WORLD ECONOMIC FORUM

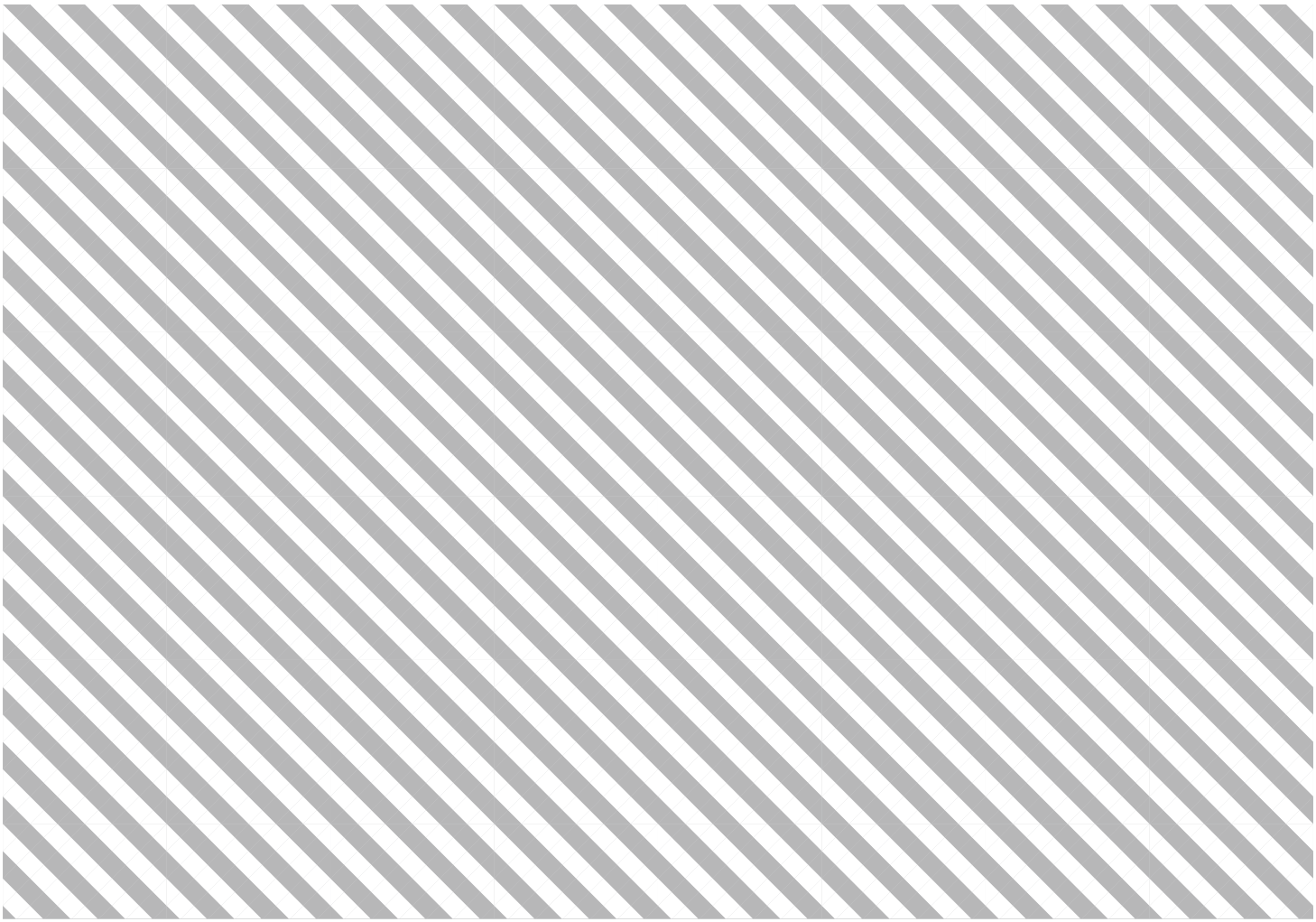
COMMITTED TO IMPROVING THE STATE OF THE WORLD

White Paper

Inclusive Deployment of Blockchain for Supply Chains

Part 2 – Trustworthy verification of digital identities

April 2019



World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

Contents

Preface

Derek O'Halloran, Head, Future of Digital Economy and Society, Member of the Executive Committee

Manju George, Head of Platform Services and Public-Private Cooperation

Nadia Hewett, Project Lead, Blockchain and Distributed Ledger Technology

Supply chains are becoming increasingly digital. A central requirement of these digital business networks is the ability to effectively make use of partners in a trustworthy way. As such, organizations need a comprehensive system for the verification and management of digital business identities that is both dynamic and trustworthy.

Despite recent improvements in digital identity verification systems, they need further development to support the supply chains of the future. New demands on the digital identities of legal entities and possibilities for supply-chain organizations will likely be ushered in by the Fourth Industrial Revolution – with shifts enabled by the internet of things (IoT), artificial intelligence (AI) and, in particular, distributed ledger technology. The pace of development is faster than ever before, and decision-makers need to re-evaluate the systems they have in place to manage digital identities.

This paper advances two topics identified by the World Economic Forum:

1. This is the second white paper in a series and part of a broader project focused on the co-creation of new tools and frameworks to shape the deployment of distributed ledger technology in supply chains towards interoperability, integrity and inclusivity. The World Economic Forum's Centre for the Fourth Industrial Revolution is working with a multistakeholder group to produce a project that includes:
   - A series of white papers published in 2019. Collectively and individually, these papers will offer insights into and explorations of specific considerations for decision-makers in harnessing blockchain technology effectively.
   - A concise, easy-to-use toolkit to be released at the end of 2019 covering important topics for supply-chain decision-makers to consider for responsible blockchain deployment.
2. It contributes to the ongoing development of understanding about and the deployment of "good digital identities" for the Fourth Industrial Revolution.

As digital business interactions flow across borders in international supply chains, there will be many cases in which parties do not know each other before they conduct business together. It is our hope that the following overview of the opportunities, risks and some suggested next steps will stimulate stakeholders to embark on a new and exciting action agenda to build digital identity systems that are prepared for future supply chains.

Introduction

Digital identity *ensures integrity in connecting the physical and the digital world. In global digital supply-chain transactions, it is essential for a legal entity to prove its own identity and check those of other parties, each of which requires a unique, verifiable and authentic digital identity.*

While this paper can be read alone, it does not introduce basic blockchain concepts. This is covered by the first World Economic Forum white paper in this series – for further reference see *Inclusive Deployment of Blockchain for Supply Chains: Part 1 – introduction*, April 2019. The first white paper covers topics such as basic blockchain concepts, blockchain features that are attractive for supply-chain solutions and the findings on concerns that supply-chain actors have for the deployment of blockchain technology, including a concern over trustworthy digital identity management that gave rise to this paper. This white paper therefore explores considerations, proposed principles and recommendations for supply-chain organizations and governments in managing the growing complexity of the digital identities of legal entities involved in global trade.

Decentralization

New technologies and current advances in IT are providing new paradigms in understanding how organizations can collaborate without relying on a trusted intermediary and may bring transformative changes.

Decentralized ledger technologies such as blockchain are transferring the authority, risk and reward – of defining and enforcing system rules and record keeping – from a central entity to a group of entities of which none has controlling power.[1]

Transactions and their details are recorded in multiple places at the same time, without a central database or administrator.[2]

Blockchain provides "trust" between and among unknown parties to transact business and exchange information without an intermediary, while ensuring data integrity and providing a full audit trail.[3]

The paper investigates the possibilities enabled by a digital Global Trade Identity[4] (GTID) for legal entities participating in global supply chains. The intention is that GTID is used for any business interactions in global supply chains and enables any supply-chain partner to dynamically validate the trustworthiness of a legal entity with which it is about to engage in a business interaction. The paper suggests that a GTID is a prerequisite for efficient digitization of global supply chains and supports the digital era's increased focus on optimizing a business's environment instead of organization-centric optimization. The emergence of decentralized identity systems is explored – which holds a unique opportunity for global supply-chain organizations and governments to create GTID systems that cater for future supply-chain interactions. The paper also highlights that decentralized identity systems are not yet ready for general use due to business, regulatory and technology challenges, but both the public and private sector can already position themselves for future success.

While blockchain is one type of distributed ledger technology, for simplicity, the terms are used interchangeably in this paper to cover all types of distributed ledger technologies. Other definitions pertaining to this paper can be found in the glossary.

Trust matters

The technology underpinning the GTID is the foundation for enabling the dynamic validation of trust globally, but there are many other non-technical considerations that contribute to the trustworthiness of an entity, including procedures for issuing and proofing identities, how IT systems are secured, how companies are managed, company ethics/cultures etc. These factors are outside the scope of this paper.

Trustworthy identity verification in global supply chains

Global supply chains span national borders and involve businesses from different industries; actors need to work collaboratively to optimize the flow of physical goods, information and financial transactions. Identity and trust assurance lie at the core of each of these interactions. Supply-chain organizations need to know and trust each partner they are engaging with, prior to offering digital services or access to resources. Organizations need to ensure they are dealing with the right entity and efficiently link a digital identity and a real organization, and more importantly evaluate the trustworthiness of a legal entity of interest. This process of dynamically verifying counterparts – digital identity management and verification – is a critical step in establishing trust and assurance for organizations participating in digital supply-chain transactions.

