Super Charging Trade With A Trusted Global Digital Identity System

Hanna C. Norberg, TradeEconomista
Emmanuelle Ganne, World Trade Organization
Nadia Hewett, World Economic Forum

Type of Contribution: Policy Brief
Word count: 3586
Keywords*: Blockchain, Digitization, Supply Chains*

Contribution to the Policy Hackathon on Model Provisions for Trade in Times of Crisis and Pandemic in Regional and other Trade Agreements

Super Charging Trade With A Trusted Global Digital Identity System

Executive Summary:

Supply chains have been shown to be both especially vulnerable and crucial in times of crisis, such as the current COVID-19 pandemic. Developing new ways to promote trusted and agile supply chains is critical to sustain trade and mitigate disruptions. A key element of agile supply chains that is often overlooked in trade negotiations is mutually recognized trusted digital identities. In the world of international trade, this means that organizations incorporated in one participating country as a trustworthy or legitimate business entity would be mutually recognized in another country. This would allow for more rapid and agile verification of organizations (suppliers, exporters, importers etc) across jurisdictions .In this contribution we discuss how global trusted digital identity systems can be the key to unlocking the trust and agility that is essential to making supply chains resilient,
We start by outlining the main pain points and challenges that typically result from supply chain disruptions in times of crises and discuss how a global trusted digital identity system could help address them. We review various digital identity initiatives taken in recent years and discuss the value of decentralized identity systems based on blockchain[1]. There are, however, no concerted efforts focused on realizing all the pieces needed for a complete global- or regional for that matter- trade digital identity solution. Our analysis of RTAs currently in force, and notified to the WTO, reveals that -while RTA provisions generally include language regarding electronic authentication and electronic signatures, as well as acceptance of electronic documents to foster paperless trade- they do not address the issue of digital identities (with the exception of the recently signed Digital Economy Partnership Agreement, which does so in a very general way).

Building an ecosystem of mutually recognized trustworthy digital identities at a global level could be a significant catalyst to facilitate trade through more agile supply chains and help build resilience to future crises – which would ultimately benefit small and medium-sized enterprises (SMEs) significantly. The need for increased digital cooperation and digital solutions is, in fact, highlighted by the United Nations Road Map for Digital Cooperation and across the Sustainable Development Goals.

We argue that priority should be given to this issue in RTAs and other trade agreements before the various initiatives under way create a spaghetti bowl of siloed approaches that make the realization of a globally trusted digital identity system difficult to realize. In conclusion, we suggest language that trade negotiators may want to include in future trade agreements to help build a regulatory environment that would support the deployment of a global trusted digital identity ecosystem hat would promote agile, fast and trust-worthy verification of supplier credentials. This would help ensure that supply chains remain supple and resilient, including in times of crisis.

[1] While blockchain is one type of distributed ledger technology, for simplicity, the terms are used interchangeably in this publication

1. Globally trusted digital identity systems, a "lifehack[2]" to supercharging supply chains

Organizations need to know and trust each partner they engage with. Identity and trust lie at the core of each trade interaction. As supply chains are becoming increasingly digital, organizations need to ensure they are dealing with the right entity. They need to efficiently link a digital identity and a real organization, and more importantly evaluate the trustworthiness of legal entities they wish to engage with. This process of dynamically verifying counterparts – supplier management and verification – is a critical step in establishing trust in trade[3].

When companies are prompted to find new suppliers, it is not only a matter of match making, i.e. finding suppliers who can meet the descriptions and quantity of the goods, but also a matter of trust, i.e. making certain that questions such as "What suppliers can I trust?" "Are these masks meeting health regulations and authorizations?" "Are these new vendors compliant? Do these suppliers meet anti-money laundering and other requirements?" are answered in a reassuring matter.

During times of crises and supply chain disruptions, the pressure and need for trustworthy supplier verification is even more critical. It is a crucial ingredient to enabling agile, transparent, and trustworthy supply chains. Why? Because during supply chain disruptions:

- There is typically a need for new supplier relations to be forged quickly
- Finding new suppliers and verifying their prominent information for compliance and other reasons take time and money.
- The increased likelihood that parties do not know each other before they conduct business together and the risk of doing business with fraudulent suppliers increase.[4] The centralized systems existing today still leave a lot of room for fraudulent players to appear trustworthy.
- There is often an increase in counterfeit and fraudulent products and transactions. This not only puts further pressure on the supply chain and supply shortages, but can also risk lives (e.g. food-quality issues or not meeting medical equipment standards).

