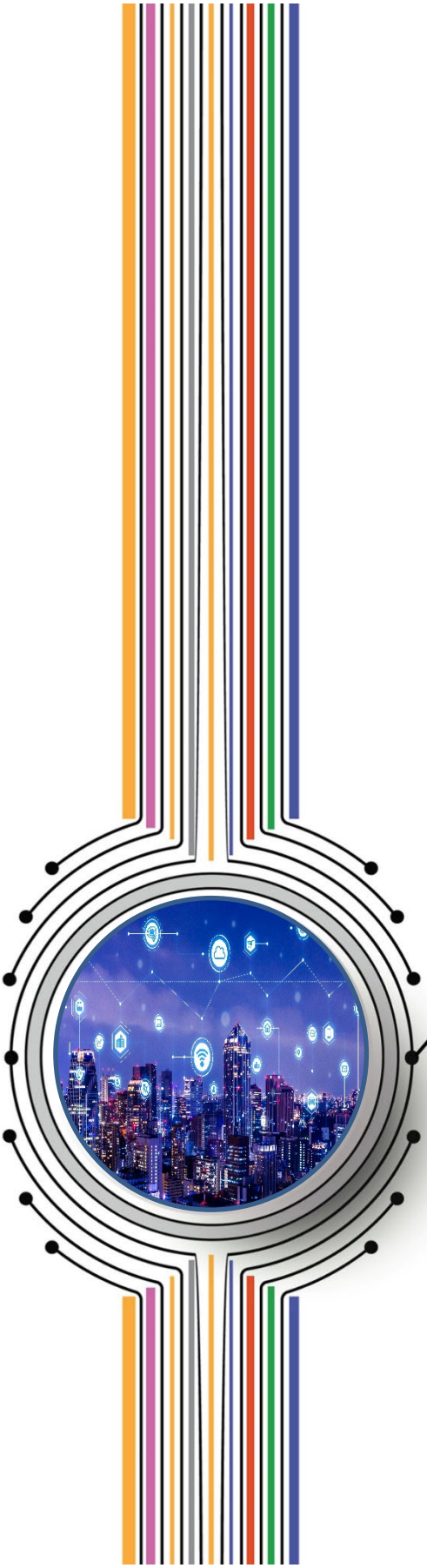

UNECE
UN / CEFACT

White Paper
Blockchain in Trade Facilitation

Version 2

This document is presented to the 26th UN/CEFACT Plenary as document ECE/TRADE/C/CEFACT/2019/9/Rev.1

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT)

Simple, Transparent and Effective Processes for Global Commerce

UN/CEFACT's mission is to improve the ability of business, trade and administrative organizations, from developed, developing and transitional economies, to exchange products and relevant services effectively. Its principal focus is on facilitating national and international transactions, through the simplification and harmonization of processes, procedures and information flows, and so contribute to the growth of global commerce.

Participation in UN/CEFACT is open to experts from United Nations Member States, Intergovernmental Organizations and Non-Governmental Organizations recognized by the United Nations Economic and Social Council (ECOSOC). Through this participation of government and business representatives from around the world, UN/CEFACT has developed a range of trade facilitation and e-business standards, recommendations and tools that are approved within a broad intergovernmental process and implemented globally.

www.unece.org/cefact

Acknowledgement

This paper has been prepared under the leadership of Virginia Cram Martos, under the guidance of Vice Chair Tahseen Khan. Lance Thompson, Tomas Malik and Helen Ross of the UNECE secretariat supported this work. The following experts contributed to parts of this work: Ahmed Abdulla, Jorge Alvarado, Ferdinando Ametrano, Anurag Bana, Pankhuri Bansal, Gadi Benmoshe, Simone Bonetti, Alex Cahana, Enrico Camerinelli, Steve Capell, Concettina Cassa, Savino Damico, Dario Delle Noci, Tom Fong, Chris Gough, Edmund Gray, Luca Grisot, Thierry Grumiaux, Rudy Hemeleers, Jahidul Hasan, Kazuo Hotta, Ravi Jagannathan, Erik Jonker, Christophe Joubert, Henry Kim, Ad Kroft, Vijay Kumar, Marek Laskowski, Wassilios Lytras, Pietro Marchionni, Gianluca Marcolongo, François Masquelier, Richard Morton, Ronan Mualem, Anushka Patchava, Anita Patel, David Roff, Hans Rook, Eiichi Sakai, Carlo Salomone, Daniel Sarr, Mohit Sethi, Lisa Simpson, Fabio Sorrentino, Kaushik Srinivasan, Akio Suzuki, Tunghua Tai, Mikio Tanaka, Max Tay, Daniele Tumietto, Frans van Diepen, Venkatraman Viravanallur, Rupert Whiting and Burak Yetiskin.

Disclaimers

Foreword

I am pleased to present this revised version of the White paper Overview on Blockchain and sectoral challenges and opportunities.

Blockchain technology is one of the most talked about topics in the sphere of information technology as well as in the facilitation of electronic business. The cryptocurrency Blockchain applications are well known and well-publicized, however, this technology has the potential to influence the way that we do business today, as its use expands to new areas.

Blockchain, which is one form of Distributed Ledger Technology (DLT), offers opportunities to increase the reliability and security of trade transactions. The repetition of data among multiple ledgers in a network, as well as the immutability of information after it has been integrated into the Blockchain, can increase levels of confidence for both traders and regulators. Additionally, these technologies have the potential to facilitate cross-border trade, increase access to global value chains for small businesses in developing economies, as well as support the effectiveness of government services that support more inclusive economic and social progress. Immutable original electronic certificates, licenses and declarations can be linked with goods, in order to facilitate regulatory procedures. Blockchain can help trade facilitation because of the following characteristics: it is immutable (nearly impossible to change once transactions are written), automated (actions can be automatically executed) and historized (have full transaction history, which can be used to track and trace).

