Opportunities provided by emerging technologies to make cross-border mutual recognition of electronic messages more effective, economical and secure

Tahseen Khan, Kaushik Srinivasan, Shantanu Godbole and Lohit Krishnan Namboodiri

* This document is expert submission, for participants at the meeting, and is not for citation. The designations employed and the presentation of the material in this document do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. Where the designation “country or area” appears, it covers countries, territories, cities or areas. The views expressed in this document are those of the author(s) and do not necessarily reflect the views of the United Nations. The opinions, figures and estimates set forth in this document are the responsibility of the author(s) and should not necessarily be considered as reflecting the views or carrying the endorsement of the United Nations. Any errors are the responsibility of the author(s). The mention of firm names and commercial products does not imply the endorsement of the United Nations.

** [https://www.unescap.org/sites/default/files/Tentative%20Agenda%20of%20the%20Eighth%20meeting%20of%20LTWG%20B.pdf](https://www.unescap.org/sites/default/files/Tentative%20Agenda%20of%20the%20Eighth%20meeting%20of%20LTWG%20B.pdf)

*** This study report is prepared by the author for contributing to the discussion on mutual recognition mechanism for trade related data and documents in electronic form.
Contents

1  Executive Summary ............................................................................................................. 1

2. Current technologies that have an impact on the mutual recognition mechanism
   .................................................................................................................................................. 2

2.1  Internet of things ............................................................................................................. 4

2.1.1  Identity .......................................................................................................................... 6

2.1.2  Authentication ............................................................................................................... 8

2.1.3  Privacy .......................................................................................................................... 10

2.1.4  Data ownership ............................................................................................................ 11

2.1.5  Legal issues .................................................................................................................... 11

2.1.6  Mutual recognition ....................................................................................................... 12

2.1.7  The way forward .......................................................................................................... 12

2.2  Blockchain ...................................................................................................................... 13

2.2.1  Identity .......................................................................................................................... 16

2.2.2  Authentication ............................................................................................................... 17

2.2.3  Authorization ............................................................................................................... 18

2.2.4  Endorsement ............................................................................................................... 19

2.2.5  Smart contract ............................................................................................................... 20

2.2.6  Immutability .................................................................................................................. 21

2.2.7  Putting it all together to engender trust in mutual recognition .................................. 23

2.2.8  The way forward .......................................................................................................... 28

3. Use cases in Blockchain and IoT ....................................................................................... 29

3.1  Blockchain ....................................................................................................................... 29

3.2  Internet of things ............................................................................................................. 33
List of tables

Table 1. Emerging technologies that can disrupt cross-border trade ............... 2
Table 2. Case study of TradeLens ................................................................. 29
Table 3. Case study of internet of things .................................................... 33

List of figures

Figure 1. Elements of an IoT system that need to be secured ...................... 8
Figure 2. Representative architecture for a Hardware Root of Trust approach .. 9
Figure 3. Mutual recognition in the Buy-Ship-Pay model .......................... 15
Figure 4. Hashing algorithm ......................................................................... 22
Figure 5. Blockchain transaction blocks ..................................................... 22
Figure 6. Blockchain transaction packet ..................................................... 23
Figure 7. Blockchain transaction blocks ..................................................... 24
Figure 8. Flow of transaction ...................................................................... 26
1 Executive Summary

International trade and commerce involving electronic transactions between two or more parties of different jurisdictions need to establish trustworthiness. The volume and velocity of such trade has increased exponentially during the past two decades as a result of improved availability, connectivity and efficiency in Internet services. Advanced technologies such as the Internet of Things (IoT) and Blockchain are showing promise of ushering in a new era of efficiency with regard to the movement of goods across borders.

Unlike physical commerce, the proliferation of trade through electronic transactions often results in transactions between parties who have no pre-existing relationship. This imposes an additional risk should either party default on the fulfilment of their obligations. The result is often the need to go through several independent organizations, such as banks and insurance companies, to protect against default, thereby resulting in higher costs. In addition, the need for enforceability in the absence of regulations related to the legal recognition of cross-border transactions can result in the continued use of physical contracts and manual signatures. This results in an extremely large volume of paper documentation, which has a damaging effect on the environment, and greater transaction costs and time. In this context, mutual recognition frameworks are necessary in enabling trusted trans-boundary electronic interactions to support cross-border paperless trade.

In the context of IoT, “mutual recognition” may be defined as the ability to reciprocally recognize the validity of sensor or connected device data collected in one jurisdiction as part of an international supply chain process and used in another jurisdiction for trade facilitation. An example is the use of temperature and humidity data on a container to expedite clearance of plants or food substances. In the context of Blockchain, “mutual recognition” may be defined as the ability to treat data input by other parties in the Blockchain network at a level of trustworthiness equivalent to that generated within your organization boundary.
2. Current technologies that have an impact on the mutual recognition mechanism

There are a number of emerging technologies that have the potential to disrupt the way cross-border trade is conducted. These are highlighted in table 1.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Description</th>
<th>Cross-border paperless trade facilitation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Blockchain</strong></td>
<td>A decentralized, distributed digital ledger that records electronic transactions in a manner so as to provide transaction integrity and immutability.</td>
<td>Ability to collaborate and share trade-related data and documents across international supply chains in near real time.</td>
</tr>
<tr>
<td><strong>Internet of Things</strong></td>
<td>An Internet network of connected objects such as sensors to facilitate communication between them and to other internet enabled devices and systems.</td>
<td>Automate the capture of supply chain data using sensors, which then can be used by customs and other entities as part of the trade facilitation process.</td>
</tr>
<tr>
<td><strong>Quantum computing</strong></td>
<td>An area of computing focused on developing computer technology based on quantum theory, resulting in either far greater computing power than what is available today, or the ability to carry out computations that are deemed infeasible by current computing paradigms.</td>
<td>The ability to process very large volumes of trade data relatively quickly; this also has implications for the use of cryptographic algorithms based on which electronic or digital signatures may have been developed.</td>
</tr>
<tr>
<td><strong>Autonomous “Things”</strong></td>
<td>An emerging technological development that allows things to work automatically without human guidance or direct intervention leveraging other technologies such as Artificial Intelligence (AI).</td>
<td>Autonomous robots, transport systems have a huge role in defining next generation logistics for international trade.</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>5G</strong></td>
<td>5G is the term used to define the next generation of mobile networks that provide very high speed data transfers.</td>
<td>5G has the potential to reshape the logistics industry by enabling machine-to-machine interaction, including transport communication systems, for better track-and-trace visibility.</td>
</tr>
<tr>
<td><strong>Edge Computing</strong></td>
<td>The ability of devices to process data locally as against transmitting to a data center.</td>
<td>As device computational power increases, Edge Computing can aid in providing better quality management that could identify a potential quality issue or defect in a supply chain process.</td>
</tr>
<tr>
<td><strong>3D Printing</strong></td>
<td>A computer-aided manufacturing device that creates or prints 3D objects on custom materials, using digital data as an input.</td>
<td>The ability to roll out certain types of products faster without the need to build an extensive assembly line, thereby giving the ability to manufacturers to lower</td>
</tr>
</tbody>
</table>
complexity and improve time to market.