The COVID-19 crisis is a case in point[5]. The surge in demand for e.g. PPE and medicines and panic buying revealed both an acute lack of robustness[6] as well as the absence of agility in current supply chains. [7] Various counterfeit scandals and record seizures of faulty masks highlighted the vulnerability of the medical device supply chain. [8] A major California labor union, for example, discovered a stockpile of 39 million masks, which was later discovered to be an elaborate scam.[9] Dubious brokers and suppliers started flooding the market with suspect offers, creating an atmosphere of confusion and distrust just as hospitals were trying to stock up essential medical equipment to protect doctors and nurses from the virus.[10] In addition, as demand for PPE and other essential medical equipment surged, a growing number of clothing and consumer goods manufacturing companies chose to temporarily adjust their production lines to make and supply masks and other needed medical supplies. However,

---

[2] Defined by Merriam-Webster as "a usually simple and clever tip or technique for accomplishing some familiar task more easily and efficiently"

[3] Inclusive Deployment of Blockchain for Supply Chains, Part 2: Trustworthy Verification of Digital Identities, *World Economic Forum*, 2019

[4] PwC's 2020 Global Economic Crime and Fraud Survey revealed that one out of five business partners cited that vendors or suppliers constitute maximum fraud risk.

[5] Miroudot (2020) offers a comprehensive overview of the COVID induced disruptions to supply chains

[6] Brandon-Jones et al (2014) defines robustness as the ability to maintain operation during a crisis.

[7] Agility refers to the ability of easily finding new ways or suppliers in order to meet the acute surge in demand.

[8], Su (2020).

[9] Guiterrez and Elhmarek (2020).

[10] Associated Press report of 12 April 2020 (https://apnews.com/8d85b333ade3b343eba01b254185b966)

as these companies were not known as medical device suppliers, there was no easy way for hospitals, governmental agencies and health care organizations to quickly find these alternative suppliers and to efficiently on-board them.[11]

Enabling trustworthy supplier verification would be a significant step towards mitigating supply chain disruptions and risks during times of crises. It requires an agile supplier and digital identity management process to ensure that supplier verification is a) fast b) trust-worthy c) agile d) transparent and d) compliant.

Supplier verification processes are currently performed in centralized siloes (see Figure 1). Different public and private solutions record, maintain and verify identical identity data - potentially hundreds of times over - and are not interoperable, creating a significant amount of redundant identity information and duplicative efforts. Not only is this a waste of resources for all parties involved, but it is also error-prone, paper-heavy, and difficult to scale. This creates specific challenges for small and medium-sized enterprises (SMEs), who are not only more sensitive to trade barriers than larger firms, such as compliant supplier verification, but are also more vulnerable to the economic pressures brought on by supply chain disruptions and crises. Reducing barriers for them to trade internationally is essential. Improved digital identity and supplier verification systems can be key in supporting SMEs. Helping them to reduce red tape when doing business abroad, by reducing the costly supplier verification process, empowers them to have more agile responses to business opportunities. SMEs are at a disadvantage when compared with more recognized, reputable brands as far as conducting trustworthy supplier verification processes.

In addition, new demands with Industry 4.0 technologies – IoT, AI and blockchain in particular – implies that that organizations will likely be doing business with "things" and autonomous software agents in the future, which further amplifies the need for redesigning supply chain digital identity systems[12].

Digital identity verification and management systems should therefore be redesigned to enable fast, trust-worthy, agile, and transparent supplier verification to support more agile and trustworthy supply chains. A critical point, however, is to ensure that such systems are interoperable and mutually recognized. This can only happen through concerted efforts. The need for increased digital cooperation and digital solutions is, in fact, highlighted by the United Nations Road Map for Digital Cooperation[13] and across the Sustainable Development Goals. Trade agreements, in particular RTAs, are the perfect vehicles to promote greater digital cooperation and the development of mutually recognized trusted digital identity systems. They should be leveraged to that effect.

[11] IBM News of 12 April 2020 (https://newsroom.ibm.com/2020-04-27-IBM-Helping-to-Battle-COVID-19-Medical-Supply-Chain-Shortages-with-the-Launch-of-IBM-Rapid-Supplier-Connect)

[12] Inclusive Deployment of Blockchain for Supply Chains, Part 2: Trustworthy Verification of Digital Identities, *World Economic Forum*, 2019

[13] https://www.un.org/en/content/digital-cooperation-roadmap/

2. What is needed to make it happen?

2.1. The need for trusted digital identities mutually recognized across jurisdictions

There are already good efforts underway to improve digital identity systems and trusted traders' schemes in supply chain. There are, however, no concerted efforts focused on realizing all the pieces needed for a complete global- or regional for that matter- trade digital identity solution[14].

Building mutually recognized systems of trustworthy digital identities at a global level could be a significant catalyst in facilitating trade, encouraging economic growth, and helping SMEs. Having access to reliable information regarding business partners is crucial for dynamic digital interactions in global supply chains[15].

