UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT

GLOBAL REPORT ON BLOCKCHAIN

AND ITS IMPLICATIONS ON TRADE FACILITATION PERFORMANCE

UNITED NATIONS
UNCTAD
Geneva, 2023

This publication has been edited externally.

United Nations publication issued by the United Nations Conference on Trade and Development

UNCTAD/TCS/DTL/INF/2023/1

Contents

List of tables

List of figures

Acknowledgements

Global Report on Blockchain and its Implications on Trade Facilitation Performance was prepared under the guidance of Shamika N. Sirimanne, Director of the UNCTAD Division on Technology and Logistics and the supervision of Angel González-Sanz. The team comprised Solomon Anzagra, Clovis Freire and Wai Kit Si Tou. Research support was provided by UNCTAD intern Henrique Pinto Coelho.

Comments and suggestions received from the steering committee of the Blockchains for Facilitating Trade and Enhancing Competitiveness project under the fourteenth tranche of the Development Account are gratefully acknowledged. Members of the steering committee include Nadia Hasham (ECA); Luca Brunello, Maria Teresa Pisani, Alla Shlykova, Jie Wei (ECE); Miryam Saade Hazin, Sebastian Herreros, Johan Mulder (ECLAC); Yann Duval, Soo Hyun Kim (ESCAP); Adel Alghaberi, Maya Dah, Nibal Idlebi (ESCWA); Arantzazu Sanchez Belastegui, Clovis Freire and Wai Kit Si Tou (UNCTAD). Comments received as part of the UNCTAD peer review process are acknowledged with appreciation, from Regina Asariotis, Raouf Benzarti, Laure Buisson, Poul Hansen, Jan Hoffmann and Erik Willems.

The team would like to express its particular thanks to Virginia Cram-Martos for her valuable advice.

The manuscript was substantively edited by Sue Littleford. Magali Studer designed the cover. Malou Pasinos provided administrative support. Overall layout, graphics and desktop publishing were undertaken by the Division of Conference Management of the United Nations Office at Geneva.

Abbreviations and acronyms

AEO	Authorized Economic Operator
AI	artificial intelligence
CBDC	central bank digital currencies
CoO	certificate of origin
DLT	distributed ledger technology
EBSI	European Blockchain Services Infrastructure
IBC	Inter-Blockchain Communication (protocol)
ICA	interchain accounts
IoT	Internet of Things
IOU	'I owe you', the acknowledgement of a debt
PoS	proof of stake
PoW	proof of work
QR code	quick response code
TCP/IP	transmission control protocol / Internet protocol
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
UNECE	United Nations Economic Commission for Europe
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business

Notes on the text

The term "dollar" ($) refers to United States dollars.

The term "billion" signifies 1,000 million.

1 Introduction

1. Introduction

Global supply chains have come under tremendous stress in recent times, causing price hikes and shortages in daily necessities around the world. Trade facilitation has become a crucial component of the global agenda to ensure that essential goods and services reach the targeted destination in time and at costs affordable for the consumer. Thus, the idea of efficiency gains in global value chains that can be driven by digitalization and automation using emerging technologies such as blockchain is particularly welcomed. Considering that supply chains have become far more fast-paced with trade volumes surging thanks to e-commerce, the global economy is increasingly interconnected with ever-broadening global value chains. Thus, governments are facing new policy and regulatory challenges, not only in ensuring compliance but also in managing issues arising from digital disruption. In this regard, digital tools such as blockchain have presented opportunities but also challenges. While they could aid governments in handling emerging and pressing regulatory challenges, they also raise questions on how to safeguard advances in digital technology in a way that ensures shared prosperity, inclusivity and broad beneficiation of digital trade among all people in the world (see also OECD, 2022).

The need for faster cross-border clearance, lower trade costs and more efficient global value chains alongside trade resilience and compliance has never been so critical. Policymakers are in search of efficiency gains when balancing regulations against bolstered supply chains and stable value chains to facilitate global commerce. Thus, digitalization and frontier technologies have been at the forefront of policy debates, both seen as major drivers of efficiencies in international trade and opportunities to boost countries' trade facilitation efforts. While digitalization and technological advancement have contributed immensely to supply chain efficiencies in recent years, challenges for broad adoption persist (Duval and Mengjing, 2017). Major progress across regions is growing, with digitalization being a key component of many governments' trade agendas. With digitalization in trade and trade facilitation becoming commonplace in the trade debate, the focus is shifting towards the role of frontier and emerging technologies in the digitalization efforts of countries.

Questions of whether countries could witness efficiency gains in the adoption of frontier technologies presented by the Internet of Things (IoT), artificial intelligence (AI) and blockchain technology are becoming a key consideration in the digitalization debates. These frontier technologies have already demonstrated the potential to improve efficiencies in cross-border trade flows in a number of areas. Major supply chain challenges experienced around the globe – as a result of the COVID-19 pandemic (ASEAN, 2022; UNCTAD, 2020), with significant commercial and legal implications of disruption and delay,[1] and the unforeseen shocks from the war in Ukraine – have shown that supply chains and established cross-border trade practices need broad reassessment, rethink, redesign, augmentation and improvement at various levels.

The question remains: to what extent can global supply chains harness the benefits of digitalization to meet the strong demand for goods and services in an ever-growing fast-paced, interconnected and challenging trade landscape while striking a balance between supply chain stability, speed of trade flows and compliance?

Furthermore, at a time when digitalization is taking centre stage in countries' trade systems, cyberintrusions and illegal hacks are increasing in scope and in number, urging technological designs to be more sophisticated with modern high-end cryptography, resilience and redundancies built in to withstand attacks (Lohmer *et al.*, 2020).

Over the years, blockchain technologies have grown in user awareness, use case expansion and technical sophistication. Their potential for multiple use cases and capabilities to be used for reimagining existing foundational technology stacks[2] is becoming better understood. From being a frontier technology to seeing growing use in modern financial tools and process engineering, blockchains have promised to impact the foundation of existing technologies broadly (Harvard Business Review, 2022). With redundancies at the core of its design, some blockchain technologies are particularly resilient against unauthorized intrusions and adversarial attacks and useful for adversarial environments with limited trust. Its decentralized and consensus-driven nature makes it more resilient to attacks directed to the network and brings new defence capabilities of cybersecurity to businesses, governments and individuals (Forbes, 2022a).

Financial engineering aside, the technology's full potential is far from being realized in various business sectors and government operations, including international trade and supply chain management. Despite the growing knowledge among sector leaders and policymakers, many still understand blockchain as the technology that powers cryptocurrencies. At the same time, while countries are at different stages of developing, deploying or delivering some financial, trade or administrative services on the blockchain (Clavin *et al.*, 2020), these initiatives are generally at pilot stages and yet to grow into broader use cases.

As a general-purpose technology, blockchain is applicable to numerous use cases based on users' needs. Across the world, governments have applied the technology to areas of use beyond trade facilitation. Some of the government initiatives using blockchain include the Government of Canada piloting blockchain for employee credential management (Leal, 2022), the Maltese government pilot of blockchain to manage educational credentials such as school certificates and diplomas, the Estonian government, which currently runs some of the country's e-government services on the blockchain,[3] Georgia using the blockchain for land registry and land record management (Shang and Price, 2019), as well as countries including Sweden and Switzerland undertaking asset management operations on the blockchain (Allessie *et al.*, 2019) among others.

Apart from these varying use cases, many governments are testing, piloting or already utilizing the technology in various areas of trade facilitation, which is the focus of this report. It includes cross-border clearance, payment processing, supply chain management, Rules of Origin, corridor management, trade-risk management and Authorized Economic Operators. This said, many policymakers and government agencies across the world are yet to fully grasp what makes blockchains different, as well as their value proposition or technical edge over traditional and legacy database systems. Many still wrestle with the technology's potential and for what government sectors the technology could be harnessed. For policymakers, a lot needs to be done by way of policy guidance, technical support and stakeholder empowerment on the technology.

This report aims to support policymakers, especially trade policymakers, to understand the basic features of the blockchain technology as well as the policy considerations and design options available in the blockchain industry that could be harnessed towards enhancing trade facilitation efforts and improving legacy trade systems and trade processes.

The research objectives are to lay the groundwork that will enable countries to effectively adopt and implement blockchains, including but not limited to:

- Providing the necessary supporting policy environment on technical guidance, regulatory frameworks, compliance and governance preconditions to accelerate blockchain adoption and implementation
- Developing model guidance for stakeholder coordination, decision-maker roles and process implementation
- Outlining present and potential use cases of blockchain for trade facilitation and trade processes for the benefit of policymakers
- Providing an overview of the evolution of the technology of blockchain over the years, where major developments in the technology are taking place and why the transformation means more use cases for the technology in general
- Establishing the basis for use cases such as certification, credentials and distributed data management to facilitate international trade

- Suggesting a framework for setting up the right policy environment, technical infrastructure and application designs in a cost-effective and interoperable manner for national, regional and global blockchain adoption
- Supporting governments to design tailored policies and regulations to facilitate the integration of blockchain with existing and upcoming key technological environments, such as AI, IoT and cloud computing
- Offering recommendations on the education of policymakers, entrepreneurs, civil servants and the public to foster a widespread use of blockchain across different actors
- Giving a better understanding to policymakers of the legal and regulatory requirements for using blockchain in trade facilitation environments
- Outlining the factors that can influence the successful implementation of blockchain technology for trade facilitation while addressing the digital divide between countries

The rest of this report is structured as follows. Chapter II describes blockchains and captures their major features as well as the evolution of the technology over the years. Chapter III presents potential blockchain use cases in international trade. Chapter IV discusses the technical considerations and policy questions for the design, development and deployment of blockchains for international trade. Chapter V concludes and suggests ways forward, with policy considerations. The annex offers a comprehensive review of the different types and features of blockchains.

2 What are blockchains?

2. What are blockchains?

A blockchain is a shared, immutable database that facilitates the process of keeping records and tracking these records in a shared environment. Blockchain, thus, is simply a technology that builds a trustworthy service in a not necessarily trustworthy environment (Clavin *et al.*, 2020). Blockchain is a form of distributed ledger technology (DLT) that allows for secure, transparent and immutable storage of information on a network of interconnected computers called nodes. It is a technology that enables the creation of a digital record of transactions or other types of data, which are recorded in blocks that are chained together in chronological order, hence the name "blockchain".

In a blockchain, each block contains a set of data, such as transactions, records or other types of information. These blocks are linked to each other using cryptography, where the information in one block is referenced by the subsequent block and so on, forming a continuous and sequential chain of blocks. Blockchains can be centralized or decentralized. These types and features, among other aspects of the blockchain, will depend on the consensus algorithm (see Annex, section B, for more on this). At their most primitive and elementary level, blockchains extend the double entry principle of debit and credit in accounting, to a triple entry/record mechanism of debit, credit and transfer.

Over the years, there have been three milestone transitions in its constitution, functionality and usability. These three shifts are generally categorized as first-, second- and third-generation blockchains, summarized in Figure 1. The first-generation blockchains, like Bitcoin, Ripple and Litecoin, focused mainly on solving the double-spend problem[4] through transaction ordering, record immutability and decentralization. The second-generation blockchains, like Ethereum, moved beyond simple record-keeping, achieving full computational capacity,[5] that is not just decentralized databases but also fully functioning computational environments that run autonomous software and business logic, often called "smart contracts", to be executed by the blockchain. These smart contracts can also work to ensure communication between blockchains. Third-generation blockchains, like Tendermint Cosmos, took a step further to create fully functioning computational capacities and improved chain capabilities, as well as enabling chain-native interoperability using protocols like Inter-Blockchain Communication (IBC).

Figure 1.
The generations of blockchains

First generation (e.g. Bitcoin, Ripple, Litecoin)	→	**Second generation** (e.g. Ethereum)	→	**Third generation** (e.g. Tendermint Cosmos)
• Ledgers • Databases • Networks • Not programmable • No native interoperability or interchain communication		• Functional computers • Programmable • Process business logic • Interchain communication and chain-to-chain interconnectivity achieved through business logic, middleware and smart contracts		• Fully functioning computers • Programmable • Chain-native interoperability through new interchain communication protocols

Source: UNCTAD.

Today, blockchains are best defined as databases or networks with human coordination as their essence. They organize data in a structured and append-only manner into blocks. These blocks are connected (chained) to one another using hash[6] functions and modern cryptography, with each subsequent block holding some historical data of the previous block, which makes it difficult for the chain to be broken or interfered with, for the records to be tampered with, or permission given for any form of unauthorized intrusion without notice. Blockchains are trust engines that enable transparency, coordination and information-sharing (Ying *et al.*, 2022). This mechanism of trust has been made possible through a combination of technical and scientific discoveries in public key cryptography, digital signatures and hash functions that set apace a new computational paradigm.

In general, participants of blockchains have a way to agree on the true state of all records on the chain and with a clear mechanism to verify that no record has suffered from any unauthorized/discretionary alteration. At the heart of every blockchain is the consensus algorithm (the engine of truth) which is the means of agreeing on what that truth is, who has the right to update that truth and when the state of the truth has changed. Blockchains create trust between contracting parties and free individuals from economic coercion by eliminating hierarchical control (Schrepel and Buterin, 2020).

Blockchains ensure anti-forgeability through their consensus algorithms – trustless or trust-minimized. They guarantee business and/or operational continuity and record integrity through distributed-ness and/or decentralization, plus the use of timestamps, redundancies, record replication and hash functions. They establish authority and validity of changes to records using digital signatures. In this manner, they broadly ensure respect for known rules without the use of legal intermediaries but rather through the act of binding parties to a pre-programmed rule book encoded and autonomously executable through computational code. This approach is new in its ability to scale and reach various aspects of human experience, from the creation and running of virtual organizations in industry to fully functional virtual communities and societies at large. But some hurdles remain. Issues around provable autonomous identities on blockchains and uniqueness of personhood will have to be solved for broad uses to be possible within such trustless environments.

Also, grasping the different implementations of blockchain and their capabilities often pose a challenge for decision makers when it comes to data governance, privacy security and standards (Clavin *et al.*, 2020). Recognizing that blockchains are generally technical backbones that users interact with through interfaces is an important step to fully understanding the technical structure. This means users never see the blockchain per se, even when they are using it. Rather, user-facing programs that provide business logic beyond the chain itself are used by the daily user to interact with the blockchain for the purposes for which the technology is intended. Hence, deploying a blockchain network is just one of many steps in implementing a blockchain-enabled service for any mainstream use. First is the technical backbone, then the communication protocols usually in the form of application programming interfaces[7] and/or remote procedure calls[8] and then the portals (applications) that allow the daily user to fully interact with the blockchain environment. Most blockchain networks also use some kind of unit of measurement (token model) native to the given network as a way to publicly settle units of records on the ledger (Lim and Pan, 2021). Even though tokens are not necessarily required to deploy and run a blockchain, they are normally useful for the security of the network, especially in public blockchain networks.

Blockchains possess multiple features that make them general-purpose tools usable as deemed necessary by the implementation entity (see the Annex for a discussion of types and features of blockchains). Their many features make them suitable for modern-day computational needs. Usually general purpose, resilient and particularly safe for preventing unauthorized intrusions and illegal hacks, they contrast with centralized databases which often become target points for cyberintruders. Blockchains distinguish themselves in a significant way by never having a central point of failure and by creating a redundant and sophisticated attack surface.

Beyond the technical evolution, the blockchain industry has also witnessed enormous inflow of talent, resources and policy attention. Since the deployment of the Bitcoin blockchain in 2009, the blockchain industry has grown from being an unknown industry to over $3 trillion market capitalization at its peak in November 2021 with an ever-increasing inflow of engineering talent, corporate capital and global investments. Bitcoin, which made the idea of Internet-native currency possible for the first time, set the foundation for many innovations that were to follow. Today, thanks to the blockchain, it is now possible to establish and fulfil Internet-native contracts through the use of smart contracts,[9] and to own and operate Internet-native organizations usually called decentralized autonomous organizations.[10] These virtual organizations currently hold billions of dollars in their corporate treasuries, autonomously acquire assets, independently invest in other entities, and manage resources through community coordination with no physical existence in any national jurisdiction.

Innovation in the blockchain landscape is very similar to the growth trajectory of the early Internet. For example, until recently, blockchains were generally containerized systems. Transporting data from one blockchain to another required trusting some central entity or pseudo-centralized entity and giving up sovereignty and/or security to move data, records or assets between independent blockchains. Then in 2021, Tendermint's IBC, a transport protocol, allowed two or more blockchains to directly connect and natively communicate with each other. With IBC, any user can now transport data packets from one blockchain to another without an intermediary. Taking IBC further, in 2022 interchain accounts (ICA) allowed users on one chain to natively query data, issue commands and execute instructions on a foreign blockchain, among other things. For the first time in the blockchain industry, chains do not just have the capacity to communicate but now have the capability to allow users to cross-compose applications and business logic across multiple chains. This brought a new era of an Internet-like blockchain bringing Internet-native money, contracts and organizations that allow full interactivity and interconnectivity. Table 1 demonstrates the evolution of major innovations and breakthroughs on the blockchain.

Table 1.
Evolution of blockchain over the years

2009	2015	2021	2022
Bitcoin	Ethereum	Tendermint interchain protocol	Interconnected blockchains
Cryptocurrency	• Smart contracts • Decentralized autonomous organizations	• Smart contracts • Decentralized autonomous organizations	Interchain accounts
Internet-native money	• Internet-native contractual agreements • Internet-native organizations	Inter-Blockchain Communication protocol	Cross-chain composability

Source: UNCTAD.

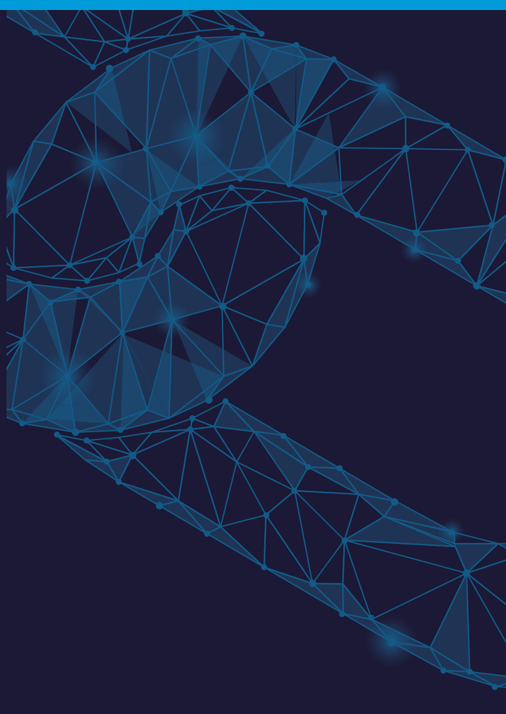
Blockchain technology is a combination of multiple computer-science innovations and most blockchains share certain core features that make them suitable for trade facilitation use cases. These features include, among other things, the use of public key cryptography, timestamps and hash functions, distributed data storage and multiple backups (redundancies). Different blockchain networks use varying forms of these technical features, and certain design choices are more favourable for certain uses than others.

Implemented well, blockchains can add value to a nation's digital-trade infrastructure. Table 2 lists some of the unique features and key functionalities of blockchains for specific international trade processes.

Table 2.
Key features of blockchains and their functionalities for international trade

Features	Functionalities that benefit from a feature
Public key cryptography	• Cross-border trade stakeholder cooperation in data exchange • Data protection from intrusions and data breaches • Non-repudiable digital signatures of stakeholders • Stakeholder digital IDs for verification and fraud prevention • Detection of data tampering
Timestamps and cryptographic hash functions	• Identification, verification and acceptance of electronic copies of trade documents • Detection of counterfeits and intellectual property theft • Preservation of integrity for data on containers and their content collected using IoT devices (e.g. temperature, humidity) • Supply chain transparency • Value chain provenance • Detection of tampering and unauthorized intrusions
Distributed data storage and redundancies	• Blockchains' distributed servers (nodes) ensure more resilient trade infrastructure • Redundancies help withstand natural disasters, system outages and cyberattacks for business continuity

Source: UNCTAD.