Furthermore, Blockchain implementation is useful to make possible contributions to the achievement of the United Nation agenda for 2030, the Sustainable Development Goals (or SDGs). Some Blockchain applications which are already being used to support the SDGs include the establishment of identities (for example for refugees); the tracking of information linked to identities (related to health, social benefits); the distribution of resources (financial and material support) and the tracing of goods and their content and original source.

I hope that this publication will offer a useful aid to all parties interested in the technical applications and implementation of Blockchain technologies and that this important process will continue to contribute to the enhancement and growth of international trade.

Maria Ceccarelli
Chief of Section, Trade Facilitation Section
United Nations Economic Commission for Europe

Table of Contents

Part I

1 An introduction to Blockchain and trade facilitation

1.1 Introduction

The UN/CEFACT Blockchain White Paper Project oversaw the preparation of two White Papers. The first, which looks at Blockchains' impact on the technical standards work of UN/CEFACT, has been published (ECE/TRADE/C/CEFACT/2019/8). This is an update of the second White Paper, which looks at how Blockchain technology could be used to facilitate trade and related business processes. In this updated version, you find potential uses of Blockchain in different sectors in the second part of the paper. The Briefing Note on how Blockchain technology could be used to support the United Nations Sustainable Development Goals (ECE/TRADE/C/CEFACT/2018/25) is being updated to include further examples. This work is also accompanied by a repository of case studies on Blockchain which is available at: http://www.unece.org/tradewelcome/un-centre-for-trade-facilitation-and-e-business-uncefact/case-study-repositories.html.

As described further below, the term "Blockchain" is being used throughout this document, although it could be interchanged with the term Distributed Ledger Technology. There are distributed ledger technologies that are not Blockchains, but at the time of publication, they are even newer and less tested than Blockchain technologies, so they are not discussed here. At the same time, the security and legal issues described in chapter 2, almost all of the implementation issues discussed in chapter 3 and the uses for Blockchain discussed beginning with Chapter 4 apply generally to Digital Ledger Technology and not only to Blockchains.

Blockchain technology is based on an innovative use of cryptography and has attracted a lot of attention due to its characteristics, which include:

- The creation of data records that are permanent (i.e. cannot be changed or deleted);
- The ability to identify the time and origin of every entry in a Blockchain;
- The collaborative potential providing access to data in a Blockchain to multiple participants; and
- The guaranteed implementation of smart contracts (programmes) that automatically execute once a set of agreed conditions are met.

The international supply chain is characterized by flows of goods and related data. These are aligned with the movement of associated funds which reflect the transactional nature of supply chains. Typically, this movement of funds is linked to specific events in the supply chain and takes place electronically, thus making it well suited to the application of Blockchain technology. Goods flow from seller/exporter to buyer/importer in return for funds that flow in the reverse direction. The flow of goods and funds is supported by a bidirectional flow of data which can potentially be short snippets of information leading to the information on tradition documents; or it can be complete documents such as invoices, shipping notices, bills of lading, certificates of origin and import/export declarations lodged with regulatory authorities.

This description highlights the relevance of Blockchain technology to the work of UN/CEFACT. Since the 1960s, UN/CEFACT and its predecessors have developed recommendations and standards to support trade facilitation. And, since the introduction of the

UN/EDIFACT[1] standard in the 1980s, UN/CEFACT has also developed and maintained standards aimed at facilitating trade through improved trade-related data flows.

The three flows described above, of goods, data and funds, are supplemented by a layer of trust. Trust, or a lack of trust, impacts almost every action and data exchange in international trade, including trust in the:

- Provenance and authenticity of goods;
- Stated value of goods for the purposes of insurance, duties and payment;
- Promises to pay;
- Protection of goods during shipping (i.e. integrity of packaging, vehicle and container conditions, etc.);
- Integrity of information that is used by regulatory authorities for risk assessments which determine inspections and clearances; and in the
- Traders and service providers involved in a trade transaction.

This layer of trust between economic operators determines which technologies are needed in order to achieve a desired level of reliability in electronic data exchanges. Where high levels of trust exist between partners, authentication methods with lower levels of control and reliability are appropriate and can be sufficiently robust. Where such trust has not been established between trading partners, authentication with higher levels of control and reliability are necessary. This "layer of (dis)trust" is still heavily supported by paper documents, manual signatures, insurance premiums, escrow funds and other trusted third-party services.

Blockchain is a type of Distributed Ledger Technology (DLT) which provides authentication methods with very high levels of reliability. Thus, it has the potential to deliver significant improvements to the aforementioned layers of trust—and often at a lower cost and greater speed than alternatives.

For the rest of this paper we will refer only to Blockchain with the understanding that it is a DLT.

As the focal point for trade facilitation and electronic business standards in the United Nations system, UN/CEFACT needs to ask itself how this new technology impacts these two critical aspects of the global supply chain. The impact on UN/CEFACT electronic business standards is examined in the first White Paper (ECE/TRADE/C/CEFACT/2019/8) whereas this White Paper looks at the impact of Blockchain technology on trade facilitation.

The UN/CEFACT Blockchain White Paper Project Team held a face-to-face meeting during the Hangzhou Forum in China in October 2018. At that meeting there was consensus that one of the most important benefits of the project to date had been the opportunity for those implementing or considering implementing Blockchain technology to have concrete discussions about opportunities, alternatives, issues, and possible solutions. There are many existing forums and conferences on Blockchain technology, but they focus on cryptocurrency or investment aspects; and/or lack the possibility for dialogue (i.e. are primarily for posting information); and/or are dominated by the sales and marketing discourse of those promoting specific Blockchain solutions.

For the next phase of the project, the project team proposed the development of a forum for the

[1] The United Nations Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT) is a standard which is now extensively used in international transport, logistics and other sectors.

discussion of Blockchain use in the international supply chain and expanding it to include the relevance of other advanced technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI). This forum could support Senior Managers responsible for making decisions about international supply chain applications, particularly in government. It could also help UN/CEFACT to identify areas where its work could facilitate the use of these advanced technologies in support of trade facilitation.