<table>
<thead>
<tr>
<th>Artificial Intelligence</th>
<th>Ability of a computer program or machine to think, learn and act like humans.</th>
<th>AI has huge potential for automation in enabling paperwork reduction, demand forecasting, warehouse management and improving compliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer vision, augmented reality, virtual reality</td>
<td>Computer vision is concerned with the automatic extraction, analysis and understanding of useful information from a single image or a sequence.</td>
<td>Automatic processing of images, videos available in shipments, border gate controls to accurately assess shipment, logistics data and enabling faster clearances.</td>
</tr>
</tbody>
</table>

Source: Author's, 2020.

The focus on this research paper is on two specific technologies, i.e., IoT and Blockchain, both of which have huge potential in enabling cross-border mutual recognition of electronic messages and documents more effectively, efficiently and securely.

This research paper is aimed at providing a high level of understanding of data and document sharing as well as how these technologies provide opportunities for enabling mutual recognition, as part of cross-border paperless trade.

2.1 Internet of things
As per the Institute of Electrical and Electronics Engineers (IEEE) explanation, an IoT is a network that connects uniquely identifiable “Things” to the Internet. The “Things” have sensing/actuation and potential programmability capabilities. Through the
exploitation of unique identification and sensing, information about the “Thing” can be collected and its state can be changed from anywhere, anytime, by anything.¹

The key features of an IoT ecosystem include:

- Interconnection of “Things”;
- Connection of “Things” to the Internet;
- Uniquely Identifiable “Things”;
- Ubiquity;
- Sensing/actuation capability;
- Embedded intelligence;
- Interoperable communication capability;
- Self-configurability;
- Programmability.

IoT ecosystems have huge potential in terms of making many novel applications possible for enabling cross-border paperless trade through the use of connected devices that sense, collect, process, share and act on data. This encompasses environmental data such as: temperature and humidity; status data such as whether a device is alive or not; and location data that include latitude and longitude coordinates.

The data are also used to power a number of use cases that rely on real-time, data-driven decision-making, such as the ability to ensure freshness of produce across a supply chain, to asset location tracking to detecting equipment failure in logistics and transportation.

Cross-border trade, in particular, is signified by this need to collect, share, use and process information across borders. In the context of IoT and cross-border trade, this issue is compounded by the fact that data could be collected in one country, aggregated with data collected in other countries and analysed in a third country (creating so-called big data) – all of which entails the ability to move and process data across borders. An IoT linked supply chain also involves a number of additional ecosystem operators such as telecom players, equipment manufacturers and IoT software providers, all of whom are party to this data transmission.

¹ https://iot.ieee.org/definition.html.
This raises important issues concerning legality, cyber security, data ownership, privacy, usage and processing rights, and the important issue of mutual recognition in the context of the usage of IoT data collected across borders.

While these issues are important, equally the usage of IoT presents interesting opportunities in trade facilitation by providing the ability to make mutual recognition of cross-border electronic messages more effective, secure and economical. IoT systems can be designed in such a way as to ensure data provenance and trustworthiness. IoT devices present the ability to capture and record data in a real-time and continuous manner, and therefore can be used to record the lineage of data from basic sensor readings to complex derived information created by software applications. This real-time data can be fed into decision systems such as a Single Window, as demonstrated by projects such as the Smart container project of the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), for further action and automation.

To understand how IoT can be effectively used to make mutual recognition mechanisms in cross-border trade more secure, effective and economical, it is important to describe the key aspects of an IoT system. This is outlined below.

2.1.1 Identity

A leading global research and advisory company, Gartner predicted that there would be 20 billion IoT devices in 2020. In such a large interconnected network of devices, and the issue of identification of a “Thing” will play a crucial role in driving key aspects of an IoT ecosystem, such as overall design and architecture, data privacy, governance etc.

Like the evolution of the Internet and discovery of resources, IoT will go through a similar evolution for resource discovery where identifiers, network addresses and discovery functions will have to be designed and implemented in order for an IoT device to be identified and accessed.

There is ongoing work at the European Commission and various bodies such as the International Telecommunication Union (ITU) and Internet Engineering Task Force (IETF) towards creating the understanding of whether a central identity scheme or a

---

decentralized interoperable identity scheme is the way forward. The evolution of this will have various legal and policy implementations including aspects of mutual recognition. A centralized scheme such as the Internet IP address will need a consensus building approach in order to ensure uniformity in implementation. A decentralized identity scheme will probably give a higher degree of flexibility, but issues of interoperability and mutual recognition will need to be taken into account either through bilateral arrangements or through intergovernmental frameworks.

The second aspect of an identity scheme in the context of an IoT ecosystem is the ability to distinguish between an identifier and network address; the former is usually a static ID that is given to the device at the time of manufacturing or creation, while the latter is a more dynamic identity that is based on the membership of the device in a network at any given point in time. While the latter generally tends to follow Internet identity schemes such as IP addresses, there is no uniformity in the former and various countries have evolved country-specific standards such as Unique Code (ucode) system of Japan which is an identification number system that can be used to identify things in the real world uniquely.