3 Potential blockchain use cases in international trade

3. Potential blockchain use cases in international trade

Blockchains are best known today for financial applications and financial engineering. However, the technology, like the Internet, is general purpose. While there is growing consensus on their possible use cases, proven large-scale use of blockchains outside finance remains limited. This is partly attributable to the nature of the technology as a multi-stakeholder–focused technical framework by default, distributed by design and communally operated by architecture. Thus, to implement and use a blockchain environment mostly requires acceptance and buy-in from all system participants. Usually without a central switch, blockchains are new to how many legacy digital systems and standard government procedures operate. Nevertheless, there is growing interest in blockchain technology as a potential foundational technology for international trade processes. For example, the UNCTAD Automated System for Customs Data (ASYCUDA), an integrated Customs management system for international trade and transport operations in a modern automated environment, has explored the potential use cases of blockchain in the ASYCUDAWorld system, e-payment and regional transit.[11] The United Nations Economic Commission for Europe (UNECE) has also highlighted the potential use of blockchain technology to improve supply chain transparency, facilitate maritime trade which accounts for over 80 per cent of global trade by volume, manage road transport and so on (UNECE, 2020).

Before an institution considers the use of blockchain, it is important to know when to use a blockchain and when not to, whether as a government or a private sector entity. A decision tree helps both governments and private sector stakeholders to consider the use of blockchain in an understandable and simple way (Figure 2). It seeks to both validate the business case for the use of blockchain and invalidate the common myth that blockchain is needed for every business problem. As a general-purpose technology, blockchains are becoming subject to a common belief that they can be a solution to every commercial, administrative and procedural business and government challenge. But the technology is not yet proven to be able to solve many problems and in some cases the use of traditional databases may provide a better fit than a blockchain. Policymakers should consider the decision tree to help ascertain that business needs fit being solved using blockchain before implementation attempts are made.

Going through the decision tree gives the decision maker – whether a government, a private sector entity, a not-for-profit or a civil society organization – three possible scenarios. It confirms whether the decision maker needs:

1. ***A blockchain environment***

   In this case the decision maker has answered a strong YES to all or most of the questions in Figure 2 and sees a clear value addition or efficiency gains in the use of blockchain technology in the business area, policy area or administrative process of the agency or organization compared to the existing system or status quo.

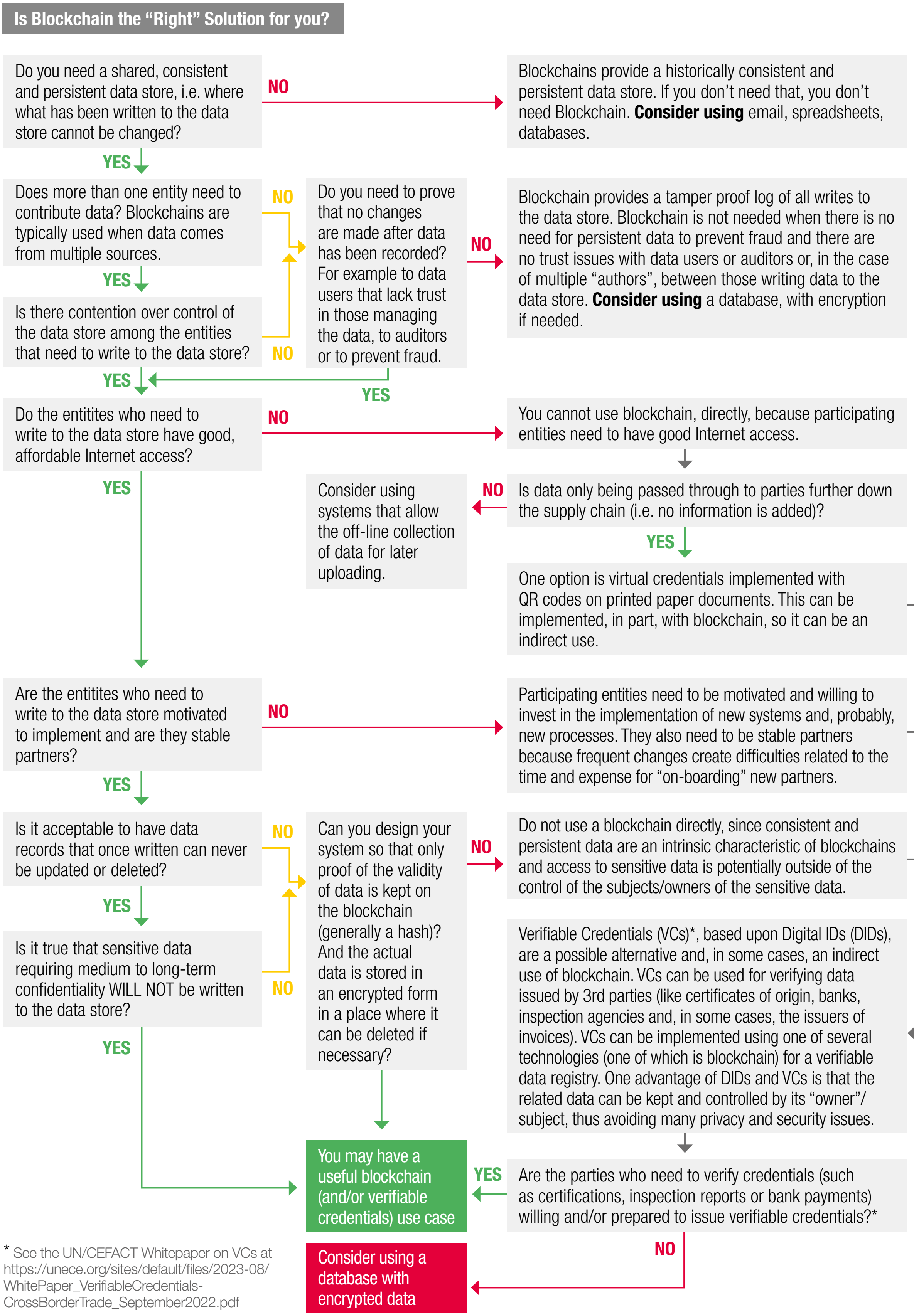
2. ***Non-blockchain environment***

   In this case the decision maker has answered a strong NO to most or all the questions in Figure 2 and does not see a clear business value addition or efficiency gains from use of blockchain technology in the existing business process or administrative procedure compared to existing digital systems in use.

3. ***A blended environment***

   In this case the decision maker has answered YES as much as NO to the various questions and, more importantly, has varying business logics that require different technical and/or regulatory considerations within a single business or administrative process. In this scenario, the decision maker sees value addition and efficiency gains from the use of blockchain technology in some of the business logics while there is no value addition or efficiency gains in other business logics within the broader business process. In this case, an application layer that runs some of its business logic on a blockchain while some of its business logic runs on a non-blockchain environment is ideal. An example might be a

Figure 2.
Decision tree for the use of blockchain technology



Source: Triangularity, 2023, based on United States Department of Homeland Security, 2018.

National Single Window application for trade facilitation that runs a business logic of data validation and verification among multiple parties on a blockchain environment on the one part, while other business logics within the same National Single Window portal run on a traditional encrypted database.

From the foregoing, and exploring the merits of the use of blockchain technology, specific use case areas – such as cross-border clearance, stakeholder coordination, payment processing and trade finance, trade-risk management, trade data reporting and management, traceability of value chains and transparency of supply chains – are identified as likely areas where blockchain application could bring efficiency gains. These areas have also seen general proofs of concepts, pilot programmes and growing use among governments and the private sector with successes and challenges. In the subsequent sections, these use cases will be explored in detail and the lessons learned by implementing agencies will be shared.

A. Cross-border clearance

The amount of time and cost spent at a country's borders has significant impact on traders' experience. This is also an indicator of the country's competitiveness and ease of doing business. Cross-border clearance and port processes serve as critical administrative gateways of a nation's trade facilitation performance. Giving a policy boost to these administrative processes at a country's borders, through technological enhancements, can improve the overall trade performance of the country and increase the country's competitiveness. For example, at a country's Customs check, goods/services must meet, among other things, the key requirements that: (1) the identity of a stakeholder is who they say they are, (2) the integrity of the data related to the goods/service declared is ensured and that value of said items is appropriately reported and recorded, and (3) the origin/source of the goods/service is correctly reported.

Guaranteeing the veracity of each of these requirements is a daunting task especially for countries that are not very well integrated in the global economy. Even in countries where these can be verified, the authenticity of the reported data heavily relies on the trustworthiness of counterparties in the trade process, causing trade information to have to be transmitted and validated multiple times. Countries aiming to cut administrative red tape, reduce trading costs and cut time to trade usually have to invest efforts in streamlining Customs procedures and promote paperless trade, as well as pursue digitalization and automation to shorten the time it takes for traders to conform with key procedural requirements at the border in order to meet compliance. A key component of the streamlining process usually has to do with data integrity – whether the trade data meet requirements, whether the trader's data are authentic and whether the trader's data are reliably reported and recorded appropriately by the various public and private sector stakeholders in the trade cycle. While some of these data can be locally verified at individual agency level, most require some form of cross-agency and cross-border coordination among stakeholders in different agencies within the country on the one hand and sometimes between stakeholders of the origin and destination countries on the other hand. This makes data quality assurance, data integrity and information validity for cross-border clearance a particularly difficult task, causing much information to be rechecked and reverified many times at different agencies for different compliance purposes. This usually leads to major delays at the Customs checks, costing traders both money and time. The question is, can blockchains help?

Given that blockchains are trust/truth networks without necessarily requiring trusted parties, their most important feature of immutability prevents any actor from being able to discretionally alter data without triggering a global alert/awareness. This means they are particularly suitable for the purpose of holding a globally valuable database that would otherwise require stakeholder-to-stakeholder contact for verification and validation. Thus, they not only facilitate traceability and trackability of the entire provenance of the document trail, but are also capable of automating the checking process of integrity of the documents that pass through them with any alterations easily noticeable because they are tamper-evident.

Furthermore, depending on the protocol used, blockchains have trust guarantees built into the core of the technology, making them automatic data verification/validation machines for their intended purpose. From trade licences to certificates of origin, much trade documentation could be automatized and made available to all relevant stakeholders both in origin and destination countries and in real time, allowing for cross-border validations limiting the need to contact the issuing authority of such documents.

Also, with encryption, pseudonymity, sovereignty and so on, blockchains can preserve the privacy of traders while speeding up global trade processes by ensuring data availability in real time to all stakeholders. While blockchains ensure that data cannot be altered without authorization, they can also, through the use of smart contracts, allow for selective data management, data sharing and data authorization on a pure need-to-have basis. Kerstens and Canham (2018) see blockchain technology as particularly well positioned in the area of being able to help bridge the trust gap that often arises between trading countries and helping to revolutionize multilateral trading agreements. They see blockchains decreasing trade friction, trade fraud and enhancing documentation without need for documents to travel physically with the goods or be exchanged between parties.

There is a major collaboration between the Stuttgart-based software provider AEB SE and the Fraunhofer Institute for Material Flow and Logistics, who work together to develop a blockchain-based end-to-end digital platform that ensures that contents of trade documents are traceable at any time, for exporters (consignors of goods), importers (consignees of goods), logistics partners, transport companies, Customs brokers and Customs authorities all at the same time. Though at an early stage, its prototype demonstrated in a post-Brexit context, especially, how a fragmented global trade environment could be connected by blockchain and trade processes be streamlined for a better trader experience internationally.[12]

Furthermore, when the Singapore International Chamber of Commerce in collaboration with cross-border trade facilitator vCargo Cloud unveiled the first blockchain-based platform for electronic certificates of origin using the Ethereum blockchain infrastructure, it made information authenticatable and accessible using simple QR codes, scannable with smart phones, thereby eliminating data duplicates and the requirement for manual re-entering of information by trade stakeholders (Giegling, 2022; see also Ganne, 2018). This use case opened the door for many more trials on the front of data authentication, validation and verification using simple applications built on top of the blockchain.

Another blockchain project that has seen wide acknowledgement is CADENA (Santamaria, 2018). Built on the LACChain[13] and implemented by Customs authorities in the Plurinational State of Bolivia, Chile, Colombia, Costa Rica, Ecuador, Guatemala, Mexico and Peru, with the support of the Inter-American Development Bank, CADENA has accelerated the processing of goods among the beneficiary countries and established information flows that aid not only Customs authorities but also other stakeholders and systems that use the information. Becoming fully operational in August 2021, Customs authorities validated it with real data and noted benefits have been seen in improvements to the operational implementation of bilateral or multilateral mutual recognition agreements and for the management of Authorized Economic Operator (AEO) programmes. Some of the acknowledged benefits of CADENA according to a joint publication of the World Trade Organization and World Customs Organization (2022) include:

- data quality assurance and data integrity, as well as the creation of data access controls through the authentication of Customs officers with assigned credentials
- a point-to-point automation of the exchange process of AEO certification status
- maintaining of historical records of shared information relating to AEO certificates with real time traceability and security
- increased transparency in data exchange and
- noticeable reduction in time and costs for AEOs through the automation of various administrative procedures at both origin and destination countries.

Many other countries see blockchain potential in facilitating Customs procedures and economies such as China, Guatemala, Indonesia, Malaysia, Morocco, Saudi Arabia and the United Arab Emirates as well as the Hong Kong Special Administrative Region of China are at various levels of testing, proofs of concept, deployment and pilots. It remains to be seen how much utility can be derived from the technology in Customs procedures on a large scale but at a time where digitization and e-commerce are taking centre stage in the international trade space, faster Customs clearance will continue to be an important component of every economy's competitiveness. Improved Customs clearance usually leads to significant reduction in the broader trading time and cost to trade, saving businesses crucial time and money. This means blockchain technologies' potential to readily deliver crucial information validity in real time and on a need-to-have basis can significantly help to improve trade efficiencies through the availability and exchange of trade data among government stakeholders on the one hand and between governments and corporate stakeholders across national borders on the other. This could lead to better business experience for traders and improved competitiveness for governments.

B. Stakeholder coordination

It takes on average 15 agencies, some 25 stakeholders and on average 35 documents with over 60 per cent of them needing manually re-entered information, to clear a typical shipment. These statistics can easily double in certain developing countries. The multi-stakeholder nature of international trade transactions means that the ability for stakeholders to streamline processes for ease of coordination is important for the overall trading experience of businesses and operators altogether. Yet, stakeholder coordination remains a leading challenge to cutting down cost and time to trade. Since the entry into force of the World Trade Organization Trade Facilitation Agreement and numerous other bilateral and multilateral trade agreements aimed at facilitating trade, administrative hurdles still form one of the single largest non-tariff barriers to trade. This is partly due to the lack of proper coordination among key stakeholders both within national borders and across borders. The lack of coordination easily leads to duplicative processes from multiple stakeholders, multiple compliance procedures, manual paper trails and a lack of single or harmonized source of trade information and trade processes. The work of UNCTAD with National Trade Facilitation Committees over the years has been with the main goal of creating a single policy platform for key stakeholders to meet and coordinate among themselves to improve their respective national trading environments.[14]

Blockchains, as multi-stakeholder databases by design with data verifiability by default, are powerful computational tools for any operational arrangement in need of collaboration, coordination and cooperation of parties with disparate needs. Data immutability on blockchains make them particularly essential for stakeholder coordination both within and across borders because the technology can remove the need to rely on the trustworthiness of counterparties and other stakeholders while achieving the goals of reliability and authenticity of the data.

With blockchain as the foundational digital infrastructure, various stakeholders in the trade process can plug in and access information while cutting back on administrative processes and improving the whole trade experience within and across borders. The multipronged nature of international trade processes makes it difficult for traders to fulfil all the differing administrative and technical requirements. Thus, a base technology stack that allows for the various stakeholders, selective accessibility, and the use of data, based on each stakeholder's unique needs, protecting user privacy while running on a single data-stream can bring significant efficiency in stakeholder coordination.

For example, in 2020, Moroccan Customs launched a blockchain-based project in cooperation with DHL and the German International Cooperation Agency (GIZ Morocco) with the aim of developing an ecosystem for the data of parties to all international transactions (traders, express mail service, Customs, other stakeholders) and the sharing of this data in a secure manner among trade-processing stakeholders for faster coordination and speedy administrative processes. The mitigation of trade risks, and enhanced accuracy to trade valuation, were among some of the expected benefits of this implementation (Moroccan Customs, 2020). Blockchains can thus help to:

- enforce information reliability and data availability
- aid business continuity through the use of blockchain-based application-specific portals that bring resilience and technical reliability
- allow for institutional and individual accessibility
- enhance better coordination among stakeholders with differing business and procedural needs in the trade cycle

To achieve this in the design of a blockchain-enabled digital infrastructure, it is important to first understand the needs of the key stakeholders in a trade cycle and which of their operational challenges can be solved with a blockchain-enabled trade environment.

Stakeholders play different roles in the international trade process. Facilitating the trade process with digitalization and automation through blockchains requires an understanding of the roles and needs of key stakeholders within and across national borders.

The key stakeholders in every cross-border trade involve private and public sector participants. While public sector players are usually policymakers at the top of the hierarchy and operational-level managers are at the middle and lower level of the government bureaucracy, private sector participants are usually commercial entities interested in doing business and looking to cut down cost and time to trade wherever possible. In the automation and digitalization process, their varying needs should be taken into consideration to build the appropriate digital environment to facilitate trade. While a blockchain would serve as a single digital backbone for relevant processes, these stakeholders would need different business logic in the design of trade portals that allow them to interact with the blockchain-based tools in the normal course of business. Thus, before implementation of a blockchain environment, it is important to understand the technical and policy needs of the stakeholders concerned in order to design the right business logic and portals that allow the participants to accept, adopt and put the digital tools to use as intended.

For example, while a Customs officer may need to check and validate commercial documents for valuation on the blockchain, a shipping company may be keen to ensure that key trade documents like bills of lading are digitalized to allow speedy transmission of the document along a string of sellers, buyers and banks to the final consignee (UNCTAD, 2023: section 5). This would reduce the incidence of delayed bills of lading, an issue that can give rise to significant risks and costs for the carrier, who is legally entitled to discharge the cargo only against surrender of the original bill of lading.[15] Hence the application logic that interacts with a blockchain environment can significantly differ according to the needs of the stakeholder within the trade cycle. Table 3 demonstrates a sketch of the business needs for key stakeholders that could be included in a portal running on a blockchain backbone. These design ideas are by no means exhaustive; rather, they are intended to give a sketch of the user needs that could be considered at the technical design level.

Table 3.
Building blockchain portals in trade facilitation for key stakeholders

Key stakeholders	Sector	Key technical design needs
National Customs	Public	Interactive portal for: • Data authentication • Trade valuation • Payment processing • Notification alerts to/from other agencies
Agriculture authority	Public	Interactive portal for sanitary and phytosanitary certification and validation
Ministry of Trade	Public	A portal for approval/authentication of trade information
Health authority	Public	Interactive interface for sanitary and phytosanitary certification and authentication
Standards authority	Public	A portal for delivery of authorizations, classifications and tariff line verification
Revenue authority	Public	A portal for tariff lines, receipt and processing of payments, alerts to other agencies
Shipping agencies	Private	A communication and authentication portal to traders, forwarders, bankers and authorities
Banking institutions	Private	A payment processing and communication portal to traders and other stakeholders
Clearance/forwarding agencies	Private	A verification portal for trader-specific data, real time trade flow, tracking of consignments and declarations
Traders	Private	A portal for access to service providers, payment processing, consignment tracking, self-declarations, certifications and credentials, and notifications alert system

Source: UNCTAD.