The Project team supported a proposal to establish an Advisory Group on Advanced Technologies in the international supply chain[2] which would support the implementation of the UN/CEFACT programme of work areas related to the use of digital technologies for exchanging trade information. Its main task would be to identify emerging strategic issues and international best practices for senior public and private sector officials on this topic. One of the first activities of this Advisory Group would be to look at specific issues raised within the sectoral analyses and the case studies in this White Paper. On the basis of this work, the Advisory Group would advise on recommendations for future work as well as guidelines and information papers for consideration and possible adoption and publication by UN/CEFACT.

2 What is Blockchain and what should you know about it?

2.1 History and background

Although some of the principles incorporated in Blockchain technology were already described in earlier cryptography papers, the basis for the Blockchain technology used today was first published in an October 2008 White Paper on a cryptography mailing list. The paper was called, "Bitcoin: A Peer-to-Peer Electronic Cash System" and was published by an author, or a group of authors, under the pseudonym *Satoshi Nakamoto*. Interestingly, the term 'Blockchain' was never used in the original paper, but rather expressions such as 'chain of blocks' and 'blocks are chained'. The first use of "block chain" appeared on the same mailing list in subsequent discussions linked to the original Nakamoto paper.

On 9 January 2009, Satoshi Nakamoto released Version 0.1 of the Bitcoin software, which was the first software to implement the principles described in the October 2008 paper. This was done on an open-source software site called SourceForge.

Satoshi Nakamoto continued to collaborate with other developers on the Bitcoin software until mid-2010. Around that time, he handed over control of the source code repository and updates to Gavin Andresen, transferred several related Internet domains to other prominent members of the bitcoin community, and stopped his involvement. Up until this day, and in spite of much speculation and detective work no one has discovered the identity of Satoshi Nakamoto.

Another important milestone in the development of Blockchain technology was the development of Blockchains that could implement small computer programmes called smart contracts that are written in computer languages having a complete set of programming capabilities (these are called "Turing complete" computer languages).

Smart contracts have given Blockchains the ability to implement a varied set of business functions involving the transfer of information and/or value, while leaving transparent and reliably auditable information trails. More about smart contracts can be found later in this text.

[2] See the proposed "Mandate and Terms of Reference of the Advisory Group on Advanced Technologies" ECE/TRADE/C/CEFACT/2019/22.

The first Blockchain to use smart contracts was Ethereum which was invented by Vitalik Buterin. He first described the use of smart contracts on a Blockchain in a White Paper in late 2013. Then, when he failed to gain agreement on this concept within the Bitcoin community, he proposed the development of a new platform called Ethereum. This new network, launched on 30 July 2015, is today the Blockchain with the largest number of transactions and is among the top three in market capitalization.[3]

2.2 Blockchain: how it works

At its heart, a Blockchain is a cryptographic protocol that allows separate parties to increase the trustworthiness of a transaction because the ledger entries in its database cannot be easily falsified (i.e. once data is written it is extremely difficult to change, albeit provided the data was correct from the outset). This "immutability" is due to a combination of factors including the cryptography used in a Blockchain, its consensus/validation mechanism and its distributed nature. As a result of this immutability, Blockchain systems can be used as an independent umpire in processes that might otherwise expose participants to the risk of one party not living up to its contractual obligations (counterparty risk) and where third-party guarantors are reluctant to intervene and assume part of that risk.

This text does not aim to provide an in-depth review of Blockchain technology—there are plenty of web resources to help readers achieve that goal. Rather, it will cover the core concepts which are needed to understand the potential application of Blockchain in international supply chains.

First, some nomenclature:

a) **Block**: Data that is appended to the ledger after validation. Once a block is written to the chain, it cannot be changed or deleted without replacing all subsequent blocks.
b) **Consensus**: An important characteristic of Blockchain systems which allows users to know that transactions have been executed and to evaluate the trustworthiness of the information about and in those transactions (for example, the date/time of execution and content). In the case of public Blockchains, the umpire that decides consensus is the society of all nodes that choose to participate. In the case of private Blockchains, the umpire is the consortium of nodes given permission to create consensus. There will be more about the different ways in which consensus can be reached in the text below.
c) **Fiat or Fiat Currency**: These are currencies backed by a central bank such as dollars, euros, yen, etc.
d) **Hash**: The result of mathematical operations carried out on the numeric representation of data—all data in a computer consists of numbers that are deciphered in order to create the words and images you see on a screen. This result has a fixed size and is a unique cryptographic fingerprint of the underlying data. A hash is a one-way function; this means that given the data, it is easy to verify that the hash is the correct one for that data. This is done by performing the pre-defined mathematical operations on the data that supposedly created the hash—if the result is the same, the data is the same. This is a key feature because it allows users to quickly confirm that no changes, at all, have been made. For example, even an additional space or empty line in a text would change its hash. At the same time, and this is what makes it a one-way function, it is almost impossible to recreate the original data if all one has is the hash (i.e. reverse engineer it).

[3] According to https://bitinfocharts.com/ (as of February 2020).

e) **Node**: A system that hosts a full copy of the Blockchain ledger. In some Blockchains, such as Bitcoin and Ethereum, all nodes participate in the consensus process, in others it may be only be selected nodes.
f) **On-chain transaction**: An automated procedure that creates or updates the status of a Blockchain asset in the Blockchain database by appending new data to the ledger. Examples include digital asset exchange, or execution of an automated business process.
g) **Validation**: Work performed by nodes, in parallel, that verifies transactions using a consensus algorithm. Different networks may use different consensus algorithms. When mutual validation results in a consensus, then the nodes all commit (record) the verified transactions onto their Blockchain as a new block.