The third aspect is one of discovery, i.e., the ability to discover an object and its attributes that are more relevant in the context of publicly connected devices. This is generally done on the Internet through Domain Name Service (DNS) schemes. An overlay scheme for IoT is one such as the Object Naming Service (ONS) and Object Directory Service (ODSD), which leverage the DNS to discover information about a product from an Electronic Product Code.

If emerging technologies such as IoT have to be able to play a vital role in cross-border trade facilitation and mutual recognition of electronic messages, the methodology in establishing the identity of devices that are part of an IoT network have to be agreed on, and this is the foundation on which data provenance and integrity, as part of a supply chain, are built on. This will need policy measures that promote convergence of identity in IoT platforms, either through standardized naming and discovery conventions or through interoperability to be able to support mutual recognition of electronic messages as part of cross-border paperless trade.
2.1.2 Authentication

IoT systems also suffer from similar security issues that current-day connected systems of computers face. To solve this, a number of security standards, protocols and technology frameworks have evolved and are used depending on the type of device, communication channel and need for security features in the network.

The following aspects are generally considered in designing a secure IoT system:³

- Usage of strong authentication systems, including keys and management of keys;
- Ability to protect data;
- Secure session establishment;
- Ability to upgrade device firmware securely;
- Monitoring and auditing;
- Boot protection.

Figure 1 provides an illustration of various elements of an IoT system that need to be secured.⁴

**Figure 1. Elements of an IoT system that need to be secured**

Since IoT security standards have generally been slower to evolve compared to the devices themselves, vendors have developed proprietary authentication methods. Many IoT devices tend to be resource-constrained, with low computing and storage capacity; in such cases, existing authentication methods are generally not a good candidate, due to their significant bandwidth and computational requirements. As the

---

³ https://www.kuppingercole.com/blog/singh/device-authentication-and-idot-for-iot
industry moves from considering security as an afterthought to including it as part of systems design process there is a huge drive towards building security standards, keeping in mind interoperability and ability of such systems to demonstrate trustworthiness.

Hardware-based security approaches such as Hardware Root of Trust and Trusted Execution Environment – which offer secure areas to execute programs – are rapidly finding relevance in securing IoT devices and providing this needed trustworthiness.

A representative architecture for a Hardware Root of Trust approach to securing IoT devices is given in figure 2. Hardware Root of Trusts allows the usage of keys stored in modules called “Trusted Platform Modules”, which are generally certified to be tamper-proof, in order to secure communication in and out of an IoT device. Thus, this offers higher assurance levels that may be expected as part of data exchanges for cross-border paperless trade.

Figure 2. Representative architecture for a Hardware Root of Trust approach

Given that mutual recognition of cross-border electronic messages will need to rely on identity assurance levels of devices collecting data, it is imperative that the authentication of such devices relies on mechanisms that are strong and accepted between parties involved in the trade facilitation process. In the context of Government-
to-Government (G2G) data exchange, this may be through bilateral agreements or through intergovernmental frameworks.

2.1.3 Privacy

IoT data flow is sometimes characterized by the flow of personal information generated from consumer and industrial use that may reveal habits, preferences, locations, affiliations, payment patterns and other critical information. IoT-connected devices are often, by design, discreet and can lack traditional screen interfaces, which may pose a challenge in obtaining informed consent from the user. The integration of IoT with other emerging technologies, such as AI, augmented intelligence, mobile computing and quantum computational applications, is not only redefining what is considered personal information but is also refining data and leading to a re-examination of how to address privacy concerns.

The European Commission (EC), which is the executive branch of the European Union that proposes new legislation and monitors its implementation, has been working since 2009 on the development of a clear IoT regulatory framework for a facilitative application of the technology system while keeping in mind privacy, data protection, consumer protection, safety, security and liability as the key issues to address to increase public trust in the IoT. General Data Protection Regulation (GDPR) is one such initiative, which also addresses IoT data privacy as part of its regulation.

From a trade facilitation perspective, the GDPR has attempted to balance out the relationship between the European Union and foreign corporations by allowing the transfer of personal data in and out of the European Union, provided that the foreign corporations apply the same rules as European corporations in dealing with personal data of individuals in the European Union.

In India, a similar data protection bill has come into force that is aimed at: protecting the autonomy of individuals in relation to their personal data; identifying the rights of individuals whose personal data is processed; creating a framework for the implementation of organizational and technical measures in processing personal data;

---


and establishing norms for the cross-border transfer of personal data. The bill emulates the GDPR in certain ways, but unlike the GDPR, the right to be forgotten is not a right to erasure. Moreover, the data protection bill is also aimed at supporting the policy on the IoT with the objective of creating a US$15 billion IoT industry by 2020 through the creation of smart cities that will encompass aspects of trade, supply chain and logistics together with health, water, waste etc.

The GDPR, the Indian data protection bill and other similar measures are gradually harmonizing the privacy requirements in dealing with personal data, and any mutual recognition mechanism in enabling cross-border trade can leverage these baseline guidelines in either adopting a similar legislation or designing their own.

2.1.4 Data ownership

The IoT and associated Machine-to-Machine (M2M) interactions also raise interesting issues on data ownership, where data are collected as part of one system, aggregated as part of other systems, processed in a third system all of which can be in different jurisdictions. Data ownership and data rights are generally associated in the context of Intellectual Property Rights (IPR). In Business-to-Business (B2B) transactions, the ownership and associated IPR is driven by data usage agreements which also govern other aspects such as identity, authentication and privacy. But in cross-border paperless trade where the parties to the transaction also include Government agencies, the ownership of data and associated IPR tends to be a tricky subject without clearly defining the term “data”, its origin, scope, ownership interests, and rights to use and process either all or part of the data.

Mutual recognition mechanisms that are either bilateral or intergovernmental must expand their scope to allow addressing the complexity involved in data ownership in cross-border trade. Projects such as the Smart Container project of UN/CEFACT present interesting possibilities where data may be collected in international waters but processed across multiple jurisdictions to facilitate making cross-border recognition of electronic messages more secure, reliable and effective.

2.1.5 Legal issues

IoT devices present interesting legal issues in terms of ability to authenticate digital evidence and trace provenance, and ascertain integrity of data through the
transmission process. The factors that are considered in evaluating the integrity of digital data include who created the evidence, what processes and technology were used, and what was the chain of custody throughout the entire digital evidence life cycle. Specifically, when the exchange of data is cross-border the issue of mutual recognition, both from the standpoint of legislation and its enforceability through the use of technology, will come to the forefront.