C. Payment processing and trade finance

In international trade performance, the time and cost associated with making payments, especially in developing countries, remains high. While trading across borders at its most basic level can be described to be simply a transaction that involves buying and selling, the trust guarantees required in payments among the multiple stakeholders, counterparties, middle parties and complementary parties in an international trade transaction are many, risking payment delays and sometimes complete payment failures. Making payments in a cross-border transaction is usually not to one party but to multiple parties at various levels of the trade cycle. Sometimes it is payment to multiple agencies within a single country for differing services, including administrative and commercial requirements. The payment process constitutes a significant part of the trading process and, to improve the trader experience, an understanding of the trader needs in payment is necessary.

For example, in a typical international trade transaction settlement, the trader is usually required to make payments to multiple parties both in the private and the public sectors. These payments are handled by a payment processing bank and sometimes multiple payment processing banks, especially in developing countries. But the trader remains ultimately responsible for checking and confirming that the payments made to all the unique private and public sector agencies through the payment processing banks is successful and in time; thus an improved payment experience for traders could save them time and cost.

In this context, countries like Jordan have seen significant potential for blockchain technology to improve digital payments and develop e-commerce (UNCTAD, 2022b), especially in the area of business-to-business payments and business-to-government processes. In India, a permissioned environment developed by Finacle Trade Connect, called the India Trade Connect, works on leading DLT vendors like R3 Corda, Hyperledger and Ethereum, as a DLT-based trade finance initiative, supporting a comprehensive end-to-end trade, supply chain processes and payment functions including open account, letters of credit, bank guarantees, bill collections, consumer-to-consumer and business-to-business transactions, invoice discounting, reverse factoring and invoice financing. The system operates using a competitive fee model aligned to the volume of transactions (see Patel and Ganne, 2020) and has seen significant efficiency gains in improving the payment experience of businesses and traders. According to the World Economic Forum, the cross-border payments landscape using traditional processes, for example, is fraught with fees, hurdles and delay with individuals incurring outsized fees (World Economic Forum, 2021). Automation of this process with blockchain-enabled payment backbones is seen to be able to eliminate several of the current need for intermediary processes, reduce the time of payments, cut back on delays and even prevent payment failures.

Payments can become even more streamlined and more reliable when smart contracts – self-executing autonomous pieces of computer code – are used. Blockchains coupled with smart contracts show promise as new tools for international settlement as well as Internet-native and cross-jurisdiction payments.[16] They, by design, can guarantee trust by code and allow many multiple parties to engage in payments that would otherwise be considered complex in a standard legacy payment system. For example, in most countries' public sector operations, depending on the content of the export, the trader must liaise with multiple agencies and ministries to obtain various clearances and documentations (ranging from certificates of origin to phytosanitary certificates) and make payments to all agencies individually. Most of these certifications and processes come at a cost and payments are usually required to be made to the issuing agency. This is in addition to all the payments that must be made to private sector counterparties such as the shipping agencies, freight forwarders, insurance parties and warehouse service providers. Automation with blockchains and smart contracts could make these processes easier, faster, less complex, and trackable, by allowing a trader to, for example, make a single deposit for a consignment for all government services, and upon fulfilment of all procedural requirements this payment will then be automatically released to the relevant agencies with individual amounts according to the charges owed to each public sector agency. Private sector payments could take same mechanism with a harmonized payment backbone using blockchain, thereby cutting the time and effort required on the side of traders to execute individual payments to each concerned counterparty. IBM identified several trade financing and payment benefits that can be attained from a blockchain-enabled trade environment to entities like banks, buyers and sellers, and especially among small and medium enterprises (IBM Blog, 2021). Some of these include:

- potential expansion of financial services to small and medium enterprises and companies that would traditionally use open account trading
- increased insights into client financial positions and transaction histories thereby reducing financing risk
- new revenue streams to banks through new financing products and alternatives to letters of credit
- reduced operating costs by digitizing slow and cumbersome paper processes
- enhanced financial controls and compliance measures through the blockchain security
- increased speed of financing approval processes and trading cycles

- reduction in the risk of non-payment or late payment
- trade deal trackability of all steps end-to-end

UNECE (2020), in a white paper, identified some key areas where blockchains hold potential in financing and payments (Table 4).

Table 4.
Use areas of blockchain payments and trade finance

Use area	Description
Credit management	A composite tool of aggregated data on counterparty risk. A blockchain-enabled environment that gives the counterparties data in a tamper-proof or tamper-evident environment could reduce fraud, reduce credit risks and improve financing experience for both the financier and the borrower
Invoice financing	Short-term loans of a trader collateralized by business receivables, a shared end-to-end payment rail where all receivables are independently verifiable by the financier could improve the financing experience and cut financing risk
Purchase order financing	Short-term capital extended to a trader backed by inventory. A trackable and transparent blockchain between the financier and the business could increase trust among the parties, reduce risks of financing and improve efficiencies
Letters of credit	An agreement between the buyer (applicant), the seller (beneficiary) and the bank, with the bank promising to make a payment on behalf of the applicant, and in favour of the beneficiary, when the terms and conditions stated in the letter of credit are met by the beneficiary. Blockchains and smart contracts can especially bring many operational efficiencies in issuance and processing of letters of credit
Financial supply chains	Suppliers' ability to get funding through account receivables can be enhanced through the transparency, security and traceability to the whole supply chain brought by blockchains
Nostros account management	The management of a foreign currency denominated account that a bank holds in another bank. A blockchain-enabled environment makes real time available and can increase operational efficiencies for banks
Insurance processing	End-to-end trackability of supply chains, business process and operational dynamics can streamline the insurance process and even reduce cost at both ends of the insurance process from client onboarding to underwriting and claims processing

Source: Adapted from UNECE (2020), part II, section 10.

Payments in an automated and secure blockchain-enabled environment brings other benefits as well to countries especially those where revenue leakages in trade processes remain a problem. While payment processes for international trade purposes in developed countries are generally safe and reliable, in developing countries payment processes remain siloed, shifting and generally unpredictable in the broader trade ecosystem. In most developing countries, multiple public agencies must be visited in person and payments made physically by the trader to obtain relevant trade clearances. This leads to cases of underhand payments, collusion, mis-invoicing, and loss of trade revenues by the governments. Automation through blockchains and smart contracts could eliminate a significant part of in-person contact, limit opportunities for corruption, reduce revenue leakages and improve government revenue.

The challenge with transparency and accountability in payment processing is a particularly significant problem in developing countries.

Data availability, validity and trackability on blockchains will improve accountability mechanisms. Stakeholders will be obliged to meet minimum compliance requirements, for example whenever the actual revenue does not match the data on the blockchain, making auditing and crime easy to prove. Data on the blockchain will thus serve as basis and evidence to query corruption and potential corruption cases.

Payment processing could thus be improved with blockchain. Policymakers looking to improve national revenue and eliminate corruption could use the technology for solutions. If relevant stakeholders are on board and key agencies collaborate, blockchains for payment processing and trade financing could be one of the areas with significant efficiency gains and value addition. Potential benefits of broader transparency, fast payments, payment traceability and revenue trackability could be a net gain for stakeholders and governments at large.

D. Trade-risk management

The need to ease trade processes while cutting back on trade risks such as trade fraud, under- or over-invoicing and corruption, to ensure rigorous trade compliance, remains a delicate balance especially at a time when global supply chains have come under tremendous pressure and trade risks remain elevated on various fronts. Furthermore, trade volumes are increasing, driven by an ever-growing e-commerce sector with millions of small parcels crossing borders annually. Manually checking and verifying every data point of these massive trade volumes is getting daunting for governments and sometimes impossible for all compliance checks. Hence, automation has become a necessity for the twenty-first-century trading system.

With blockchains, the ability to smooth out trade flows globally with attention to only those traders or consignments flagged as having elevated risk profiles could improve procedural compliance and at the same time allow many genuine traders an improved trading experience. While they can assure data integrity and information validity at a global level, blockchains further make the use of selective trader checks on a case-by-case basis not just possible but also very useful in eliminating trade risks, while keeping the larger trader population unaffected. Digitalization and automation through blockchains can thus ensure compliance, reduce manual operations and speed up processes, to keep countries competitive. There is a wide array of areas where trade risks could be minimized or even eliminated while improving the traders' experience using blockchains. For example, the Geneva trade-processing platform, Komgo, whose platform is built on the permissioned blockchain environment called Quorum Blockchain[17] today allows commodity traders to submit digital-trade data and documents to finance institutions and apply for credit directly on the platform. The platform improves compliance and manages trade risks by providing various Know Your Client solutions, standardizing and facilitating the process while maintaining privacy of its users by transmitting data on a need-to-know basis. Users benefit from a single source of trust to exchange documents on a secure and private network to perform all Know Your Client tasks. The system further provides a certification feature that allows Komgo users and even non-users to stamp their documents on the network to ensure their digital authenticity. Today, more than 150 companies use the platform for various trade processes and compliance purposes (Patel and Ganne, 2020). The tamper-proof nature of blockchains makes them suitable for trade-risk management in handling trade documents like commercial invoices, insurance documents, ocean bills of lading and bills of exchange.

Furthermore, it was argued that blockchain technology could reduce the room for risks by simplifying the trade process, and their decentralized nature also allows point-to-point transactions without any need for approval and verification by any central authority (Sun *et al.*, 2020). According to W3C, the World Wide Web Consortium, the adoption of blockchain-based decentralized identifiers, for example by supply chain stakeholders (including global government regulators, trade standards institutions, vendors, shippers and retailers), could more accurately verify the origin and destination of products and services, which will streamline and enable the reporting designed to apply correct tariffs, prevent dumping and monitor transhipment (W3C, 2022).

An unalterable global database (blockchain) of trade flows and freely exchangeable data that is automatically available on a case-by-case basis presents some unique opportunities for decision makers, especially regarding trade fraud prevention, under-invoicing, over-invoicing, misclassifications and the protection of intellectual property rights. TradeTrust, which uses a set of globally accepted standards and frameworks, connects governments and businesses to a public blockchain to enable trusted interoperability and exchanges of electronic trade documents across digital platforms and across different jurisdictions. This system is compliant with the Model Law on Electronic Transferable Records and offers title transfer, document authentication, document provenance, and selective disclosure, providing open-source software to enable the digital verification of documents.[18] Open and available to everyone, and anchored on a number of public blockchains with smart contract capabilities, the TradeTrust platform presents some of the major potential use cases of blockchains in trade-risk management by leveraging digital capabilities, including digital signatures and automation through smart contracts. Trade risks arising from fraud, document falsification, illegal alterations of trade information, under- and over-invoicing, counterfeit products, misclassifications and intellectual property infringements still cost governments significant revenue. While the use of blockchains could eliminate these risks, improve trade performance and bring various net gains to countries, there are numerous technical problems related to scale and interoperability to be resolved.

E. Trade reporting, trade data and trade policy planning

Trade assessment, trade information, trade data and trade reviews are critical for policy planning, trade facilitation improvements, performance and national competitiveness. Unfortunately, most countries' trade data remain disaggregated and siloed within institutional data servers, agency databases and sometime several cloud service providers. This creates many data gaps in the trade processes of an economy and makes trade reporting unreliable, trade performance easily overreported or underreported, trade valuations inaccurate, and assessment of trade challenges difficult. Trade data availability remains key to policy planning and trade assessment and makes feedback more constructive in removing trade bottlenecks.

Blockchains do not only make data available in real time to all key stakeholders and participants, but they also make that data immutable and verifiable. Supported by the efforts of the stakeholders, this could significantly improve trade reporting and reviews, offer clearer understanding of supply chains, and make trade bottlenecks more visible for policy redress. With blockchains, policymakers can address trade hurdles on a timelier basis with more accurate data for trade reporting and a reliable database for continuous reference. The use of blockchain technology could also make data easily available, accessible and verifiable for trade valuation purposes without the need to rely on counterparties and stakeholders' goodwill. It is important to acknowledge the existence of current data gaps and institutionally siloed data systems that make trade reporting unreliable and the need for a more reliable automatically verifiable data availability for trade reporting, policy guidance and trade improvements within countries and across borders. Blockchain possesses significant potential that could improve the data flow and data quality within the trade cycle.

F. Supply chain transparency and value chain traceability

Supply chain management is generally considered an area with both present and potential use of blockchain technology. Introducing blockchains for the purpose of supply chain provenance and transparency as well as value chain traceability easily reveal efficiency gains. This is partly because of the key features of blockchain as necessarily a multi-stakeholder tool but also because of the current challenges besetting supply chains and the growing demand by consumers for transparent value chains. There is growing demand for proof of sources of goods and services being consumed by the consumer. Many companies have developed blockchain applications that allow for the tracking of origins of products, prove their authenticity and use this as a basis to assert ethical claims as well as gain fair-trade qualifications. Since a number of consumer outrages regarding quality standards shook the food industry in recent years, major food and retail companies are turning to blockchain, not only to enhance transparency of the food supply chain, but also to enable them to track tainted products quickly and help restore trust in food quality, though establishing a credible link between offline and online events remains costly (Ganne, 2018). The rapid and growing adoption of blockchains especially in the supply chain industry could be attributed to three areas where blockchains provide superior advantages while conventional centralized systems face technical challenges (Song *et al.*, 2019):

- **Complex chain of actors in a supply chain:** traceability requires the active engagement and well-concerted collaboration of many participants or actors in the entire supply chain. Building and operating a centralized system across the complete supply chain often becomes impractical.
- **Ensuring trustworthiness of actors:** in a complex supply chain with many actors, a good supply chain cannot be built without strong trust in the entire chain. Hence partners in the supply chain find the democratized and tamper-proof record-keeping system of blockchains ideal for trust and reliability.
- **High-cost and barriers to entry on legacy centralized systems:** many legacy centralized systems have been implemented with expensive systems from major tech companies. This raises barriers to entry for the inclusion of small participants in the supply chain – such as farmers, truck drivers and fishermen – generally referred to as the last-mile stakeholders. Blockchain-based traceability systems for supply chains could allow the development of applications where these small actors participate in a supply chain traceability system via smartphone.

Furthermore, there is growing interest among producers to prove that their goods meet certain sustainability standards in order to enter niche markets and earn sustainability premiums, given that the sustainability question within supply chain debates is growing stronger, and consumers increasingly demand independent and autonomous verifiability of sources of goods. Green value chains, in particular, have become a central focus among policymakers, civil society and not-for-profit organizations as well as the private sector. Consumers' sustainability concerns such as whether businesses adequately protect the environment in their production process and whether they meet minimal social and human rights standards have led to various sustainability certifications designed for businesses to prove their sustainability performance. But acquiring, verifying and presenting these sustainability data in a reliable manner has been a major challenge for policymakers, civil society, not-for-profit organizations and business leaders. According to UNECE (2022), establishing reliable traceability on a supply chain requires information about assets (goods), including information about their what, where, when, who and why. This is done by recording, at specified events, unique identifiers for these five or six data components:

- **party** (company or individual – farmer, tanner, ginner, weaver, subcontractor, etc.)
- **traceable asset** (raw material, intermediate or finished product, production or product batch, or trade unit)
- **facility** (farm, manufacturing site, etc.)
- **process** (harvesting, spinning, dyeing, etc.)
- **location** (farm, production site, etc.)
- when applicable, **transport** (means of conveyance for goods and logistics units used for transporting traceable assets)

The reliability of a traceable system therefore depends to a very large extent on the reliability of the identifiers. Blockchains' immutability, timestamps, distributed redundancies and shared nature are features that can play a key role in ensuring the traceability of these identifiers. While technical standards on enabling traceable supply chains are maturing, supply chain provenance concerns have seen significant interest from the consumer and the producer as well as governments and not-for-profit organizations. That is because issues like carbon footprints, green washing and the reliability of sustainability certifications are all becoming critical components in the sustainability equation. Some areas witnessing the growing interest in sustainability standards that could profit from the data immutability provided by blockchain technology include:

- **Sustainability certification:** various sustainability certification programmes exist today with the aim of proving and verifying the sustainability compliance and performance of the actors within these supply chains. Sustainability certifications like Fair Trade and Fair for Life rely on the trustworthiness and reliability of information provided by the certifiers and product investigators. Consumers have to rely on the honesty of the designers of the programmes and the information presented on the package of the product for reliability of claims of the sustainability compliance of beneficiary companies. Blockchains' role for disintermediation has been considered as one of the most reliable approaches to see if all actors are in compliance with sustainability standards, entering data as and where required. If data are illegally falsified by a supply chain actor, such actors could lose sustainability scores or even lose their entire sustainability compliance status.
- **Tracking of carbon footprints:** another area gaining prominence in the sustainability discourse regarding supply chains is how to calculate and verify data that shows the carbon footprints of products within certain supply chains. Carbon data is notoriously difficult to capture and confirm due to the high level of technical complexities involved in both capturing these data along a complex supply chain and verifying their veracity among actors. Thus, a trustless environment where actors' carbon footprints are trackable and easily verifiable based on technical standards, especially when coupled with IoT devices without relying on the honesty or trustworthiness of the actors, remains promising.
- **Demonstration of compliance and voluntary reporting:** on almost all levels of the sustainability equation, voluntary reporting and demonstration of compliance need a trusted set of actors willing and able to report their data to serve as a reliable basis of a sustainable supply chain. With the variety of actors and their diverse roles and needs, a distributed unalterable database with peer-to-peer anchors that allow for a means of channelling data in a verifiable and secure manner among willing and interested actors, and along the life cycle of the products in the production process, could bring value addition. This could be done in a way that captures and updates data at every level of significant transformation or value addition to the product with the compliance mechanism started at the commencement of the value chain all the way to the consumer. This peer-to-peer driven compliance with supply chain sustainability could ensure new forms of transparency and actor compliance across whole chains of actors.

While technical features of blockchains like immutability through the use of cryptographic functions and traceability through timestamps are useful in creating record trails, making the technology suitable for supply chain provenance, two major conditions are critical for the blockchain to be useful for this purpose:

- **Data quality:** this has to do with the accuracy and source of data entered into the blockchain. The data at first entry, which begins and accompanies a good's journey, must first be accurate and should have captured the true state of the goods at origin. This requires that the reference data on the blockchain capture and correspond to a piece of some of physical manifestation (information) on the product or at the very least the product package with constant updates to that physical product data at every transition point, adequately capturing the value addition, the extent to which the product has been transformed, and a record update to the next entity on the value chain with all events being correspondingly captured on-chain. Data quality and reliability is thus critical for supply chain transparency to be considered reliable on the blockchain. Data immutability on blockchains means that while computers are well known for GiGo (Garbage in, Garbage out) blockchains are best known for GiGF (Garbage in, Garbage Forever). Once data is compromised or inaccurate at the outset, the data trail becomes useless and completely fails the purpose for which the date have been entered on the blockchain in the first place. While the technology of blockchain may be suitable for this purpose, coupling it with the use of off-chain data integrity tools like DNA markers have been shown to be a reliable way to ensure that data on the blockchain correctly correspond to the physical properties of the product, making data compromises less likely.