2.2.1 Blockchain is a distributed ledger technology (DLT)

Ledgers are lists of records where transactions are recorded once and cannot be subsequently updated. This means that any changes must be recorded as new transactions (book-keeping entries). Digital ledgers may be stored as a database, also known as a journal database. Each record can be read many times but written only once. The term ledger comes from accounting where entries, once written into a ledger (accounting journal), cannot be changed. A Blockchain database is a ledger because it uses hashes to ensure that none of the data it contains has ever been changed.

A Blockchain ledger database is described as being distributed because there are multiple copies kept on different nodes. The multiple copies are updated with new data blocks in a coordinated way that ensures that they remain consistent with each other, using a consensus algorithm of which there are different types.

In summary, the content and sequence of the data blocks in a Blockchain are determined by a consensus of the participating nodes and each block contains a fingerprint (hash) that can be used to recursively verify the content of all previous blocks.

2.2.2 It writes transactions

Each block of data written to a Blockchain ledger contains at least one record of a transaction, although most blocks contain many records of transactions. A simple example of a transaction would be "debit one coin from account A, and credit one coin to account B", although many other kinds of transactions are possible. Some Blockchains support a limited sub-set of transactions (operations or algorithms) such as this simple double-entry bookkeeping operation. Some Blockchains support a much wider set of transactions covering any solvable algorithm (i.e. a Turing-complete computer programming language[4]). These types of transactions are variously called smart contracts, chaincode, transaction families, or other equivalent terms. In summary, all Blockchains support a variety of data operations on their chains, but not all Blockchains support Turing-complete transaction languages.

2.2.3 These transactions are written to a cryptographically signed block

Blockchains implement two kinds of cryptographic technology: hash functions and

[4] A Turing complete programming language can solve any mathematical problem computationally (if you know how to program it). In general, this means it must be able to implement a conditional repetition or conditional jump (while, for, if and goto) and include a way to read and write to some storage mechanism (variables).

public/private key cryptography. Hash functions are used to construct the fundamental proof that links each block to the rest of the chain before it. Hashes, in a different context, can also be used to provide proof of validity for data that is referenced by blocks and they are used in Proof-of-Work consensus algorithms where a hash with a specified number of leading zeros serves as the "difficult problem" that nodes must solve in order to reach consensus.

Public/private key cryptography is used for identifying parties to a transaction and controlling access to data. An analogy is email, where the public key is your email address which others can use to send messages to you, and the private key is your password which gives access to the private material, which is your messages. So, on a Blockchain, a public key can be used, for example, to implement a transaction that sends a document or a payment to a party, but only the party with the private key can access those documents or payments after they are sent.

A critical aspect to keep in mind when designing Blockchains is the management and security of users' private keys, given that there is no centralized management system. If a user loses their private key, all assets related to that key are lost as well, unless a way to recover that key has been put in place. On the other hand, the classic solution to this problem, the creation of a centralized key management system, would most likely create a single point of failure, and such a system would no longer meet the basic principles that a distributed, decentralized model is based upon. As a result, creative solutions are needed.

2.2.4 Independent nodes must verify the cryptographically signed block

There are various consensus algorithms used by different Blockchain systems. For example, Bitcoin, a public Blockchain, uses Proof of Work algorithms which allow data miners to recover the cost of computationally expensive work in exchange for transaction fees and these fees also provide a way to initially put electronic coins into circulation. Permissioned ledgers use a consortium of nodes to agree on the output of a consensus process—which is generally cheaper and faster than Bitcoin's Proof of Work. All consensus processes require a mechanism to settle disputes, or uncertainty, about which block should be written next. Most of these mechanisms are based upon using the block, which is agreed upon by more than 50 percent of the nodes. A more detailed description of public and permissioned Blockchains can be found below.

The nature of the consensus mechanism determines some key characteristics of a Blockchain system. For example, mining the creation of blocks has deliberately been made expensive. This protects the Blockchain by making the cost of capturing more than 50 percent of the nodes—the number needed to approve a block, and thus to manipulate the Blockchain—prohibitively expensive. To compensate for this cost, miners are rewarded both an amount of Bitcoin for each block they create and fees for each transaction written to the Blockchain.[5] Each block has a size limit and transaction costs are determined on a free-market basis, so the more transactions are requested, the more the price increases for each transaction. This is necessary for the Bitcoin economic operating model, which seeks to obtain an honest consensus in an unregulated market of potentially anonymous and economically rational operators (i.e. operators who might, being anonymous, and having no costs for doing so, steal assets). As an additional incentive, if a node/miner does not accept the block voted on by over 50 percent of the other nodes, it is effectively kicked off the Blockchain, thus losing the possibility of earning future Bitcoins and transaction fees. Consequently, Bitcoin has extremely low bandwidth due to the cost of

[5] Bitcoin is designed so that, over time, mining rewards are reduced with the objective of eventually having all mining rewards come from transaction fees.

generating blocks with transactions taking on average 10 minutes to be confirmed. In addition, its very large number of nodes and users, generating large amounts of data, together with its block-size limits, makes storing data on the Bitcoin Blockchain expensive as well as being inefficient.

Given the duplication of information across all nodes on a Blockchain, it is generally inefficient to store significant amounts of data on Blockchains. Bitcoin still supports many billions of US dollars' worth of Bitcoin and other high-value transactions, but its speed and volume limitations make it unsuitable for many enterprise applications and the direct implementation of small-value transactions.

Permissioned ledgers strike a different balance between bandwidth, capacity and trustworthiness. For example, because they have more control over who participates, permissioned ledgers can use other consensus mechanisms—even if some of them are somewhat less robust than the Proof of Work used by Bitcoin. For example, there are consensus mechanisms based on the amount a node has invested in a network (called Proof of Stake), or where a consensus by a subset of nodes is verified by a larger group.

In addition, there is a great deal of research by foundations, universities and companies looking to identify and test other consensus mechanisms. Some of these alternative consensus mechanisms will allow ledgers to support hundreds or even thousands of transactions per second, rather than an average of one new block per 10 minutes, as with Bitcoin. There is also research going into the maintenance and accessing of data on petabyte-scale (i.e. truly gigantic) databases.