Increased awareness regarding the need for mutually recognized trusted digital identities in trade has prompted the development of various separate initiatives in the past few years, such as the Legal Entity Identifier (LEI) and the Trade Identification Number (TIN). In the wake of the 2008 financial crisis, regulators worldwide acknowledged the problems stemming from their inability to identify parties to transactions across markets, products, and regions. As a result, the Financial Stability Board (FSB), together with the finance ministers and central bank governors represented in the Group of 20 (G20), advocated developing a universal Legal Entity Identifier (LEI) applicable to any legal entity that engages in financial transactions. Implementation of the LEI increases the authorities' ability to evaluate systemic and emerging risk, identify trends and take corrective steps[16].

For entities involved in financial transactions, the Global Legal Entity Identifier Foundation (GLEIF) is used to support the implementation and use of the ISO standard of Legal Entity Identifier (LEI). It connects to vital reference information that enables precise and unique identification of legal entities participating in financial transactions. Each LEI contains information about an entity's ownership structure and thus answers the questions of "who is who" and "who owns whom"[17].

In parallel, the World Customs Organization developed the Trade Identification Number (TIN), which is now commonly used by customs, in particular in the context of Authorized Economic Operator (AEO) programmes. AEO programmes are trusted traders' schemes which aim at facilitating customs processes for companies deemed trustworthy.[18] Unlike the LEI, the TIN is not open source, and it is a system limited to customs operations.

---

[14] The concept of a Global Trade Digital Identity (GTID) is introduced and explored in further detail in the World Economic Forum's white paper on Inclusive Deployment of Blockchain for Supply Chains, Part 2: Trustworthy Verification of Digital Identities, *World Economic Forum*, 2019

[15] Inclusive Deployment of Blockchain for Supply Chains, Part 2: Trustworthy Verification of Digital Identities, *World Economic Forum*, 2019

[16] https://www.gleif.org/en/about/history

[17] World Economic Forum, A Blueprint for Digital Identity, 2016

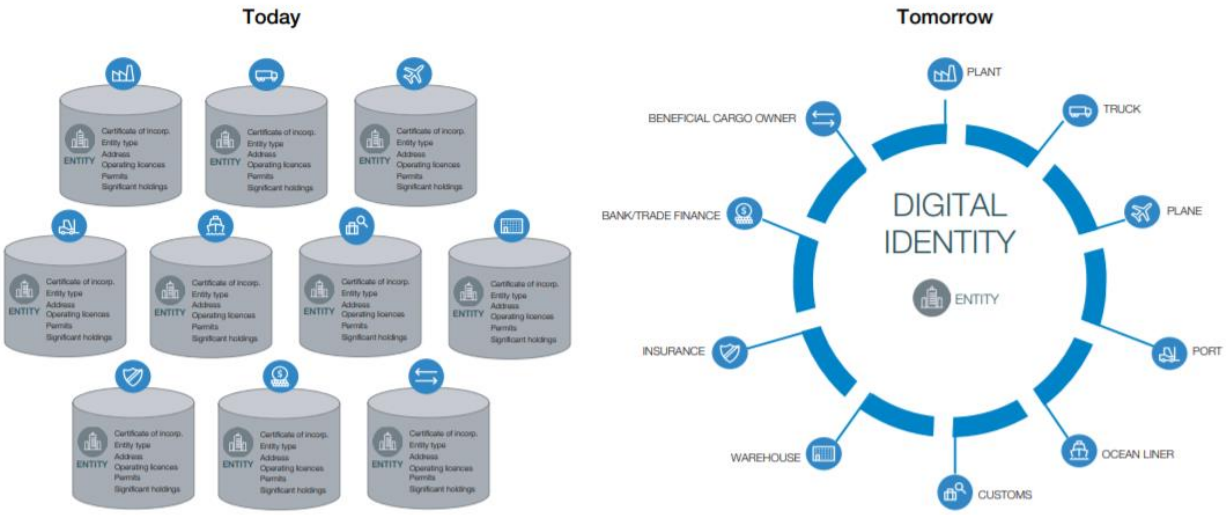
[18] An Authorized Economic Operator (AEO) is defined by the WCO SAFE Framework of Standards as a party involved in the international movement of goods, in whatever function, that has been approved by, or on behalf of, a national Customs administration as complying with WCO or equivalent supply chain security standards (http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/aeo-implementation-guidance.pdf?la=en). To qualify as an AEO, companies have to meet a certain number of criteria. AEOs can be manufacturers, importers, exporters, brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses and distributors. In 2019, there were 84 operational AEO programmes and 19 AEO programmes under development (http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/aeo-compendium.pdf). The WTO Trade Facilitation Agreement calls on WTO Members to put in place AEO programmes (Article 7.7 of the TFA).

While both the LEI and the TIN initiatives aim to enhance trust by building systems of identification of companies, their scope is limited to only parts of the supply chain. Building an ecosystem of mutually recognized trusted digital identities is critical for trustworthiness and fluidity of the entire supply chain.