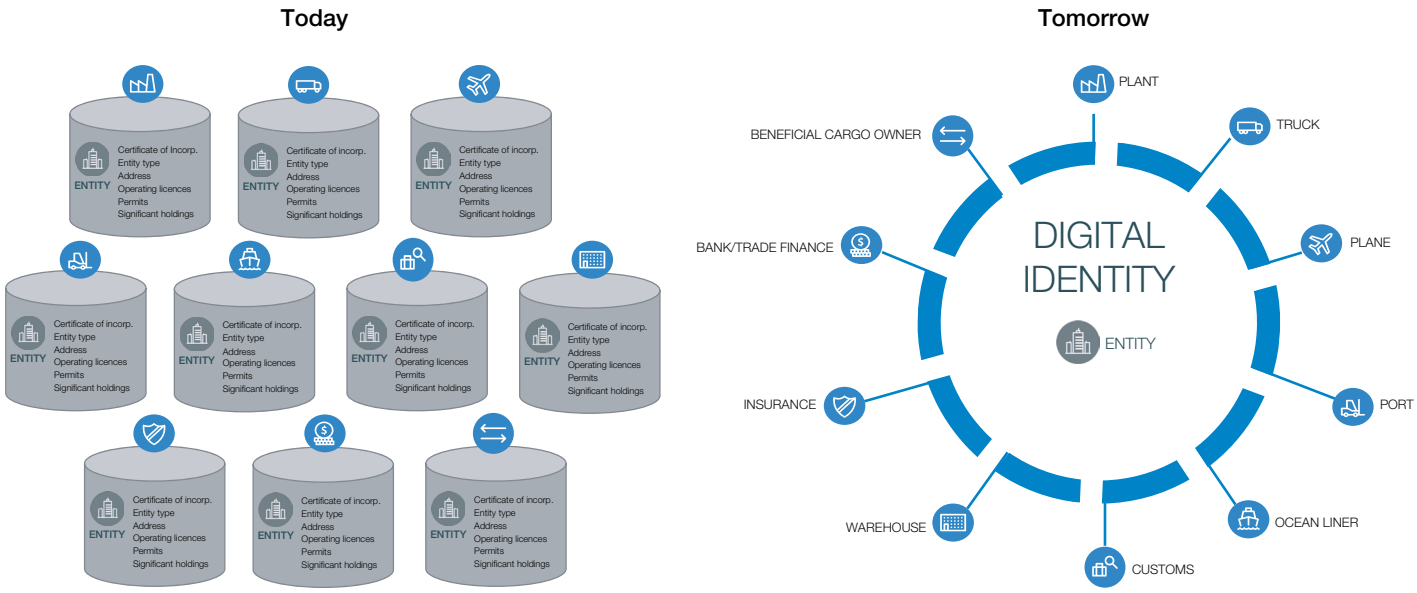
Why this is important: the digital identity landscape

To prepare your organization's supply chain for the complexities of an increasingly digital world and the adoption of emerging technologies such as blockchain, this paper encourages governments, organizations and the supply-chain industry to review the possibilities for new emerging technologies and a digital GTID.

The current state of identity management consists of inefficient manual processes that could benefit from new technologies and architecture to support digital growth. As the number of digital services, transactions and entities grows, it will be increasingly important to ensure that transactions take place in a secure and trusted network in which each entity can be dynamically identified and authenticated.[5]

Today, most identity systems exist in isolation. Different public and private solutions record and maintain identical identity data potentially hundreds of times over, and are not interoperable, creating a significant amount of redundant identity information. This is a waste of resources for the network in question, is difficult to scale and is buried in error-prone and paper-heavy processes.[6]

Figure 1: Identity management that is isolated today is moving towards becoming decentralized tomorrow[7]



Also, the case for robust and scalable GTID becomes clear when considering the advance of Fourth Industrial Revolution technologies. As technologies such as blockchain, internet of things (IoT) and artificial intelligence (AI) advance supply chains, the systems by which organizations verify identity should also do so. For example, the capabilities of blockchain mean that some future supply-chain transactions and business processes might be handled by autonomous software agents (ASA) and IoT, dynamically interacting with various parties on behalf of legal entities, so placing greater emphasis on seamless verification of identities.

The digital-business era requires enterprises to rethink many aspects of their business models. Several enterprises in global supply chains have moved their digitalization focus outwards towards the business networks of which they are part. A GTID should enable identity verification that can be more efficient, scalable and sustainable and therefore support digital optimization of business networks.

With the adoption of emerging decentralization identity technologies – a nascent technology looked at in more detail later in the paper – there is the potential for a technology that supports a GTID without giving power to a centralized administrator.

Trustworthy digital identities of legal entities are a topic on the agenda across international trade organizations and governments, including:

- The Belgium, Danish, Azerbaijani governments and local governments such as the Government of British Columbia and Ontario, as well as the European Union's eIDAS initiative
- The United Nations (e.g. United Nations Economic and Social Commission for Asia and the Pacific [ESCAP] and United Nations Commission on International Trade Law [UNCITRAL]), and the World Economic Forum public and private collaboration on advancing good, user-centric digital identities
- Private organizations such as Alastria, which focuses on Spanish-speaking countries

What is a digital identity?

Digital identity is a unique representation of a legal entity engaged in an online transaction.[8] It enables remote interactions and trust between entities by providing vital information about the entity, ensuring that it exists in the real world.[9]

In this paper we use the term *proof of existence* to cover any electronic information that can document that an entity is a legal entity under a specific jurisdiction. Digital identity tools can be used for other purposes, such as for authorization and providing information (e.g. export licences or C-TPAT certification) beyond simply authenticating a legal entity's identity.[10]

This paper focuses on digital business-to-business (B2B), business-to-government (B2G) and government-to-government (G2G) interactions, and therefore does not cover individual or citizen-to-citizen relations and digital identity considerations, requirements and solutions. We will briefly cover the employee-to-business relationship, but the paper's focus is on legal entities.

Proof of existence

In the identity context, a "proof of existence", in its simplest form, is a way to prove that an entity exists. In this paper, "proof of existence" covers any electronic information which can document that an entity is a legal entity under a specific jurisdiction. A globally recognizable proof of existence does not need to exist. However, if any country issues some kind of digital or physical proof of incorporation (incorporation is the legal process used to form a corporate entity or company), that should be used as proof of existence. In many countries the financial institutions are used as the trusted party that confirms the validity of a physical proof of incorporation and issues a digital identity. How much trust an entity can place on such proof is up to each entity.

Please note, digital identities issued within a country will not themselves constitute a GTID; however, these can be used as the proof of existence to obtain a GTID.

This also means that internal digital identities for businesses and public authorities are not a requirement for a country's participation in paperless trade. As long as a trusted third party can convert physical proof of incorporation into a digital proof of existence, this can be used to obtain a GTID.

Digital identifier[11]

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.

In addition to engaging with legal entities, there are also other types of actors that participate in business interactions in future digital supply-chain solutions and therefore need to be identified as trustworthy:

- **Public authorities** that sign documents, submit events about activities and make agreements/transactions, issue certificates, permits, licences etc. Public authorities act on behalf of governments and are special cases in terms of being legal entities – because of their role within global trade, they are treated separately in this document.

- **Employees** who always act on behalf of a legal entity. An employee identity should therefore be traceable to the legal entity the employee represents. This also includes the concept of individual registered agents who receive and sign official legal documents on behalf of a company.

- **Autonomous software agents (ASA)** that act on behalf of a legal entity or public authority. This requires identification of the autonomous software agent as well as the legal entity for which it is acting.

- **Physical objects** that interact either actively or passively with supply-chain actors on behalf of a legal entity – enabled by IoT and other protocols to directly or indirectly participate in a business interaction. The Mobility Open Blockchain Initiative's (MOBI) work on vehicle identification is an example of a global digital identifier for participating vehicles.[12]

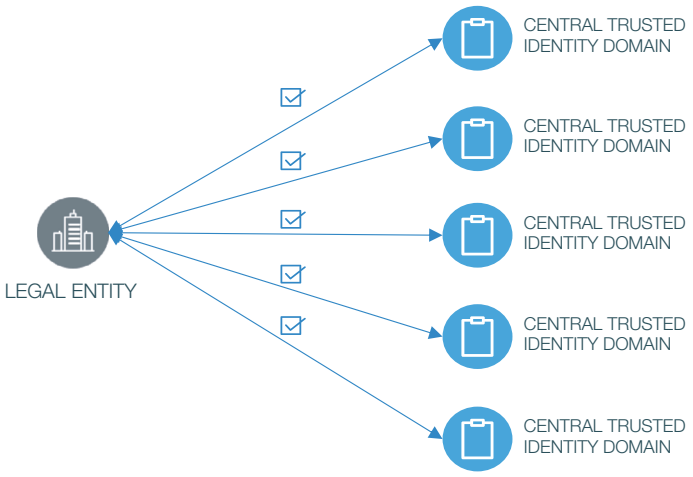
Choosing between three archetypes

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 on 28 September 2018: *Identity in a Digital World: A new chapter in the social contract*.

Centralized

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 2). Under this system, the service consumer has almost no ability to manage its own identities and related attributes and must abide by the service provider's terms and conditions in order to establish and maintain its digital identity. It must rely on the service provider's processes and trust the service provider can handle its identity securely, which puts obligations on the service provider and requires investment.