2.2.5 The block is written to the ledger after it is verified

When consensus is reached, which includes agreeing that a block contains legitimate data, and that it is the block that should be written next, each node adds the agreed block to their local copy of the ledger. In this way, all nodes maintain an identical copy of the ledger each time a block is written. This is proven by the next block to be written, because it will contain a hash of the block before it.

2.2.6 The new block is linked to previous blocks—creating immutability

Remembering that a hash is a one-way function that produces a unique fingerprint of selected data and also noting that a hash function produces a fixed-size fingerprint regardless of the amount of data being hashed it can be assumed that as a result, there is no way to know from looking at the hash if the data was a single, small document or a database holding many billions of records.

Each block in a Blockchain contains some transaction data plus the hash of the previous block, which is always the same size no matter how much data it represents. Given a consensus that this new block forms part of the chain, it is possible to verify the previous block from its hash—and from the previous block, the block before it, and so on all the way to the first or genesis block in the chain. The hash of the previous block is said to be anchored in the subsequent block.

Tampering with the contents of any block in the chain will change the hash of that block, which will change the hash of the block after it, and so on for every subsequent block in the chain. If this occurs then the tampering is easily detectable by any node, and the consensus algorithms will prevent new blocks from being written to the chain because the hashes don't match.

This characteristic is the origin of the word "chain" in "Blockchain" because each block is anchored to the previous block and proves the existence of all the data it references going back to the first "block" of data in the "chain".

2.2.7 Some time is needed before the existence of a new block can be "confirmed"

Each node creates new blocks based on the information available to it at a specific point of time. Because of network latency, whereby nodes may receive information at different times, this can result in different nodes publishing different blocks at the same time, without this being caused by errors or inaccurate data. This can, temporarily, result in differing versions of a Blockchain ledger existing which is called a "ledger conflict". For example, in a Blockchain-based digital currency system, the same money could show as spent and unspent, depending on at which Blockchain ledger version we were looking. However, these conflicts are resolved automatically as the longest chain available becomes the official Blockchain. Any data that was in a shorter block and is not included in the longest, selected block, is returned to the unused transaction pool to be included in a later block.

Because of the possibility of ledger conflicts resulting in a processed transaction being returned to the unused transaction pool (because the block it was included in turned out not to be the longest one), a concept called confirmations is deployed for users to measure the probability of a transaction being permanently present in a Blockchain. A transaction's confirmation is the number of blocks present after the block where the transaction is found. For example, in the Bitcoin network 6 confirmations are considered very safe as it would be extremely difficult for so many blocks to be rejected due to ledger conflicts or for a forking to happen before the block containing the said transaction if it is followed by six new valid blocks. The number of confirmations considered to ensure that a transaction is safe is different for different protocols based on the block creation time and whether the Blockchain is permissioned or permission less.

2.3 Blockchain types

2.3.1 Public ledgers

Public ledgers can be read by anyone. They are also permissionless because anyone can participate and utilize the consensus mechanisms without needing permission to do so and without depending on a regulator to enforce acceptable behavior. Bitcoin, Ether and a range of other cryptocurrencies with market capitalizations going up to 59 billion United States dollars[6] operate this way, allowing any transaction that is logically valid between any parties on the network, including anonymous and pseudonymous parties.

One of the fears about Blockchain technology is that, if a malevolent actor were to control a majority of the nodes, then they could decide to reach a consensus in contradiction of the interests of other stakeholders. This threat is called a Sybil, or 51 per cent attack in cryptographic literature. A successful Sybil attack on a public Blockchain cryptocurrency could result in a catastrophic redistribution of assets and/or double spending. Other possible consequences include:

- Not recording transactions from specific users, nodes, suppliers or even countries;

[6] https://bitinfocharts.com/ (as of February 2020).

- Creating an alternate chain that is longer than the original chain which nodes will switch to because they will automatically think that the longer chain has had the most verification work done to it; and
- Disrupting how and where information is distributed by thwarting or not transmitting blocks to other nodes.

Public Blockchain ledgers are designed to operate according to rules that do not require governance or regulatory mechanisms to intervene in order to prevent antisocial transactions, because those mechanisms might themselves be exploited for antisocial outcomes—for example, if a governance mechanism were to be hacked by a third party or abused by a regulator. Public Blockchains operate with absolute assurance in their algorithms and are designed to avoid any need to trust any counterparties. Public Blockchains are sometimes referred to as being trustless.

Public ledgers typically compromise other aspects of performance in order to achieve a strong resistance to Sybil (51 per cent) attacks. They also rely on the transparency of the public ledger, and on the transparency of the open-source software involved.

Public Blockchain systems, which typically have thousands of users, are difficult to manage and maintain because of the need for consensus (being 51 per cent or more of users) in order to make changes. This can also be true of permissioned Blockchains, depending upon their governance structure. Within Blockchains, changes are implemented through forks, of which there are two types:

- Soft forks - These represent software changes that do not prevent users from using the changed Blockchain system.
- Hard forks - These are software changes that prevent users who have not adopted the change from using the changed Blockchain system. This requires a decision from users to either upgrade and stay with the main fork or continue without the upgrades and stay on the original path. Users on different hard forks are prevented from interacting with each other, which helps to avoid conflicts between ledgers.

As with all information technology systems, developers are responsible for changes to the underlying software. These developers maintain some level of control over the direction of the Blockchain on which they are working, primarily the power of proposal. For example, a group of developers may recommend a change in the hashing algorithm or changes to the block structure. In public and some permissioned Blockchains, these proposed changes will then require a majority of the nodes (validators) on the network to agree and require a hard fork. It is very difficult to obtain the permission of a majority of nodes for a hard fork, resulting in an underlying difficulty in maintaining and updating Blockchains. It is therefore important to look at the governance mechanisms in place when selecting a Blockchain and at the trade-offs involved between stability and the ability to evolve over time.