2.2. Possibilities enabled by blockchain

The advent of blockchain[19] technology has opened new opportunities to improve verification of the credentials of suppliers. Because of its synchronized and tamper-proof characteristics, blockchain not only enhances trust, but it has also enables d*ecentralized* holding of information (unlike traditional databases, which are administered by a central entity). In the case of identities, this implies decentralization of identities through self-sovereign identities, i.e. the possibility for entities to self-manage their identity (see Appendix 1 for a description of blockchain technology). Decentralized identity infrastructure allows each legal entity to manage its identity, related verifiable credentials and their usage throughout global supply chains, thereby breaking existing identity siloes (see Figure 1 and Appendix II).

Figure 1[20]: The evolution from the current siloed set up, to decentralized identity management on blockchain



Various blockchain based identity solutions are already in production across the world. The Sovrin Network, for example, is a public-permissioned blockchain designed as a global public utility exclusively designed to support self-sovereign identity and verifiable claims[21], which is used by the British Colombia and Ontario's Verifiable Organizations Network (see Box 1). Other initiatives include Civic (CVC)[22] and uPOrt[23].

[19] This paper, like many others, uses the term blockchain in its generic sense to mean Distributed Ledger Technology, DLT.

[20] Inclusive Deployment of Blockchain for Supply Chains, Part 2: Trustworthy Verification of Digital Identities, *World Economic Forum*, 2019

[21] https://sovrin.org/

[22] https://www.civic.com/company/

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

As the Covid-19 pandemic hit the world, disrupting supply chains in an unprecedented way, the unique characteristics of blockchain has led various actors to leverage the technology to help buyers identify new trusted suppliers and efficiently vet and onboard them.[24]

As these various solutions are further expanded on post COVID-19, it holds much value for trade long-term. The emergence of decentralized identity systems holds a unique opportunity for global supply-chain organizations and governments to create global digital identity systems that cater for future supply-chain interactions. However, that requires that governments, in collaboration with the industry, enable a concept in which government identities, signatures and verifiable credentials are mutually recognized across regions and ultimately globally[25].

Without a common framework that allows these various digital identity solutions to be mutually recognized, and therefore to interoperate, the opportunities that such solutions open to make supply chains more agile and trustworthy will remain vain and digital identity siloes will continue to co-exist, hindering supply chain efficiency.

Box 1
Example: British Colombia and Ontario's Verifiable Organizations Network

The Canadian provinces of British Colombia and Ontario designed the Verifiable Organizations Network (VON) to enable a trusted digital environment for their businesses. Using the decentralized identity system Sovrin Network, where they have placed their credential definitions and verification keys, it aims to furnish businesses with a trusted digital identity issued by their local government with which they can conduct their affairs globally. As per mid-March 2019, VON had issued more than 7 million verifiable credentials for Canadian companies.

2.3. Building globally interoperable trusted digital identity systems

The importance of interoperability of digital identity systems to support cross border operations has been acknowledged at the EU level in the eIDAS (electronic IDentification, Authentication and trust Services) regulation which entered into force 2014 with an application date of July 2016. The eIDAS regulation was developed to enable businesses to "take advantage of cross-border business opportunities to increase the efficiency and security of […] businesses and improve user experience".[26] eIDAS regulates electronic signatures, electronic transactions, involved bodies, and their embedding processes and puts significant emphasis on the importance of interoperability and transparency. Member states are required to create a common framework that will recognize electronic identification (eIDs) from other member states and ensure its authenticity and security to facilitate the conduct of business across borders. The eIDAS regulation provides for a list of trusted services that may be used within the centralised signing framework.

Several elements necessary to realize a global trade digital identity system are also being discussed in the context of the United Nations. UNCITRAL Working Group IV, for example, is working on a draft legislative text on identity management and trust services which includes cross-border aspects (i.e. legal recognition).[27]

Global concerted efforts are now needed to realize all of the pieces for a complete global trusted trade identification solution. Trade agreements, starting with RTAs, can play an instrumental role in operationalizing such a solution.

[24] See for example the IBM Rapid Supplier Connect project (https://www.ibm.com/blockchain/solutions/rapid-supplier-connect).

[25] Inclusive Deployment of Blockchain for Supply Chains, Part 2: Trustworthy Verification of Digital Identities, *World Economic Forum*, 2019

[26] https://ec.europa.eu/digital-single-market/en/discover-eidas

[27] https://uncitral.un.org/en/working_groups/4/electronic_commerce

Unfortunately, provisions on digitization contained in the 305 RTAs currently in force and notified to the WTO up to June 2020[28] exclusively focus on electronic authentication and electronic signatures, as well as paperless trade, i.e. the process of making trade administration documents submitted by traders available and accepted electronically. None of the 305 RTAs analysed address the issue of identity.