Figure 2: Centralized identity system



The service provider guarantees the identity of network participants, thereby acting as the central third party that facilitates trust among otherwise unknown entities. In a business network where supply-chain actors are interacting with multiple digital services, these actors need to repeat registration activities for any digital service they intend to use. For example, if a shipper/exporter uses its third-party logistics provider for documentation management, does ocean freight shipping for one trade lane with ZIM, which is using Wave's blockchain-based bill of lading solution, and deploys CargoX's blockchain-based bill of lading solution for all other trade lanes, it should repeat the identity process across all solution providers.

This is cumbersome, requiring identity and security experts in place across processes and entities, and duplication of work at each service provider. Handling trust multiple times across all supply-chain solutions results in hidden overhead costs within the supply chain.

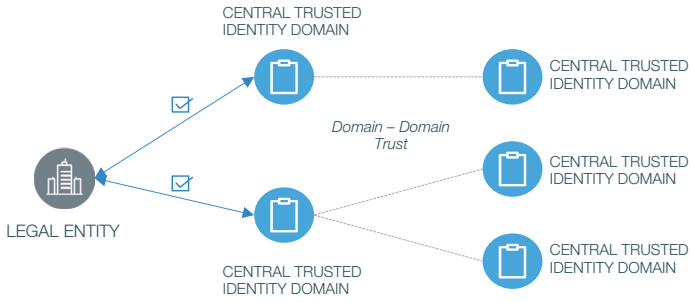
Today, centralized identity systems are mature, with well-defined standards and processes, and this is probably why current providers of blockchain solutions mostly depend on centralized identity systems.

Federated

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.

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. As a result, the identity role is shared among multiple institutions and enables domain-to-domain trust (Figure 3). However, most of these federated identity services still rely on a central system to establish and maintain trust.

Figure 3: Federated identity system



For example, for many shippers and logistics operators trying to plan cost-effective, time-efficient supply chains, the lack of visibility is a real obstacle. The International Port Community System Association (IPCSA) has created a Network of Trusted Networks, enabling the Port Community Systems (PCSs) to trust each other, relying on the authentication of a separate PCS to identify a new user. IPCSA's track-and-trace infrastructure makes it possible to receive information not only from the PCS in the region but globally from other PCSs.[13]

Examples of private federated identification systems in Europe are Mobile ID and Smart ID in Estonia, Belgium and Azerbaijan. Both of these systems have been created by consortiums of leading banks, mobile operators and other market participants. The Republic of Azerbaijan has also established federation between its digital identity and Alibaba and Amazon, thereby enabling anyone with an Azerbaijan eID to immediately access Alibaba's and Amazon's services.

Decentralized

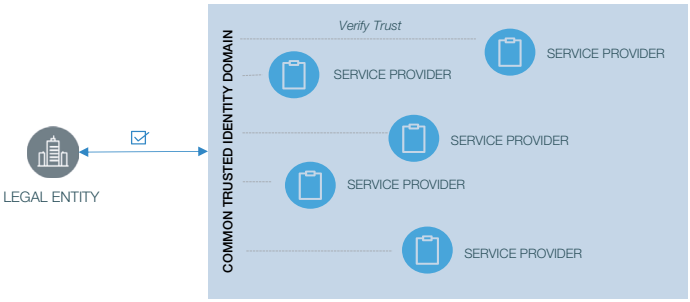
Decentralized identity solutions have emerged to address the issue of having third parties managing a business's or government's identity. It is still considered a new and emerging identity system, and still needs to mature in many areas as systems in production do not yet exist within global trade. The detailed mechanisms of decentralized identity are described in more detail in Appendix 1.

In a decentralized identity infrastructure, 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.

A credential is a piece of information that an organization (the credential issuer) has about an entity: e.g. Authorized Economic Operator, export licence, freight forwarder licence, custom brokerage licence, authorization to issue certificate of origin, etc. A *verifiable credential* is digitally signed by the credential issuer and includes a mechanism for dynamically verifying the validity of the credential (see Appendix 1).

The issuing of standardized, tamper-resistant and non-repudiable 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.[14]

Figure 4: Decentralized identity system



It is likely that centrally trusted entities which issue verifiable credentials will form a federated trust: e.g. a financial institution can verify credentials issued by other financial institutions. Similarly, trusted industry collaborations such as IPCSA's Network of Trusted Networks can issue verifiable credentials for their members.

If a supply-chain solution provider registers all events during a container transport (container filled, estimated/actual time of arrival, container picked up, etc.), then with decentralized identities, the solution provider does not have to register all empty depots, trucking companies, warehouses, forwarders, customs agents, etc. globally beforehand. Instead, the solution provider can dynamically validate the submitter of an event's trustworthiness, reducing onboarding time, barriers and cost. If the event is submitted from an IoT container, it is digitally signed by the IoT container, and this signature can be tracked to the legal entity responsible for the container.

To enable the ability to interact with the right partner at the right time it is important that each entity's internal business rules determine the level of trust of a self-managed identity and related verifiable credentials. Compared to centralized identity solutions this gives more control to the entity but also shifts responsibility for managing its own identity and validating other parties' identities from the service provider to the entity: This can be challenging to achieve, especially for small to medium-size businesses, and may increase the risk of fraud, so the most effective controls must be identified and implemented.

Federated system versus decentralized system

In a federated system, a single entity would register with an organization: Organization A. Other organizations, such as Organization B, may choose to trust the identities provided by Organization A – thereby allowing a single entity to access services provided by both Organization A and Organization B with a single digital identity. That digital identity is provided by Organization A directly to Organization B.

In a decentralized system, however, that single entity is managing its own identity data. Rather than relying on Organization A to provide identity to Organization B, the entity itself provides pieces of verified identity data to access services. Organizations choose whether to accept the digital identity, and organizations are often part of the consortium that runs the decentralized identity system.

How to determine the appropriate archetype

A comparison of the system features can help you decide which archetype is appropriate (see Figure 5). Due to the immaturity of technologies for decentralized identities, the decentralized solution is an idealized scenario that has not been truly implemented yet.

Figure 5: Comparison of identity system archetypes

System archetypes	Centralized – register once, trusted by one	Federated – register once, trusted by many	Decentralized – create once, trusted globally
Definition	A single organization establishes and manages a point-to-point trust relationship with each business identity and adds tailor-made credentials	Different standalone systems, each with their own trust anchor, establish domain-to-domain trust. Credentials are standardized within the domain	Business entities manage their own digital identities. Multiple entities contribute to an identity's credentials
Examples	INTTRA, GT Nexus, Amazon, Alibaba	Sweden's BankID, Denmark's NemID, Canada's SecureKey Concierge, GS1's GTIN (products) and GLN (locations), Amazon, Facebook and Google Identity Federation	British Colombia's Orgbook and Ontario's Verifiable Business Organisation Network (VON), Alastria Digital Identity
Level of adoption and trust	Typical system today; widespread usage; identity standards and protocols are mature	Some solutions in large-scale production; standards and protocols are mature	Adoption currently in early stages (mostly pilot, proof-of-concept). Standards and protocols to be defined
Trade cost implications	Needs limited capital cost to realize at each service provider. All service providers have operational costs	Needs medium capital cost to realize within each domain. Operational cost is split at several service providers	Needs more capital cost upfront to realize but once operational, it has lower operational cost
Number of individual identities for participating in global trade	New digital identity required for every digital service provider. Business credentials created at each service provider	New digital identity required for every domain. Business credentials shared throughout the domain	One global trade identity for each organization. Business verifiable credentials from external independent sources
Direct interactions in a peer-to-peer (P2P) system	Requires intermediary to facilitate trust	Requires intermediary to facilitate trust	Does not require intermediary to facilitate trust; this is done by the protocol
Managing, controlling and protecting identity	Organizations have low control of their identity as this is done by service provider	Organizations have low control of their identity as this is done by service provider and federation partners	Organizations control their own self-managed identity. Can be a complex task
Tailoring	Identity tailored to service providers' needs	Identity tailored to domain requirement	One size fits all as service provider needs to tailor the solution to the decentralized identities. However, the verifiable credentials can be tailored to specific service providers' needs
Siloed identity architecture	Several siloed identity architectures	Several siloed identity architectures	No identity silo – requires a decentralized ledger
Single trusted and shared identity in global trade	Requires one centralized entity to issue one identity for all entities globally	Several centralized entities can issue identities; the global recognition is performed through federation	Requires a global recognized decentralized infrastructure network and related protocols

Centralized, federated and decentralized identity trust systems are not mutually exclusive; an organization or government can deploy some or all systems to perform different functions. Experts assume that most use-cases in global supply chains might require a hybrid system that includes an integrated mix of the three and could come in many shapes.

Regulatory and legal considerations

Note: This section[15,16] is not an exhaustive list of all possible regulatory and legal considerations. Data localization laws and personal data laws (such as GDPR) must be considered when relevant.

The use of digital identity systems in global supply chains is inherently cross-border, which means parties operate in multiple jurisdictions. At present, national legal regimes take divergent approaches to legislating/regulating for digital identity. With the cross-border nature of international trade, several legal issues arise. For instance, which law will apply to establish the validity of a contract – and to an arbitration clause contained in an email exchange?

