; • Performance impact negligible if stored onchain; • Possible need to support multiple data models.	• Can be stored offchain; • May require governance to control who can update the data model.
Access policies	Policy defining who can read packing list, and who can create and update packing list.	• Access policies can be stored onchain; • If stored onchain, business relations need to be protected.	• Access policies can be stored offchain.
Hash and commitment	Hash value of packing list, hash value of price and currency.	• Onchain	
Transaction history	History of validated transactions.	• Onchain	

Table C.2: Red flags for financial related risks and business areas. Often, AD/CVD non-payment risks, illicit financial flows, mis-invoicing, and etc. share similar red flags. Blockchains can be applied to share red flag profiles.

	Trade	Logistics	Payment
Nature of goods ordered not match with expected activity of buyer and seller	X		
Change of source patterns	X		
Relation between buyer and seller (transaction parties affiliated)	X		
Payment instructions amended many times			X
Complexity of financial product	X		
Shell company	X		
Discrepancies invoiced value of the goods and the fair market value	X		
L/C contains non-standard clause	X		
B/L goods discrepancy to description in the invoice		X	
Miss info such as port of loading, destination		X	
B/L match with L/C (goods described, quantity)		X	
Packing inconsistent with goods shipped		X	

Table C.3: Summary of desired blockchain characteristics and the enabling technologies.

Confidentiality	Decentralized access management, zero-knowledge proof, multi-party computation
Integrity	Chained blocks, immutable ledger
Authenticity	Decentralized identity management, verifiable credentials
Tamper resistance	Distributed book keeping, consensus based validation
Transparency	Shared ledger
Traceability	Linked transaction history
Efficiency of data synchronization	Improved BFT protocols

D

Appendix: Guided Interview

Questionnaire (Guided Interview)

Questions related to sharing data in advance

If E2E cross border supply chain is adopted by stakeholders to maintain transactions, and technology allows importers, suppliers, and brokers to share entry related data in advance (way ahead of the time as today required, for instance at time when business agreement is made between buyers and sellers, or purchase orders are issued):

1. Is there any non-technical barrier for sharing entry data in advance with the Customs?

2. Regarding completeness, certainty, accuracy, quality related to the data shared in advance with government Can the accurate data be provided at a fixed time? If not, then in your opinion how can the data be modified in that fixed time without compromising the existing agreement between the CBP and the importer.

3. Is there any preferred practice from the government side if data is shared in advance? for instance, less guarantee that the data would not change, less punitive government policy if the data is inaccurate, easiness to make changes, or cost to make changes?

4. What will be the best approach to implement such data sharing environment? Volunteering based? Consent from the data owners?

5. Are there any legal concerns related to data sharing in advance with customs?

6. Any thoughts on unique challenges or opportunities related to data sharing in advance with the Customs? Different from data sharing with other private entities within the global supply chain?

7. What will be the key ingredients for such advanced data sharing practice with the Cus-

toms to succeed? For instance, benefits to the importers/filers, volunteer based, clearly defined values to both the private sectors and the Customs?

Questions related to timeliness and data quality

8. How often the same piece of information is replicated or copied in E2E global supply chain process, for instance different copies in multiple stakeholders' private databases? Do these copies lead to problems such as data quality, administrative cost, process delay, and etc.?

9. In terms of reliability and quality, how will adopting blockchain based entry process change the data ?

10. Is there a need for supply chain related data to be shared in faster pace along the value chain? Is there any benefit if data can be propagated or disseminated faster with other government agencies (PGAs) within the Single Window framework?

Questions related to benefits as result of data collaboration along the value chain

11. What is your thought on sharing data in advance with the Customs and reduced clearance delay? Is it possible that cargo is cleared before shipping or during shipping?

12. What are the benefits of having faster clearance due to data sharing in advance (compared with the existing practice)?

13. Will involving customs earlier in the process bring benefits to trade finance or insurance? (for instance due to less risk of denied entry, shipping delay risk, impact to finance based on receivables, and etc.)

Questions related to payment

14. Is there any need to implement faster or more automated payment transactions as an alternative to today's payment system when dealing with the Customs related fees? Is there any space for improvement related to the current payment system or solution? For instance, cost, delay, manual work? payment to the Customs in context of e-commerce scenario? or the case of cross-border goods with low value?