2.3.2 Permissioned/Private ledgers

Like conventional databases, the contents of a private Blockchain ledger may be a guarded secret that is only available to selected users, and node operators, through a role-based access control mechanism. Some examples of access control include restricting some users so they can only: write to the Blockchain under specific, defined instances; perform certain queries; and/or interrogate a limited set of data. Various roles that could be specified include: miner, validator, administrator and auditor. Likewise, a private Blockchain can be set up so that everyone can read the data, but only designated nodes can add new data. This can also be done

on a public database using smart contracts, however, authorities might be concerned that there is a greater security risk since anyone who wants to could see (and try to hack) the smart contracts in question. Such a database might be desirable for official records such as land deeds, licenses, certificates, etc. Unlike a traditional database, a private Blockchain ledger is immutable (i.e. cannot be updated) and transactions are verified by a consensus mechanism that is established by the network operators.

Private ledger technology is typically applied in enterprise use cases where immutable transactions are required that can be verified by a closed community of nodes. These nodes may be independent of parties to the transactions on the Blockchain and may be subject to oversight and governance that is not possible, or considered desirable, in a permissionless, public Blockchain system.

Permissioned ledgers operate with a different threat model to the public ledgers. The operators of permissioned ledger nodes are not anonymous; they are subject to some kind of governance controls and are collectively trusted by the users. Antisocial behavior by a node or participant could result in that party being evicted from the network and their transactions blocked. The expectation of users of a permissioned ledger is that the operators will intervene in antisocial behavior but not commit antisocial behavior themselves.

On permissioned ledgers, the level of security, and the confidence that users can have in the immutability of the data, varies depending upon the rules established for that permissioned ledger, including its consensus mechanism. Permissioned ledgers can also create a false sense of security because only known participants are allowed to maintain nodes and participate in verification. At the same time, even known participants can become untrustworthy upon being hacked; permissioned ledgers with single points of failure are also vulnerable should anything happen to that single point, and poorly tested smart contracts can create bad consequences for participants—even if no harm was originally intended—especially if the Blockchain network does not have adequate controls in place.

2.3.3 Accessing external (off-chain) data

Because of space limitations and the cost of storing data directly on a Blockchain, it is often more efficient to include in a Blockchain only a link to the appropriate data and a calculation (i.e., hash) in order to prove that the content of the data has not been changed. Linked data uses hashes and may also use digital identifiers and public key cryptography. This will work as long as the rules are used consistently across the Blockchain and the system(s) the linked data is stored on. This implies that the more standardized the use of public-key cryptography, the easier and less expensive it will be to link data—and the same can be said for the semantics defining the data. The use of common semantics (i.e. data definitions) greatly simplifies the job of interpreting data from different sources and the UN/CEFACT Core Components Library plus its reference data models (SCRDM and MMT RDM)[7] is a very complete source of globally harmonized trade-related semantics and their relationship to each other which would be beneficial to be reused in this context.

Blockchain references (also known as anchors) which point to external data can also contain information, such as hashes, to be used to prove the existence or unchanged nature of the data referenced. This is different from a hyperlink or Uniform Resource Locator (URL) on the Internet where the information at an address may change depending on the time it is accessed.

[7] See for example the Buy-Ship-Pay Reference Data Model Business Requirement Specification: http://www.unece.org/fileadmin/DAM/cefact/brs/BuyShipPay_BRS_v1.0.pdf (as of February 2020)

For example, if you click on a link on a television news website, which changes on a regular basis as it is updated, what you find tomorrow may be different from what you find today. With a Blockchain anchor data link, the information in the Blockchain is a guarantee (proof of existence) that the data being pointed to has not been changed.

The location for data found in a Blockchain anchor data link is identified with a Universal Resource Identifier (URI). The URI can be registered as part of a Blockchain transaction or referenced in (or used by / created by) a Blockchain smart contract. The URI may point to data in public/open distributed data systems such as those located on the Internet and accessed using standard protocols (i.e. FTP, HTTP, HTTPS, or IPFS[8]) or it may reference data in private databases that are selectively available to permissioned ledger users. With private off-chain or cross-chain references, it is possible for network operators to know that some data exists, but to have their access limited by additional controls (for example, with a technique called zero-knowledge proofs). This can be very interesting from a privacy standpoint as it is possible to access data in order to know that, for example, someone is over 21 without giving their age, or that they live in London, without giving their address.

These sources of external data are sometimes called oracles which are described in more detail below.

2.3.4 Interledger: implementing transactions across Blockchains

Today, many different Blockchains exist and in the future, there will be even more. Already, a supply chain transaction, from beginning to end, could involve writing or reading data from multiple Blockchains. For example, an exporter might need to use a bank Blockchain, one Blockchain per transportation mode, a Blockchain used for traceability by the importer and one or more used by regulatory authorities. In addition, it is easy to foresee an increasing need for the exchange of information and the implementation of transactions across Blockchains (i.e. interledger). As described in the previous section, Blockchains have the possibility to reference data outside of that Blockchain. This includes data in other Blockchains as well as from non-Blockchain systems.

Interledger (Blockchain-spanning) transactions use cross-chain references and smart contracts (see description below) on both Blockchains that interact in a coordinated way. This is an emerging field, however there are mechanisms that already exist and are in use. These are primarily focused on exchanging value (i.e. digital assets) between ledgers, for example Ripple Interledger and the Lightning Network.

2.4 Other things you should know

2.4.1 Smart contracts

Smart contracts are self-executing computer programs that encode business logic. They execute when pre-defined conditions are met. In other words, their execution is not launched, or at least not directly, by human intervention. These can be as simple as “transfer specific amount of asset from account X to account Y.” Smart contracts are based on the conditional If-This-Then-That (IFTTT) model where some activity is automatically executed when certain conditions are met. These conditions can be a certain period of time, a specific value (for example the

[8] FTP = File Transfer Protocol, HTTP = HyperText Transfer Protocol, HTTPS = HyperText Transfer Protocol and IPFS = InterPlanetary File System. For not too technical explanation of IPFS see https://medium.com/wolverineBlockchain/what-is-ipfs-b83277597da5 (as of February 2020).

price of some asset, such as stock) or a specific event such as the delivery of ordered goods to a customer.