- **Stakeholder capabilities and participation:** stakeholders along the supply chain need to understand the concept of value addition, product transformation and the central idea of how this information is captured and transferred among them. With data on the blockchain, every supply chain is as strong as its weakest link. The multiplicity of participants in every supply chain, with each stakeholder adding value at various stages or sometimes in parallel, means that capturing data that show things like percentage and nature of product transformation, percentage of value added and proportions discarded in the production process can get daunting. Thus, while origin data may capture critical features of the goods and include physical footprints on the goods, the extent to which blockchain technology can be useful largely depends on the length, complexity and number of entities between origin and destination of the good. The length of the supply chain coupled with significant transformation and value addition can drastically weaken data quality on the blockchain along the way. Hence participants' capacity to capture the granular details of events occurring in the production cycle, such as level and nature of value addition as well as degree of product transformation, can greatly enhance data reliability and supply chain provenance on the blockchain. Moreover, it is crucial to obtain buy-in and active participation by stakeholders. Stakeholders tend to avoid changing the entire infrastructure of business for a new one which demands risks and investments. Progressive adoption on a small scale is easier and helps demonstrate the benefits of blockchain technology.

G. Other use cases of blockchain in trade facilitation

The use cases elaborated above are by no means exhaustive. While some of these use cases are specific in nature, some are cross-cutting and include use cases such as cargo integrity, corridor management, AEO management and Rules of Origin.

1. Cargo integrity

Assessing the quality of the content in a shipping container without opening or accessing its material content can be difficult, especially in a manual inspection environment. Whether for goods in transit or at destination, the sheer work of verifying the integrity of a cargo for local standards requirements or for onward boarding can generally require Customs to open shipping containers, take samples and repackage them after inspections. This easily damages most perishable goods or exposes them to hostile environmental conditions thereby reducing their shelf life. Blockchains coupled with modern IoT devices can provide a reliable database of real time data of goods across the full shipping cycle and offer even more benefits such as capturing the various environmental conditions through which the consignment has passed while on-board shipment. The process of ascertaining the integrity of the cargo can then be easily ascertained by a more non-intrusive approach of resorting to the data on the blockchain regarding the product quality and whether it meets local standards. Also, quality issues regarding product origin, processing and transport can be ascertained on-chain should such data be captured beforehand at the country of origin. According to IBM, the amalgamation of IoT and blockchain technologies offers extraordinary applications for cargo monitoring and security and the market is expected to grow at a compound annual growth rate of 93 per cent, from $113 million in 2019 to over $3 billion by 2024 (IBM Blog, 2020). Today, most documentation in logistics businesses are still paper-based, making the implementation of IoT systems less optimal without integrity assurance from technologies like blockchain, according to IBM. For example, with the use of blockchain, smart bills of lading documents can be digitally stored and shared with a succession of different parties with an interest in the cargo covered, and all parties are able to rely on the security of the information provided. With the immutability of such data assured by the use of blockchain, manipulation by any single party once it is anchored on the blockchain cannot be possible without the tampering being noticed and queried. Hence, the transition to digitalization with the combination of IoT and blockchain could increase efficiency of supply chains, help fleet operators manage their cargo-handling operations seamlessly, especially regarding sensitive goods, and make Customs and other government administrative actors undertake inspections in a less intrusive way compared to manual inspections.

2. Corridor management

International corridor management is a major component of the global trading system. Given the increasingly interconnected global economy, goods go across many countries and sometimes multiple regions to make it to the target destination. This is not without challenges, especially when the multiple stakeholders within critical corridors do not have a commonly shared digital backbone for trade data and information-sharing. The complexity of multinational trade flows makes critical corridors particularly important for ease of trade flows and serve as critical determinants of the time and cost to trade. Facilitating critical trade corridors thus possesses the potential for eliminating major bottlenecks in the trade cycle. As corridors manage goods in transit, corridor efficiency naturally involves improving the transit process of goods across countries and regions. According to the World Bank Trade and Transport Corridor Management Toolkit (Kunaka and Carruthers, 2014), the key requirements for a well-functioning corridor system include:

- **Secure load compartment:** this is about Customs ensuring that the cargo is secure and the load compartment (closed trailers or containers) cannot be tampered with once sealed. However, verifying that no tampering has occurred in the course of the journey by Customs at transits largely depends on the trustworthiness of the cargo carriers and the Customs of origin. A blockchain-enabled environment that allows Customs to check and verify that the physical packaging in these trailers and containers has not been tampered with, in a trustless manner using a commonly shared database on that blockchain, could improve security, standards and, most importantly, compliance.
- **Guarantee:** this entails the fact that the principal of the transit operation (the owner of the goods or, more often, their agent – a freight forwarder or trucker), should act as surety by depositing a guarantee (or a bond) covering the value of taxes and duties at risk in the transit country or countries. The amount of the guarantee may depend on the fiscal risk of the operation. The guarantee may be flexible and reflect the transit operator's status (trustworthiness); in some modes (such as railways), it may even be waived, and proof of the guarantee can take various forms. Ensuring information quality in this regard is particularly important as it depends on the trustworthiness of multiple parties to ensure that guarantees are appropriately filed and the value, as well as risk, of goods intended to be covered by the surety are appropriately classified and ascertained. Running operations like this on a blockchain-enabled environment can bring the added benefit of information reliability and stakeholder compliance since the multiple parties at the origin of the goods and the transit points along the corridors will have access to the necessary data regarding the content of the cargo in real time, on a tamper-evident environment and on an immutable digital backbone.
- **Controlled access to the regime:** this regards the control of transit operators, needed from both a Customs and a transport perspective; the transit operator must be trustworthy and qualified for the service it provides. But vouching for the trustworthiness of such operators cannot always be guaranteed without the added benefits of technical automation. In an environment requiring such a high level of trust among the operators, an unalterable (immutable) database of operators and their historical performance can serve as a reliable profile for other operators to use as reference in assessing the reliability of an operator. This can significantly increase compliance and reduce risk within corridors.
- **Mutual trust:** this entails that Customs controls performed at the departure office and certified by an agreed seal should be recognized by all Customs offices enroute. It recommends that the Customs seal should remain intact until the cargo reaches the destination office, as long as there is no suspicion

or evidence of fraud. This ensures both safety of the goods and protection of the cargo integrity over the whole period. However, ensuring seal integrity in a trustless manner is not possible without close contact between the origin and transit Customs. This may involve an enormous amount of time, cost and delays and possibly affect the quality of perishable consignments. Collaborating on a blockchain environment where seal data is anchored for shared and independent verification of seal originality and authenticity without needing to contact the issuing authority and country of origin means a significant reduction in the precious time and cost of the administrative process to check and verify the quality of cargo seals. Thus delays are eliminated at transits along corridors and losses of perishable cargo are prevented. In the case of suspicion of fraud or any wrongdoing, a blockchain environment will be useful for selective audits and the targeted selection of flagged traders for further checks, while allowing the majority of compliant traders fast and speedy processes for a better trading experience.

- **Monitoring mechanisms:** this requires Customs to properly manage the information on goods in transit and reconcile information on entries into and exits out of the Customs territory (or during clearance, in the case of national transit), in order to identify violations and potential diversions or leakages. These reconciliations can be daunting, error ridden and time-consuming. Digitalization and automation with a number of proprietary software applications have become common among operators in this regard but the experience can be significantly better if there exists a shared blockchain environment where this data is exchanged in real time. This will mean automatic reconciliation while variations will be flagged as unusual for special attention. This can improve the operator's efficiency by a significant margin while cutting back on the time at the transit points, and delays. A blockchain environment will ensure reconciliation by default and the operator will only need to intervene in exceptional cases of information variation, saving all the stakeholders concerned much time spent on manual reconciliations.

Satisfying the abovementioned requirements without a trustless environment largely depends on cargo integrity, data availability, information authenticity and stakeholder trustworthiness. In a multi-stakeholder environment spanning many countries and sometimes multiple regions, corridors are known to have to handle numerous trade flows and a deluge of data. This means that delays and disruptions at transit points are still commonplace, turning transit points into some of the major bottlenecks in the global economy. Digitalization, automation and paperless trade handling have long been considered some of the best approaches to ease trade at these major corridors. Hence, corridor management is long anticipated as one of the suitable use cases of blockchains as tools for automation and digitalization.

Across all corridors, data exchange forms the core component of corridor management and stakeholder collaboration within a shared digital platform run on a blockchain backbone that guarantees data integrity by default, bringing significant efficiency gains. A blockchain-enabled environment will easily allow secure and automatic exchange of data based on consignment specificities, cargo details and stakeholder operational data, all in a privacy-preserving manner and in real time. This said, there is yet to be major large-scale use of the technology in corridor management despite its suitability in such a multi-stakeholder environment requiring many trust guarantees. This could be attributable to the fact that running a blockchain digital infrastructure for corridor management will necessarily require a multinational architecture, needing more than one country to collaborate, and an ecosystem suitable for all parties, for it to be considered acceptable and reliable for multi-stakeholder, multinational cross-border use.

Limited use cases and pilot projects in this regard include the Export Logistics Blockchain Project of the Government of the Republic of Korea, with Samsung, Hyundai Glovis, Busan Port Terminal, Shinhan Bank and more than 60 companies of the Republic of Korea, which aimed at exploring whether blockchain could enhance the accuracy and transparency of data generated by the logistic community for purposes of exports, imports and transit (Global Trade Single Window Project, 2019). Also, projects like the CADENA blockchain project have components for trade data exchange that could aid regional corridor management and stakeholder collaboration across critical corridors. For example, a major collaboration between the CADENA project and the LACChain alliance aims to see importers, exporters and other trade participants' operations run on the blockchain with information exchange becoming automatic thereby cutting red tape, increasing trust and bringing transparency that ensures goods move faster across corridors in the Latin America and Caribbean region (Corcuera-Santamaria and Moreno, 2019).

3. Authorized Economic Operators

AEOs are normally stakeholders with special profiles in a country's trading ecosystem who play an important role in many spheres of the countries' trading environment and are an important constituency in the simplification of trade procedures aimed at reducing time and cost to trade. An AEO as defined by the World Customs Organization SAFE Framework of Standards[19] is any stakeholder 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 World Customs Organization or equivalent supply chain security standards.[20]

These AEOs normally include traders, freight forwarders and shipping agencies. To qualify as an AEO, the selected stakeholder usually requires a certain amount of time and commitment to operations as well as meeting a number of operational criteria such as solvency, security and competency to be able to earn a certified status. Once certified, they earn certain benefits such as being subjected to less stringent measures in the trade process, enjoy fewer inspections, priority treatment for inspections, mutual recognition with foreign AEO programmes, reduced security and guarantee requirements, expedited release and pre-clearance, simplified procedures and priority treatment in emergency situations. This helps them cut back on time and cost to operate within the trading ecosystem. In this way the AEOs in turn help to improve the overall trading experience in a country's trading space while helping to reduce trade risks. This special status makes the certification of AEOs a coveted achievement in most countries.

The level of safety and reliability of the AEO certified status largely depends on the reliability of the certification process for the qualified stakeholder. Today many countries largely depend on proprietary digital infrastructure and some form of paper-based process to issue certification and authorization for AEOs. Thus, as certificates usually involve international exchanges, validation of these certifications is heavily dependent on contacting the issuing national body, or Customs authority, to verify certificates of the qualified AEO to other foreign Customs. This introduces many risks into the certification process and potential compromises into the international trading system, thereby elevating trade risks. It is difficult to notice a fake/unauthorized certificate issued by a rogue custom official to an unqualified stakeholder, or a counterfeit certificate forged by an operator to obtain benefits of AEO status, because there is no global database to verify the reliability of a particular certificate or validity of the status of every individual AEO.

In a blockchain environment each AEO could be assessed and their scores and performance data on these key criteria rated and entered in a reliable shared ledger to prove not only the authenticity of their certification and status but also the details that constitute the rationale behind the certification, the decision-making process of their national Customs, the justification of the performance of the AEO and the reasons why they merit AEO status. This will make the AEO certification process more reliable across borders for all operators. It will also ensure that Customs authorities in different countries are able to independently verify the validity of certification based on the shared and globally accessible database of AEOs, their historical performance and general records over time. Such a database may not only constitute the basis for issuing AEO status but could also, over time, serve as the basis for renewing or revoking AEO certificates and statuses. In a globally shared blockchain environment, all such data become available to Customs authorities in real time and easily verifiable without the need to contact issuing national counterparts. According to the World Customs Organization, in the current architecture, businesses have to wait within cycles when these certificates are issued for qualifying AEOs, and this can lead to loss of revenue for the operators (Corcuera-Santamaria, 2018). A few countries have been looking into the use of blockchains for the qualification and certification of AEOs, with many still early-stage pilot projects. Malaysia has been one of the early countries to launch a piloted blockchain for AEOs certification project, but results and the extent of success of the project is not well documented. Another case of blockchain for AEOs was within the CADENA project, which enabled Customs administrations of Costa

Rica, Mexico and Peru to share a single view of the status of an AEO certificate in real time while adhering to the highest standards of security, traceability and confidentiality within a mutual recognition arrangement. This facilitated the automated validation of AEOs using smart contracts (Corcuera-Santamaria, 2018) and granted private sector stakeholders independent access to information about their own certificates, which further increased trust and transparency and, ultimately, the active participation of the private sector.

4. Rules of Origin

Fulfilling Rules of Origin requirements remains one of the major trade hurdles for both governments and traders. Yet implementing various tariff and non-tariff measures such as reduced tariffs, preferential trade regimes, embargoes, quotas and other anti-dumping measures depends largely on the effectiveness of the implementation of Rules of Origin. As proof of nationality of the goods in question, the certificate of origin (CoO) is the main document that testifies to the source or origin of goods. According to Deloitte, some Chambers of Commerce already issue electronic CoO, however authentication, authorization and privacy often remain a challenge for CoO documentation. Thus, the firm sees key benefits of blockchain supported CoO to the four main stakeholders as importers, exporters, Chambers of Commerce and the Customs authorities (Deloitte, 2021: 11). Some envisaged benefits include:

- **Decreased cost:** major cost of manual processes can be reduced for the importers, exporters and the Chambers of Commerce, as well as the Customs authorities, with a blockchain-based automation system for CoO. In a blockchain-enabled environment, trade certificates and other related data are digitalized, automated and made available to all key stakeholders in real time for checks, validation and archiving.
- **Avoidance of delays:** the elimination of manual verification process of the CoO and replacing it with real time data availability in a blockchain environment means that major delays at ports and transit along transit corridors can be largely eliminated, because documents like CoO can even go ahead of the goods instead of accompanying them or being behind the goods.
- **Increased trust:** the availability of an independent mechanism to register and validate CoO through a blockchain environment can increase trust among key stakeholders such as the Customs authorities and the Chambers of Commerce, leading towards a more harmonious trade cycle.
- **Decreased time:** blockchains can bring a near-real-time verifiability of the authenticity of CoO, thereby increasing the speed at which goods are processed, categorized and dispatched.

Demonstrating Rules of Origin through CoO in a blockchain-enabled environment can bring the benefits of document authenticity and speed of trade processing, as well as eliminate the chances that goods get stuck at ports, and thus reduce cost to all parties. In May 2018, paperless trade platform provider essDOCS unveiled the essCert with new features offering blockchain/DLT options, enabling Chambers of Commerce to connect to blockchain platforms and IoT devices to improve Rules of Origin verification (see also Ganne, 2018). As a technical backbone, the blockchain may only serve as an authentication layer with user-facing applications plugged to it using various application programming interfaces. For example, the issuance and transfer of a CoO for specific goods on a blockchain backbone between two trading countries may take place in the following fashion: country A issues a CoO based on a request of the trader / Chamber of Commerce and the issuance is recorded on the blockchain. Then, every subsequent change of ownership of the goods within the national borders of country A goes along with a change in the holder of the accompanying CoO. Once the goods cross the border to country B accompanied by the CoO running on the blockchain, the new ownership is registered within the borders of country B and the authenticity of the CoO is verified. Various trade-related activities such as exemptions, preferential tariff regimes and special duties are rendered based on the CoO and goods that proceed to onward passage within country B are still accompanied by the CoO which originated within country A.

4 Deploying blockchains for international trade

4. Deploying blockchains for international trade

Implementing blockchains can be a daunting task. The technical considerations and policy coordination required to design, develop and deploy a blockchain demand a lot of human and financial resources. Governments are in a particularly challenging position in implementing the technology given that there are many stakeholders and that the design options available, the technical requirements for each use case and the security guarantees of every implementation approach are open to debate. Implementation challenges range from policy choices to technical models that must be considered by the implementing body. Before a government considers adopting a blockchain environment for any purpose, policy questions that must be answered to ensure proper deployment and stakeholder acceptance include, but are not limited to, the following:

1. Does the government's proposed application need a blockchain in the first place?
2. What kind of blockchain is suitable for what business/government application?
3. Should a government develop its own blockchain or deploy an application (business logic) on an existing blockchain?
   (a) Which existing blockchains (public or private) could the government use?
   (b) What makes some blockchains more suitable for a government's administrative, regulatory, legal and procedural services than others?
   (c) What design choices will ensure security, speed and resilience?
   (d) What are the trade-offs of the various design options available?
4. What policy guidelines are needed to ensure stakeholder adoption and ease of use?
5. What existing digital-trade facilitation systems could integrate the use of blockchain or be migrated to a blockchain-based system?
6. What are the cost considerations of each design option and policy choice?

After answering these questions, governments will realize the application areas where blockchains may be beneficial, plus the technical trade-offs in the implementation process and the cost considerations for adopting blockchain over other digital infrastructure options. Once a government is clear about which application areas of their trade processes could potentially benefit from the use of blockchain, the next step is to assess the technical capabilities of blockchains, that is to say, what the technology can feasibly bring to facilitate the trade processes in question. For example, while blockchains are generally acknowledged to possess the technical capabilities to transform paper contracts into smart contracts, challenges regarding privacy and conversion of legal clauses in contractual processes into computer code remain a significant hurdle. Alongside the multifaceted complexities of international trade processes, the lack of technical capacity of the average government administrator to undertake the basic cyberhygiene that protects their practices online is equally a hurdle. This is because, while compromising a blockchain record can be very difficult, corrupting the business logic or application that provide data to a blockchain or smart contract(s) that run on the blockchain is much easier and can disrupt government operations. Given the challenges ahead, decision makers and the leadership must consider the policy environment, stakeholder capacity, international practice and the technical feasibility of the technology to improve processes in the intended area of use before considering implementation. Resource requirements for adoption and deployment can be significant depending on the implementation approach.

Based on their technical merits and value proposition, some of the areas where use and application of blockchain has shown promise and can bring value addition in trade processes include: Customs clearance, supply chain provenance and value chain transparency, payment processing, trade-risk management, trade data management, implementation of Rules of Origin, and a combination of cross-cutting use cases such as corridor management, certification, and management of AEO schemes. On a broader scale, the application of blockchain in trade processes is yet to see particularly wide adoption, but the technical architecture of blockchains makes it easy to evaluate both feasibility and policy viability. It can be seen as suitable for such use cases based both on the key features of the technology and the procedural challenges governments face in these areas that could be resolved by blockchain to improve trade performance in general. The technology is particularly suitable for areas in trade facilitation where there is need for:

- multi-stakeholder coordination locally and globally for lower time and cost to trade
- de-risking fraud: data tampering, information alterations, under-invoicing and over-invoicing
- disintermediation of processes to reduce the number of administrative steps and enhance information flows in a timely manner
- counterparty verification across multiple jurisdictions without trustworthy guarantees
- trackability and traceability of processes and information for the purposes of certification and authenticity, for example in the area of sustainability requirements
- data immutability of trademarks, property rights and packaging to meet Rules of Origin requirements and Intellectual Property Rights standards

Understanding these areas of application for blockchains and their policy implications will allow governments to design proper guidance on implementation of blockchains allowing policymakers to communicate justifications to the diverse stakeholder base of the government regarding technical merits, value addition, ease of processes, improved workflows and lessening of procedural difficulties.