2.1.6 Mutual recognition

The IoT presents very interesting possibilities in helping cross-border mutual recognition of electronic messages become make economical, secure and effective as it presents the ability to transmit data required as part of the supply chain in a secure, cost-effective manner. This helps further to create cross-border supply chains that are less reliant on paper, less prone to manual errors and are able to drive decisions based on data from IoT devices.

For mutual recognition arrangements to be accepted and effective, there is a dependency on the level of trustworthiness and assurance that IoT transactions can guarantee. This is subject further to issues such as identity authentication addressed above as part of this research paper. Therefore, for IoT to be effectively used to make mutual recognition better, the foundation of what constitutes a trustworthy IoT system must be agreed upon. This can be done through bilateral, multilateral or intergovernmental frameworks driven by bodies such as the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP) and UN/CEFACT, among others.

2.1.7 The way forward

The IoT presents opportunities to automate various processes as part of cross-border trade as it obviates the need for physical data capture as part of shipping, logistics and transportation through the use of sensor technology. As IoT technology matures and interoperates with other emerging technologies such as Blockchain and Artificial Intelligence, it presents interesting possibilities in automating a number of supply chain-related processes that today involve considerable manual processing and data entry. As the usage of IoT systems is extended across borders, the key question is that of trustworthiness of IoT systems in capturing accurate and authentic data. This
may be driven through the adoption of standards and necessary framework arrangements outlined as part of mutual recognition.

In terms of the way forward towards leveraging IoT for facilitating cross-border mutual recognition of electronic messages, countries can look at:

- Defining trade processes that could leverage IoT data and M2M data exchange automation;
- Create pilot projects through public-private partnerships in areas of customs, logistics and shipping in order to evaluate data exchange and integration feasibility with existing customs, Single Windows and other systems;
- The adoption of international standards such as ISO 21823-1 for interoperability of IoT data exchange as well as for security and trustworthiness of IoT networks as part of various trade processes;
- Enabling legislative frameworks that support the usage of IoT data for cross-border exchange and mutual recognition of electronic information;
- Extend pilot projects to fully-fledged rollout of IoT systems that can then be integrated into domestic and international supply chains for facilitating cross-border paperless trade.

2.2 Blockchain

Blockchain is an emerging technology that has been capturing the imagination of academia, industry and the public sector alike. It is a technology that facilitates trusted information sharing in the absence of central trusted entities, which is a scenario that regularly arises in cross-border trade. This paper does not aim to introduce the technology itself. There are detailed published reports available publicly that describe this very well. In particular, refer to the WTO report, Can Blockchain Revolutionize International Trade, available at https://www.wto.org/english/res_e/booksp_e/blockchainrev18_e.pdf.

Cross-border paperless trade focuses on collecting, sharing, processing and using information about trade activities, including the flow of goods, information about goods, and financing associated with goods across borders. Typically, information about trade as represented in a country within its technical and legal context, may have limited applicability, visibility or acceptance by another trading partner country (for example, in a simple export-import scenario). In real-world supply chains this cross-border flow
of goods, information, and money is commonplace in the increasingly intertwined economies of the twenty-first century. Applications of Blockchain technology are emerging that consider entities involved in cross-border trade transactions, including natural persons, legal persons (companies), regulatory entities (authorities), impersonal entities (shipping containers instrumented with IOT devices), that share and maintain information and events on to a shared distributed ledger. This raises important issues concerning legal and regulatory issues with regard to information, what it represents and its ownership in the context of cross-border trade.

This report builds upon an earlier study of existing mutual recognition mechanisms, *Mechanism for Cross-border Mutual Recognition of Trade-related Data and Documents in Electronic Form*, which is available at https://www.unescap.org/sites/default/files/Mechanism%20for%20cross-border%20mutual%20recognition_Draft%2B.pdf. The study looks at existing schemes, including Mutual Recognition Agreements (MRAs) of Authorized Economic Operators (AEOs), the Asia-Pacific Economic Cooperation’s Telecommunications and Information Working Group (APEC TEL) effort, the Pan-Asian E-Commerce Alliance (PAA) mutual recognition scheme involving a Public Key Infrastructure (PKI) and the Eurasian Economic Union (EAEU) PKI mutual recognition agreement, among others. The study found commonalities in these approaches including:

- The existence of a governing stakeholder;
- A legal instrument binding the parties together;
- A clear ownership of requirements between parties involved in mutual recognition;
- Identification of implementing bodies of mutual recognition;
- Definition of the object of mutual recognition and a specific execution method;
- The maintaining trust in the technical execution of mutual recognition;
- The underlying technical standards needed.

This paper explores the potential of Blockchain technology for acting as one unifying framework/mechanism that addresses some of the technical mutual recognition requirements, including (e), (f) and (g), articulated in the study. The description is based on one specific implementation and case study for ease of understanding, but the technology underpinnings of Blockchain are more generic than a specific implementation and case study, and carry over to other instances as easily. The case
study on TradeLens, a large private sector Blockchain effort in the trade logistics and documentary trade space, is presented; it includes an overall description and the specific approach to mutual recognition.

Here the focus is on the issue of mutual recognition, acknowledging that it is equally (if not more) a legal issue and describing how Blockchain technology fits very nicely in facilitating several concepts that underlie the trust issues behind cross-border mutual recognition. This section is based on an example trade transaction from the Buy-Ship-Pay model, available online at http://tfig.unece.org/contents/buy-ship-pay-model.htm, i.e., the issue of a purchase order transaction initiated by an importer with an exporter.

As a trade transaction example, figure 3 shows where mutual recognition lies in the Buy-Ship-Pay model and describes a simplistic trade business network comprising an importer, an exporter, the respective import and export customs regulatory clearances, and a shipping line for logistics. Several other parties are involved in real-life scenarios, but the description in this section can easily be extended to those complex, more realistic networks and scenarios.

**Figure 3. Mutual recognition in the Buy-Ship-Pay model**

Before describing the example transaction in Blockchain terms, this study first explains six technical aspects of Blockchain technology that should be understood before looking at how they contribute to building trusted information sharing, thereby facilitating mutual recognition at least technically. The six aspects are:

- **Identity**;
- **Authentication**;
• Authorization;
• Smart Contracts;
• Endorsement;
• Immutability.