Questions related to cost

15. In your opinion, what will be the anticipated cost to adopt new technology such as distributed ledger for cross-border trade in your business or by your customers or by importers who you do business with? For instance, operational cost, human resource cost (expertise, qualified IT personnel, training), development cost, cost to switch or cost to work with multiple IT systems?

16. What will be your major concerns related to cost if there is?

Questions related to multiple platforms

In recent years, many distributed ledger related consortia were created with the purpose to serve different industry sectors and customers, for instance, consortium focusing on retailers, blockchain consortium created for freight forwarder industry, consortium focusing on trade finance and compliance.

17. In your view, what will be the strategy for industry to engage with these consortia? Join every relevant consortium? Join one of the most relevant one? Join many as an observer? Or any other approach in terms of participation?

18. To your knowledge, is there a lack of effort for these consortia to integrate support for the Customs brokers' filing need? Do they have dedicated workgroups that actively engage with the government and the private industry stakeholders to incorporate support for filing requirements with the Customs?

19. In your opinion, what strategy or approach should be adopted by these consortia to support cross border trade, in particular functionality relevant to the Customs and brokers? For instance, support for standards? communication channels with the Customs and brokers? assurance of inter-operability, and etc.?

Open questions

20. In your perspective, what will be the major issues that need to be resolved for such technology to succeed in the short term, midterm, or long term?

E

Glossary

Table E.1: Definitions.

Term	Definition
Access control	A means of controlling access by users to computer systems or to data on a computer system. Different types of access exist. For example, "read access" would suggest that the user has authorization only to read the information he or she is accessing (e.g., data stored in or protected by a blockchain), whereas "write access" would suggest that the user has authorization to both read and alter accessed data. Access control often includes authentication, which proves the identity of the user or client machine attempting to access the system. Access control policies are high-level requirements that specify how access is managed and who may access information under what circumstances. Access control policies can be enforced by a blockchain where the policies are protected as immutable and tamper proof records, and enforcement of the policies are performed using distributed consensus and secret sharing.
Automated Commercial Environment	ACE is the system through which the trade community reports imports and exports and the government determines admissibility. ACE has modernized and streamlined trade processing across all business capabilities, including Manifest, Cargo Release, Post Release, Export and Partner Government Agencies (PGAs).
Activity	A task that transforms inputs into outputs via the work of mechanisms under the instruction of controls. Activities occur over time and have identifiable outputs.

Activity diagram	The activity diagram displays a sequence of activities including alternative and concurrent execution.
Actor	An actor represents a role played in relation to a use case by someone or something in the business domain.
Advance ruling	Advance rulings are binding decisions by Customs at the request of the person concerned on specific particulars in relation to the intended importation or exportation of goods. Advance rulings can be requested with regard to either the classification, the origin or the Customs value of the goods in preparation for importation or exportation.
Attribute	Any named property used as a data abstraction to describe its enclosing object, class, or extent.
Authentication	Verifying the identity of a user, process or device, often as a prerequisite to allowing access to resources in an information system (NIST SP 800-128).
Authorization	The process of verifying that a requested action or service is approved for a specific entity (NIST SP 800-152).
Authorized Economic Operator	A party involved in the international movement of goods, in whatever function, that has been approved by, or on behalf of, a national customs administration as complying with WCO or equivalent supply-chain security standards. (WCO SAFE Framework of Standards)
Bill (of lading)	document issued by a carrier to the exporter and importer detailing the cargo on-board. Contains similar information as the manifest.
Blockchain	A type of distributed digital ledger, secured by cryptography. Data in the chain is recorded sequentially and permanently (i.e. it is immutable) in “blocks”. Each new block is linked to the immediately previous block with a cryptographic signature, forming a ‘chain’. This tamperproof self-validation of the data means transactions are processed and recorded without recourse to a 3rd party certification agent. The ledger is not hosted in one location or managed by a single owner, but is shared and accessed by anyone with the appropriate permissions. Blocks Transactions from the network fill blocks; the blocks are then sequentially linked in the chain. And, as the transactions are validated, they are compiled into the blockchain permanently. Blocks include a timestamp. They’re built in such a way that they cannot be changed once recorded.
Bill of exchange	A bill of exchange is a written order once used primarily in international trade that binds one party to pay a fixed sum of money to another party on demand or at a predetermined date.