A. Creating an enabling environment for blockchain adoption

For the adoption of any major frontier technology that touches on the fundamental level of a government's digital infrastructure, countries have to prepare a conducive national environment for its implementation and adoption. This includes practical, policy, regulatory and technical readiness for the technology to function well within the national context, as well as interconnectedness with external digital environments. It involves, among other things, building the supporting enabling infrastructure that ensures the new technology works. For example, a blockchain will not function well in a national environment where there are incessant electricity/power disruptions or where there is no readily available stable Internet. Many developing countries, for example, are yet to realize the full benefits of the Internet because electricity and connectivity remains limited. The lack of reliable national environments is considered one of the major drivers of the digital divide. With blockchains, the level of preparedness required becomes even higher. Since blockchains are generally truth machines that serve data in real time constantly, the network must remain live and safely reachable by the consensual stakeholder base servers (nodes). Hence, as technical digital backbones, issues like electricity and Internet connectivity are considered basic requirements for blockchain networks to meet minimum functionality.

While blockchains deployed at a national level and in a sovereign context could present a unique value proposition in ensuring that critical data is protected by their redundancies and multiple backups of data across nationally authorized servers, it is important to take into consideration that the chains could suffer disruptions and halt if electricity or Internet disruption affects the majority of the network validators (block creators), thereby disrupting the ability of the validators to achieve consensus on the true state of records on the blockchain. This makes it critical for a government that is considering implementing or adopting blockchains as infrastructure backbones to assess its national systems, taking into account important factors such as national electricity distribution, Internet service reliability and the cost involved in running these services all year round to keep blockchain networks functional.

For instance, in a country where Internet connectivity and electricity are unreliable, a government may be better off adopting a public, global blockchain or a private blockchain with controlled membership and running the government service as an application on top of such a blockchain instead of deploying a government-owned blockchain. This relieves the government of the technical burden and allows the government to focus only on the application and business logic it has built on the public blockchain. However, this comes with certain trade-offs that are worth knowing before implementation, and which are important to consider when selecting a blockchain that is not government controlled. For example, the government gives up a measure of sovereignty by building on a network that it does not own (although governments often do this when implementing critical infrastructure on privately provided software systems). The government also commits to lifelong payment of network fees to process all record-keeping activities on the selected blockchain network whose amount may be unpredictable in the long term.

One interesting alternative to public, global blockchains, private blockchains and national, government-owned blockchains that is growing in importance in some regions is regional blockchain networks with multiple government, government-agency and government-endorsed participation. Examples of this are the European Blockchain Infrastructure Services (EBSI) of the European Union and LACNet in Latin America.

Thus, a government preparing for the implementation and adoption of blockchains must assess their national environment around issues of existing infrastructure such as electricity, Internet reliability, resources for deployment and maintenance of the network, and an understanding of the technological trade-offs of selecting a particular technical design option or policy choice over others. Here, these issues have been categorized into the four major themes of:

1. implementation approach
2. policy guidance for stakeholders
3. integration with existing infrastructure
4. legal and regulatory framework

1. Implementation approach

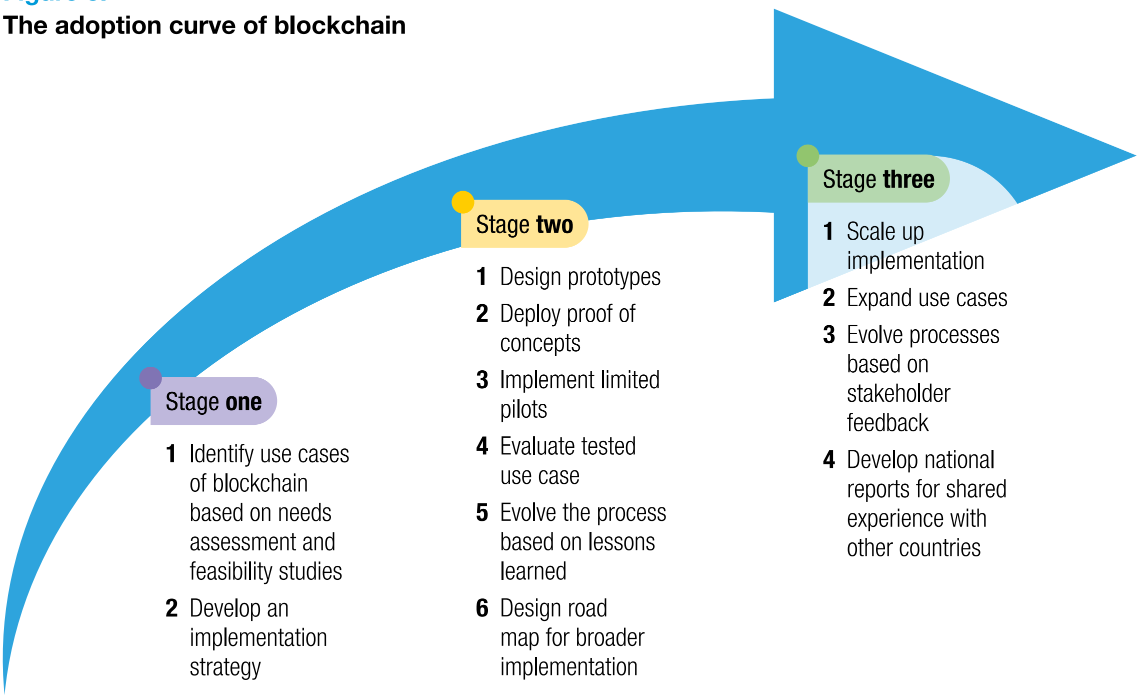
The implementation approach requires the country to consider the crucial questions of technical characteristics, implementation process and stakeholder needs. As technical tools, blockchains require governments to make technical and policy trade-offs that meet the needs of the numerous stakeholders in the government on the one hand and the private sector participants on the other. It also behoves the government to implement the technology with pre-existing national condition in mind. This requires a thoughtful approach in adopting the technology that leads to stakeholder acceptance and makes the least disruption to existing digital-trade infrastructure. Achieving this will require three major steps from needs assessment to large-scale adoption.

As a first step, decision makers will have to go through a process of self-assessment to ascertain whether the targeted use case would benefit more from a blockchain technology implementation to improve performance (use case approach) as opposed to the use of another technology. Policymakers could also simply carry out a broad national assessment of which areas of government processes will witness value addition if blockchain technology were to be used instead of the existing tools (technology-merit approach).

Based on this assessment, governments that ascertain a particular area meriting the use of blockchain can proceed to develop implementation strategies. At this stage of strategy design, key stakeholders and implementation partners could be identified, as well as the roles of these key stakeholders. Also, potential areas of collaboration between the different government agencies as well as collaboration between the government and the private sector should be identified at this stage. India is one of the countries that has reached this stage with their national blockchain strategy (Ministry of Electronics and Information Technology, 2021).

Before implementing blockchain technology, it is useful to select one or more potential application areas for testing its application using proofs of concept, prototypes and pilot programmes. This allows the stakeholders to confirm in practice the use case of the technology at minimal cost and with little or no disruption to major operational processes. It also allows key stakeholders to learn and revise their views on possible use cases and related business process changes as well as consider implications for broader adoption before major implementation. At this stage, once value addition and efficiency gains have been confirmed and adoption of the technology is net positive, the process of designing a road map for broader implementation can be undertaken and shared with key stakeholders for review and inputs. The next stage (stage three) will then entail broader implementation arrangements, scaling and multiple implementations. The process will keep evolving after the last stage with continuous monitoring and evaluation as well as the sharing of lessons learned with other peers in different sectors and agencies, and other countries, in the form of quarterly and annual reports, to allow interested parties and stakeholders to give feedback for further iteration of the process and continuous improvement. Figure 3 demonstrates the adoption curve of implementing a blockchain environment in a national context.

Figure 3.
The adoption curve of blockchain



Source: UNCTAD.

2. Policy guidance for stakeholders

While blockchains could speed up processes at both local and global levels, stakeholder preparedness, readiness and awareness play a crucial role in the success and sustainability of the technology in a national context. Implementation will require a holistic approach of training, preparing and supporting the broader stakeholder ecosystem to understand and fully engage in the development, design and deployment of the technology. As multi-stakeholder systems by design, blockchains not only need stakeholder acceptance, but also stakeholders' active participation to attain proper function and to achieve the intended purpose. Thus, policy guidance from decision makers becomes critical after implementation design is completed and well understood by all key stakeholders.

This includes issues regarding technical approach, policy considerations, design choices and policy trade-offs considered for the use of blockchains to allow stakeholders to grasp the scope of change and the technical transformations and policy dynamics being introduced into existing systems. It will prepare stakeholders for the changes that may be required in terms of capacity upgrades, stakeholder training and possible role shifts. Policy guidance also gives the government the opportunity to gain stakeholder awareness and acceptance towards implementing a successful blockchain ecosystem in the country. Practical implementation of such policy guidance may include policy documents such as policy briefs, technical guides, training seminars and flyers. Undertaking policy dialogues and forums with a multi-stakeholder participation and multi-agency dialogues will be instrumental in ensuring broad policy support.

3. Integration with existing infrastructure

As with other new technologies, implementing blockchains requires a rethink of existing trade infrastructure, bearing in mind the extent to which existing digital-trade infrastructure may need to be revised, replaced or used in different ways. With their unique value propositions, blockchains bring different technological stacks to the digital space. Given that most government digital-trade infrastructure is based on applications that run on proprietary technical servers and digital backbones like the cloud and sometimes on-premises servers, implementation of blockchains will require, at the bare minimum, a redesign of these technical foundations while avoiding extreme interruptions to the business logic and the existing user-facing interfaces. This design approach will help to minimize the disruption to existing user experience, trade processes and administrative procedures. While the technology promises value addition in different areas, the extent to which its application will be successful largely depends on how seamlessly the blockchain stack is integrated into the existing digital infrastructure as well as allowing room for upcoming technologies that may be adopted in the future. Meanwhile, the level of transformation required will depend on the function that the application is designed for and the implementation process of the technology.

4. Legal and regulatory framework

Legal and regulatory adjustment and clarity constitute major components of creating an enabling and facilitating policy environment for blockchain adoption and implementation. Achieving a reliable blockchain-enabled trade environment will depend on the extent to which the regulatory and legal environment has been established and adapted to facilitate the adoption of the technology and ensure that it can work within existing national legal and regulatory systems.[21] Blockchains by design come with new legal and regulatory features that may not fit in existing national regulatory frameworks, typically designed for paper-based rather than digital transactions. This puts issues like compliance with standard procedures and legal requirements into question. For example, the use of blockchains necessarily mandates the use of digital signatures by key stakeholders, hence a country that does not have any existing regulations on digital signatures within its jurisdiction will run into the challenge of fitting blockchain-based digital signatures into its implementation process if this is not addressed ahead of implementation of the technology. A successful implementation of blockchain-based trade processes thus critically depends on sound legal and regulatory provisions within legal frameworks that are aligned in each jurisdiction and with the technical guarantees of the technology.

Hence a country that intends to prepare for a blockchain-enabled trade environment, according to the UNECE White Paper on the Technical Application of Blockchain to UN/CEFACT deliverables (UN/CEFACT, 2019a; see also UN/CEFACT, 2019b) should have legal provisions such as the following:

- recognition of records on blockchain in courts of law
- cross-border (cross-jurisdiction) boundary, and dispute resolution
- data capture, storage, ownership, sharing and security provisions regarding blockchains
- minimum standards for certification or compliance with regard to digital processes
- registrations of blockchains

New digital contracts such as smart contracts form an integral part of modern blockchains, suggesting that countries aiming to adopt the technology will have to create new legal instruments that cover adoption, acknowledgement and procedural handling of these new contractual designs within the national legal systems and in their procedural jurisprudence. It further implies that some laws may need rewriting, some may need to be reviewed and others may need to be completely abolished. On designing the legal and regulatory environment, the European Union Blockchain Observatory and Forum, a community run under the aegis of the European Commission's Directorate General for Communications Networks, Content and Technology, has recommended eight key considerations, elaborated in Table 5.

Table 5.
Guiding principles for establishing legal and regulatory environment for blockchains

Principle	Description
Craft simple yet usable definitions of the technology	Policymakers must clearly define what blockchains and smart contracts are under the law of the jurisdiction in conformity with international standards
Communicate legal interpretations as broadly as possible	Authorities must make an extra effort to communicate to the wider community when blockchain is added into a law, or when a binding or highly certain interpretation of the law with regard to blockchain is reached
Choose the right regulatory approaches for the question at hand	When it comes to regulating new technologies like blockchain, regulators can choose from three basic approaches, each of which has its own advantages and disadvantages: (1) apply existing law as is to the new technology, (2) amend the law to consider the new case or (3) craft new laws or ad hoc rules for each special case on a case-by-case basis
Harmonize the law and interpretations of it	Whatever the approach individual regulators take, blockchain and smart contract regulation should be coherent and harmonized with international practice
Policymakers should develop an understanding of the technology	Getting it right will require the respective authorities and the full ecosystem to understand the new technology and what can (and cannot) be achieved with it
Work on high-impact use cases first	This encompasses the regulatory questions around digital assets as well as bringing clarity to blockchain and existing laws
Closely monitor developments in less mature use cases and encourage self-regulation	Intervening too early in novel use cases of any new technology can be counterproductive
Make use of blockchain as a regulatory tool	Regulators must get involved themselves to be able to monitor and regulate the sector. For example, regulators could plug themselves into new blockchain-based platforms as they come online, unleashing new opportunities to improve the efficacy but also efficiency of their operations

Source: European Union Blockchain Observatory and Forum (2019).

B. Barriers and drivers of blockchain adoption

In existence a little over 10 years, blockchains are still emerging technology in search of mass adoption. Across industry, governments and civil society, blockchain adoption remains low and in limited areas. This is because barriers abound in the large-scale adoption and deployment of the technology, whether in government or in industry. Some barriers include the skills gap, financial resource commitments, technical interoperability limitations, inadequate speed of adoption to achieve network effects, and the lack of trust of, especially, public blockchains. While these challenges remain, new developments are seeing emerging drivers to overcome the barriers to adoption. For example, the lack of trust for public blockchains, despite their high-level security, is seeing the increasing deployment of private permissioned blockchain environments that strike a balance between security and sovereignty to allow for meaningful feasibility in the use of the technology in government trade processes. Also, the interoperability limitations of first- and second-generation blockchains have seen innovations of general-purpose communication protocols. Some of the barriers to blockchain adoption and how industry is working around them to overcome the challenges and achieve mass adoption are:

- **Cost of deployment:** until now the cost of designing, developing and deploying a blockchain on proprietary digital infrastructure remained prohibitive. This forced many industry users to resort to using public blockchains. But that also quickly brought to the fore issues like the high transaction fees for processing operations on the public blockchains, privacy concerns and data protection, as well as user sovereignty especially for governments. With current new developments and major innovations around consensus algorithms, however, the cost of deploying blockchains, whether within permissioned environments or even as public networks, has significantly reduced. This has led to an increased number of consortium chains, private chains and permissioned networks for various purposes at very low cost.
- **Lack of interoperability:** while first- and second-generation blockchains lacked native interoperability, which required an entity to build bridges that will allow any form of interoperability with other chains, third-generation blockchains came with a solution. The current generation of blockchain design modules allow entities to not just spin off chains when needed at nearly no cost, but also allow these chains to have native chain interoperability with other chains from the start, utilizing interchain communication protocols like IBC.[22] This has lowered the barriers to entry and could increase mass adoption of blockchains as they get to interconnect and interact with one another at a native level from the start of their design.
- **Skills gaps:** blockchains, as new technologies, come with one significant demand on all organizations looking to use the technology: skilled people to manage them. The skills required to implement blockchains or even to simply operate one, are not readily available and are in high demand. This adds to the cost component of blockchain adoption. Even organizations willing to pay high remunerations are still running short of skilled staff. In recent times, this challenge has led to the rise in "Blockchain as a Service" platforms offering various kinds of services to allow organizations to deploy blockchain-based services on these platforms at minimal cost and requiring less technical skill. Governments have already developed such services including the Blockchain Service Network platform of China[23] and the EBSI platform.[24] These services are meant to abstract away the major work required in implementing blockchains and increase the speed of development and deployment for organizations looking to use the technology while lacking the technically skilled personnel to help them do that.
- **Lack of trust in public blockchain environments:** despite being generally more secured, globally accessible and usable by anyone without permission, public blockchains raise concerns about privacy, data protection and stakeholder sovereignty. Thus, industry and organizations looking to use blockchain usually end up choosing to develop and deploy proprietary, permissioned blockchain environments instead of relying on public blockchains. Use of permissioned blockchains, however, introduces new barriers to adoption and are generally resource-intensive to operate. The arrival of Blockchain as a

Service and new technical architectures have made it easier today to create proprietary blockchains for unique business cases and government services without much resource requirement and with less difficulty.

- **Limited standards:** the inadequacy of international standards on the use of blockchains remains a major hurdle for mass adoption and large institutional use. Although there exist numerous chain-specific technical standards such as the Ethereum ERC20 or the Cosmos CW20 standards, these standards are mostly chain-specific and are mainly focused on asset specifications and not necessarily data standardization. The first general-purpose technical standard that is focused on data standardization and not chain-specific is the IBC protocol, implementable across any chain with light client support and allowing for the transfer (relay) of any kind of data packets among these chains in a standardized manner. Also, the ISO307 standard working group on blockchain is focused on bringing in major standards on blockchain tokenization, interoperability, security and privacy, as well as smart contract specifications to aid governments and any institutions that need clarity on standards to adopt blockchain.
- **Full legal recognition of blockchain and other electronic records as equivalent to paper-based documentation:** blockchain transactions need to work within legal and regulatory frameworks often designed with traditional paper-based documentation in mind. Electronic bills of lading, for instance, are not fully recognized as equivalent to paper documents in most legal systems, primarily because of the document of title function of the bill of lading, which provides the holder with constructive possession and with the exclusive right to demand delivery of the goods from the carrier. Replicating the paper-based bill of lading in an electronic environment has been possible for some time, but the legal framework is still lagging behind (UN/CEFACT, 2019a, 2019b).

5 Way forward and policy considerations

5. Way forward and policy considerations

Blockchains have seen key transformation since their conception in 2008. But major limitations remain if the technology is to attain mass adoption and usage beyond finance. The limitations notwithstanding, many governments, policymakers and international organizations have been engaged, at various levels, in exploring the potential of the technology. Varying results have been achieved with numerous proofs of concept, pilot projects and early-stage deployments. Large-scale deployment, implementations and adoption, however, remain few. Going forward, policymakers, governments and international organizations looking to grow understanding of the technology, implement and use it as a technical tool or adopt it for use in national and international contexts, are advised to consider the following aspects to see success in the adoption cycle:

- Blockchains are no longer just immutable data stacks. The technology has experienced major evolution over the years and it is now rather more than ledgers of records. Blockchains have incorporated computing capacities that make them capable of creating, giving, receiving and executing computational instructions based on data received by the blockchain (such as user input, IoT data, etc.). This has significantly expanded their functionality and potential use cases. In the past few years, there has been growing use of blockchain in non-financial sectors such as in supply chain trackability, value chain transparency, trade finance and cargo tracking.
- Implementing, deploying and using blockchains in certain cases may require different scale or scope of transformation of existing digital infrastructure. While using blockchains for certain purposes or in certain environments may require the full and complete overhaul of the existing digital infrastructure of the user, in certain environments and for certain use cases there can be a seamless integration of the technology into existing and future digital infrastructure without major disruption to the user's existing digital tools. Blockchains by nature are technical backbones that serve specific purposes and users have to interact with the technology through business logics built in the form of web portals and applications. Hence users do not necessarily have to see or even know that a business logic is using a blockchain on the backend, for purposes like infrastructure resilience, stability, reliability and safety.
- Some of the areas witnessing major blockchain revolution are: interchain communication, which allows chains to communicate to each other without trusted middle parties or trusted middleware; chain programmability, which allows more sophisticated business logic to be built on blockchains; ICA, which allow for cross-chain composability and multichain business logics; environmentally friendly consensus engines mainly driven by proof of stake networks, which are lowering the barriers to entry in the adoption and usage of blockchains and, at the same time, consuming less energy and keeping the environmental footprints of blockchains low.
- Use of blockchain in areas other than finance remains limited and at an early stage. Many obstacles to adoption remain and these hurdles must be made a priority if adoption beyond finance is to expand. The major hurdles include: skills gaps, cost of deploying and maintaining blockchains, lack of trust for public permissionless blockchain environments, and limited regulatory and legal clarity. Eliminating these obstacles alongside improvement in areas of international collaboration for peer-learning and knowledge-sharing, and improvement in regulatory and policy standards to complement the myriad industry-level technical standards can propel adoption and lead to large-scale harnessing of the technology for good.