Before proceeding, this section focuses on one specific and popular technical implementation of Blockchain, called Hyperledger Fabric [https://www.hyperledger.org/use/fabric], to substantiate the technical description in this paper. This paper does not recommend one technical implementation over the several other choices available – such as Ethereum [https://ethereum.org], Corda[https://www.corda.net] or other Hyperledger projects – but it uses the one that is based on familiarity. With other implementations the following specifics would change but the underlying concept of Blockchain and fostering trusted information sharing remains invariant. Technical documentation for most of these implementations is publicly available and searchable; the documentation for Hyperledger Fabric is available at https://hyperledger-fabric.readthedocs.io/en/release-2.0/.

2.2.1 Identity

Each entity or actor in a Blockchain network needs to be digitally identified in that network by every other entity. One of the ways of doing this is using Public Key Infrastructure (PKI)[cite]. PKI works on the principle of hierarchical trust. Although there are other alternatives to PKI, such as PGP[cite], Symmetric Key Cryptography[cite] etc., these would have to be evaluated for their suitability in a specific Blockchain implementation. For the purposes of this paper PKI is described as a popular working technology choice while noting that neither Blockchain nor mutual recognition need to be tied to the specific implementation of PKI. However, the authors chose to be specific and hence the description below goes into the details of PKI. As already noted, this can also be applied to other identity mechanisms as long as the principles this paper is interested in are satisfied; as such, this paper does not recommend one implementation over the other. Technological neutrality on the subject is also recommended.

PKI involves a pair of asymmetric keys – a private key and a public key. These keys are mathematically computed numbers that are used to encrypt and decrypt pieces of information that are going to be sent over a communication medium, such as EDI
messages or Internet messages using technical protocols etc. The act of using a private key to encrypt a message is called “signing” the message. The act of decrypting the message using the sender’s public key is called “verification” of the message source.

The PKI system is such that once someone signs a piece of data with his/her private key, anyone having the corresponding public key can verify whether it was signed with the right private key. Usually, keys issued in a PKI setup involve verification of identity of the individual and/or organization, and associating this identity information as part of the certificate issued.

This is done by creating a hierarchy of trust, starting from a trusted certificate authority, and is circulated to the final entities of each of the participants of the network (e.g., administrator of import customs authority). In the case of the Blockchain system using digital signatures, while PKI could help solve the identity issue as keys have an associated identity, digital certificates used in one jurisdiction need to be respected in other jurisdictions for cross-border paperless trade using Blockchain. This also depends on the context of use of Blockchain, such as B2B or G2G – each of which may require varying identity assurance levels and/or bilateral/multilateral or intergovernmental frameworks to recognize digitally signed transactions across borders. There have been regional attempts to do this, such as the PAA initiative, and the best practices and lessons learnt can be instructive.

Examples of mutually recognizing identity and digital signatures include the European Union’s electronic Identification, Authentication and Trust Services (eIDAS) Regulation, which aims to harmonize and cross-recognize identity and trust services across the European Union.

2.2.2 Authentication

When the Smart Contract is substantiated in the network, the parties also decide on the set of authorized parties for each type of transaction. For example, a purchase order can only be issued by an importer. This is referred to as the “access control” mechanism for the system. In Blockchain, this is achieved by adding the authorized party to a lookup table (which is called “Access-Control-Lists” in Hyperledger Fabric) for the Smart Contract.
Every type of transaction in the system is documented in this table together with the set of parties who can invoke those transactions. This information resides with every participant in the network. Before committing the transaction, every participant verifies that the transaction was invoked by the right party.

In this study’s example, the importer is the only participant who can invoke an “issue-purchase-order” function. If any other participant tries to create a transaction invoking the above function, all other parties would reject it. In fact, the request for endorsement would be rejected in the first place. Endorsement is described below as a technical aspect. Since Blockchains require parties to reach an a-priori real-world understanding and agreement of transaction participation, the question of who can initiate or participate in which transaction is pre-determined and agreed upon, and codified in the rules of execution of the Blockchain. As such, Mutual Recognition of every trade transaction is agreed upon beforehand through discussion or MRAs, or by following existing international standards between parties in a Blockchain network. This includes intergovernmental authorities such as customs referred to in the example transaction in this paper, or more formal intergovernmental agreements between sovereign nations or an arrangement such as the Framework Agreement (FA) on Facilitation of Cross Border Paperless Trade in Asia and the Pacific7.

2.2.3 Authorization

Every transaction on the Blockchain is authorized using the signature of the invoking party and all the endorsers. Every participant who receives a block of transactions would validate that the transaction was authorized correctly.

At the time of commitment into Blockchain, all nodes verify whether:

- The transaction was initiated by someone authorized to invoke the particular Smart Contract function;
- All the endorsements for this transaction are consistent with each other;
- The endorsements are provided by relevant parties by checking their digital signatures.

In the example in this paper, after the transaction is executed everyone is aware that the transaction was indeed invoked by the importer.

Another aspect with regard to authorization is data visibility. In this study’s example, the shipping line does not need to know every purchase order that is signed between the importer and the exporter. Therefore, if the transaction is put on Blockchain, every participant in the network can see the details. This can be avoided using private data collections. The idea is that although the data are not visible to everyone, a unique identifier of the data (called hash) is committed on the Blockchain and is visible to everyone. The data reside in each of the parties “private data collection”. An example of this is described at the end of this section, in what a Blockchain-based bill of lading needs in order to be technically and legally accepted as a valid instrument. In that situation, it is noted that specific legal pre-conditions need to be met, including the passage of relevant laws, to enable what is technically achievable through trusted information sharing, as in Blockchains.

2.2.4 Endorsement

Every transaction in Blockchain will be initiated by one of the parties and each transaction has to be vetted by specific parties. This endorsement means that the transaction is attested by required parties in the network. Attestation involves signing the transaction with the endorser’s digital signature. In this study’s case, an “issue purchase order” transaction needs to be endorsed by both the importer and the exporter, while endorsement by the shipping line is not required. The endorsement scheme is pre-defined when starting the Blockchain network. In Hyperledger Fabric, the endorsement parties for each function in the Smart Contract can be defined.