Business process	The means by which one or more activities are accomplished in operating business practices.
Business rule	regulations and practices for business.
Byzantine Fault Tolerance	Byzantine fault tolerance refers to property of distributed computing systems that can tolerant Byzantine fault. A Byzantine fault is a condition of a distributed computing system, where components may fail and there is imperfect information on whether a component has failed. The term takes its name from an allegory, the "Byzantine Generals Problem", developed to describe a situation in which, in order to avoid catastrophic failure of the system, the system's actors must agree on a concerted strategy, but some of these actors are unreliable.
Consortium	A group of people, countries, companies etc. who are working together on a particular project.
Contract	A legally binding agreement between two parties in which the specific titles, rights, commitments, and obligations of both parties are defined.
Credentials	An object or data structure that authoritatively binds an identity – via an identifier or identifiers – and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber (NIST SP 800- 63-2).
Customs bond	A customs surety bond is a contract used for guaranteeing that a specific obligation will be fulfilled between customs and an importer for any given import transaction. The main purpose of a customs bond is to guarantee the payment of import duties and taxes.
Delivery Terms	Terms agreed between supplier and customer under which the supplier undertakes to deliver goods or services to the customer.
Distributed hash table	A distributed hash table (DHT) is a distributed system that provides a lookup service similar to a hash table: pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key.
Delivery Time	The day/time at which the supplier contracts to deliver the goods or service at the location specified in the delivery term.
Diagram	A graphical depiction of all or part of a model.
Digital document	Digital information that has been compiled and formatted for a specific purpose, that includes content and structure and may include context. (Glossary of Archival and Records Terminology).

Digital identity	A unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but does not necessarily need to uniquely identify the subject in all contexts (NIST SP800-63-3).
Digital signature	A specific type of electronic signature (e-signature) that relies on public-key cryptography to support identity authentication and provide data and transaction integrity.
Distributed Ledger Technology	DLT Often used interchangeably with blockchain, the distributed ledger is central to and at the core of blockchain applications, but not the blockchain itself. Distributed ledgers are a type of database that are spread across multiple sites, countries or institutions. Records are stored one after the other in a continuous ledger (or chain).
Enterprise resource planning	ERP is a process used by companies to manage and integrate the important parts of their businesses. Many ERP software applications are important to companies because they help them implement resource planning by integrating all of the processes needed to run their companies with a single system. An ERP software system can also integrate planning, purchasing inventory, sales, marketing, finance, human resources, and more.
Entry	Forms submitted by importer or broker to CBP for approval of admittance to the United States.
Entry release	When CBP clears an entry.
Entry declaration	When the filer submits their entry to CBP.
Entry liquidation	Liquidation is the process through which Customs completes its review of an entry and finalizes its position as to the duties.
Event	An event is an occurrence that may cause the state of a system to change.
Framework Contract	A contract agreed between a customer and a supplier setting out the conditions of trade and technical details under which a customer may place orders with the supplier for products over a specified period.
GDPR	The General Data Protection Regulation is the European Union's new data privacy law. It gives people more control over their personal data and forces companies to make sure the way they collect, process and store data is safe. The EU hopes to achieve a fundamental change in the way companies think about data – its central idea is "privacy by default.

GS1	GS1 is a not-for-profit organization that develops and maintains global standards for business communication. The best known of these standards is the barcode, a symbol printed on products that can be scanned electronically.
Hash/Hashing	The result of applying an algorithmic function to data in order to convert them into a random string of numbers and letters. This acts as a digital fingerprint of that data, allowing it to be locked in place within the allowing it to be locked in place within the blockchain. In cryptocurrency, “hashing” is the primary activity of “miners”.
Hold	Order issued by CBP or PGAs to prevent imports from leaving a port of entry until some action has occurred.
Homomorphic encryption	Homomorphic encryption (HE) is a form of encryption that allows computation on ciphertexts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext. Practical HE schemes can be applied to the blockchain applications or can be combined with MPC. It could be used for machine learning and AI applications integrated with distributed ledgers.
Immutability	A fundamental advantage of blockchain technology. Each stored block is linked to its previous block in the chain with an encrypted digital fingerprint, making it almost impossible for hackers to subsequently change blocks. The validated, encrypted digital fingerprint also includes a date and time stamp. Any attempt to change data will be apparent, because the new digital fingerprint will not match the old one. This also provides full transparency on the history of transactions in the chain.
In-bond	refers to goods for which the filer decides to hold off making entry upon arrival and issue a bond to customs in lieu of payment of duties. These goods can either move to another port within the country or be held in a bonded warehouse for up to 30 days, at which point entry must be made and duties paid.
Invoice	A document claiming payment for goods or services supplied under conditions agreed by seller and buyer.
Letters of Credit (LCs)	LCs allow an Issuing Bank to substitute its own creditworthiness for that of its client, providing the exporter with better assurance of payment.
Line Item	The identification of one individual product or service and its specific conditions for purchase.
LPCO	License, Permit, Certificate and Other Documentation.