A novel and notable exception is the Digital Economy Partnership Agreement (DEPA) between Singapore, Chile and New Zealand, which was signed on 12 June 2020 and had not yet been notified to the WTO at the time of writing. This agreement breaks new ground in this respect. It is a first of its kind, establishing new approaches and collaborations in digital trade issues with a view to promoting interoperability between different regimes and addressing the new issues brought about by digitalisation. The DEPA includes a whole section on digital identities, one of the key objectives of the DEPA being to facilitate end-to-end digital trade based on safe and secure digital identities that are mutually recognized. DEPA provisions on digital identities focus on interoperability and comparable levels of protection. They remain, however, relatively general[29], and leave plenty of room for discussion with regards to details and practical implementation.

A more ambitious approach to digital identities in trade agreement is needed to build globally mutually recognized trusted digital identity systems to support more agile supply chains and help build resilience to future crises. Digital identity initiatives are still in their infancy. Now is the time to act before a spaghetti bowl of siloed approaches makes the realization of a globally trusted digital identity system difficult to realize .Priority should be given in RTAs and other trade agreements to establishing trustworthy and agile trade digital identity systems that are recognized across jurisdictions with global standardized verifiable credentials for businesses and governments.

2.4. Expanding the use of digital identity tools to authentication and authorization of trade documents

Verifying the trustworthiness of a legal entity is only the beginning. Digital identity tools can be used for other purposes, such as for authorizing and providing other information (e.g. export licences or C-TPAT certification). Expanding the use of digital identity tools to authentication and authorization of trade document, for example, is a natural next step and can further bring value in reducing trade barriers. Ultimately, the goal should be a to develop an ecosystem based on more fluid and interoperable supply chain and identity verification to engage legal entities, things and autonomous software agents. This

[28] Building on the work of Monteiro & Teh (2017), which analysed 275 RTAs in force until May 2017, we further reviewed another 30 RTAs currently in force and notified to the WTO between May 2017 and June 2020.

[29] The DEPA article on digital identities read as follows:
Article 7.1: Digital Identities
1. Recognising that the cooperation of the Parties on digital identities, individual or corporate, will increase regional and global connectivity, and recognising that each Party may have different implementations of, and legal approaches to, digital identities, each Party shall endeavour to promote the interoperability between their respective regimes for digital identities. This may include:
(a) the establishment or maintenance of appropriate frameworks to foster technical interoperability or common standards between each Party's implementation of digital identities;
(b) comparable protection of digital identities afforded by each Party's respective legal frameworks, or the recognition of their legal and regulatory effects, whether accorded autonomously or by mutual agreement;
(c) the establishment or maintenance of broader international frameworks; and
(d) the exchange of knowledge and expertise on best practices relating to digital identity policies and regulations, technical implementation and security standards, and user adoption.
2. For greater certainty, nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 1 to achieve a legitimate public policy objective.

may be too ambitious to build into trade agreements at this stage, but nevertheless should be kept in mind once a global trusted digital identification framework has been put in place.

3. Wanted: Concerted efforts to enable mutually recognized digital identity systems - Proposed recommendations for inclusion in RTAs and other trade agreements

While RTAs have come a long way in dealing with digital developments such as e-commerce, attention of trade negotiators has not yet turned to the critical issue of enabling more efficient, scalable, and sustainable trusted digital identities, or only to a very limited extent.

Specific provisions on trusted digital identities should be systematically included in RTAs and other trade agreements. Below are key elements that we believe should be included in such provisions:

Article 1 - Mutual recognition of trusted digital identities

- The Parties recognize that trusted digital identity schemes contribute to more secure and agile supply chains and can be a catalyst in facilitating trade.
- The Parties agree to develop or maintain an enabling legal framework for a trusted digital identity system. Such framework should be consistent with the principles of the UNCITRAL Working Group IV and other relevant principles and standards already in existence.
- The Parties agree on mutually recognized procedures for issuing and proofing identities (legally incorporated entities in the Parties jurisdiction), including:
    - Agreement on the minimum level and type of information (or attributes) to be proofed and validated for issuing trusted identities. This 'digital identifier'[30] will consist of one or more attributes that can uniquely characterize an entity.
    - Agreement on electronic information or data sources to be used to document that an entity is a legal entity under the Parties' specific jurisdiction.
    - All Parties must ensure that updates to the legal status of an entity are continuously maintained and immediately communicated. As soon as a legal entity changes status, it should be communicated directly from the Party and made available to other Parties in order to flag those who intend to interact with the legal entity.
    - Each Party has the right to authorize an agency (trusted party) to approve the establishment of a legal entity within its jurisdiction
    - Agree on which institutions can act as the trusted party (for instance financial institutions) that confirms the validity of a physical proof of incorporation (and subsequently issues a digital identity). These trusted parties need to be agreed as trustworthy by all Parties.
    - Proposed new verifiers (trusted parties) should be agreed upon by all Parties to the Agreement.
    - If a digitization process is not already in place, the trusted authorities of each Party shall work towards digitalizing the process of legal entity incorporation as soon as practically possible
- Each Party shall endeavour to avoid any unnecessary regulatory burdens.
- The Parties shall endeavour to work on common standards.
- All Parties should adopt or maintain laws and regulations for the protection of personal information (PIIs) of information provided. The trusted digital identity system should be executed in a way that allows involved institutions to protect sensitive data and recognize cultural and ethical expectations