Decentralized systems, such as blockchain, can encourage the development of digital identity. However, where existing laws and regulations have been drafted to consider digital identity (e.g. the eIDAS regulations in the European Union), they have tended to be drafted with a traditional view of data and digital identity – i.e. based on centralized, rather than decentralized systems. This means the regulations are not fully consistent with a decentralized system of digital identity, therefore organizations could miss out on a potentially promising archetype.

A possible solution lies in formulating uniform legal rules across jurisdictions on a global scale. Such legislative efforts aimed at creating an enabling legal environment for electronic exchanges across borders is a work-in-progress. Useful pieces of legislation already exist. Some of them may be found in recent free trade agreements and others in the United Nations Commission on International Trade Law (UNCITRAL) texts. At the same time, it is important to update work while considering emerging concepts (e.g. identity management) and emerging technology (such as blockchain).

Decentralized identity systems also raise questions about private-key custody and storage. If the security of an organization's digital identity is only as secure as the private key tied to that identity, should service providers that sell custody and storage solutions be subject to common regulatory standards to protect their customers and the system as a whole?

Finally, the liability for systemic failure needs to be clear. Where the identity system is powered by a permissionless decentralized network, there is no single centralized operator of the network. There are also no legal acts or precedents answering the conflicts of law issues inherent in a decentralized system.

UNCITRAL work on cross-border legal recognition of identity management and trust services

In 2018, UNCITRAL asked its **Working Group IV** to investigate legal aspects of identity management and trust services, namely to facilitate cross-border legal recognition in commercial transactions. Ongoing discussions include relevant entities (physical and legal persons as subjects of rights and objects of identification; physical and digital objects as objects of identification only) and legal mechanisms to achieve cross-border recognition. Moreover, mapping identity schemes against outcome-based descriptions of levels of assurance to establish their equivalence has been suggested. The availability of certification and supervision schemes may also play a significant role in the recognition process.

Designing identity systems for future supply chains

The move to digitally optimizing business networks favours a model of dynamic validation of trustworthiness of any legal entity. Ultimately, the goal should be the most fluid supply chain and identity verification to engage legal entities, things and automonous software agents. This means the right services can be offered at the right time – without the cumbersome task of registering and approving supply-chain partners ahead of the interaction, and without a central entity controlling a legal entities' GTID.

The paper assumes there will only be one GTID platform; however, there will likely be several that connect behind the scenes. This is similar to the many internet service providers connecting to give the impression of one internet.

Identity system principles for future supply chains

The following principles are proposed for a GTID model to enable governments and business entities to have one self-managed digital identity throughout global supply chains:

- **Global trustworthiness**: Any government and business should be able to verify the trustworthiness of a legal entity's GTID and allow each legal entity to have internal rules for trust validation.
- **Self-managed**: Each government and business must fully manage its own identity: e.g. it will not be politically acceptable to have a third party managing a government's GTID.
- **Support any digitization level**: Countries and businesses can benefit from the GTID irrespective of their level of technology and digitization readiness: e.g. within a country, there are no internal requirements for digital identities or digital issuance of incorporation documents.
- **Independence of jurisdiction**: Each jurisdiction decides how much trust they will put into each GTID.
- **Cost-effective**: The required investment must be affordable for any country irrespective of its economic development and for any business irrespective of its budget and technological readiness.
- **Politically neutral**: The infrastructure must be politically neutral and support national policy frameworks, meaning that no single country/region/organization can control the infrastructure.
- **Competitively neutral**: The GTID model should not give a competitive advantage to any one organization.
- **Independence**: There should not be a lock-in to any one entity for any important system functions or processes.[17] There cannot be a single entity controlling critical parts of the GTID.
- **Viable and sustainable**: The system is sustainable as a business and is resilient to shifting political priorities.[18]
- **Enable participation**: The model should enable all types of companies, including small and medium-sized enterprises, to more effectively participate in international trade and enhance their competitiveness.

Proposed digital identity model for future supply chains

Based on these principles the next section illustrates a model for GTID that aims to establish trust between government-to-government (G2G), business-to-government (B2G) and business-to-business (B2B) scenarios.

The first section illustrates how a government can obtain a GTID and authorize its Cross-Border Regulatory Agencies (CBRA)[19] to issue and sign digital licences, permits, certificates or other authorizations (LPCOs),[20] an authorization that can be validated dynamically by another country's CBRAs. The second section extends the GTID concept to B2G interaction, followed by the third section that focuses on B2B interactions.

The illustrated model is based on decentralized technologies; however, the model can also be realized with centralized technologies by one supranational organization, with centralized technologies by several organizations that federate trust, or with decentralized technologies without a controlling organization, but still governed by a consortium of nations.

Several elements necessary to realize a GTID are progressing, such as the legal work under UNCITRAL, standardization and digitization of trade documents as well as several decentralized identity solutions like Civic, Sovrin, Hyperledger Indy and uPort. However, there are no concerted efforts focused on realizing all of the pieces needed for a complete GTID solution.

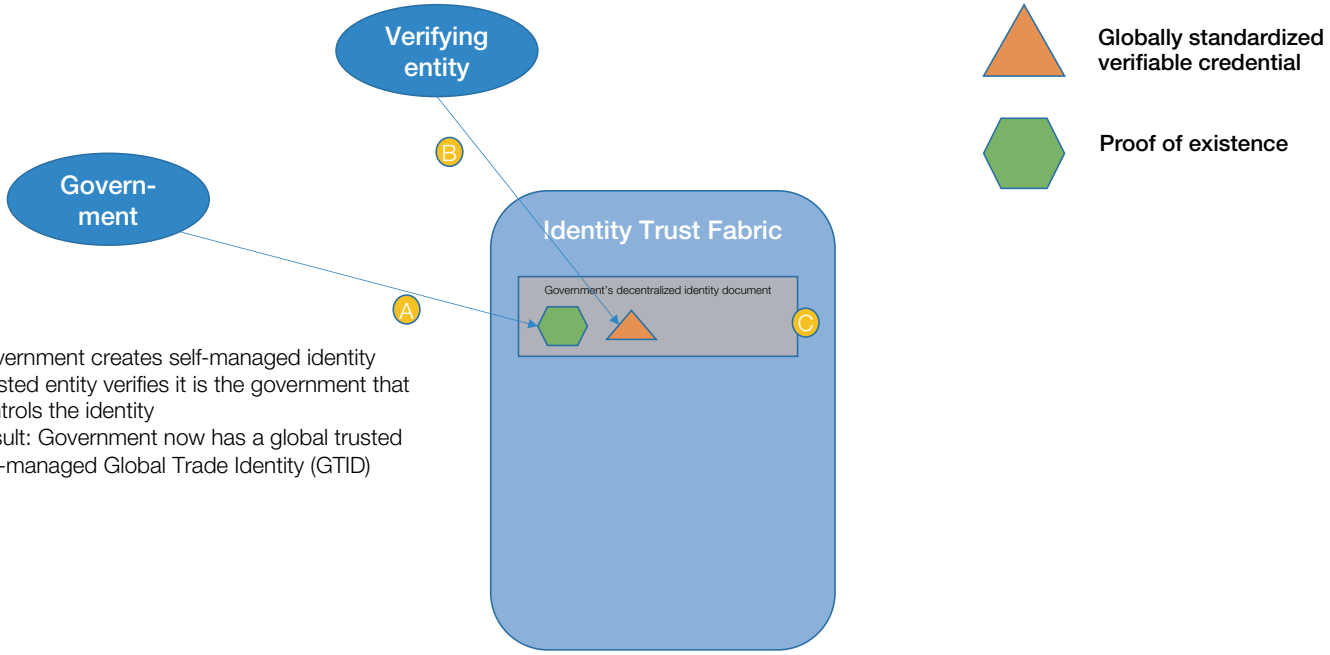
It is not the intention of the illustrations to be technically accurate and/or to include all possible details and exceptions. The purpose is mainly to illustrate the model.

Trust between governments

The main challenges in digital G2G interactions include trusting that a digital LPCO – such as a certificate of origin, an inspection certificate, a special duty-free certificate etc. – was issued in the exporting country by an authorized CBRA, that the LPCO hasn't been tampered with and that only authorized entities have access to the LPCO.

First step – establishing national government identity (Figure 6): Each government issues a globally recognized self-managed digital identity (the GTID) to itself. It is necessary to have a global trusted mechanism through which governments can manage their GTIDs. This is referred to as the Identity Trust Fabric (ITF).[21] An entity verifies that it is genuinely the government that requested the GTID. To support the political neutrality principle, it is recommended that each government decides the verifying entity itself. The identification of the verifying entity is stored as a verifiable credential. If the government has not chosen a trustworthy verifier, then other governments may not trust the GTID. Therefore, there will likely be a global consensus on several entities that are trusted to verify a government.