Machine learning	Machine learning (ML) studies of algorithms and statistical models that provides computer systems the ability to automatically learn and improve from experience without being explicitly programmed. It is seen as a subset of artificial intelligence. Machine learning algorithms build a mathematical model based on sample data, known as "training data", in order to make predictions or decisions without being explicitly programmed to perform the task.
Manifest	document issued by a carrier to customs officials detailing the cargo, passengers, and crew onboard. Contains similar information as the bill of lading
Manufacture ID	Manufacturer's identification number (MID) A unique identifying reference number allocated to each manufacturer that imports goods into the United States. Unlike other numbering systems for manufacturers which may be more widely used, this system is employed by U.S. Customs in its electronic data processing.
MLETR	The UNCITRAL Model Law on Electronic Transferable Records is a uniform model law that has been adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 2017. Its scope is to allow the use of transferable documents and instruments in electronic form. Transferable documents and instruments typically include bills of lading, warehouse receipts, bills of exchange, promissory notes and checks. National law qualifies a document or instrument as transferable. Transferable documents and instruments allow to request delivery of goods and payment of a sum of money based on possession of the document or instrument. However, it has been difficult to reproduce the notion of possession, which has to do with control over tangible goods, in an electronic environment. The MLETR addresses such legal gap.
Model	Any abstraction that includes all essential capabilities, properties, or aspects of what is being modelled without any extraneous details. Any cohesive set of requirements or design information.
Model law	A model law (also known as a uniform law) is a proposed series of laws pertaining to a specific subject, that the states may choose to adopt or reject, in whole or in part. If a state adopts the model law then it becomes the statutory law of that state.

Node	A computer or server connected to the blockchain network. Any node that is active, possesses a copy of the blockchain providing "redundancy" of the chain. As a result, no single point of failure exists (see REDUNDANCY).
Operation	Any discrete activity, action, or behavior that is performed by an object or class.
Order	A document by means of which a customer initiates a transaction with a supplier involving the supply of goods or services as specified, according to conditions set out in an offer, or otherwise known to the customer.
Partner Government Agency (PGA)	U.S. government entity other than CBP with an interest in international trade to the country
Payment	A transfer of money in exchange for goods or services received
Payment Term	Terms agreed between customer and supplier under which the customer agrees to pay the supplier for goods or services.
PKI	A public key infrastructure is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.
Port of arrival	Port where a specific shipment first arrives on U.S. soil. Some PGAs require inspections be done at the port of arrival if it differs from the port of entry.
Port of entry	Port where filers submit entries for a specific shipment.
Product	Goods or services that can be purchased and sold
Proof of Work PoW	This is the real value that "miners" (validators) do in the chain. By providing proof (via a highly encrypted signature) that a transaction is valid (i.e. meets the protocols/rules, is performed by a legitimate participant, and at a valid sequence (time stamp)), the PoW ensures consensus on the validity of the transaction and provenance of the chain. This is NOT trivial (i.e. check the box): it is performed by high-powered computers at great complexity and cost
Quote	A document issued by the supplier setting out terms for the supply of goods or services in response to a customer's request for a quotation.
Regulation	Legal conditions governing how trade must be conducted
Release into commerce	point at which all government holds are removed from a shipment and no further government actions are required. The broker or importer is then free to take the goods.
RFI	A request for information on products or services sent from a customer to potential suppliers.