A. For policymakers

On the policy front, a number of measures could improve stakeholder capacity and preparedness for blockchain technology, including:

- Improving understanding of the technical nature of blockchain through stakeholder capacity-building programmes. This will help key stakeholders in different economies assess the areas of their trade needs that may require implementation and use of blockchain.
- Coordinating policy among countries towards building common standards for the implementation, deployment and adoption of blockchains. This could lay the global foundations for greater adoption and increased application of blockchain in facilitating international trade.
- Creating the environments needed for blockchain adoption would necessarily require the commitment of human and financial resources directed to the capacity-building of policymakers, civil servants and private sector actors, to ensure that the skills gaps are closed before any large-scale implementations of the technology are considered. Initiatives such as hackathons, competitions and workshops could promote knowledge exchange.
- Developing national regulatory frameworks, aided by a set of global regulatory and legal standards, for a truly reliable adoption and implementation of blockchain technology in facilitating trade. Blockchains by design are collaborative technologies, requiring different actors with a shared goal, that lack the mechanisms needed to achieve the trust guarantees that will help realize these shared goals. Hence blockchains serve as the trust layer to aid the achievement of shared goals of counterparties in need of a trustable mechanism that removes the necessity of relying on the trustworthiness of the counterparties.
- Setting legal recognition in place for significant technical aspects of blockchains, like digital signatures, to be valuable and usable in a national context. The adoption of blockchain in many national contexts will require the review of existing legal frameworks, enactment of new legal schemes, and the possible abolishment of certain laws, to ensure the technical capabilities of the technology are in conformity with legal regimes.

B. For international organizations

The role of international organizations will only grow in significance in the blockchain industry. The risk of widening the digital divide is increasingly apparent in the blockchain era. Despite a collaborative technology by default and multi-stakeholder by design, there is growing concern about the level of concentration of advancement of blockchain technology. While most governments still lack policy and regulatory clarity on the technology, the private sector is advancing the technology with most patents and intellectual property registrations concentrated in only a few countries.[25]

International organizations are advised to consider the following suggestions:

- Closing the digital divide will require international organizations to, among other things, provide capacity-building support to all countries on both the policy and technical levels to enhance a balanced and inclusive blockchain industry and ensure that the technology becomes a leading enabler in the achievement of the Sustainable Development Goals.
- While there exist hundreds of technical standards for blockchain-specific environments, especially around areas of tokenization, value representation, asset-referenced specifications, interchain connectivity and chain-to-chain communication, these multiple chain-specific technical standards have only led to a more disharmonized blockchain environment with little regard for semantic/data and policy standards. Hence establishing a more harmonious global framework on semantic/data and policy standards could enable global adoption. This will both aid stakeholder communication and a common understanding around the technology among decision makers and industry at large.

- The challenge of forging international consensus around the technology falls to international organizations. There is an increasing need for a global platform and a shared stage for consensus-building among policymakers, civil society and industry on the use of new technologies such as blockchain and what can be done to ensure more balanced, inclusive and fair outcomes for the global economy. International organizations could build the discourse around blockchain and new technologies in support of this goal. This will foster peer-learning and knowledge exchange among countries, international bodies and industry, and provide an avenue that helps close the digital divide.
- International organizations could provide guidelines for countries that want to adopt and implement blockchain technology. This could aid the efforts of most countries that are looking to build the necessary national environments and help policymakers to understand the technical and regulatory requirements, especially in dealing with industry vendors who provide technical services on the technology to governments. In government–vendor relations, governments that are supported with appropriate guidelines will be in a better position to ask the crucial technical questions and to better communicate their needs to vendors and seek better outcomes for a more successful implementation of blockchain environments and platforms.
- Achieving legal and regulatory clarity in jurisdictions where the technology is being adopted has remained a challenge because of the fast-evolving nature of the technology. Hence, building a forward-looking, future-oriented legal and regulatory framework for the adoption of blockchain has been one of the major challenges. International organizations could help design broad legal blueprints and general regulatory templates based on the shared experience of stakeholders within the global blockchain space to support countries looking to implement the technology.

Annex
Types and features of blockchains

Annex: types and features of blockchains

The arrival of blockchains was an important convergence of different technological designs in cryptography, computer science, economics, finance, network design and governance. At the most fundamental level, blockchains are generally categorized based on features such as accessibility and the record creation mechanism, as well as privacy and data protection.

A. Accessibility

Blockchains are categorized as either open networks accessible without authorization or as gated networks only accessible with authorization from existing participants, generally described as permissionless or permissioned networks respectively. As the names imply, permissionless networks are public networks with open access to any participants and stakeholders with the freedom of entry and exit without need for approval. A prime example is the Bitcoin network. On the other hand, permissioned networks are mostly private blockchains that require authorization from key stakeholders to participate in. Public permissionless networks like the Bitcoin network are non-proprietary but private permissioned networks are mostly proprietary, owned or spearheaded by an entity or group of entities using the network for a particular government/business purpose. The majority of known blockchain networks today are public permissionless networks with global accessibility for all. These include major networks like Bitcoin, Ethereum, Solana, Cosmos, Algorand and Avalanche. At the same time private permissioned blockchains are on the rise, especially with the arrival of government-backed central bank digital currencies (CBDCs). Many governments are piloting CBDC projects on private permissioned blockchains and it remains unclear whether these CBDCs will someday go on public permissionless blockchains or they will forever remain in controlled environments anchored on permissioned blockchains.

There are pros and cons of running each type of network. This largely depends on the intended use case and objectives of the implementing entity. For example, while permissionless blockchain networks are generally costly, resource-intensive, limited in block capacity and slow, they offer maximum security and safety for value preservation and reliability. Permissioned blockchains on the other hand are generally known for faster speed and larger block capacity, and for being less costly and less resource-intensive, but they are generally less secure, less safe and may not fully guarantee record integrity and business continuity in the event of adversarial attack. Permissionless blockchains are characterized by certain key principles around the concepts of:

- **Software development:** permissionless networks are normally heavily community-driven with open-source development and not-for-profit funding for major development works. Funding normally comes from donations and not-for-profit foundations.
- **Lack of authority:** permissionless networks usually have no top-down hierarchy and no central authority to control the development work or give the direction of work. Work being community-driven, developers usually come from different parts of the world and are naturally driven by a community consensus of what is considered necessary and critical at every time.
- **Transparency:** permissionless networks operate on full transparency and open accessibility of transactions and records on the blockchain except for privacy-oriented public chains. Transparency is usually baked into the core of most non-privacy-preserving permissionless blockchains which means they are not very suitable for certain sensitive data.
- **Anonymity and pseudonymity:** stakeholders/participants are not necessarily known or identified unless they want to be. This aspect of permissionless blockchain networks is what allows them to be generally transparent without loss of identity. They operate with transparency of records but with full anonymity/pseudonymity of stakeholders.

- **Tokenization:** the commonest way to incentivize stakeholders to commit resources to the security of the network is through tokenization in a permissionless network, hence these networks depend on network-based tokens to incentivize stakeholder participation for network security.

Permissioned blockchains, on the other hand, operate with principles almost the opposite of permissionless networks. Regarding network development, transparency, tokenization, anonymity of participants and authority, they achieve their end goals differently:

- **Trust with low transparency:** in permissioned blockchain environments, network participants know and trust one another, hence the public do not always have access to all the operational goings-on on the network, thus they generally have low transparency.
- **Closed-source software development:** most software development is done and funded by private entities. Hence development is generally proprietary and closed-source. Although it is common for permissioned blockchain network entities to adopt open-source software from the open-source software communities, their operations still usually remain closed-source.
- **No anonymity or pseudonymity:** Participants know and are known by one another; hence the network does not necessarily operate as an environment of adversarial collaboration. It is, rather, an environment of checks and balances instead of being an environment of total trustlessness.
- **Optional tokenization:** permissioned blockchains have one important trait that differentiates them from permissionless blockchains. That is, they do not necessarily need or require a token or native network-based digital asset to incentivize participants, since other business gains could be achieved by stakeholders and this can well serve as incentives for stakeholder participation, support and protection of the network. Hence permissioned networks' security does not necessarily need to be directly linked to the network's tokenomics.[26]
- **Presence of authority or hierarchy:** though not always needed, permissioned networks generally have key participants who serve as the centre of authority of the network, with more influence on network safety and liveness. These authorities or high-ranking stakeholders usually have more power than other participants and they can coordinate to halt a network in cases of attack, emergency upgrades, unauthorized intrusion or high security/sensitive upgrades.

Both permissioned and permissionless blockchain environments come with pros and cons and this determines their fit for certain use cases over others. Although they could have similar or even the same underlying technical designs, their use cases differ significantly because of the nature of collaboration among network participants, the incentive mechanisms and the security guarantees of each environment. Table 6 demonstrates the various pros and cons of deploying a permissionless or permissioned blockchain environment for any business or government use case.

Table 6.
Pros and cons of permissioned and permissionless blockchains

Permissionless blockchains		Permissioned blockchains	
Pros	Cons	**Pros**	Cons
Global accessibility and redundancies mean high security, reliability and protection against attacks	Global redundancies and multiple servers (sometimes in the millions) mean suboptimal use of resources like energy and computation power in pursuit of security	**Fewer network participants mean less redundancy. Hence resources like energy and computational power are used less**	Network security is less assured, and 51 per cent of attacks can easily be executed on the network, especially if any of the network participants choose to act dishonestly
Open access of networks means a more democratic system for a global audience	Community decisions, network upgrades and transaction processing are generally slower than counterpart permissioned blockchains	**Network participants can coordinate faster and quickly take decisions regarding critical issues of network health, upgrades and general processes**	Risks and cost of collusion/corruption is elevated because the network relies on the honesty and trustworthiness of network participants
The transparency of permissionless networks means less need for trust, checks and balances which can require less resources (especially human resources)	Requires other resources like energy and computational power with limitations to scalability and performance	**Permissioned blockchains generally have fewer limitations on performance and scalability because of fewer redundancies, which allows for faster block creation and consensus**	Participants with more authority can override consensus, change network rules and compromise immutability, reliability and security
Global accessibility, high transparency and lack of authority mean a great measure of censorship resistance	High transparency and open access mean once a user is identified, their privacy is compromised as their every move can be tracked	**Guarantees a high level of privacy because permission is required to access information on the permissioned environment**	Less transparency and tight-knit operators means permissioned networks are not scalable for a global audience

Source: UNCTAD.

Both permissionless and permissioned blockchain environments propose similar or sometimes even the same business use cases with similar underlying technical designs. But the differences in the way participants collaborate makes them suitable for different use cases. For example, while all permissionless blockchain environments almost always necessarily require a financial component in the form of network tokens to ensure network participants are incentivized with transaction fees and other financial incentives, permissioned environments, on the other hand, enable similar value propositions but mostly without need of any network-specific tokens as a financial component to incentivize participants. Permissioned networks can usually grant other business value propositions to incentivize the network participants that are willing to establish and operate the network infrastructure. Over the years, there have been widening differences in use cases of permissionless blockchains vis-à-vis permissioned blockchains. As the technology matures and achieves common use, the appropriateness and suitability of one network over another for certain use cases is becoming clearer. Some common areas with growing use of permissionless vis-à-vis permissioned blockchains are shown in Table 7.

Table 7.
Common use cases of permissionless vis-à-vis permissioned blockchains

Permissionless blockchains	Permissioned blockchains
Decentralized finance	Identity management
Decentralized gaming	Credentials management
Crowdfunding	Trade finance
Decentralized file storage	Supply chain management
Decentralized identities	Value chain provenance and tracking
Decentralized organizations	Notaries
Public cryptocurrencies	Central bank digital currencies

Source: UNCTAD.

B. Consensus algorithm

The consensus engine of every blockchain serves as the major means of agreeing on the true state of records on the blockchain by all stakeholders. It also defines the mechanism of participants' credibility and the roles of participants. It defines those with the authority to add new records to the network. Thus it is acknowledged as one of the most significant technical innovations that made blockchains possible by creating new ways of human coordination and stakeholder cooperation even in adversarial environments where participants cannot necessarily rely on the trustworthiness or honesty of one another. It constitutes the means of creation and addition of records on the blockchain and holds the mechanism for quality assurance and validity of the records on the network. Given its significance, the consensus engine design is not without controversy as to what constitutes sound engineering and solid security design. While there exists no consensus among experts as to what the best consensus engine entails, some believe it should be a computationally intensive process for reasons of security and others believe that this computational intensity is an unnecessary waste of energy, leaving too great a carbon footprint and negatively impacting the environment. This broadly categorizes blockchains as either proof of work (PoW) or proof of stake (PoS). Networks that run on PoW consensus engines are those that generally require commitment of computational power and are energy intensive, while networks that run on PoS consensus engines mainly require commitment of direct capital/resource without much use of energy and computational power. This broad categorization admittedly leaves a large array of versions of the two major consensus designs, because many blockchains today run on consensus engines with significant modification of the consensus features of these two broad categories. Thus, there exists a significant spectrum of versions of PoS in particular, as a major means of reaching consensus/agreement on the validity of records on the blockchain network. Because most public permissionless blockchains require every participant to commit some form of resource (computational energy/direct capital) to participate in the decision-making process of that network, proponents of PoS networks believe that network security should be achievable through software design, allowing stakeholders to commit direct capital instead of computational energy, while proponents of PoW believe that network security is only achievable through hardware computational intensity, usually referred to as the hash rate of the network.

Since arrival of Bitcoin, many design options have been demonstrably significant in cutting back on computational intensity and energy use by rather taking the PoS design approach that guarantees security without wasting energy. Thus, PoS today has gained major traction, with many major networks running on various versions of it. Notably, the Ethereum network, which is the second largest network, shifted its consensus engine from one of energy-intensive PoW to a more environmentally friendly PoS in September 2022. This has led to a significant reduction of energy consumption by the Ethereum blockchain network, cutting its electricity use by over 99 per cent.

Regarding security guarantees, while PoW networks guarantee their security through the network hash rate attained by the computational energy committed to the network, most PoS networks, on the other hand, operate using Byzantine Fault Tolerant[27] mechanisms to protect and secure the network, with all actors staking various amounts of network tokens and operating in tandem for the interest of the network; any actor who acts dishonestly loses their stake in the network as a punishment. Most emerging networks like Tendermint Cosmos, Solana, Algorand and Avalanche, which run on PoS network consensus engines, today use a tiny fraction of the energy consumed by major PoW networks like the Bitcoin network and still guarantee significant levels of security. Given its growing popularity, there is growing innovation in the PoS consensus space with new design options emerging often, as well as an increasing iteration of the existing PoS algorithms with varying security guarantees. Some common versions of PoS in use today include proof of authority (e.g. Binance Smart Chain), pure PoS (such as Algorand) and delegated PoS (Cosmos Tendermint-based chains). These versions of PoS designs all seek to reach consensus on the blockchain while cutting back on computational intensity, to lower the barriers to participation in the blockchain space, and to reduce energy consumption while ensuring network security.

As a PoW network grows and the resources it must secure expand in value, so does its security requirement and its energy consumption. Thus, today PoW consensus engines like the Bitcoin network have become a complex system powered by industrial-scale power plants, while PoS engines are generally accessible and operational with home-based computers irrespective of how large the network grows. But each consensus mechanism comes at a cost of certain trade-offs and with certain strengths and weaknesses, distinct security guarantees, accessibility requirements, speed and performance. Some of these are elaborated in Table 8.

Table 8.
Considerations and trade-offs of proof of work versus proof of stake consensus engines

Consideration	Proof of work	Proof of stake
Weakness	Significant energy consumption	An actor with a controlling stake of tokens can take control of network
Strength	Indirect link between network tokens with higher security	Low energy requirements and more optimized consensus design allows for speed, performance and scalability
Participants who create data/records	Miners	Validators
Resource commitments from participants	Infrastructure and energy	Network-based coins or tokens
Cost of participation	Equipment cost and energy to operate the equipment	Cost to acquire and stake network tokens
Barriers to entry	High for new participants	Modest to low for new participants

Source: UNCTAD.

These various trade-offs give the different consensus engines unique pros and cons making them suitable for different business use cases. The pros and cons of PoW and PoS consensus engines are elaborated in Table 9.

Table 9.
Pros and cons of proof of work versus proof of stake blockchains

Permissionless blockchains		Permissioned blockchains	
Pros	Cons	Pros	Cons
Equipment and energy requirements abstract security from tokenomics making the networks less vulnerable to economic capture	Networks' dependence on physical equipment makes operations vulnerable to seizure, which can create censorship	**Without vast equipment and infrastructure, it is hard to locate or find a proof of stake validator, hence operators are less susceptible to seizures and censorship**	Network tokenomics are directly linked to network security making the networks vulnerable to economic capture
Networks' dependence on energy ensures that energy that would otherwise go to waste can be channelled to good use as network operators seek the cheapest energy for best returns	High energy intensity and consumption is not environmentally friendly	**Uses less energy and still achieves higher speed, scalability and performance**	Heavy dependency on token-based network security encourages token hoarding, which over time causes centralization that could lead to elite capture and network cabals

Source: UNCTAD.

C. Privacy and data protection

The third significant way blockchains differ is whether the data and records on those blockchains can be read by anyone or they are protected with privacy-preserving encryption. Thus, a blockchain could be a public permissionless or private permissioned PoW or PoS network but the records on such blockchains can be exceedingly private, opaque and highly protected without any means for the public to see, read or access these records, or the records on the blockchain could be made openly accessible, readable and analysable by any member of the public. That is, while a blockchain could be a public permissionless network, records on such a blockchain network could be made private. In this case the data is generally considered to be obfuscated.[28] These types of blockchains hold privacy-preserving records, with data protection of users at the centre of their architecture. Permissioned blockchains are generally privacy-preserving as their data and records are not necessarily accessible to or viewable by the public. However, a private network is not necessarily privacy-preserving. While the idea of a private network has to do with whether it is a permissioned/proprietary network as compared to a publicly permissionless network, the concept of privacy-preserving networks concerns whether the records on the network are easily accessible and readable by everyone or whether they are obfuscated. Hence private/permissioned/proprietary networks deal with the ownership of the network while privacy-preserving networks deal with the data protection of records on the particular network. Thus, there are privacy-preserving (simply private) public permissionless networks, though the majority of public blockchains today are non-private, with the records on-chain completely accessible. Public blockchains that are purely focused on privacy, with transactions inaccessible, untraceable, strongly obfuscated and highly protected, include the Monero, Zcash and Secret networks. On these privacy-preserving blockchains, participants' data is not available to the public, transaction records are not accessible, and the transacting parties cannot be known.