Some example endorsements are:

- For the exporter’s transaction of “Ship goods to importer”, the shipping line, exporter and export customs need to endorse this transaction to make it valid;

- In a hypothetical case where banks are also involved, the importer’s transaction of “payment to exporter” needs to be endorsed by the importer’s bank and exporter’s bank so that the transaction can be accepted by other parties in the network.

Thus, endorsement is the process of collecting approval from the stakeholders of a transaction to later prove that it has been executed correctly. The endorsement process involves:
○ Simulation by the endorsing parties of the function with the user-given inputs and recording of the final state of different keys in the Blockchain;
○ The simulation inputs, outputs and the function itself make up the endorsement packet from each endorser, which is given back at the end of endorsement process;
○ In the final stage of commitment, nodes in the network make sure that all the endorsements are consistent with each other.

(Note: The example below shows the flow of a complete Blockchain transaction. To make cross-border recognition of transactions based on key oriented systems such as PKI possible, it is necessary to embrace a system that recognizes keys across jurisdictions and makes them interoperable, both technically and legally. Prior efforts exist that try to make PKI-based systems interoperable as well as mutually recognized across countries.)

2.2.5 Smart contract

Smart Contracts embody the well-known technology functionality of automatic execution of business rules against incoming data in a database. The term was popularized in public Blockchain networks but it is the simpler traditional definition that is relevant in the context here.

One of the important aspects of Blockchain is the fact that there is automatic execution of a transaction using pre-programmed functions. Every operation in the network is pre-programmed by all the participants in the form of functions – these are called Smart Contracts. This is the common code agreed upon by all participants and supported by the legal framework of all the jurisdictions under reference that runs on each participant’s server. Each transaction is just an invocation of some particular function in the Smart Contract with user-defined inputs.

Invocation of a function is restricted to specific parties as mentioned in the next point. In this study’s use case, the Smart Contract would have many functions such as “issue-purchase-order”, “payment-acknowledgment” etc. The importer invokes one of the functions, “issue-purchase-order”, from the Smart Contract while creating the transaction. This transaction is then sent to the endorsers. In the Hyperledger Fabric implementation, endorsers simulate the function invocation with the user-given inputs and decide the output of the function.
How would a sample Smart Contract be executed? Assume that all the data in the Blockchain network are stored in terms of key-value pairs. Each transaction either adds or updates a set of key-value pairs.

Smart Contract: Transfer money (US$100 from A to B):
- Look for key “A-Balance”;
- Check if “A-Balance” has more than US$100;
- Decrease value of “A-Balance” by US$100;
- Look for key “B-Balance”;
- Increase value of “B-Balance” by US$100.

The above steps are performed by every participant in the network. Before everyone makes the above changes, they check if they have the endorsements from the required participants as per the endorsement policy.

2.2.6 Immutability

Once the transaction is accepted by every participant in the Blockchain, it is virtually impossible to alter the transaction without changing the transaction on every other node in the Blockchain. This is because each block of the transaction is cryptographically linked to previous blocks, which makes it difficult to change.

Moreover, each participant in the network is convinced that each transaction is indeed endorsed by required parties. In the example here, when the “issue-purchase-order” transaction is committed, everyone in the network knows that this transaction was indeed approved (endorsed) by both the importer and the exporter.

The cornerstone of immutability is the one-way hash function. This is a mathematical function that takes a set of plain text and outputs a set of random looking characters as shown in figure 4.
The interesting property of such functions is that although it is computationally cheap to compute this function, it is virtually impossible to invert this function, i.e., given the hashed output, it is impossible to get the plain text back. In Blockchain, a block is a set of transactions (figure 5). Every block stores the hash to its previous block. This ensures that if someone wants to change an intermediate block, she would need to change all the blocks ahead of it.

In the above example, if we want to change a transaction in block 1, we would need to change block 2 as well since it stores the hash to block 1, which is now changed. Since block 2 is changed, it will be necessary to change block 3, and so on. This means that the older the blocks are in the Blockchain, the more difficult it is to manipulate them. Since every participant in a Blockchain maintains this blockchain of transactions, no one can make changes to blocks 1, 2 and 3 without being found out by the other members in the network. This inability to change the history of transactions leads to the immutability of data transactions once they are written on the Blockchain by all the participating members.
2.2.7 Putting it all together to engender trust in mutual recognition

Having reviewed the six technical aspects of Blockchain that comprise a transaction, the example issue-purchase-order transaction can be revisited to see how it all comes together and how this technology facilitates mutual recognition. Together, these six technical aspects ensure that information and data-sharing on correctly designed and implemented Blockchains are reliable, tamper-proof, secure and only allow authorized access.

When an importer wants to issue a purchase order, he/she creates a transaction packet with the Smart Contract function name (issue-purchase-order) and the inputs to that function (figure 6).

**Figure 6. Blockchain transaction packet**

This packet is then sent to “the exporter for endorsement. He/she checks if the details shown in it are correct. Once validated, the exporter adds her digital signature the transaction packet as part of the endorsement. The importer also endorses the same packet (figure 7).
Thousands of such transactions could be created at the same time. In Hyperledger Fabric, every transaction together with the endorsement is sent to a special node called an “orderer”, which sequences/orders transactions. The orderer bunches together a set of transactions into a block that is broadcasted to every participant.

Every participant checks if all the signatures are present in the transaction packet inside every block. Once everything is validated, the block is added as the next block in the Blockchain. Thus, the transaction is placed on the Blockchain. For convenience, every participant stores the current state of keys. This would be updated based on the Smart Contract function. Now, assuming that majority of the parties in the Blockchain network are non-malicious, the Blockchain will successfully run and allow only authorized persons to invoke a transaction.