RFQ	A request to suppliers sent from a customer specifying goods or services required and the conditions for supply and inviting quotations.
Scalability	For a technology to succeed it must be scalable: that is, applicable widely enough to justify the cost of investment and to grow seamlessly as the need grows (in terms of market size, application to related uses, etc.).
Smart Contracts	Computer protocols that facilitate, verify, or enforce the negotiation or performance of a contract, or that make a contractual clause unnecessary. Smart contracts may offer the opportunity to drastically reduce 3rd party (esp. legal) fees and improve efficiency and contractual term adherence.
Self-managed	In a self-managed interaction, a user can control its own identity and attributes.
Service provider	An entity that delivers application functionality and associated services across a network to multiple service consumers
Single transaction bond	Single entry bond (STB), is an indemnity procured by an importer and provided to Customs to assure payment of duties, taxes, fines, and penalties associated with the compliant import of cargo. Often, bonds are purchased from Customs brokers. A STB is procured for each shipment; whereas, a continuous bond is purchased for a defined time period.
Stakeholder	Someone or something that is materially affected by the outcome of the system but may or may not be an actor.
System	A System is a set of items which interact with each other and interact also with an external environment. The system is aimed at specific goals.
Time to release	Time required for imports to enter commerce following their arrival in a country
Trade	Refers to the private entities involved in importing goods to the United States, particularly importers, exporters, and their representatives
Trade-Based Money Laundering	Trade-based money laundering (TBML) is defined as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins.
Trade document	Trade documents are any documents used in global trade, whether certificates, licenses, permits or business documents such as purchase orders, bills of lading etc. We spell out specific document types only when it is relevant.
Single Window system	A facility that allows parties involved in trade and transport to lodge standardized digital trade information and trade documents with a single entry point to fulfill all import, export and transit-related regulatory requirements.

Transshipment	Transshipment or transhipment is the shipment of goods or containers to an intermediate destination, then to another destination.
Trusted execution environment	Trust execution environment is a hardware assisted secure runtime environment to protect privacy and integrity of software and data. It prevents local user from tampering the input and output to the software executed in the trust execution environment. It may defend against both software and certain hardware based attacks. Examples of TEE includes, Intel SGX, AMD Memory Encryption, ARM TrustZone, and etc.
Uniform Commercial Code	The Uniform Commercial Code (UCC) is a standardized set of laws and regulations for transacting business. Then UCC code was established because it was becoming increasingly difficult for companies to transact business across state lines given the various state laws. The UCC covers transactions pertaining to the sale of goods and commercial transactions. The sale of goods refers to the buying or selling of a tangible product. Commercial transactions include many banking activities, such as personal, bank, certified and cashier checks. The UCC code consists of nine separate articles. UCC Article 5 governs letters of credit, which are typically issued by a bank or other financial institution to its business customers in order to facilitate trade.
UNCITRAL	The United Nations Commission on International Trade Law is a subsidiary body of the U.N. General Assembly responsible for helping to facilitate international trade and investment.
Use case	A use case is a description of the possible sequences of interactions among a system and one or more actors in response to some initial event from an actor to the system. A use case includes events and system operations that are visible to the actors.
Zero-knowledge protocol	A zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that they know some value, without conveying any information apart from the fact that they know the value. Zero-knowledge protocol in context of blockchain allows nodes to verify that transactions are valid without revealing any information about the transactions, providing privacy.

Table E.2: Actors in global supply chain.

Term	Definition

Advising Bank	A bank asked by the issuing bank to advise the credit to the beneficiary when payment is guaranteed by a documentary letter of credit.
Authority	A statutory body existing within a jurisdiction and a specific area of responsibility that administers legislation to regulate trade and/or monitors compliance with existing legislation.
Broker	Actor hired by importers to prepare and file Customs entries, arrange Customs payments, and represent the importer in Customs matters.
Carriage Insurer	A party who provides insurance cover for the goods during carriage.
Carrier	A party undertaking or arranging transport of goods between named points. (Employed by either the buyer or seller)
Credit Checking Agency	A commercial organisation that carries out checks on the financial state of the buyer, his ability to pay for the goods and his credit risk.
Cross-border regulatory agency (C.B.R.A)	Cross-border regulation of international trade involves many government agencies. These include agencies dealing with trade in goods that affect human health (e.g. food safety, pharmaceuticals, cosmetics and dangerous drugs, to name a few). Other agencies might, for example, deal with public, environmental or biosafety. The precise number of agencies depends on the compliance profile of the country. (World Customs Organization)
Customer	A party who acquires, by way of trade, goods or services.
Exporter/Seller	A party who supplies goods to the buyer (or Importer). He has title to the goods and is able to sell this to the customer for a consideration.
Filer	Entity, either the importer directly or the broker representing them, who submits an entry to the CBP.
Freight Forwarder	An Intermediary employed by buyer or seller (depending on the terms of trade) who may carry out a variety of tasks concerned with the movement of goods. These can include collection and transport of goods and the completion of an export /import declaration on the exporter's behalf.
Importer/ Buyer	A party who purchases the goods from the seller(or exporter).
Intermediary	A party who provides commercial or transport services to Customers, Suppliers or Authorities within the international supply chain.