Figure 6: Establishing national government GTID

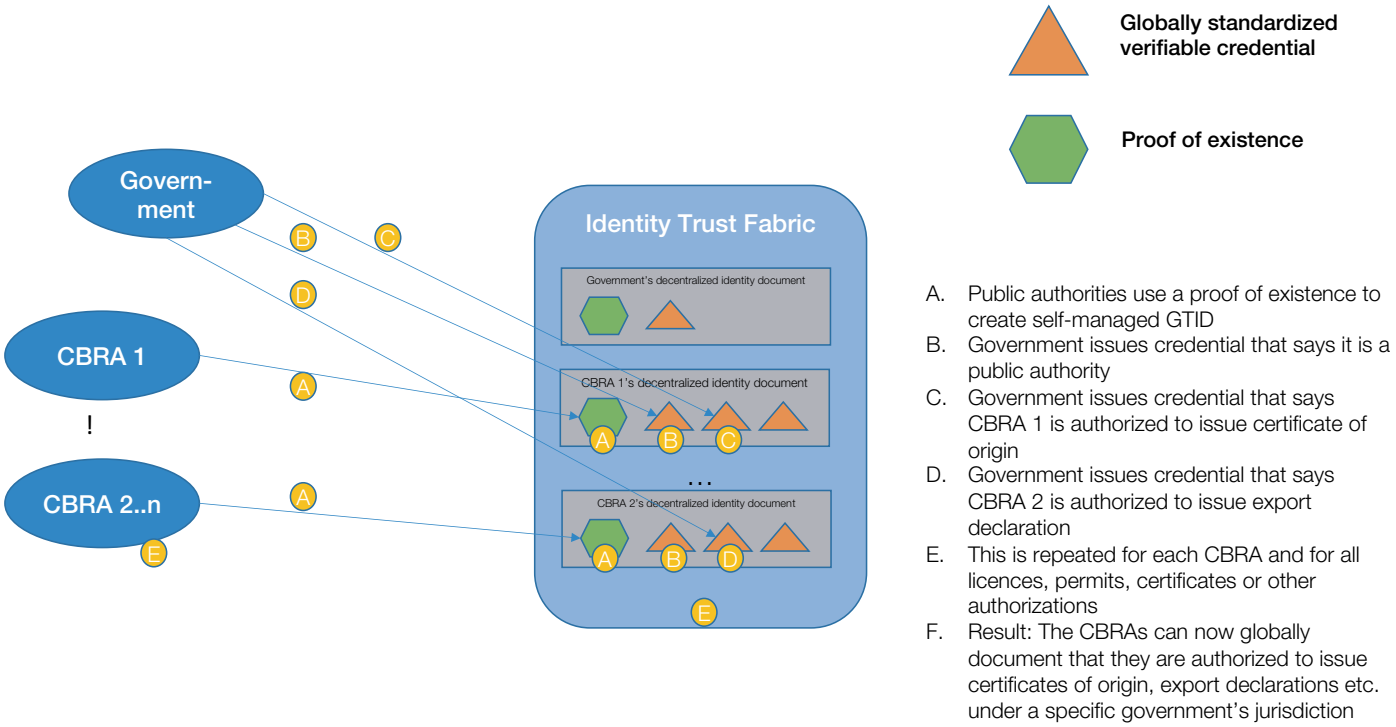


A. Government creates self-managed identity
B. Trusted entity verifies it is the government that controls the identity
C. Result: Government now has a global trusted self-managed Global Trade Identity (GTID)

Second step – establishing each CBRA's GTID (Figure 7). The government issues a proof of existence to a CBRA acknowledging it is a public authority under its jurisdiction. The CBRA uses the proof of existence to obtain its self-managed GTID. This step is repeated every time a CBRA in a country is established.

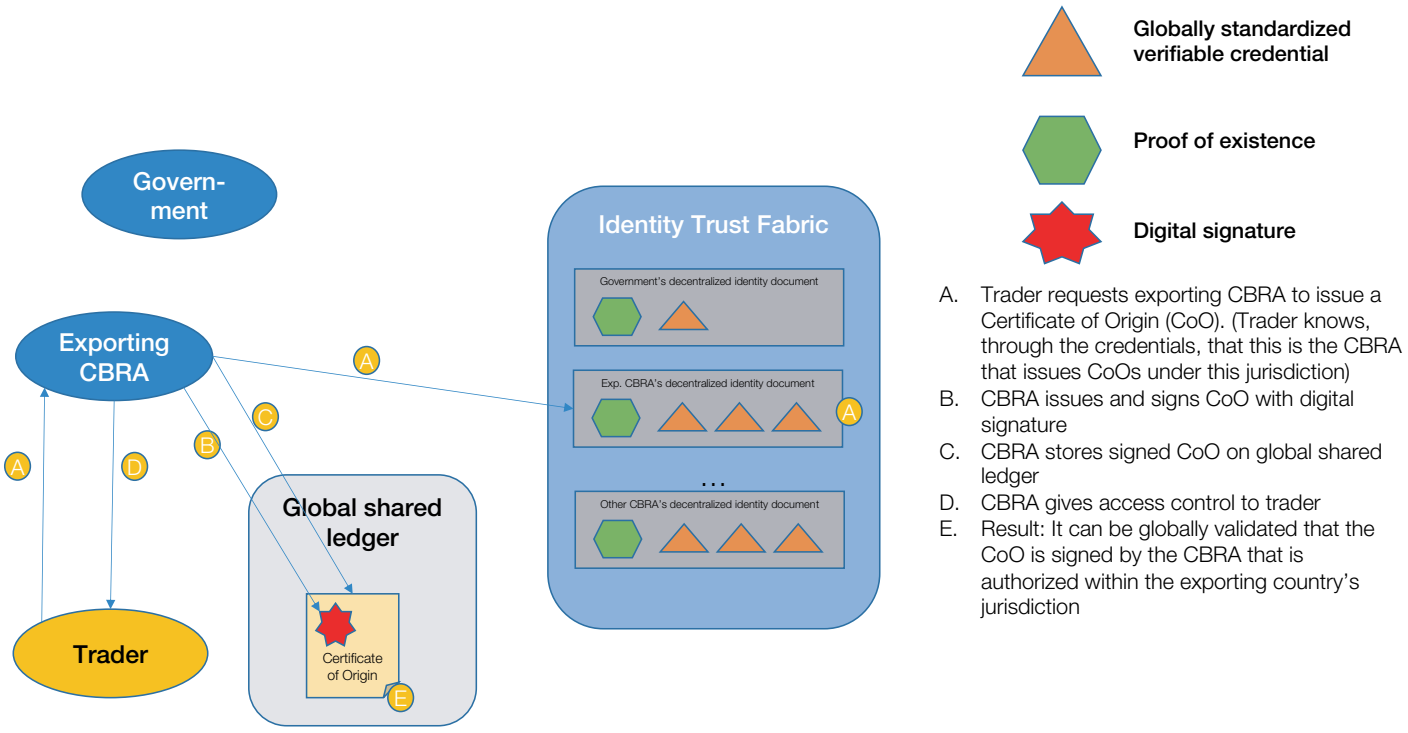
The government endorses a CBRA to issue a specific LPCO by giving globally recognizable and verifiable credentials to the CBRA. In global trade, there are fewer than 100 kinds of LPCO used regularly. It will be necessary to standardize the verifiable credentials informing that a CBRA is authorized by a government to issue a specific type of LPCO. This results in technically simple, cost-effective and politically neutral components that enable a government to confirm that a CBRA is a trusted authority under a specific jurisdiction. The CBRA can document through the verifiable credential that it has been authorized to issue a specific LPCO.

Figure 7: Authorizing a CBRA to issue a specific LPCO



Third step – an exporting CBRA issues an LPCO in response to a request from a trader (Figure 8). An example of an LPCO can be a 'certificate of origin' (CoO), a document widely used in international trade, which a trader typically requests from the CBRA. Figure 8 illustrates how the CBRA uses the GTID to sign the CoO and thereby enable other entities to validate that it is authorized to issue a CoO.

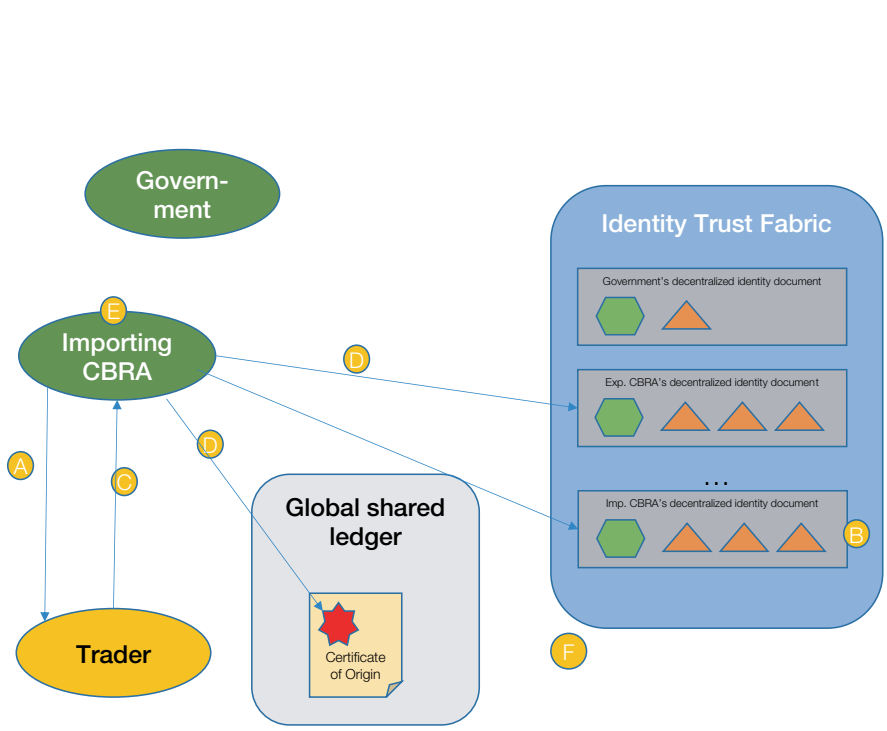
Figure 8: Trader requests a digitally signed CoO to be issued



Fourth step – an importing CBRA verifies the LPCO (Figure 9): A CBRA in the importing country can verify that the exporting CBRA which has digitally signed the LPCO is an authorized issuer of a specific LPCO under the exporting country's jurisdiction. How the importing CBRA reacts based on this verification depends on the local jurisdiction, the amount of trust it has in the exporting country's proofing, validation and governance process, and the CBRA's internal business rules.