While celebrated by anonymity-loving blockchain industry leaders, these networks present new regulatory challenges to policymakers. Undertaking audits, law enforcement or compliance efforts is nearly impossible on these privacy-focused chains. Hence, blockchains with these technical capabilities present both a policy challenge and a technical dilemma for regulators and policymakers. An example of such a policy dilemma came in August 2022, when the Office of Foreign Assets Control of the Government of the United States of America blacklisted Tornado Cash – a privacy-preserving application that runs on the Ethereum blockchain – and had the developer arrested, indicating that billions of dollars had been laundered through the application. These policy challenges notwithstanding, privacy-preserving blockchains and blockchain applications can be a great fit for user data protection, especially as user data integrity and privacy concerns are on the rise. Thus, as regulations catch up with innovation in the blockchain industry, privacy-preserving public permissionless blockchains present a new uphill struggle for regulators and policymakers. Because they operate within environments of trust and compliance with institutional oversight, this challenge does not exist when it comes to permissioned blockchains. The concerns about privacy-focused chains and cryptocurrencies being used for illegal activities such as ransomware attacks have already dominated many spheres and policy debates, while they are also acknowledged as useful in environments of political persecution of dissidents, journalists and other legitimate users seeking data protection and privacy in their use of public ledgers.

D. Areas witnessing major evolution in blockchain technology

New chains and unique applications keep emerging alongside increasing research work. Talent inflow is on the rise and capital expenditure on experimentation remains high as well. Industry funding remains elevated, with billions in investment flowing into innovative frontiers aimed at improving user experience, building commercial viability and promoting mass adoption. This has created the need for governments to step up efforts on policy, regulation and compliance to catch up with advancements in the industry. The speedy progress raises the need for international organizations and civil society to endeavour to build capacity, especially in developing countries with a view to closing the digital divide. For example, while the Internet has brought great gains to many across the world, it has revealed major gaps in the digital economy and blockchains could exacerbate the digital divide if conscious efforts are not taken by governments to close the digital gaps (Shirazi and Hajli, 2021).

Since the emergence of first-generation blockchains like Bitcoin, the technology of blockchain has evidently evolved and expanded beyond simply providing financial ledgers, showing signs of potential to upend the digital economy. Blockchain has long moved from being just data immutability (as is the case of first-generation blockchains like Bitcoin) and simple chain-specific programmability (as in the case of the second-generation blockchains like Ethereum) to new frontiers that focus on solving the real-world problems of individuals and society. Also, major progress has been made on solving difficult problems around multichain interoperability, native chain interconnectedness, strong scalability, improved speed, strengthened security, interchain communication, cross-chain composability, modularity, low barriers to implementation, environmental friendliness in consensus engines and improved programmability, among many other things. While the technology is advancing on many fronts, current frontiers experiencing the leading evolution in the industry can be categorized into five pillars comprising: interchain communication, consensus design, programmability, ICA and modularity.

1. Interchain communication

If chains are cities, then interchain communication is the intercity transport system. Until recently, blockchains communicated with other blockchains through some form of third-party service, infrastructure or middleware that served as passage for data packets between the communicating blockchains. These middleware services are usually trusted bridges running on multi-signatures[29] infrastructure (shortened as multi-sigs) operated and signed by a few people and require users to give up a significant measure of security and sovereignty to be able to pass information or assets between chains. This led to multiple cyberhacks of these middleware bridges, costing users billions of dollars. This is because bridges, as managed by small groups of people, inherit multiple chain security assumptions as well as create new security assumptions, making them less secure than the native chains they connect. For example, in March 2022 over $600 million was syphoned from a single bridge (Bloomberg, 2022) and in the first half of 2022 alone, cyberhackers had drained over a billion dollars from interchain bridges (Blockworks, 2022). In practice, chain bridges operate by the clever combination of debts, IOUs and custody. For a user to move assets, data or funds from one chain to another, the user has to first hand it over to the trusted bridge (which is also a form of custody in this regard). The bridge then issues the equivalent amount of the assets handed over by the user in a form of an IOU and with the destination chains token standard, which makes such tokens compatible with the destination chain's technical specifications, thus creating a debt between the user and the bridge. Once the user returns the issued tokens from the destination chain to the bridge, their original tokens or assets are released to them. This allowed for one native asset of a chain to be transformed into the native token of another chain for use within the foreign chain's ecosystem. But this design required the bridges to hold assets in tens of billions to undertake the complex operation of issuing debts and IOUs and redeeming them on a daily basis. But since the bridges are not as secured as the native chains, they quickly became prime targets for hackers and exploiters. Also, given the level of complexity involved in bridging these chains, it became easy for developers to miss critical bugs and code vulnerabilities at many levels, thereby risking user assets, user records and user data. Bridges of the first-generation of interchain communication and chain interconnectivity have worked albeit with strong risk assumptions and security hypotheses that make them prime targets for hackers (see also Forbes, 2022b). At certain times, bridges could hold more assets by value compared to any of the individual native chains they tend to connect. This was partly because of the number of interchain functionalities (such as decentralized financial use cases) that the bridge could offer, that are usually more attractive or superior compared to the functionalities of each of the native chains.

With security ever more important and funds lost to hackers on the rise, interchain communication justifiably becomes a leading innovation frontier in the blockchain industry, witnessing significant advancements in the past few years. This is a result of years of research and significant resources that have been committed by corporations, open-source software foundations and major not-for-profit organizations to see success in interchain communication and direct chain interconnectivity without bridges. First-generation blockchains can best be described as siloed data chambers without interoperability; second-generation blockchains like Ethereum brought chain-to-chain communication through bridges and middleware (but with significant risks). It was third-generation blockchains that brought direct interchain communication between chains without middleware or bridges. Third-generation blockchains, such as Tendermint Cosmos, took a significant step in interchain communication by removing the trusted middleware of bridges and replacing it with a general-purpose protocol, the IBC protocol – an end-to-end, connection-oriented, stateful protocol for reliable, ordered and authenticated communication between modules on separate blockchains – allowing native chain-to-chain communication of data packets (Goes, 2020). The IBC as a transport protocol is not just for the transfer of digital assets between chains, it also makes it possible for the first time to send any piece of data from one blockchain to another or from one blockchain to multiple blockchains without relying on a trusted middleware or bridge. As a message-passing standard like TCP/IP for the Internet, IBC is at the fundamental level of blockchain interoperability that handles reliable data transport, authentication and ordering of data across blockchains, ushering in a new form of blockchain intercommunication and eliminating most of the trust and security assumptions of bridged middleware. Thus, IBC became the first time blockchains achieved some parity with the architecture of the Internet protocol of TCP/IP, where TCP is to the Internet what IBC is to blockchains, as a transport protocol. It is worth noting that second-generation blockchains only managed to achieve direct chain-to-chain intercommunication through a vertical layering of chains into layer one, layer two, layer three and so on where higher layers interoperate with lower layers but also inheriting some or all of the security assumptions of the lower layers. This also further affected scalability and security of the higher layer chains and brought other limitations in terms of speed and risk guarantees. Thus, third-generation blockchains took a shift away from the bridge and the layered chains approach and instead designed what is generally referred to as the horizontal scaling approach where no chain exists on top of another, but rather each chain achieves full sovereignty, independence and speed with its own security assumptions and risk guarantees, while ensuring direct interchain communication, interconnectedness and data transport among them through IBC.

In summary, chain-to-chain communication and scalability attempts by the different generations of blockchains and the improvements over the years have been aimed towards achieving direct blockchain interconnectedness. Since the concept of interchain communication did not even exist with first-generation blockchains and multichain scalability was not yet on the horizon, attempts at interchain communication started with second-generation blockchains like Ethereum, which ushered in the era of chain-to-chain communication through bridges and scalability through vertical layering mechanism designs. The arrival of third-generation blockchains together with protocols such as IBC was when true chain-to-chain communication was achieved.

Although all three generational design mechanisms are still in use today to convey data between blockchains, the IBC protocol is increasingly being adopted by major chains. However, it remains limited in use because it is an early-stage technology and many major public blockchains will need significant design upgrades, especially at the consensus level, to be able to adopt it.

2. Consensus design

Another area in the blockchain industry witnessing significant evolution is the consensus design. As one of the most important technical components of blockchains in general and, at the same time, the most controversial area among experts, the consensus is where blockchains achieve security. Thus, the debate is whether blockchains' security should be software-based or hardware-based. Throughout the three generations of blockchains, this component of blockchains may have seen the most iteration and improvement because it is the core of blockchains. The fact that most first- and second-generation blockchains are so computationally demanding and energy intensive is what has brought much controversy around the environmental soundness of blockchains in general. The computational intensity and energy consumption levels at an industrial scale of most first- and second-generation blockchains have also elevated barriers to entry, impacted the environment significantly and created negative externalities.

Third-generation blockchains have seen shifts on the technology of the consensus engines, with the aim of moving away from the energy-intensive, environmentally unfriendly PoW algorithms to the now increasingly common versions of PoS algorithms. This has brought advantages to the industry and promises to be one of the major panaceas to mass adoption and broad acceptance of blockchain technology. PoS consensus engines have also lowered the barriers to entry in the blockchain industry as most networks today only require a home-based computer to be a major stakeholder, instead of industrial facilities as required by the Bitcoin blockchain. They consume far less energy and hence are generally more environmentally friendly (Akbar *et al.*, 2021), with increased scalability and speed without compromises on security. That is why it is welcome news that leading networks like Ethereum have moved to PoS-based consensus engines.

3. Programmability

Programmability – the ability of the blockchain to dynamically create, receive, send and execute computational instructions – came with second-generation blockchains, notably Ethereum. This was the first time blockchains moved from being a static-state engine of immutable data and records into dynamic state machines. This marked a major shift from the first-generation blockchains that served the single purpose of holding records immutably and solving the single overarching problem of digital money – the double-spend problem.

Since Ethereum, which first brought the concept of smart contracts – the major innovation at the core of chain programmability – there have been major developments on the front of the computational capabilities of blockchains. More and more complex business logic can now be created, executed and processed on blockchains. Today, full organizations, notably decentralized autonomous organizations, run on smart contracts while owning billions of dollars in their organizational treasuries; and there are a growing number of digital-first firms that are purely chain-based, with their entire corporate structure and governance executed on the blockchain without any physical or geographic presence. The programmability of blockchains has, thus, greatly advanced since the deployment of the first smart contracts on Ethereum. But the design space of smart contracts and programmable blockchains remains vast and yet to be fully explored. It is worth noting that, while second-generation blockchain environments remain the leading environments for existing smart contracts, third-generation blockchains have far more extensive possibilities with chain programmability and support more programming languages, which lowers the barriers to entry for new developers. This has helped increase the use of blockchain-based business logic for solving real-world business problems in increasingly reliable and diverse ways in complex multi-stakeholder environments. Bringing real-world governance and stakeholder coordination to the blockchain through programmability has revealed the possibilities and promise of the technology for governance and human coordination on a large scale.

4. Interchain accounts and cross-chain composability

ICA and cross-chain composability is a more recent advancement in blockchain technology made possible by the IBC protocol. ICA allows an entity on Chain A to execute commands on chain B remotely without need to leave the home chain (Chain A). This allows the entity to, for example, build a business logic application on Chain A that inherits properties of an application or business logic existing on Chain B. Composability is the ability of a business logic, smart contract or a blockchain application to inherit properties of a pre-existing business logic, smart contract or application. Before ICA, applications and smart contracts could only inherit properties of other applications and smart contracts on the same blockchain. Thus, an application on Blockchain A could only inherit properties and business logic of an existing application on Blockchain A but not on Blockchain B. It was not possible to build an application or business logic on the Ethereum blockchain, for example, that inherits properties of an application or smart contract on the Algorand blockchain. With ICA, it is now possible for an application or smart contract running on the Osmosis blockchain to inherit properties of an existing application that is built on the Juno blockchain (CoinDesk, 2022).

The ability of an actor on chain A to build a business logic that inherits properties of an application on a foreign chain is referred to as cross-chain composability. As an early-stage innovation, ICA remains in limited use, but its potential, especially in a controlled and compliant environment, is apparent especially in the design of national and global architectures of CBDCs. It can be envisaged that applications or business logics running on commercial banks' ledgers can inherit properties of applications running on central bank ledgers, opening the potential for financial compliance and the automation of back-office operations as well as the protection of financial records and enforcement without unnecessary intrusion on clients' privacy. Citizens have shown a general preference for financial privacy as a necessary component in the architecture of CBDCs. For example, in 2020 and 2021, the European Central Bank undertook public consultation on what constitutes the most important aspects to the public regarding the design and deployment of the digital euro and a major component of respondents (over 40 per cent) considered financial privacy and user confidentiality as a priority.[30]

5. Chain modularity

Modular blockchains, as compared to monolith blockchains, are relatively new forms of blockchain design and are attempting to separate the three key components – the data availability component, the settlement layer and the consensus engine – of blockchains. First- and second-generation blockchains have been built with the full technological stack well integrated and delivered as a single complex engineering logic without the chance to take them apart and put them to use in any flexible way (called monolithic chains). Third-generation blockchains however, are beginning to take a different approach to the core design of blockchains. Separating the data availability layer from the settlement layer as well as the consensus engine could ensure faster development time, better reliability of blockchain ecosystems and further lower the cost of developing a blockchain. Thus, modular blockchains present a potential for unique performance improvements in the current breed of chains without compromising security. Designing blockchains as modular chunks also allows designers to adopt the strengths of various existing blockchains and combine these superior features into improved new chains without additional cost or new research. Modularity of chains brings a new age of a plug-and-play type of blockchain design where, for example, the deployment of a business-specific blockchain may only need the interested entity to design the business logic of the chain and then simply plug it into a pre-existing consensus layer / data availability layer without needing to wholly create a blockchain from scratch constituting consensus engine, data availability and settlement layers. Thus it could further reduce the barriers to entry into the blockchain industry, reduce the resource requirements for implementation and cut back on time and cost of adopting blockchains by allowing businesses to focus solely on their business logic.

A leading technical example of modular blockchains include the Celestia network, which seeks to design consensus-agnostic data availability and settlement layers that allow any blockchain with any consensus mechanism to plug in and use their data availability and settlement layers for enhanced security and reliability or opt to use only their consensus engine using their data availability and settlement layers (Celestia, 2022).

Table 10 summarizes the key discussion in this section of the annex.

Table 10.
A summary of the five key areas of evolution in blockchains and their implications

Area of technical evolution	Major shift	Implications for users
Consensus design	Move from PoW to PoS and PoS variants	• Barriers to entry lowered • Reduction of carbon footprints • Environmental friendliness of blockchains
Interchain communication	Move from trustful bridges/ smart contract–based interchain communication to chain-native interchain communication	• Interoperability • Scalability • Security for users of app-specific chains
Programmability	Shift from simple transaction ordering and record immutability to execution of complex business logic and full computational functionality of chains	• Allows for multiple use cases and the execution of many kinds of complex business logics, including decentralized autonomous organizations
Interchain accounts and interchain composability	Operator on Chain A can now query data on Chain B as well as create, give, receive and execute computational instructions and business logic on Chain B	• Brings full interoperability • Multichain interconnectedness • Multichain business logic • Cross-chain composability
Modularity	Separation of consensus engines from data availability and settlement layers	• Achieve performance (speed) and scalability without compromising security

Source: UNCTAD.

E. Ongoing developments on technical standards for blockchain technology

International standards on blockchain are still at the early stage. UN/CEFACT together with UNECE have been at the forefront of advocacy for shared global semantic (data) and technical standards for the blockchain industry (UNECE, 2020). The International Organization for Standardization (ISO) has also convened a working group on ISO/TC 307 focusing on blockchain and distributed ledger technologies, with eight ISO standards already published and eight more under development. The ISO/TC 307[31] working group covers areas such as: governance, security and privacy, audit, identity, tokenization, interoperability and smart contracts applications. While these standards are still in the early stages, technical standards within the industry count in the hundreds and are growing. But these technical standards remain fragmented, chain-specific and disharmonized. For example, ERC (Ethereum Request for Comments) standards such as ERC20 and ERC71 are specifically focused on Ethereum and the CW (CosmWasm) standards such as CW20 and CW71 are Cosmos-specific. With growing interoperability, chain-agnostic protocols and the growing potential of a multichain world, both data standards and protocol-level standards are becoming more important so their development and testing should be strongly encouraged.

References

AEB (2022). Blockchain paves the way to end-to-end digital customs processing. 11 May. Available at https://www.aeb.com/en/magazine/articles/blockchain-digital-customs-processing.php (accessed 21 July 2022).

Akbar NA, Muneer A, ElHakim N and Fati SM (2021). Distributed hybrid double-spending attack prevention mechanism for Proof-of-Work and Proof-of-Stake blockchain consensuses. *Future Internet*. 13(11):art 285. Available at https://doi.org/10.3390/fi13110285.

Ali MS, Vecchio M, Putra GD, Kanhere SS and Antonelli F (2020). A decentralized peer-to-peer remote health monitoring system. *Sensors*. 20(6):art 1656. Available at https://doi.org/10.3390/s20061656.

Allessie D, Sobolewski M and Vaccari L (2019). Blockchain for digital government: An assessment of pioneering implementations in public services. JRC Research Reports No. JRC115049. Joint Research Centre (Seville site) (accessed 11 July 2022).

ASEAN (2022). Digital and sustainable trade facilitation in the Association of Southeast Asian Nations (ASEAN) 2021: based on the United Nations Global Survey on digital and sustainable trade facilitation. Available at https://asean.org/book/digital-and-sustainable-trade-facilitation/ (accessed 10 July 2022).

Blockworks (2022). Cross-chain bridge thefts top $1B in 2022. 29 June. Available at https://blockworks.co/cross-chain-bridge-thefts-top-1b-in-2022/ (accessed 11 July 2022).

Bloomberg (2022). Axie-Infinity developer to reimburse hack victims, restart Ronin. 23 June. Available at https://www.bloomberg.com/news/articles/2022-06-23/axie-infinity-developer-to-reimburse-hack-victims-restart-ronin (accessed 9 May 2023).

Celestia (2022). Basics of modular blockchains. Available at https://web.archive.org/web/20220524151555/https://celestia.org/learn/basics-of-modular-blockchains/ (first accessed 6 August 2022; Wayback Machine accessed 14 May 2023).

Clavin J, Duan S, Zhang H, Janeja GP, Joshi KP, Yesha Y, Erickson LC and Li JD (2020). Blockchains for government: use cases and challenges. *Digital Government: Research and Practice*. 1(3):art 22. Available at https://doi.org/10.1145/3427097.

CNBC (2022). China has been quietly building a blockchain platform: here's what we know. Available at https://www.cnbc.com/2022/05/16/china-blockchain-explainer-what-is-bsn-.html (accessed 20 July 2022).

CoinDesk (2022). Cosmos gains interchain accounts as upgrade kicks in. Available at https://www.coindesk.com/tech/2022/04/14/cosmos-gains-interchain-accounts-as-upgrade-kicks-in/ (accessed 4 July 2022).

Corcuera-Santamaria SC (2018). CADENA, a blockchain enabled solution for the implementation of Mutual Recognition Arrangements/Agreements. WCO News 87:60–62. Available at https://mag.wcoomd.org/magazine/wco-news-87/cadena-a-blockchain-enabled-solution-for-the-implementation-of-mutual-recognition-arrangements-agreements/ (accessed 2 August 2022).

Corcuera-Santamaria S and Moreno LM (2019). How blockchain can make trade safer. Beyond Borders. Available at https://blogs.iadb.org/integration-trade/en/blockchain-trade-safer/ (accessed 2 August 2022).