Issuing Bank	A bank instructed by the applicant (normally the Exporter) to issue a Documentary Credit and who undertakes that payment will be made to the Beneficiary upon presentation of stipulated documents.
Supplier	A party who provides, by way of trade, goods or services.
Surety	The company issuing the U.S. import customs bond is called the surety. An import customs bond guarantees that the taxes, duties and fees are paid on all imports. If the importer cannot pay those costs, the company that issued the import customs bond will pay the remaining costs.

List of Figures

List of Tables

Bibliography

[1] Business Guide on the WCO Data Model. World Customs Organization.

[2] How Blockchain Can Bring Greater Value to Procure-to-Pay Processes. Accenture.

[3] Business Requirements Specification (BRS). Buy-Ship-Pay reference data model. United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT).

[4] Performance and Accountability Report, Fiscal Year 2016. https://www.cbp.gov, . CBP.

[5] Business Rules and Process Document for Trade. https://www.cbp.gov, . CBP.

[6] Antidumping and Countervailing Duty Enforcement Actions and Compliance Initiatives: FY 2017. https://www.cbp.gov, . CBP.

[7] Entry Summary Filing and Response Guide. ACE ABI CATAIR. Customs and trade automated interface requirements. https://www.cbp.gov, . CBP.

[8] ACE Cargo Release. https://www.cbp.gov, . CBP.

[9] Continuous interconnected supply chain. Using blockchain Internet-of-things in supply chain traceability. Deloitte.

[10] Does blockchain hold the key to a new age of supply chain transparency and trust? How organizations have moved from blockchain hype to reality. Capgemini Research Institute.

[11] FDA's Food Safety Modernization Act. www.fda.gov.

[12] GAO-17-618. https://www.gao.gov/products/GAO-17-618, . U.S. Government Accountability Office (GAO).

[13] GAO-17-650. https://www.gao.gov/products/GAO-17-650, . U.S. Government Accountability Office (GAO).

[14] GAO-18-271. https://www.gao.gov/products/GAO-18-271, . U.S. Government Accountability Office (GAO).

[15] GAO-16-542. https://www.gao.gov/products/GAO-16-542, . U.S. Government Accountability Office (GAO).

[16] Hyperledger. Hyperledger Aries Proposal.

[17] Hyperledger. Hyperledger Indy.

[18] IPFS. https://ipfs.io.

[19] ISO/TC 307 "Blockchain and distributed ledger technologies". https://isotc.iso.org/livelink/livelink/open/tc307.

[20] UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001.

[21] Sovrin. https://sovrin.org.

[22] The Technical Applications of Blockchain to United Nations Centre for Trade Facilitation and Electronic Business. Blockchain Project Team. UN/CEFACT.

[23] Uport. https://uport.me.

[24] Customs Risk Management Compendium. WCO.

[25] ZKProofs. Zero-Knowledge Proofs. https://zkp.science.

[26] IAF/ILAC Multi-Lateral Mutual Recognition Arrangements (Arrangements):Narrative Framework for Reporting on the Performance of an Accreditation Body (AB) A Tool for the Evaluation Process. IAF/ILAC-A3:07/2011, 2011.

[27] Technical Notes on Trade Facilitation Measures. UNCTD, 2011.

[28] Banks' Control of Financial Crime Risks in Trade Finance. TR13/3. PUB REF: 004720., July 2013.

[29] Final Rule on Accredited Third-party Certification. FDA, Nov 13 2015.

[30] Cargo Time Release Study. Prepared for the Department of Homeland Security Directorate for Science and Technology Capability Development Support Group (CDSG) Operational Requirements and Analysis Office (ORA), May 26 2015.

[31] Digital Innovation in Trade Finance: Have We Reached a Tipping Point?, October 2017. Boston Consulting Group.

[32] Selfkey. https://selfkey.org/wp-content/uploads/2017/11/selfkeywhitepaper-en.pdf, 2017. The SelfKey Foundation.

[33] Trade Remedy Law Enforcement/Office of Trade Bond Working Group. COAC, July 17 2018.