The model uses conventional technologies such as digital signatures, hashing and standard encryption to ensure non-repudiation. As a result, the importing CBRA knows it is the original document and that it has not been tampered with.

Figure 9: CBRA in the importing country verifies that the CoO is signed by the authorized CBRA



Globally standardized verifiable credential

Proof of existence

Digital signature

A. Importing country's CBRA requests Certificate of Origin (CoO)
B. Trader verifies that this CBRA is authorized to request CoO within importing country's jurisdiction
C. Trader gives access to CoO
D. Importing CBRA verifies that the document hasn't been changed, and that it is issued by a CBRA in the exporting country that is authorized to issue CoOs under that jurisdiction
E. It is the sole decision of the importing CBRA to determine how much trust it will place in these verifications
F. Result: A globally trusted self-managed GTID that is politically and competitively neutral and affordable for any country

To ease the importing CBRA's validation process, the exporting country's government should digitally sign and publish a simple tamper-resistant table stating which authorities should sign which LPCO. It enables the importing authority to validate that the digital signatures from the right authorities are on the LPCO.

The LPCO can be in any digital format: XML, JSON, PDF or even a JPG picture taken with a mobile phone. An authorized CBRA's digital signature on an LPCO increases the document's trustworthiness. This flexibility lowers the demands of a country's technical readiness and can be an important first step in its digitization of LPCOs, supporting the *any digitization level* principle.

Trust between business and governments

Direct interactions between business and government during import/export/transit processes occur when a CBRA issues an LPCO to a business, and when a business presents an LPCO to a CBRA. Indirect interactions occur when a CBRA, as part of its risk assessment, uses information from miscellaneous data sources that include identity information about a business.

Where G2G interactions only require trustworthy authentication and authorization of the government and its CBRAs, the identification of businesses is more cumbersome, primarily due to the number of entities and the many different types of businesses and interactions.

A government can start with identification of businesses that have a special role in global trade that typically requires a certificate/permit/licence (e.g. customs broker, forwarder, chambers etc.). Similar to CBRA identities, the starting point is when a government, using verifiable credentials, has authorized an agency to approve the establishment of a legal entity within its jurisdiction. When a business is incorporated, it will be equipped with a proof of existence that it can use to request a GTID.

With that in place, it is possible for everyone to see that this business is a legal entity under a specific jurisdiction – and the business can request trusted entities to issue relevant verifiable credentials to be used in requests to access services. Generic verifiable credentials used within global trade must be standardized.

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 has issued more than 7 million verifiable credentials for Canadian companies.

For other businesses involved in global trade, it is recommended that GTIDs are obtained and for governments to accept them. However, the time frame for this to occur could be lengthy, therefore the current centralized system for Trade Single Windows (TSW), for example, could continue, with federations eventually occurring among TSWs on a bilateral or regional scale.

A single GTID in global trade will improve governments' risk assessments, as it is easier to correlate the activities undertaken within the supply chain and understand the activities performed by entities handling cargo during its global journey.

Trust between businesses

The GTID can also be used when businesses are interacting digitally with other businesses. This enables each business to immediately understand with whom it is interacting and to validate the trustworthiness of this business, based on relevant verifiable credentials (see Global Legal Entity Identifier Foundation example).[22]

The Global Legal Entity Identifier Foundation (GLEIF)

For entities involved in financial transactions, the GLEIF is tasked with supporting 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".[23]

Today, many B2B interactions happen via third-party platforms with centralized identities. It is expected that these platforms will be reluctant to move to decentralized identities, as centralized identity can be an important part of their value proposition. Therefore, it is likely that this paradigm will remain in place for some time, eventually with some federation between the different platforms. However, in cases where the collaboration platform is an industry initiative – such as IPCSA – moving to GTID will be worth pursuing, as it will likely reduce the total cost and increase the efficiency of participating in such a collaboration.

It is likely that multiple GTID consortiums will exist within global supply chains. As a result, it is important that these consortiums federate trust among each other. This enables each legal entity to register their GTID only once and reuse the associated digital verifiable credentials across supply chains and geographies, where the federation mitigates technical differences in the representation of identities and verifiable credentials. This also includes standardization of verifiable credentials used within global trade.

Next steps

If the current isolated identity approach continues, the digitization of global trade will likely be slowed, and more dynamic digital interactions between the various parties could be challenging and costly.

Today, we are just starting to see efforts around decentralized identity taking off, while working through legislative, regulatory and technical barriers. Not all barriers are easily surmounted, nor will the benefits of a GTID come automatically. The opportunities and rewards for digitization can be enormous. To facilitate digitization of global trade, three initiatives are proposed for realizing the GTID:

– Blockchain-based solutions that go into production within the next year(s) should, while currently using traditional centralized identities, plan for the transition to decentralized identities when standards and protocols have matured.

– The industry should collaborate to realize the concept of GTID. To stay in control, the industry must start defining the base work that future solutions for GTID can build upon. See the Global Legal Entity Identifier Foundation (GLEIF) for inspiration.

– Governments should, in collaboration with the industry, act to realize a concept in which government identities, signatures and verifiable credentials are recognized globally (e.g. they should intensify digital transformation, set up the legal framework to enable digital identity and encourage trust and mutual recognition with other governments). This could be a significant catalyst in facilitating trade through paperless initiatives.

GTID is only one step in digitizing global trade, but it is a foundational one. Other steps include the standardization of LPCO documents, IoT communication protocols and trade system interoperability. These steps are also important. However, if you do not know who your business partners are, dynamic digital interactions in global supply chains will never happen. Therefore, priority should be given to establishing a GTID with global standardized verifiable credentials for businesses and governments.

Appendix 1: Workings of a decentralized identity model

In a decentralized identity model, both the original proof of existence of the legal entity as well as updates to the legal entity's verifiable credentials should be stored on a trusted shared ledger. The shared ledger should support trust, assurance, provenance, security, scalability and efficiency.

A Decentralized Identifier (DID) is a globally unique identifier that does not require a centralized registration authority and is created in a common trust domain called an Identity Trust Fabric (ITF) that stores the proof of identities and their verifiable credentials cryptographically and immutably on the blockchain. The ITF is where supply-chain partners can verify the authenticity of an identity as well as related verifiable credentials. The ITF is the component that circumvents the need for a central identity provider to manage trust. Once a decentralized identity is established, any supply-chain partner can verify relevant attributes regarding another supply-chain partner with which it is about to engage in a business interaction, either by granting access or conducting a transaction. The decision on how much trust to place in the identity and its verifiable credentials is made by each supply-chain partner individually. Please note, the DID is handled on a blockchain separate from the transactional blockchain.

A DID document is tied to the decentralized identity. It describes the DID and contains the mechanism that an entity can use to authenticate itself as the DID – typically, the public keys whose corresponding private keys are controlled by the identified entity, as well as a set of service endpoints for interacting with the entity and other attributes or verifiable credentials describing the entity. A service endpoint may represent any type of service the entity wishes to advertise.

The DID of the government in each country is the starting point for establishing the identity for any business (see section *Trust between governments*). It is therefore necessary for all actors in global supply chains to trust these government DIDs. This can either be achieved by every business registering and maintaining these DIDs in their internal system, or there could be a trusted service keeping track of the government DIDs. This trusted service can be operated by a central organization, but this will give a significant amount of authority to this organization. Instead, a decentralized service in which more entities could share the authority and governance would distribute the authority across the globe, preventing central control by a single organization.