Smart contracts offer several benefits:

- Improved security and predictability because they eliminate the human element and potential contract breaches intentionally or unintentionally caused by human action;
- Transparency because the code of a smart contract can be public and visible, anyone can review it and predict how transactions under a given contract will behave; and
- Simplified programming for systems that need to accept, match and then act upon data from a wide variety of parties, many of whom may be unknown.

One example of a smart contract explained in everyday language could be:

- **Precondition**: when I deposit a certain amount of cryptocurrency and the other party deposits a certain amount of FIAT currency;
- **Condition**: if the amounts are equal according to the current exchange ratio; or
- **Action**: then currencies are exchanged between involved parties' accounts.

Another example could be when renting a car; the rental agency could require that an advance currency deposit be made on a Blockchain. The amount would then only be released to the rental agency after the renter confirms that he/she received the car's keys. This way smart contracts can prevent scams based on advance payments and create an additional layer of security.

Because smart contracts are basically small programs, they can be developed and customized for many situations, making them potentially powerful tools for business.

At the same time, lawyers, programmers, visionaries and regulators are having heated debates surrounding the question of whether the code can be law.[9,10] Specifically, the debate centres on whether people could rely exclusively on the authoritative execution of a smart contract to enforce agreements without involving previous paper-based legal engagements. For example, there are trials which have illustrated a templating tool to generate smart contract code based on specific keywords and jargon.[11] However, in all these cases, trustworthiness and/or enforceability must be present. Furthermore, questions arise on who, where and what audits and enforces Blockchain trades placed between disparate national and international jurisdictions? This discussion is abstract and complex because it requires reconciling both legal jargon and the verification of syntactic and semantic information - a topic usually reserved to the fields of computation and mathematics.

2.4.2 Oracles

The primary function of oracles is to provide secure and trustworthy data to a Blockchain smart contract. Smart contracts then look at this data to see if it meets the conditions defined in the smart contract's code and, if this is the case, the contract automatically executes.

The key words here are "secure and trustworthy data". Blockchains cannot, and should not, store large amounts of data, so information needs to be submitted to the Blockchain via an

[9] del Castillo, M. (2016, 06 28). *The Inventor of the Merkle Tree Wants DAOs to Rule the World*. Coindesk: https://www.coindesk.com/ralph-merkle-is-back-and-he-wants-to-resurrect-daos/ (as of February 2020)
[10] Kolber, A. (2016, 10 28). *Code is not the Law: Blockchain Contracts and Artificial Intelligence*. Youtube: https://www.youtube.com/watch?v=MBKjpRuCvNE (as of February 2020)
[11] R3. (2016, 04 18). Smart contract templates. *Barclays' Smart Contract Templates*. London, London, UK.

oracle. This makes the oracle (just like user interfaces) a weak point in the security and integrity of a Blockchain. It is also where the old adage of "garbage in—garbage out" comes into play (although in the case of Blockchains it may be garbage in—garbage forever). Therefore, it is very important in Blockchain-based applications to carefully design the process for obtaining the data used by oracles as well as their interfaces with Blockchains to ensure the quality and integrity of the data and related processes.

2.4.3 Tokens and Digital Twins

Tokens are a consistent set of logic contained in a small smart contract. They function on top of another Blockchain, although not all Blockchains allow them. Tokens must be programmed according to the standard for tokens on their Blockchain. For example, tokens used on top of Ethereum (who invented tokens) are programmed using a standard called ERC-20[12]. There are different types of tokens, including currency tokens which are not discussed here[13]. Other tokens provide access to a product or service. Each token within a defined token type is worth the same amount as all other tokens of that type, so they are the closest possible thing to a standardized digital asset (other than a cryptocurrency). Tokens can be defined to represent (i.e., act as a proxy for) a standard unit of something which can then be traded (such as bonds, energy, oil, or a fraction of an artwork or building, etc.). In the case of fungible products such as oil or energy, access to the physical good may be based on an agreement external to the Blockchain or be done via an automated process that is controlled by is smart contract also on the Blockchain (for example, a process that sends energy to a home). The cryptographic techniques embedded in the network, help to avoid the double-spending of such digital assets, protecting users from bad actors that intend to defraud the system in order to obtain an unfair advantage.

A digital twin in Blockchain represents an individual product and allows the tracing of transactions that involve that product. The key to a good "digital twin" is being able to create a link between a product and a digital identifier that is verifiable and cost effective. Some products have "fingerprints" such as the fractal signatures of diamonds or another unique pattern, much like biometric data, which can be registered on a Blockchain and used for identification of individual products. These are the easiest physical products to create digital twins for and thereby accurately trace. Other products need to be marked with codes, for example with QR codes, RFID tags or embedded markings which are then read at various points along a supply chain or other process. These solutions have varying costs and levels of reliability, depending upon the technology and the system within which they are used. At the same time, these solutions are more reliable, and can be more cost effective, than most alternatives. There is also significant research being invested in finding the most reliable and cost effective possible digital twins for use with different products for Blockchain supported traceability.

Blockchains trace a digital twin by creating a "token" based on the digital information that constitutes the twin. This token is then "exchanged" each time a transaction/event using the digital twin is registered and these transactions can be traced back all the way to the creation of the token (just as all of the transactions for an individual crypto coin can be traced).

[12] https://cointelegraph.com/explained/erc-20-tokens-explained (as of February 2020).
[13] For further explanation of different tokens, the reader can refer to https://www.bitdegree.org/tutorials/token-vs-coin/ (as of February 2020).