[34] Code Is Not Law: The Legal Background for Trade Finance Using Blockchain. July 6 2018. R3, Shearman and Sterling LLP, BAFT.

[35] Small Entity Compliance Guide for Importers, Distributors and Retailers. EPA-712-B-17-001. United States Environmental Protection Agency, May 2018.

[36] LifeID, An open-source, Blockchain-based Platform for Self-sovereign Identity. https://lifeid.io/whitepaper.pdf, 2018.

[37] CBP Did not Maximize Its Revenue Collection Efforts for Delinquent Debt Owed from Importers. OIG-19-11, Dec 4 2018. Office of Inspector General.

[38] Illicit Financial Flows via Trade Mis-invoicing. WCO, 2018.

[39] WCO Guidelines on Trader Identification Number. WCO, June 2018.

[40] Technical Guidelines on Advance Rulings for Classification, Origin, and Valuation. WCO, June 2018.

[41] Inclusive Deployment of Blockchain for Supply Chains Part 2 – Trustworthy Verification of Digital Identities, Apr 2019.

[42] Business Rules and Process Document. ACE Entry Summary. `https://www.cbp.gov`, June 2019. CBP.

[43] CBP 21st Century Customs Framework Public Meeting, March 1 2019. CBP.

[44] Report of the Work of the COAC Subcommittee on Intelligent Enforcement (IE). COAC, Feb 2019.

[45] Report of the Work of the COAC Subcommittee on Intelligent Enforcement. COAC, Aug 2019.

[46] Harmony. Technical Whitepaper, 2019. Harmony Team.

[47] Saveen A. Abeyratne1 and Radmehr P. Monfared. Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger. volume 5, Sep 2016.

[48] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone. PBFT vs Proof-of-Authority: Applying the Cap Theorem to Permissioned Blockchain.

[49] Atin Angrisha, Benjamin Cravera, Mahmud Hasana, and Binil Starlya. A Case Study for Blockchain in Manufacturing: "FabRec": A Prototype for Peer-to-Peer Network of Manufacturing Nodes. *46th SME North American Manufacturing Research Conference, NAMRC 46.*

[50] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 514–532. Springer, 2001.

[51] Sean Cao, Lin William Cong, and Baozhong Yang. Auditing and Blockchains: Pricing, Misstatements, and Regulation. Working Draft, 2018.

[52] John A. Cassara. *Trade-Based Money Laundering : The Next Frontier in International Money Laundering Enforcement.* John Wiley Sons Inc., 2016.

[53] Miguel Castro and Barbara Liskov. Practical Byzantine Fault Tolerance and Proactive Recovery. *ACM Transactions on Computer Systems (TOCS)*, 20(4):398–461, 2002.

[54] David Chaum, Ivan B. Damgård, and Jeroen van de Graaf. Multiparty Computations Ensuring Privacy of Each Party's Input and Correctness of the Result. In Carl Pomerance, editor, *Advances in Cryptology — CRYPTO '87*, pages 87–119, Berlin, Heidelberg, 1988. Springer Berlin Heidelberg. ISBN 978-3-540-48184-3.

[55] Lin Chen, Lei Xu, Nolan Shah, Zhimin Gao, Yang Lu, and Weidong Shi. On Security Analysis of Proof-of-Elapsed-Time (PoET). pages 282–297, 10 2017. ISBN 978-3-319-69083-4. doi: 10.1007/978-3-319-69084-1_19.

[56] Reed D, Sporny M, Longley D, Allen C, Grant R, and Sabadello M. Decentralized Identifiers (DIDs) v0.12 – Data Model and Syntaxes for Decentralized Identifiers, 2019.

[57] Temoshok D and Abruzzi C. Developing Trust Frameworks to Support Identity Federations. Technical report, 2018.

[58] Sasson EB, Chiesa A, Garman C, Green M, Miers I, Tromer E, and Virza M. Zerocash: Decentralized Anonymous Payments from Bitcoin. *IEEE Symposium on Security and Privacy*, pages 459–474, 2014.

[59] Ziyang Fan and Pablo M. Garcia. Windows of Opportunity: Facilitating Trade with Blockchain Technology. July 2019. World Economic Forum.

[60] Tiago M. Fernandez-caramesi and Paula Fraga-lamas. A Review on the Application of Blockchain for the Next Generation of Cybersecure Industry 4.0 Smart Factories. Feb 2019.