Deloitte (2021). Digitalising trade with blockchain: the Certificate of Origin. March. Available at https://www2.deloitte.com/content/dam/Deloitte/be/Documents/tax/Digitalising%20trade%20with%20blockchain_CoO_March2021.pdf (accessed 11 May 2023).

Duval Y and Mengjing K (2017). Digital trade facilitation: paperless trade in regional trade agreements. Asian Development Bank Institute Working Paper No. 747. Available at https://www.adb.org/sites/default/files/publication/321851/adbi-wp747.pdf (accessed 9 May 2023).

European Central Bank (2021). Eurosystem report on the public consultation on a digital euro. Available at https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf (accessed 9 May 2023).

European Union Blockchain Observatory and Forum (2019). Legal and regulatory framework of blockchains and smart contracts v.1.0. Available at https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf (accessed 20 July 2022).

Forbes (2022a). Council post: how blockchain could revolutionize cybersecurity. Available at https://www.forbes.com/sites/forbestechcouncil/2022/03/04/how-blockchain-could-revolutionize-cybersecurity/ (accessed 10 July 2022).

Forbes (2022b). Hackers steal another $100 million in crypto from a blockchain transfer protocol, total lost in 2022 above $1 billion. 24 June. Available at https://www.forbes.com/sites/mariagraciasantillanalinares/2022/06/24/hackers-steal-another-100-million-in-crypto-from-a-blockchain-transfer-protocol-total-lost-in-2022-above-1-billion/ (accessed 5 August 2022).

Ganne E (2018). *Can Blockchain Revolutionize International Trade?* WTO Publications. Geneva. Available at https://www.wto.org/english/res_e/booksp_e/blockchainrev18_e.pdf (accessed 11 May 2023).

Giegling J (2022). In blockchain we trust? Certificates of origin as a case for distributed ledger technologies. *Journal of Law, Market & Innovation*. 1(1):66–96.

Global Trade Single Window Project (2019). Windows of Opportunity: Facilitating Trade with Blockchain Technology. World Economic Forum. July. Available at https://www3.weforum.org/docs/WEF_Windows_of_Opportunity.pdf (accessed 2 August 2022).

Goes C (2020). The Interblockchain Communication protocol: an overview. ArXiv, June. arXiv:2006.15918v1 [cs.DC] June. Available at http://arxiv.org/abs/2006.15918 (accessed 4 July 2022).

Harvard Business Review (2022). Why Build in Web3. 16 May. Available at https://hbr.org/2022/05/why-build-in-web3 (accessed 10 May 2023).

IBM Blog (2020). IoT and blockchain: technologies for universal cargo monitoring. 25 August. Available at https://www.ibm.com/blogs/blockchain/2020/08/iot-and-blockchain-technologies-for-universal-cargo-monitoring/ (accessed 1 August 2022).

IBM Blog (2021). Blockchain and trade finance. 8 March. Available at https://www.ibm.com/blogs/blockchain/2021/03/blockchain-and-trade-finance/ (accessed 21 July 2022).

Kerstens J and Canham J (2018). Blockchain: mapping new trade routes to trust. WCO News 87:52–55. Available at https://mag.wcoomd.org/magazine/wco-news-87/blockchain-mapping-new-trade-routes-to-trust/ (accessed 4 June 2022).

Kunaka C and Carruthers R (2014). *Trade and Transport Corridor Management Toolkit*. World Bank. Washington, DC. Available at https://documents1.worldbank.org/curated/en/719971468325781473/pdf/Trade-and-transport-corridor-management-toolkit.pdf (accessed 2 August 2022).

LACChain (2022). See https://www.lacchain.net/home?lang=en (accessed 21 July 2022).

Leal N (2022). Canada pilots blockchain staff records. Global Government Forum. 17 June 2019, updated 4 February 2022. Available at https://www.globalgovernmentforum.com/canada-pilots-blockchain-staff-records/ (accessed 11 July 2022).

Lim A and Pan E (2021). "Toward a global social contract for trade" – a Rawlsian approach to blockchain systems design and responsible trade facilitation in the New Bretton Woods era. *Journal of Responsible Technology*. 6:art 6100011. Available at https://doi.org/10.1016/j.jrt.2021.100011 (accessed 10 May 2023).

Lohmer J, Bugert N and Lasch R (2020). Analysis of resilience strategies and ripple effect in blockchain-coordinated supply chains: an agent-based simulation study. *International Journal of Production Economics*. 228:art 107882. Available at https://doi.org/10.1016/j.ijpe.2020.107882 (accessed 10 May 2023).

Ministry of Electronics and Information Technology (2021). National strategy on blockchain: towards enabling trusted digital platforms. December. Government of India. New Delhi. Available at https://www.meity.gov.in/writereaddata/files/National_BCT_Strategy.pdf (accessed 13 May 2023).

Moroccan Customs (2020). Dematerialization of customs procedures: feedback from Moroccan Customs. WCO News 94. Available at https://mag.wcoomd.org/magazine/wco-news-94/dematerialization-of-customs-procedures-morocco/ (accessed 22 July 2022).

OECD (2022). Digital trade. Available at https://www.oecd.org/trade/topics/digital-trade/ (accessed 10 July 2022).

Patel D and Ganne E (2020). Blockchain & DLT in trade: where do we stand? Trade Finance Global and World Trade Organization. London. Available at https://www.wto.org/english/res_e/booksp_e/blockchainanddlt_e.pdf (accessed 11 May 2023).

Republic of Singapore (2021). Electronic Transactions (Amendment) Act 2021. Available at https://sso.agc.gov.sg/Acts-Supp/5-2021/Published/20210312?DocDate=20210312 (accessed 13 May 2023).

Schrepel T and Buterin V (2020). Blockchain code as antitrust. *Berkeley Technology Law Journal*. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3597399 (accessed 10 May 2023).

Shang Q and Price A (2019). A blockchain-based land titling project in the Republic of Georgia: rebuilding public trust and lessons for future pilot projects. *Innovations: Technology, Governance, Globalization*. 12(3/4):72–78.

Shirazi F and Hajli N (2021). IT-enabled sustainable innovation and the global digital divides. *Sustainability*. 13(17):art 9711. Available at https://doi.org/10.3390/su13179711 (accessed 10 May 2023).

Song JM, Sung J and Park T (2019). Applications of blockchain to improve supply chain traceability. *Procedia Computer Science*. 162:119–122.

Statista (2022). Global share of blockchain patents in 2021, by country. 23 May. Available at https://www.statista.com/statistics/1285542/worldwide-share-of-blockchain-patents-by-country/ (accessed 3 August 2022).

Sun H, Yang J and Xu X (2020). Research on the application of blockchain technology in international trade risk management. *Journal of Asian Research*. 4(3):6–49.

Triangularity (2023). See https://triangularity.net/ (accessed 31 May 2023).

UN/CEFACT (United Nations Centre for Trade Facilitation and Electronic Business) (2022). *White Paper: eDATA Verifiable Credentials for Cross Border Trade. Available at https://unece.org/sites/default/files/2023-08/WhitePaper_VerifiableCredentials-CrossBorderTrade_September2022.pdf* (accessed 13 May 2023).

UN/CEFACT (United Nations Centre for Trade Facilitation and Electronic Business) (2019a). *White Paper: Technical Applications of Blockchain to UN/CEFACT Deliverables, Version 2*. ECE/TRADE/C/CEFACT/2019/8. Available at https://unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain_TechApplication.pdf (accessed 13 May 2023).

UN/CEFACT (United Nations Centre for Trade Facilitation and Electronic Business) (2019b). *White Paper: Blockchain in Trade Facilitation, Version 2*. ECE/TRADE/C/CEFACT/2019/9/Rev.1. Available at https://unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain.pdf (accessed 13 May 2023).

UNCITRAL (United Nations Commission on International Trade Law) (2018). *UNCITRAL Model Law on Electronic Transferable Records* (United Nations Publication. Sales No. E.17.V.5. New York).

UNCTAD (2020). COVID-19: A 10-point action plan to strengthen international trade and transport facilitation in times of pandemic. UNCTAD/PRESS/PB/2020/3 (No. 79). Available at https://unctad.org/system/files/official-document/presspb2020d3_en.pdf (accessed 10 May 2023).

UNCTAD (2021a). COVID-19 implications for commercial contracts: carriage of goods by sea and related cargo claims. UNCTAD/DTL/TLB/INF/2021/1. Geneva.

UNCTAD (2021b). COVID-19 implications for commercial contracts: international sale of goods on CIF and FOB terms. UNCTAD/DTL/TLB/INF/2021/2. Geneva.

UNCTAD (2021c). ASYCUDA Programme Presentation, March. Available at https://p166.unctad.org/pluginfile.php/38647/mod_page/content/13/ASYCUDA_Program_Blockchain_Presentation_March%202021-RB.pdf (accessed 7 June 2023).

UNCTAD (2022a). Contracts for the carriage of goods by sea and multimodal transport: key issues arising from the impacts of the COVID-19 pandemic. UNCTAD/DTL/TLB/INF/2022/1. New York and Geneva.

UNCTAD (2022b). *Jordan: eTrade Readiness Assessment*. UNCTAD/DTL/STICT/2021/6 and Corr.1. Geneva. Available at https://unctad.org/system/files/official-document/dtlstict2021d6_en.pdf (accessed 11 May 2023).

UNCTAD (2022c). Training course on implications of the COVID-19 pandemic for commercial contracts. 7–10 June. Available at https://unctad.org/meeting/training-course-implications-covid-19-pandemic-commercial-contracts-2 (accessed 10 May 2023).

UNCTAD (2023). COVID-19 and international sale of goods: contractual devices for commercial risk allocation and loss prevention. UNCTAD/DTL/TLB/2023/1. New York and Geneva.

UNECE (United Nations Economic Commission for Europe): United Nations Centre for Trade Facilitation and Electronic Business (2020). *White Paper: Blockchain in Trade Facilitation*. ECE/TRADE/457. Geneva. Available at https://unece.org/trade/publications/white-paper-blockchain-trade-facilitation-ecetrade457 (accessed 11 May 2023).

UNECE (United Nations Economic Commission for Europe): United Nations Centre for Trade Facilitation and Electronic Business (2022). Recommendation No. 46: enhancing traceability and transparency of sustainable value chains in the garment and footwear sector. ECE/TRADE/463. Geneva. Available at https://unece.org/trade/publications/recommendation-no46-enhancing-traceability-and-transparency-sustainable-value (accessed 11 May 2023).

UNESCAP (United Nations Economic and Social Commission for Asia and the Pacific) (2022). Implications of the COVID-19 pandemic for commercial contracts covering the transportation of goods in the Asia-Pacific region and beyond. Available at https://unttc.org/documents/implications-covid-19-pandemic-commercial-contracts-covering-transportation-goods-asia-0 (accessed 31 May 2023).

United Kingdom Parliament (2023). Electronic Trade Documents Bill [HL]. Available at https://bills.parliament.uk/bills/3344 (accessed 13 May 2023).

United States Department of Homeland Security (2018). Beyond Blockchain Basics: Lessons Learned and Next Steps from 3+ Years of R&D and Implementations. Available at: https://www.acsac.org/2018/program/Wed-1030-John.pdf

W3C (2022). Decentralized Identifiers (DIDs) v1.0 becomes a W3C Recommendation. 19 July. Available at https://www.w3.org/2022/07/pressrelease-did-rec.html.en (accessed 25 July 2022).

World Economic Forum (2021). How blockchain technology is fixing payments and what's next. 29 April. Available at https://www.weforum.org/agenda/2021/04/how-blockchain-technology-is-fixing-payments-today-what-comes-next/ (accessed 21 July 2022).

World Trade Organization and World Customs Organization (2022). *The Role of Advanced Technologies in Cross-Border Trade: A Customs Perspective*. Geneva and Brussels. Available at https://www.wto.org/english/res_e/booksp_e/wcotech22_e.pdf (accessed 21 July 2022).

Ying W, Wu Y, Cimen H, Vasquez JC and Guerrero JM (2022). P2P energy trading: blockchain-enabled P2P energy society with multi-scale flexibility services. *Energy Reports*. 8:3614–3628.

Endnotes

[1] For further information and guidance on this complex of issues, see the analytical reports and training materials by UNCTAD on the commercial law implications of the COVID-19 pandemic, prepared as part of its COVID-19 related technical assistance. Available at https://unttc.org/stream/key-international-commercial-law-implications. See also UNCTAD, 2021a, 2021b, 2022a, 2022c, 2023; UNESCAP, 2022.

[2] "Technology stack" refers to the unique architectural design of a software from the very foundation to the user interface.

[3] E-Estonia. See https://e-estonia.com. See also Ali et al., 2020.

[4] The double-spend problem, especially with regard to money, is a potential flaw in a digital cash scheme in which the same single digital token can be spent more than once.

[5] This means these second-generation of blockchains functioned as computers that could receive, give, create and execute computational instructions based on specific computer code.

[6] A hash is like a fingerprint for a piece of information. It is a unique code that is generated from the information and it can be used to identify it. Just like a fingerprint, even a small change to the information will create a completely different hash. They are often used for things like checking if data has been changed or for organizing information in a certain way; it is much used in cryptography and it is the basis of blockchain technology.

[7] An application programming interface is normally a way for two or more computer programs to communicate with each other.

[8] Remote procedure calls are normally software communication protocols that one program can use to request/send instructions or service to or from a program located in another computer on a network without the need to fully understand the network's details.

[9] Smart contracts are automated self-executing computer codes on blockchains for specific business logic.

[10] Decentralized autonomous organizations are blockchain-native virtual organizations running as pieces of code on blockchains, designed with a specific governance structure and have features of a modern-day organization, functioning as if they had a physical existence.

[11] The ASYCUDA programme is UNCTAD's largest technical cooperation initiative, with 102 countries and territories worldwide adopting ASYCUDA and 90% of them using or migrating to the latest version – ASYCUDAWorld. An important objective of ASYCUDA projects is to implement systems as efficiently as possible with a full transfer of know-how to national Customs administrations at the lowest possible cost for countries and donors. Projects also utilize harmonized international standards, while simultaneously leading to active and mutually beneficial cooperation among ASYCUDA user countries. See UNCTAD, 2021c and for more information, see https://asycuda.org/en/programme/.

[12] Formed by a consortium of companies including the Dortmund Fraunhofer Institute for Material Flow and Logistics and the Fraunhofer Institute for Software and Systems Engineering with funding from the public sector, Blockchain Europe Initiative supported the Stuttgart-based software provider AEB SE and the Fraunhofer Institute for Material Flow and Logistics to build the blockchain end-to-end platform prototyped in a post-Brexit context of trade between the United Kingdom of Great Britain and Northern Ireland and the European Union. The project is still in an early stage. See AEB, 2022.

[13] LACChain is considered a global alliance made up of different actors in the blockchain environment, led by the Innovation Laboratory of the Inter-American Development Bank Group (IDB Lab) for the development of the blockchain ecosystem in Latin America and the Caribbean with the goal of accelerating the enablement and adoption of blockchain technology in the region for the promotion of innovation and the reduction of economic, social, gender and other inequalities, as well as the promotion of quality and security of jobs, promoting financial inclusion, consumer protection and market integrity. See LACChain (2022) for more information on the blockchain ecosystem.

[14] UNCTAD services to National Trade Facilitation Committees as a multi-stakeholder platform for coordination of key trade facilitation participants include training, expert advice and a digital platform called Reform Tracker where Trade Facilitation Committees can visualize their national trade facilitation performance and seek to improve this performance over time. For more, see: https://unctad.org/topic/transport-and-trade-logistics/trade-facilitation/empowerment-programme.

[15] For an overview of the legal implications of delayed bills of lading, see UNCTAD (2022a), section C.1.6.

[16] The combination of AI and smart contracts creates opportunities for innovation and automation. It can lead

to increased automation of various processes in industries such as finance, supply chain and insurance. AI-powered systems can interact with smart contracts to execute actions based on predefined conditions, reducing manual intervention and increasing efficiency. AI and smart contracts can also be used to create new forms of decentralized finance that are more efficient and secure. On the other hand, blockchain can enhance data security and privacy, facilitate data sharing and build trust in AI systems.

[17] Quorum is an Ethereum-based distributed ledger protocol that enables the creation of a permissioned blockchain application with benefits such as user privacy and data protection. It was initially developed by JP Morgan and later acquired by Consensys.

[18] More on the TradeTrust open-source portal can be found on their website: https://www.tradetrust.io/.

[19] Adopted in 2005 to enhance security and facilitation in global trade, the WCO SAFE Framework rests on two pillars: Customs–Customs network and Customs-to-business partnerships, with the core elements of harmonizing advance cargo information, introducing risk management mechanisms, exchange of inspection results of high-risk containers by Customs authorities and enhanced benefits for compliant traders.

[20] See also Authorized Economic Operators by the UNECE, https://tfig.unece.org/contents/authorized-economic-operators.htm.

[21] See, for instance, the UNCITRAL Model Law on Electronic Transferable Records (MLETR) (UNCITRAL, 2018), which seeks to ensure full legal recognition of electronic records as equivalent to traditional paper-based documentation. Relevant legislation has been adopted, for instance, in Singapore (Republic of Singapore, 2021). An Electronic Trade Documents Act broadly based on the UNCITRAL MLETR has been adopted in the United Kingdom (United Kingdom Parliament, 2023).

[22] See the deployment of IBC-enabled blockchains using the Cosmos Software Development Kit of Tendermint, https://tendermint.com/sdk/.

[23] The China Blockchain-based Service Network allows anyone in the world to develop and deploy any application on selected public blockchains using a hosted environment, a platform developed by the Government of China. It allows developers to work on many of the existing major public networks such as Ethereum, Algorand, Nervos, Tron and EOS without the need to handle the infrastructure required to build on these networks. It is accessible at: https://bsnbase.io/g/main/index and is open to everyone. See also: CNBC, 2022.

[24] The EBSI is a blockchain network of distributed nodes across Europe to support important applications. It is a joint effort of all European Union Member States, Norway and Lichtenstein and the European Commission, known as the European Blockchain Partnership (EBP) and EBSI is an initiative that results from this partnership, https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi

[25] According to Statista (2022), as of 2021, China was the largest owner of blockchain-related patents, accounting for 84 per cent of global patents. Despite the country banning the mining and use of cryptocurrencies, the interest in blockchain technology has remained high. In the same year that the country banned mining and use of cryptocurrencies, the number of patent applications in China almost reached 16,000.

[26] Tokenomics is an all-inclusive concept that seeks to capture the nature of emission, distribution and stakeholder incentivization mechanisms of a blockchain network with the network-native tokens. It comprises the concepts of economic reasoning behind the token design, the relationship between this economic reasoning and the security of the network, and the drivers of value of the token to stakeholders in the network.

[27] A Byzantine Fault Tolerant system is one that can keep functioning correctly as long as two thirds of the participating servers agree on the true state of records or reach consensus. It is a property of distributed system design that can resist up to one third of the servers or nodes failing or acting maliciously.

[28] Record obfuscation is the process of protecting transactions by the technical mixing of those transactions in a way that makes them hard to disentangle and trace by everyone.

[29] Multi-sig wallets are usually digital wallets that operate with the use of multi-signature addresses requiring more than one private key to sign and authorize transactions or requiring that several different keys be used to generate a signatory.

[30] See European Central Bank (2021): what respondents wanted most from a digital euro is privacy (43 per cent), security (18 per cent), usability across the euro area (10 per cent), the absence of additional costs (9 per cent) and offline use (8 per cent).

[31] The Working Groups on ISO/TC 307 standards for blockchain and distributed technologies, https://www.iso.org/committee/6266604.html.

Designed at United Nations, Geneva – 2311141 **(E)** – August 2023 – **UNCTAD/TCS/DTL/INF/2023/1**