[30] A digital identifier is one or more attributes that uniquely characterize an entity in a specific context. It is used as the key by the parties to agree on the entity being represented (ISO/IEC 29115:2011)

about data protection and privacy. It shall take into due consideration international standards of data protection.
- Mutual recognition of trusted digital identity systems can be temporarily paused or all-together suspended if government identity issuance systems and processes are compromised or destroyed/corrupted. The Parties endeavour to assess alternatives or other mechanisms which can be available.
- Nothing shall prevent a Party from adopting or maintaining measures inconsistent with the points above to achieve a legitimate public policy objective.

Authenticating a legal entity's identity is only a first step towards paperless trade. A second step would involve using the system for authorization and provision of trade documents such as licences and certificates. The parties may want to consider including language along the following lines in their RTA in addition to the provisions listed above.

Article 2 - Ensuring trusted digitally signed trade documents

- The Parties recognize the importance of ensuring that digitally signed trade documents are issued by an authorized agent, that they have not been tampered with and that only authorized entities have access to them.
- The Parties mutually agree which public authorities or other organizations are authorized to sign trade documents, submit transactions, and issue such documents. These public authorities need to be identified as trustworthy by all Parties.
- An agent in the importing country can verify that the exporting agent which has digitally signed the trade document is an authorized issuer of a specific document under the exporting country's jurisdiction.

Article 3 - Cooperation

- The Parties shall endeavour to maintain a dialogue on regulatory issues raised by trusted digital identity schemes. In particular, they shall endeavour to:
    - Exchange information and good practices on:
        - The functioning and management of trusted digital identity schemes;
        - Policies, regulations, enforcement and compliance regarding how IT systems are secured.
    - To cooperate to address legislative, regulatory and technical barriers as soon as practically feasible.
- The Parties will work together to assist SMEs. to fully participate in such schemes.
- The Parties affirm the importance of actively participating in relevant fora, including multilateral fora, to promote the development of trusted digital identity schemes and issuance of trusted digitally signed trade documents.

Consideration should also be given to including similar provisions in other trade agreements, starting with the new set of rules being developed in the context of the WTO JSI on ecommerce.

4. Conclusion

The Covid-19 pandemic has shaken the world in an unprecedented way and highlighted the urgent need to make supply chains more robust and agile. It has also shown that going digital is no longer optional. The purpose of our contribution has been to highlight that with the

digitization of supply chains comes the need to put in place a global trade digital identity system, as a prerequisite for more efficient, agile and trustworthy supply chains.[31]
If the current isolated identity approaches continue, the digitization of global trade will likely be slowed, and enabling more dynamic digital interactions between the various parties could be challenging and costly. This is especially hard on SMEs, who are not only most vulnerable to economic pressures brought by disruptions, but also crucial to revitalizing supply chains.

The realities of the digital-business era and a post-COVID world requires trade agreements to be reimagined. Priority should be given in trade agreements to establishing mutually recognized digital identity schemes to support the development of a global trusted digital identity ecosystem. Digitization can't happen in a regulatory vacuum, or within national jurisdictions. It will require regulators to step in and finding ways of collaborating internationally and with other actors, such as in the pretext of negotiating RTAs. While our paper maps out the way to move forward in the sense of updating the texts in RTAs, there is still much work to be done involving a multi stakeholder approach, to ensure that the systems get practically and productively implemented.

References:

Baldwin, R and S. J. Evenett (2020) COVID-19 and Trade Policy: Why Turning Inward Won't Work, A CEPR Press VoxEU.org eBook, https://voxeu.org/content/covid-19-and-trade-policy-why-turning-inward-won-t-work

Baldwin, R. (2013) *Global supply chains: why they emerged, why they matter, and where they are going* in Global Value Chains in a Changing World, Fung Global Institute (FGI), Nanyang Technological University (NTU), and World Trade Organization (WTO), 2013.

Brandon-Jones, E., B. Squire , C.W. Autry and K.J. Petersen (2014), *A Contingent Resource-Based Perspective of Supply Chain Resilience and Robustness*, Journal of Supply Chain Management 50:3, 55-73.

Chaney, T. 2018. "The Gravity Equation in International Trade: An Explanation." *Journal of Political Economy*, vol. 126, no. 1. April.