[61] Emmanuelle Ganne. Can Blockchain Revolutionize International Trade?, 2018.

[62] Katz J, Ostrovsky R, and Rabin MO. Identity-based zero-knowledge. *International Conference on Security in Communication Networks*, pages 180–192, 2004.

[63] Arnout Jaspers. Sharing Secrets (Without Giving Them Away). ACM News, Oct 31 2017.

[64] Fariha Kamal and Ryan Monarch. Identifying Foreign Suppliers in U.S. Import Data. *International Finance Discussion Paper*, 2017:1–36, 10 2017.

[65] Rüdiger Kapitza, Johannes Behl, Christian Cachin, Tobias Distler, Simon Kuhnle, Seyed Vahid Mohammadi, Wolfgang Schröder-Preikschat, and Klaus Stengel. CheapBFT: Resource-efficient Byzantine Fault Tolerance. In *EuroSys '12*, 2012.

[66] Manisha Khanna. Trade-Based Money Laundering – Capturing the New Frontier through Analytics. CAMS AUDIT white paper.

[67] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford. OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 583–598, May 2018. doi: 10.1109/SP.2018.000-5.

[68] Loïc Lesavre, Priam Varin, Peter Mell, Michael Davidson, and James Shook. A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. `https://doi.org/10.6028/NIST.CSWP.07092019-draft`, July 9 2019.

[69] Xuepeng Liu and Huimin Shi. Anti-dumping Duty Circumvention through Trade Rerouting: Evidence from Chinese Exporters, Aug 2016.

[70] Sporny M, Longley D, and Chadwick D. Verifiable Credentials Data Model 1.0 – Expressing Verifiable Information on the Web. W3C, 2019.

[71] J-P Martin and Lorenzo Alvisi. Fast Byzantine Consensus. *IEEE Transactions on Dependable and Secure Computing*, 3(3):202–215, 2006.

[72] D. Mazieres. The Stellar Consensus Protocol: A Federated Model for Internet Level Consensus, Stellar Development Foundation.

[73] Lesley K. McAllister. Harnessing Private Regulation, Aug 2013.

[74] Rena S. Miller, Liana W. Rosen, and James K. Jackson. Trade-Based Money Laundering:Overview and Policy Issues. Congressional Research Service, June 22 2016.

[75] Yotaro Okazaki. Unveiling the Potential of Blockchain for Customs. WCO Research Paper No. 45., June 2018.

[76] Mell P, Dray J, and Shook J. Smart Contract Federated Identity Management without Third Party Authentication Services. 2019.

[77] Serguei Popov. The Tangle. `https://iota.org`.

[78] B. Reid and B. Witteman. EverID Whitepaper. `https://coinosophy.files.wordpress.com/2018/05/everid-whitepaper.pdf`, 2018. The SelfKey Foundation.

[79] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to share a secret. *Communications of the ACM*, 22(22):612–613, 1979.

[80] Goldwasser S, Micali S, and Rackoff C. The Knowledge Complexity of Interactive Proof Systems. *SIAM Journal on Computing*, 18:186–208, 1989.

[81] Anthi Tsilimeni-Archangelidi. Blockchain Technology in Supply Chain. Conceptual Redesign of Crude Palm Oil's Trading Business Process. Master's thesis, 2018.

[82] Giuliana Veronese, Miguel Correia, Alysson Bessani, Lau Lung, and Paulo Veríssimo. Efficient Byzantine Fault-Tolerance. *Computers, IEEE Transactions on*, 62:16–30, 01 2013.

[83] Andrew Chi-Chih Yao. How to Generate and Exchange Secrets (Extended Abstract). In *FOCS*, pages 162–167. IEEE Computer Society, 1986. ISBN 0-8186-0740-8.

[84] Mahdi Zamani, Mahnush Movahedi, and Mariana Raykova. RapidChain: A Fast Blockchain Protocol via Full Sharding. Cryptology ePrint Archive, Report 2018/460, 2018. URL `https://eprint.iacr.org/2018/460.pdf`.

Acknowledgement: This material is based upon work supported by the U.S. Department of Homeland Security under original Grant Award Number 2015-ST-061-BSH001-03.

Disclaimer: The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

U.S. DEPARTMENT OF
HOMELAND SE
GARDINER
GOMEZ
PAT
·MAY 28,