In the use case in this study, once an “issue-purchase-order” transaction is committed, every player in the network has: (a) visibility about the transaction; and (b) validation that this was indeed signed by the authorized parties. Once the data are entered on the Blockchain, due to the chaining of blocks with hash function (as explained above) every transaction is tamper-proof. Moreover, hackers getting into one system and changing the value (which is done traditionally) won’t suffice, since the copy of Blockchain is maintained by all the members of the network. Hackers would need to hack a group of different machines to really bring down the Blockchain network.
The flow of the entire transaction is shown in figure 8. The importer creates a transaction to invoke the “issue-purchase-order” function, using the pre-agreed upon Smart Contract between the importer and exporter. As per the specific rules of the “issue-purchase-order” Smart Contract, this transaction is signed and then endorsed by the importer and sent to the exporter for subsequent endorsement, as detailed below:

- The importer gives the endorsement since the importer initiated it;
- The exporter validates the request he/she receives, and then checks the governing rule in the “issue-purchase-order” Smart Contract and gives the endorsement;
- The endorsement is sent back to the importer;
- In the case of the Hyperledger Fabric Blockchain, the transaction is then sent to the ordering service to order different transactions on the network. This means the endorsed transaction is lined up to be entered into the Blockchain by the ordering service;
- The ordering service then finalizes the order of transactions to be submitted committed (together with any other transactions across the supply chain that it receives) and sends the final transaction to all the committing persons to write on to the Blockchain;
- Every committing person checks the validity of endorsements (signatures of the parties like Importer and Exporter as per the pre-agreed rule of the “issue-purchase-order” Smart Contract) and stores the transaction into Blockchain.
It should be noted that most Blockchain implementations use PKI for digital signatures, which are widely accepted in the digital world as a result of their acceptance under respective national legislations for signing digital transactions. This provides good security for Blockchain networks; however, Blockchain is not tied to or dependent on PKI in any way and it can conceptually switch to other identities and security implementations based on the context of use, i.e., B2B, G2G or Business-to-Government (B2G). The choice of technology should be determined in the context of the level of identity assurance and data integrity required in order to effectively support mutual recognition of cross-border electronic transactions on Blockchain.

Hyperledger Fabric also uses a PKI framework to achieve authenticity, identity and authorization in the Blockchain network. Rather than getting certificates from worldwide trusted Certifying Authorities (CAs) such as VeriSign, Fabric Network employs its own certifying authority called Fabric-CA. In a modified version of fabric, it can be safely
assumed that PKI can be replaced with other cryptographic methods such as Pretty Good Privacy (PGP), Symmetric Key Cryptography etc. The alternatives are either outdated with known vulnerabilities or are infeasible in the current setting, but there is nothing in the technical underpinnings of Blockchain that needs PKI.

An example event as well as a document exchange transaction are used in the example in this section. Other documents in the trade process or other events (or both) are similarly handled in Blockchain networks as this example without loss of generality.

This study has shown how trust in information sharing across borders is facilitated by technologies such as Blockchain, using its underlying technical principles here. However, it is necessary to revisit the comments made at the beginning of this section. Mutual Recognition is equally a legal and a technical issue as explained in the beginning of this article under Section 1 (b). Take the example of the overloaded function of a Bill of Lading (BL) which is: (a) a title to the goods; (b) a receipt of the goods issued by a shipping line; and (c) the terms and conditions of the contract of carriage.

A BL is usually explicitly excluded from coverage in electronic transaction actions and electronic communication actions in the legal systems of most countries. The overloaded nature of this instrument and its negotiability as a financial instrument is precisely why this is done. Modern legal instruments do exist, such as the UNCITRAL Model Law on Electronic Transferable Records (MLETR), which provide a legal framework for the digitalization and hence subsequent Blockchain technical implementation of a true “e-bill of lading functionality. However, it is still early days for the MLETR. Until the beginning of 2020 only one country (Bahrain) had passed a law derived from it, although other countries are debating this internally.

A true “e-bill of lading” has certain requirements, such as:

- Assigning ownership to a specific participant in the network;
- An owner having exclusive control over the instrument and ability to transfer it to another participant in the network;
- An owner having an exclusive right to submit the bill to the shipping line and claim the goods;
• An owner may at any time be able to opt for a paper BL and get it issued by the shipping line without loss of history of ownership endorsements, contract of carriage, and being a receipt of goods.

It can be seen that the aspects of Blockchain described above in this section clearly and cleanly satisfy the technical requirements for supporting the implementation of MLETR.

While Blockchain is an appropriate emerging technology option for facilitating Mutual Recognition, this study argues that there is a need for constructs that help countries work together towards complete legal and technical mutual recognition of trade-related documents and information across borders. The ESCAP Framework Agreement on Cross-border Paperless Trade Facilitation (FA-PT) – which is a supporting treaty for the WTO Trade Facilitation Agreement (TFA) – is one such multilateral treaty being pursued by Asian and Pacific countries. That Agreement can potentially bring about mutual recognition for trade if ratified and implemented in the near future.

2.2.8 The way forward

This report reviews Blockchain as an emerging technology that has significant transformative potential for trade and logistics across the public and private sectors. Using specific use cases and implementation examples, this study shows how Blockchain works in the context of international documentary trade. It can clearly bring about benefits of trusted information sharing across the entire supply chain, which has been a long-standing point of contention due to lack of trust among involved parties.

However, as a technology in itself, Blockchain cannot fully solve the trust problem in supply chain ecosystems for a number of reasons. The main issue is that Blockchain itself works on the principle of information sharing and running business processes across organizational boundaries (including cross-border), which requires large-scale adoption in order to succeed. This remains a work in progress along with the other related issues of interoperability between the various Blockchain initiatives, technical implementation etc. As a technology, Blockchain will continue to evolve and embrace emerging standards; a significant enabler to this will be a regulatory and legal environment that recognizes business objects (such as documents and events) on the Blockchain as the single source of truth having legal credibility that will come about as a result as digitalization advances across sectors.
This study would like to encourage further dissemination of Blockchain technology across the public and private sectors, as the successful realization of its promise rests on wide scale adoption. Countries need to experiment and participate actively in Blockchain initiatives in sectors such as trade and finance, and to look at creating regulatory environments that help technology-based transformation to thrive.

3. Use cases in Blockchain and IoT

The following use cases in Blockchain and IoT highlight the benefits of these emerging technologies in enabling cross-border mutual recognition.

3.1 Blockchain

Table 2 details a case study of TradeLens, a large private sector international trade logistics initiative between shipping lines, port authorities, technology providers and other entities.