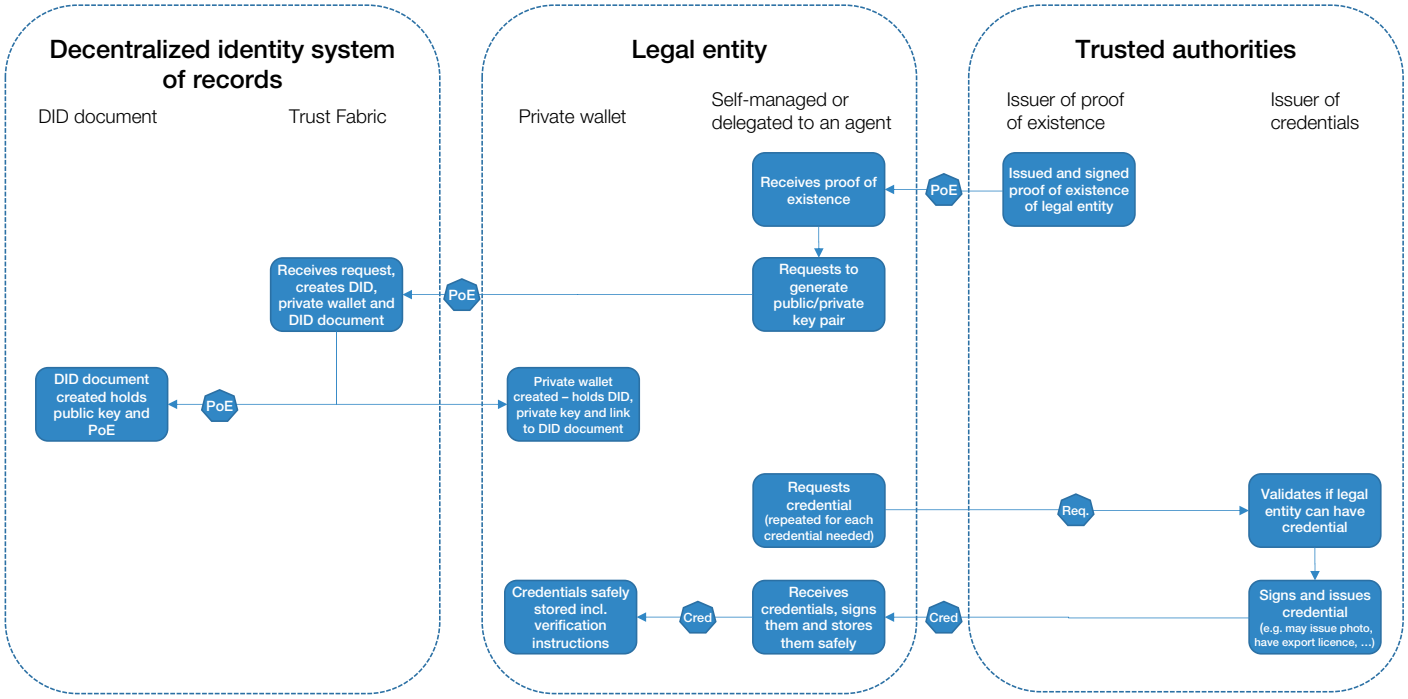
To enable trust between IoTs as well between IoTs and other business entities, an entity should associate the identifier of IoTs and other agents that operate on its behalf with its business identity.

An identity system can be completely decentralized by using trustless, permissionless blockchain networks. However, this model typically does not meet most business risk-management requirements. As a result, permissionless blockchains may not be usable, though they eliminate the need for a central governing body. The required control can be achieved if a single organization operates the Identity Trust Fabric, but this will only be a simulated decentralization. It is more realistic that the Identity Trust Fabric will be formed by a consortium of preselected trusted nodes building a permissioned blockchain. Please note that partners in the consortium do not have to be part of the supply chain; the supply-chain partner simply needs to trust the consortium. This should give sufficient decentralization and thereby offer sufficient neutrality in the Identity Trust Fabric operating model. An example is the G2G model discussed on page 13, where each country could operate one blockchain node or have regional blockchain nodes: e.g. for the European Union.

Verifiable credentials in decentralized identities

A credential is a piece of information that a credential issuer has about an entity. The credential issuer digitally signs the credential and gives it to the entity, which then includes it in its request for access to a service. The service provider should then be able to verify the cryptographic signatures of the credential issuer before granting access to the service (see Figure 10).

Figure 10: Sample of registration and validation of a decentralized identity

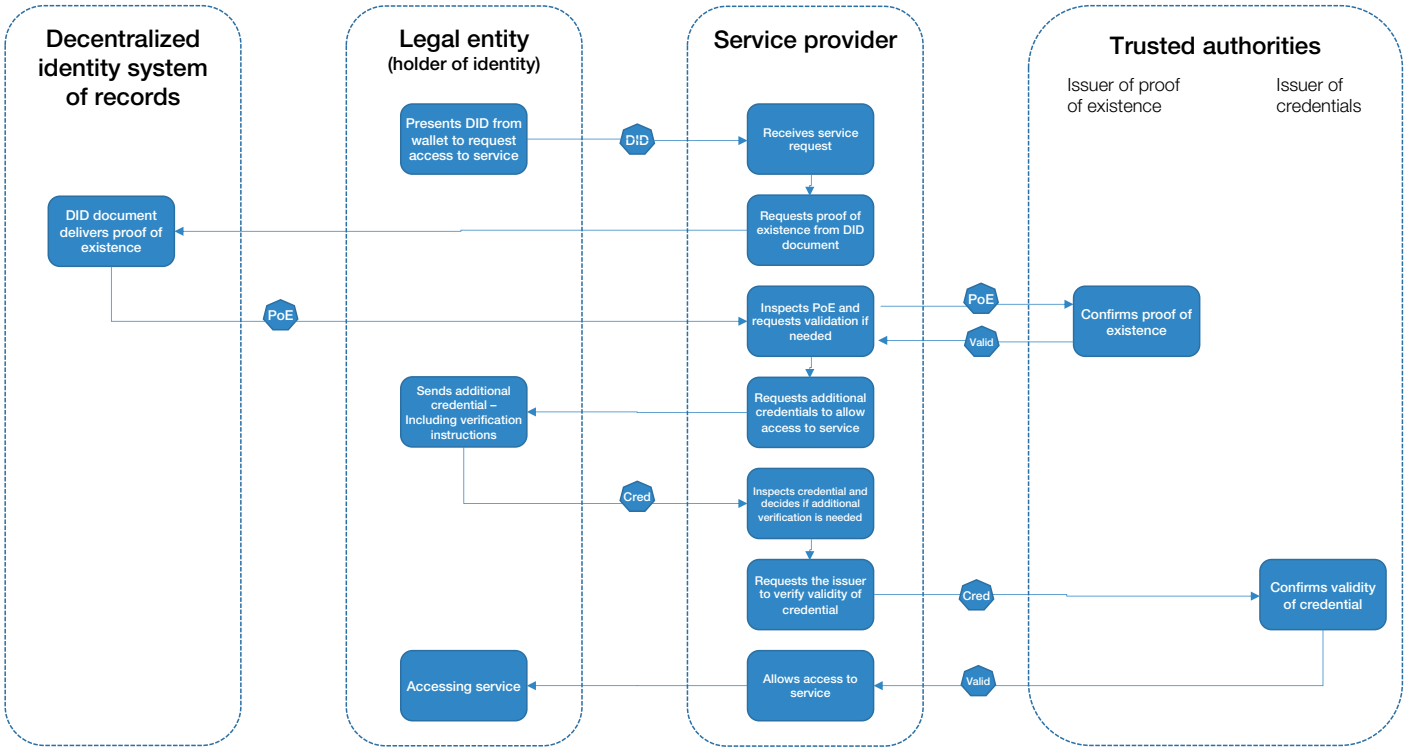


Verifiable credentials should be based on standardized credential schemas that are available on the Identity Trust Fabric, thereby making verifiable credentials understandable for any supply-chain actors. It should also be possible for each entity to request additional information regarding the DID from other parties (e.g. if the shipper has an export licence for specific cargo). However, it must be controlled by the holder of the DID, so the holder is always in control of identity-related interactions.

This enables a dynamic concept, as the trust can increase after the basic level of trust through the initial proof of existence has been established, by having more service providers to attest a business identity and verify additional profile credentials with their digital signature. This history of trust will be available in the Identity Trust Fabric. Please note this also includes the possibility of degrading trust and attributes.

During an interaction, an entity presents the identity and credentials and the other party should be able to verify it. This means that issuers of verifiable credentials and proof of existence should be ready to immediately verify the validity of its assertion, in addition to having trustworthy processes for maintaining the identifiers (see Figure 11).

Figure 11: Sample flow of presentation, verification and interaction to access service



Identifiying a legal entity

In a government-controlled model, the government creates a legal foundation that outlines how to identify public authorities and how legal entities are created and governed within that jurisdiction. Government-issued identities are typically stable and uniquely identify a business entity and, as such, are the foundation of all interactions with the outside world. Government-issued identifiers are a must in the current, primarily centralized identity model – and governments continue to have a vital role in a decentralized global supply-chain solution.

A public authority registers and identifies legal entities within its jurisdiction, based on the legal foundation. This assumes that the government identity issuance systems and processes are not compromised or destroyed/corrupted. In that case, as well as with war-torn countries, alternatives like the United Nations or other mechanisms should be available for legal entities wanting to participate in global supply chains.

The public authority 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 public authority and made available for all participants in the supply chain that intend to interact with the legal entity. For example, this status can be a filing for bankruptcy, a change of ownership, the redrawing of licence to transport dangerous goods etc.

Building upon the government-controlled model, there are also non-government-controlled models, such as an industry identification scheme. Here, all entities in the network trust that the non-government entity has verified the existence of the legal entity. The non-government entity typically adds industry-specific verifiable credentials to the identity, which can be in different contexts, such as finance, insurance, logistics, audit/compliance etc. These DIDs do not replace government-issued DIDs but complement them in an industry-specific context. A business partner should still be able to track the industry DID to the government DID.

Glossary

Authentication: Verifying the identity of a user, process or device, often as a prerequisite to allowing access to resources in an information system. (NIST SP 800-128)

Authorization: The process of verifying that a requested action or service is approved for a specific entity. (NIST SP 800-152)

Authorized Economic Operator: A party involved in the international movement of goods, in whatever function, that has been approved by, or on behalf of, a national customs administration as complying with WCO or equivalent supply-chain security standards. (WCO SAFE Framework of Standards)

Autonomous software agent (ASA): An autonomous software agent is a component that has the intelligence necessary to autonomously decide when to perform an action. An ASA runs autonomously on the blockchain and enables members of a network to collaborate and negotiate transactions among themselves on behalf of, and instructed by, the entities controlling them. It is also called a decentralized application (Dapp).