Evenett, S. J. (2020) Tackling Covid-19 Together, the trade policy dimension, Global Trade Alert, University of Saint Gallen, Switzerland, 23 March 2020, https://www.globaltradealert.org/reports/51

Guiterrez, M. and A. Elhmarek (2020) How a stockpile of 39 million masks was exposed as fake, Los Angeles Times, 11 April 2020.

Ganne, E. (2018) C*an Blockchain revolutionize international trade*? World Trade Organization, Geneva, Switzerland.

Government of France (2020), "Décret n° 2020-190 du 3 mars 2020 relatif aux réquisitions nécessaires dans le cadre de la lutte contre le virus covid-19", 3 March 2020.

[31] Inclusive Deployment of Blockchain for Supply Chains, Part 2: Trustworthy Verification of Digital Identities, *World Economic Forum*, 2019

Inclusive Deployment of Blockchain for Supply Chains, Part 2: Trustworthy Verification of Digital Identities, *World Economic Forum*, 2019, http://www3.weforum.org/docs/WEF_Trustworthy_Verification_of_Digital_Identities_2019.pdf

Javorcik, B. (2020) "Global supply chains will not be the same in the post-COVID-19 world" In COVID-19 and Trade Policy: Why Turning Inward Won't Work.

Keynes, S (2020) "New trade barriers could hamper the supply of masks and medicines", The Economist, 11 March 2020.

McDaniel C. and H.C. Norberg (2019) "Can Blockchain Facilitate International Trade", *Mercatus Research Paper*, Mercatus Center at George Mason Institute, Virginia, VA, USA, April 2019.

Miroudot, S. (2020) "Resilience versus robustness in global value chains: Some policy implications" in COVID-19 and Trade Policy: Why Turning Inward Won't Work, A CEPR Press VoxEU.org eBook, https://voxeu.org/content/covid-19-and-trade-policy-why-turning-inward-won-t-work

Montiero, J.-A. and R. Teh (2017) "Provisions on Electronic Commerce in Regional Trade Agreements", WTO Working Papers, July 2017.

Norberg, H. C. (2019) "Unblocking the Bottlenecks and Making the Global Supply Chain Transparent: How blockchain technology can update global trade", *SPP Briefing Paper,12:9,* March 2019, The School of Public Policy, University of Calgary and the Canadian Global Affairs Institute

PwC's 2020 "Global Economic Crime and Fraud Survey, Fighting fraud: A never-ending battle", https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html

Su, A. (2020) " Faulty masks. Flawed tests. China's quality control problem in leading global COVID-19 fight", Los Angeles Times, 10 April, https://www.latimes.com/world-nation/story/2020-04-10/china-beijing-supply-world-coronavirus-fight-quality-control.

Tapscott, D. and Tapscott, A. (2017) "Realizing the Potential of Block chain, A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies", *World Economic Forum White Paper*, June.

WEF (2019)" Inclusive Deployment of Blockchain for Supply Chains, Part 2: Trustworthy Verification of Digital Identities".

WTO (2018) "World Trade Report, The future of world trade: How digital technologies are transforming global commerce*"*, World Trade Organization, Geneva, Switzerland.

WTO (2020) "Trade in Medical Goods in The Context of Tackling COVID-19", Information Note, Geneva: World Trade Organisation.

Zago, Matteo. 2018. "50+ Examples of How Blockchains are Taking over the World." Blog. 3 May, https://medium.com/@matteozago/50-examples-of-how-blockchains-are-taking-over-the-world-4276bf488a4b.

Appendix I

What is blockchain and how does the digital identity application work?

Blockchain technology is a technology that first appeared in 2008 and that allows to record and store digital transactions in a decentralized, distributed and secured way using a blend of proven cryptographic technologies. Information added to the ledger is stored in a near inalterable way using cryptographic techniques. Unlike traditional databases, which are administered by a central entity, blockchains are managed by computers or servers – called "nodes" – on a peer-to-peer basis without the need for the intermediaries who traditionally authenticate transactions (such as banks in the case of financial transactions). Authentication of transactions is achieved through cryptographic means and a mathematical "consensus protocol" that determines the rules by which the ledger is updated, which allows participants with no particular trust in each other to collaborate without having to rely on a single trusted third party. Data added to the blockchain are time stamped, shared in near real time with all participants in the network, and are verified and validated by anyone with the appropriate permissions on the basis of the consensus protocol of the blockchain. Records added to the ledger are quasi-immutable and are linked to one another which allows for easy traceability of transactions.

While technically speaking blockchain is only one type of distributed ledger technology (DLT), the term is often used in a generic sense to refer to DLT. The term blockchain is also used interchangeably to refer to the technology itself and to its applications through blockchain platforms.