<table>
<thead>
<tr>
<th>Question</th>
<th>Reply</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong></td>
<td><strong>Short description</strong></td>
</tr>
<tr>
<td><strong>2.</strong></td>
<td><strong>Proposing/implementing/testing organization</strong></td>
</tr>
</tbody>
</table>
### Long description

TradeLens consists of the ecosystem of participants in global trade, the Blockchain platform that connects them, and the set of applications and services that sit on top of it.

The ecosystem includes TradeLens participants, such as ocean carriers, ports, 3PL, customs authorities, and shippers, that connect to, provide data to, and use the platform.

The platform is accessible via an open API and brings together the ecosystem through a set of open standards. It enables the industry to share information and collaborate. Blockchain and cloud technologies power the platform. The platform securely hosts the TradeLens data.

The Marketplace is an open platform that allows both TradeLens and third-parties to publish fit-for-purpose services atop the TradeLens platform.
TRADELENS IS BUILT ON AN OPEN TECHNOLOGY STACK AND IS UNDERPINNED BY BLOCKCHAIN TECHNOLOGY
<table>
<thead>
<tr>
<th></th>
<th>Description of business benefits from the use of TradeLens</th>
<th>Every participant in the network now has complete visibility (as per pre-agreed upon rules of visibility) on items that they are handling and which in silos earlier.</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Special concerns and challenges (legal, technical etc.)</td>
<td>At the time of this study, TradeLens was jointly owned by Maersk and IBM with IBM managing technology development. TradeLens is currently expanding its network and ecosystem of ocean carriers, ports, freight forwarders, and shippers.</td>
</tr>
<tr>
<td>6.</td>
<td>Rationale and trade-offs considered when selecting TradeLens</td>
<td>TradeLens technology deployment is currently managed by IBM and is built on Hyperledger Fabric. Currently, inter-operability with other Blockchains is limited. However, that is evolving with ongoing standards work (ISO TC 307) as inter-operability in Blockchains becomes further understood in the community.</td>
</tr>
<tr>
<td>7.</td>
<td>Describe data management techniques</td>
<td>All the data are stored in nodes of the Blockchain network. TradeLens permissions are determined through a combination of the organization’s role and the data type. The TradeLens platform then permits access to data according to a published permission matrix.</td>
</tr>
<tr>
<td>8.</td>
<td>In the implementation, where does data evaluation/processing take place?</td>
<td>In a Blockchain Smart Contract, on every participant’s node connected to the Blockchain network.</td>
</tr>
</tbody>
</table>
9. **Any open-source software being used/proposed?**
   TradeLens uses *Hyperledger Fabric* as the base to develop a Blockchain solution.

10. **Data-exchange standards used**
    A data-sharing standard has been defined –
    
    Standards used include UN/CEFACT, WCO, GS1 etc.

11. **Links to related information, including technical White Papers**
    GitHub for Hyperledger Fabric –
    Hyperledger Fabric technical paper –
    TradeLens website –
    https://www.tradelens.com/.

12. **Contact for further information**

### 3.2 Internet of things

An example of the usage of Smart Containers is Traxens (www.traxens.com), which fits Smart Containers across a range used in shipping, road transportation and logistics for collecting valuable data. Similarly, many use cases can be built leveraging Smart Containers to capture time, location and other events, based on which important decisions can be made. Some of these use cases can be seen at https://www.unece.org/fileadmin/DAM/cefact/brs/BRS-SmartContainer_v1.0.pdf.

**Table 3.**

<table>
<thead>
<tr>
<th>Question</th>
<th>Reply</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Short description</td>
<td>A container fitted with smart devices such as sensors to capture data on</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
</tbody>
</table>
| 3. Long description                         | Traxens is a company that works on providing Smart Containers, i.e., containers that have the capability to:  
(a) Use a sensor device fitted on or included in the container;  
(a) Collect data using a platform, process it and share with different stakeholders;  
(b) Communicate using different protocols including wireless communication technologies enabling multi-hopping and collaboration between devices.  
Through these sensors, smart containers gather important data, as demonstrated by Traxens, about:  
(a) Location, temperature, humidity and vibration to power a number of use cases including the time of arrival or transit;  
(b) Deviations such as unexpected door opening, and temperature and humidity changes;  
(c) Missing or overloaded containers;  
(d) Daily status of containers. |
| Description of business benefits from the use of Smart Containers | Some of the benefits of using smart containers include:  
(a) Better visibility and transparency in the supply chain;  
(b) Automation as part of logistics and transport execution;  
(c) Seamless collaboration between stakeholders;  
(d) Improving trustworthiness and enabling mutual recognition. |
|---|---|
| Special concerns and challenges (legal, technical etc.) | Since IoT data may be moving across borders, mutual recognition arrangements for the exchange of such data where required must be taken into account.  
From a technical standpoint, IoT ecosystems use different data formats etc., and aspects of interoperability and standardization must be taken into account for cross-border data exchange. |
<p>| Rationale and trade-offs considered when selecting Smart Containers | The major tradeoff is the incremental cost in developing a Smart Container-based ecosystem that will involve extensive investment in IoT equipment, infrastructure, communication channels, data collection and processing platforms etc. |
| Describe data management techniques | IoT uses a point-to-point data transfer. Therefore, data from multiple IoT devices can be collected centrally, using gateways that can then be further |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>distributed to various downstream systems for data processing.</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td><strong>In the implementation, where does data evaluation/processing take place. Check as many as are relevant</strong></td>
<td>In IoT ecosystems, data evaluation and processing takes place both at the edge as well as at centralized servers.</td>
</tr>
<tr>
<td>9.</td>
<td><strong>Any open-source software being used/proposed</strong></td>
<td>IoT data exchange could rely on open protocols such as MQTT or even HTTP as well as communication channels such as 3G/4G or LoRA etc.</td>
</tr>
<tr>
<td>10.</td>
<td><strong>Data-exchange standards used</strong></td>
<td>The data exchange standards used include MQTT, HTTP and CoAP.</td>
</tr>
<tr>
<td>12.</td>
<td><strong>Contact for further information</strong></td>
<td>Hanane Becha, (<a href="mailto:h.becha@traxens.com">h.becha@traxens.com</a>).</td>
</tr>
</tbody>
</table>