Consortium: A group of people, countries, companies etc. who are working together on a particular project. (Oxford Learner's Dictionary)

Credentials: An object or data structure that authoritatively binds an identity – via an identifier or identifiers – and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber. (NIST SP 800-63-2)

Cross-border regulatory agency (CBRA): Cross-border regulation of international trade involves many government agencies. These include agencies dealing with trade in goods that affect human health (e.g. food safety, pharmaceuticals, cosmetics and dangerous drugs, to name a few). Other agencies might, for example, deal with public, environmental or biosafety. The precise number of agencies depends on the compliance profile of the country. (World Customs Organization)

Cryptographic techniques/Cryptography: A discipline or technique that embodies principles, means and mechanisms for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. (ISO/IEC 74498-2: 1989, ISO/IEC SD6)

Digital document: Digital information that has been compiled and formatted for a specific purpose, that includes content and structure and may include context. (Glossary of Archival and Records Terminology)

Digital identity: A unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but does not necessarily need to uniquely identify the subject in all contexts. (NIST SP800-63-3)

Digital signature: A specific type of electronic signature (e-signature) that relies on public-key cryptography to support identity authentication and provide data and transaction integrity.

eIDAS: The eIDAS Regulation 910/2014 sets a framework for electronic identification and trust services for electronic transactions in the European single market. (European Commission)

Electronic Product Code Information Service (EPCIS): A GS1 standard that enables trading partners to share information about the physical movement and status of products as they travel throughout the supply chain. (GS1)

Fourth Industrial Revolution: A technological revolution driven by advances in science and technology. Scientific breakthroughs and emerging technologies are advancing at an unprecedented speed and include technologies such as blockchain and distributed ledger technology, artificial intelligence, autonomous driving, precision medicine, drones and the internet of things, among others.

The General Data Protection Regulation (GDPR): A regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. (Regulation (EU) 2016/679)

Global Location Number (GLN): The GLN is part of a GS1 standard used for any location (physical, operational or legal) that needs to be identified for use in the supply chain. (GS1)

GS1 barcode: Barcodes are symbols that can be scanned electronically using laser or camera-based systems. They are used to encode information such as product numbers, serial numbers and batch numbers. Barcodes play a vital role in supply chains, enabling parties like retailers, manufacturers, transport providers and hospitals to automatically identify and track products as they move through the supply chain. (GS1)

Identity Trust Fabric (ITF): A common trust domain where entities immutably store the proof of identities and their verifiable credentials on the blockchain and where supply-chain partners can verify the authenticity of an identity as well as related credentials.

Internet of things: A network of items – each embedded with sensors – that are connected to the internet.
Mutual recognition: A principle of international law whereby states party to mutual recognition agreements recognize and uphold legal decisions taken by competent authorities in another member state.

Port Community System (PCS): A PCS is an electronic platform that connects the multiple systems operated by a variety of organizations that make up a seaport or airport community. It is shared in the sense that it is set up, organized and used by firms in the same sector – in this case, a port community.[24]

Repudiation: The rejection or denial of the validity of something.

Smart Contract: Blockchains can be programmed to automate business processes (e.g. making payments) in different entities. A smart contract is a computerized transaction protocol that automatically executes the terms of a contract upon a blockchain once predefined conditions are met.

Self-managed: In a self-managed interaction, a user can control its own identity and attributes.

Trade document: Trade documents are any documents used in global trade, whether certificates, licences, permits or business documents such as purchase orders, bills of lading etc. We spell out specific document types only when it is relevant.

Trade Single Window (TSW) system: A facility that allows parties involved in trade and transport to lodge standardized digital trade information and trade documents with a single-entry point to fulfil all import, export and transit-related regulatory requirements.

Trust anchor: An organization that conducts identity proofing, then issues physical documents and/or digital credentials/attestation on which others rely.

Service provider: An entity that delivers application functionality and associated services across a network to multiple service consumers.

Contributors

The World Economic Forum's Centre for the Fourth Industrial Revolution's Blockchain for Supply Chain project is a global, multi-industry, multistakeholder endeavour aimed at co-designing and co-creating frameworks. The project engages stakeholders from multiple industries and governments from around the world. This report is based on numerous discussions, workshops and pieces of research and the combined effort of all involved. Opinions expressed herein may not necessary correspond with those of each individual involved with the project.

Sincere thanks are extended to those who contributed their unique insights to this report. We are also very grateful for the generous commitment and support of the fellow at the Centre dedicated to the project: Soichi Furuya from Hitachi.

Lead Authors

Henrik Hvid Jensen, Senior Blockchain Advisor, Trustworks, Denmark
Nadia Hewett, Project Lead, Blockchain and Distributed Ledger Technology, World Economic Forum, United States

Contributors

Alexandra Ashpole, Digital Identity Consultant, Accenture, United States
Andres Ojamaa, Lead Researcher, Guardtime, Estonia
Andrew Tobin, Managing Director, EMEA, Evernym
Christine Leong, Managing Director, Accenture, United States
Dominique Guinard, Founder & Chief Technology Officer, EVRYTHNG, Switzerland
Douglas S. Hill, Chief Operating Officer eBusiness, GS1 Denmark, Denmark
Francis Jee, Manager, Deloitte, United States
Gadi Benmoshe, Chief Information Officer, Israel Ports Development & Assets Company, Israel
Hanns-Christian Hanebeck, Founder & Chief Executive Officer, Truckl.io, United States
Jana Krimpe, Co-Chair, Global Alliance for National Mobile Identities, Azerbaijan
Javier Gallardo, Director, Portic Barcelona, International Port Community Systems Association, Spain
John Choi, Chief Executive Officer, Markany, South Korea
Jon Shamah, European Association for e-Identity and Security, United Kingdom
Luca Castellani, Legal Officer, The United Nations Commission on International Trade Law, Austria
Lucy Hakobyan, Head of Program, Mobility Open Blockchain Initiative, United States
Madhav Durbha, Group Vice President, Industry Strategy, LLamasoft, Inc., United States
Martin Riedel, Product Manager, Civic, Germany
Michele Nati, Lead Technology Analyst, IOTA Foundation, United Kingdom
Mikael Lind, Research Manager, Research Institutes of Sweden, Sweden
Ramón Gómez Ferrer, Deputy Director of Strategic Planning, Port of Valencia, Spain
Robert Maslamoney, Managing Director, Maersk, Angola
Soichi Furuya, Senior Researcher, Hitachi, United States
Stuart Davis, Senior Associate, Latham & Watkins, United Kingdom
Sumedha Deshmukh, Project Specialist, World Economic Forum, United States
Vijay Kumar, Chief Technology Officer, eMudhra, India
Wolfgang Lehmacher, Senior Supply Chain Executive, Switzerland
Yusuke Jin, Senior Researcher, Hitachi, Japan

Commentators

Ashley Lannquist, Project Lead, Blockchain and Distributed Ledger Technology, World Economic Forum, United States
John Jordan, Executive Director, Emerging Digital Initiatives, Province of British Columbia, Canada
Kai Wagner, Partnership Development, Jolocom, Germany
Kimberley Botwright, Community Lead, Global Trade and Investment, World Economic Forum, Switzerland
Saverio Puddu, Tech and Data Protection, Baker McKenzie, Italy

Endnotes

1. Homan Farahmand, *A Technical Primer for Assessing a Blockchain Platform*, Gartner, 21 March 2017.
2. ibid.
3. Tae Il Kang, Director General of the Information and International Affairs Bureau, Korea Customs Service, "Korea Pilots Blockchain Technology as it Prepares for the Future", WCO News: https://mag.wcoomd.org/magazine/wco-news-88/korea-pilots-blockchain-technology-as-it-prepares-for-the-future/ (link as of 26/3/19).
4. This term was coined by Henrik Hvid Jensen, 2019.
5. World Economic Forum. *Digital Identity: On the threshold of a digital identity revolution*, 2018.
6. World Economic Forum. *Identity in a Digital World: A new chapter in the social contract*, 2018.
7. World Economic Forum. *Identity in a Digital World: A new chapter in the social contract*, 2018.
8. https://www.nist.gov/ (link as of 26/3/19).
9. World Economic Forum, *Making Deals in Cyberspace: What's the problem?*, 2017.
10. ibid.
11. ISO/IEC 29115:2011
12. Lucy Hakobyan, Mobility Open Blockchain Initiative, 2018.
13. https://ipcsa.international/ (link as of 26/3/19).
14. https://github.com/bcgov/von (link as of 26/3/19).
15. Prepared by Stuart Davis, Latham & Watkins, 2019.
16. Prepared by Luca Castellani, United Nations Commission on International Trade Law, 2019
17. Global Legal Entity Foundation (GLEIF).
18. World Economic Forum principles of digital identity systems for people.
19. World Customs Organization, 2011.
20. ibid.
21. Christy Pettey, *The Beginner's Guide to Decentralized Identity*, Gartner, 28 June 2018, https://blogs.gartner.com/smarterwithgartner/author/cpettey/ (link as of 28/3/19).
22. https://www.gleif.org/en/ (link as of 26/3/19).
23. World Economic Forum, *A Blueprint for Digital Identity*, 2016.
24. https://ipcsa.international/ (link as of 26/3/19).

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org