At the technology level, there are many different types of distributed ledger technologies that underpin existing blockchain projects and that use different consensus mechanisms and ways of storing data.

At the application level, blockchain platforms vary in terms of the degree of decentralization and access. Blockchain platforms can be permissioned (access is restricted) or permissionless (open to anyone with a computer, with no restrictions imposed on who can access the platform and validate transactions), and they can be public (no specific entity/entities manage(s) the platform, transactions are public and individual users can maintain anonymity) or private or consortium blockchains (i.e. permissions to validate and write data onto the blockchain are controlled by one entity or a group of entities). The rights to read and write therefore differ from one blockchain platform to another.

Using the technology for decentralized identity infrastructure (as proposed in the paper), legal entities have a self-managed digital identity independent of individual service providers, thereby breaking existing identity isolation. This allows each legal entity to manage its identity, related verifiable credentials and their usage throughout global supply chains.

The issuing of standardized, tamper-resistant and nonrepudiable verifiable credentials by trusted entities is an important component of decentralized identities. The entity manages the distribution of verifiable credentials to providers of digital service and includes relevant verifiable credentials in its request to access a service. The service provider then verifies the verifiable credential before granting access. An example is the Verifiable Organizations Network (VON), established by the Government of British Colombia to create an improved methodology of finding, issuing, storing and sharing trustworthy data about incorporated organizations.

Source: Ganne (2018), Norberg (2019).

Appendix II

Different forms of Digital Identity Systems

Available identity systems can be categorized into three archetypes: centralized, federated and decentralized. As the names indicate, it is their fundamental structures that set them apart from each other – with implications for adoption and trust levels, and advantages and challenges for digital entities. For more details, please see the World Economic Forum report published Inclusive Deployment of Blockchain for Supply Chains, Part 2: Trustworthy Verification of Digital Identities, *World Economic Forum*, 2019. Figures below were adopted from this World Economic Forum paper.

Figure 2: Centralized identity system

In a centralized identity system, the provider of a digital service (the service provider – like a government's Trade Single Window, a digital platform or a business application) establishes and manages a consumer of digital service's (service consumer) identities and related data in its systems. Digital identities are currently mostly governed centrally, in isolated architectures. A legal entity typically must prove itself to each service provider to create its digital identity.

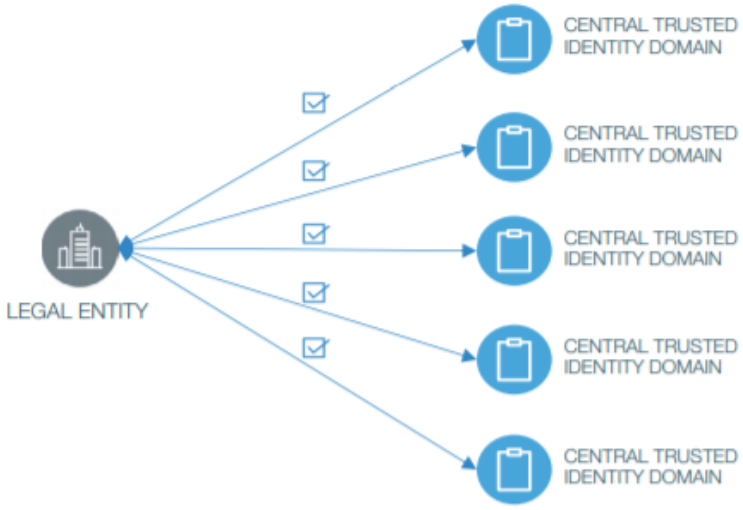


Figure 3: Federated identity system

Federated identity solutions have emerged to reduce the burden of registering digital identities at each service provider. In a federated system, two or more centralized system owners establish mutual trust – either by distributing components of proofing and trust or by mutually recognizing each other's trust and proofing standards. The federated identity concept is probably best known in the consumer space, where, for example, Facebook and Google identities are trusted by many apps through standardized protocols.

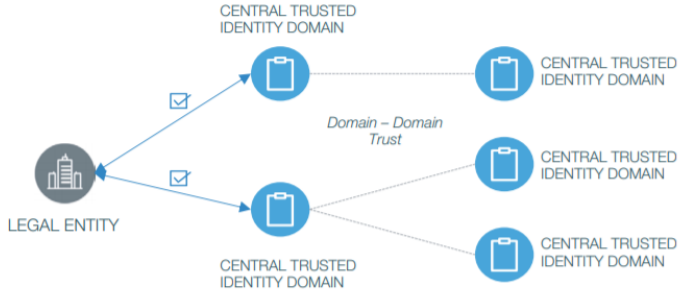


Figure 4: Decentralized identity system

A decentralized identity system 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. The emergence of decentralized identity systems holds a unique opportunity for global supply-chain organizations and governments to create systems that cater for future supply-chain interactions.