2.4.4 The Internet of Things and Blockchain

The Internet of Things (IoT) refers to sensors and small computing devices or chips embedded in physical objects (assets) which communicate via the Internet. These communications can be with one another, with larger computers and computing systems and even with humans—for example modern security systems that notify a homeowner if they detect motion in the owner's home and connect the owner with the video camera in his or her living room.

IoT devices can collect a wide variety of data. Examples of information related to trade and transport communicated by IoT devices include truck or maritime container location and movements via GPS coordinates; the opening and closing of container doors; container temperatures; external shocks to containers/pallets/products; and, for very expensive items such as some pharmaceuticals or luxury goods, the tracking or identification of individual packages or products.

IoT devices can be a useful way to capture data that is analyzed by other systems that then supply the analyses' results to a Blockchain (i.e. systems that are Blockchain oracles), or they can be oracles themselves by providing data directly to a Blockchain. Nonetheless, IoT devices tend not to be used directly as oracles because of security concerns, and because systems that are connected to tens of thousands of IoT devices might be overwhelmed by data volumes. Also, writing constant data readings to a Blockchain could be expensive for those networks where every time you write data you have to pay a small amount. As a result, data from IoT devices is often filtered so that only data which goes outside of defined ranges is communicated, or the data is communicated as a total set of readings at the end of a process.

A classic example of the use of IoT data by a Blockchain is for monitoring temperature-sensitive goods (i.e. fruit that is supposed to be kept at between 4 and 15 degrees Celsius during shipment) for insurance purposes. During transportation an IoT device in a cargo container records that the fruit was kept at 0 degrees Celsius for 2 entire days. This information is given to the smart contract which notifies the insurance company that a payment should be made to the exporter to compensate for the goods destroyed by the excessively low temperature and that payment is automatically made by the smart contract without any further intervention by either the importer, the exporter or the transport company. This significantly decreases the cost for insurance companies of processing claims because they do not have to reconcile information submitted by the shipper/exporter with the insurance policy, evaluate the truth of the insurance claim (the IoT data provided the proof) and then request payment. In addition, it reduces the costs for the shipper/exporter as they do not have to undertake any further documentation of the problem which occurred, and they receive their insurance payment more quickly.

2.4.5 Interoperability, data interpretation & standards

Interoperability is fundamental to digital freedom because it helps to ensures that the parties involved in the collection and use of information cannot abuse their position. The International Telecommunications Union's (ITU's) definition of interoperability is the "ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged," a definition which is also used by the ISO/IEC standard 17788:2014.

The digitalization within the systems of organisations has led to profound changes in the way in which public administrations can provide services to a citizen or a company as well as methods for regulating and collecting taxes. However, many of these services, and/or the

ability to take full advantage of them, depend upon interoperability between systems and networks, which includes Blockchain networks.

Interoperability should also be understood as a concept that supports implementation of the principle of free movement of goods and, services in the digital world. Interoperability is also essential as a tool to regulate and support competition in the digital world. This is because the lack of interoperability creates technical boundaries which, for example, the European Commission has long sought to eliminate in order to achieve the EU internal market (White Paper on completing the internal market, 14 June 1985, COM (85) 310 final[14]).

The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) has an important contribution to make to interoperability through its semantic standards (i.e. its Core Components Library and reference data models) and its data exchange choreography modelling work.[15]

[14] https://eur-lex.europa.eu/procedure/EN/116494 (as of February 2020).
[15] See for example (as of February 2020): http://www.unece.org/uncefact/mainstandards.html

3 Implementing Blockchain for trade facilitation

In 2018, a survey[16] found that "65 percent of responding enterprises with over 10,000 employees are considering or actively engaged in Blockchain deployment. This marks a significant rise from 2017, when the corresponding figure was 54 percent."

This survey also found that "nearly a quarter of companies considering deploying Blockchain had moved beyond proof of concept into trials and commercial rollouts, with dramatic diversification in use cases over the past year. Only 15 percent of proposed deployments were now related to payments (compared with 34 percent last year), with significant interest in opportunities across diverse fields including logistics, authentication and smart contracts."

Professionals experienced in this field have identified common patterns fuelling the success and business value of Blockchain experimentation. In order to turn a Blockchain first project into a robust business tool delivering tangible value, it is worth focusing on the following points:

a) **Find a business problem to be solved, that cannot be more efficiently solved with other technologies**
   This may sound obvious, but the only way for a business to really get to grips with Blockchain is for the project to be sponsored by business users in an organization who have a problem, are unhappy with how things work today and can see how Blockchain might help them to improve.

b) **Detect an identifiable business network, with participants, assets and transactions**
   Business never exists in isolation. Business networks generate wealth by transferring assets between participants using transactions. Within this framework, a Blockchain-based approach with a shared replicated ledger can help deliver tangible value in terms of process optimization/automation (e.g. lowering the reconciliation/settlement processes) and adding value to these network ecosystems.

c) **Satisfy a need for trustworthiness (i.e. consensus, immutability, finality or provenance)**
   Blockchain business value corresponds to the level of increased trustworthiness it can engender among participants through consensus, immutability, finality, data reconciliation and provenance-tracking. Indeed, the more important trustworthiness is to the use case, the more value Blockchain could potentially add.

To assist those who are evaluating Blockchain implementation in their organization, the remainder of this section goes into greater depth on, "When to use Blockchains and when not to" and "Implementation challenges".

3.1 When to use Blockchains and when not to

The decision to implement Blockchain, whether in the public or private sector, should be a business decision based on the ability of the technology to support one of the following:

- New and improved services;
- Faster processes and/or implementation; or

[16] https://www.juniperresearch.com/press/press-releases/nearly-two-thirds-of-large-enterprises-currently (as of February 2020).

- More economical processes and/or implementation.

Having identified a business process that is a candidate for a Blockchain application, it may be useful to apply the decision tree in the diagram below at the next level of analysis.

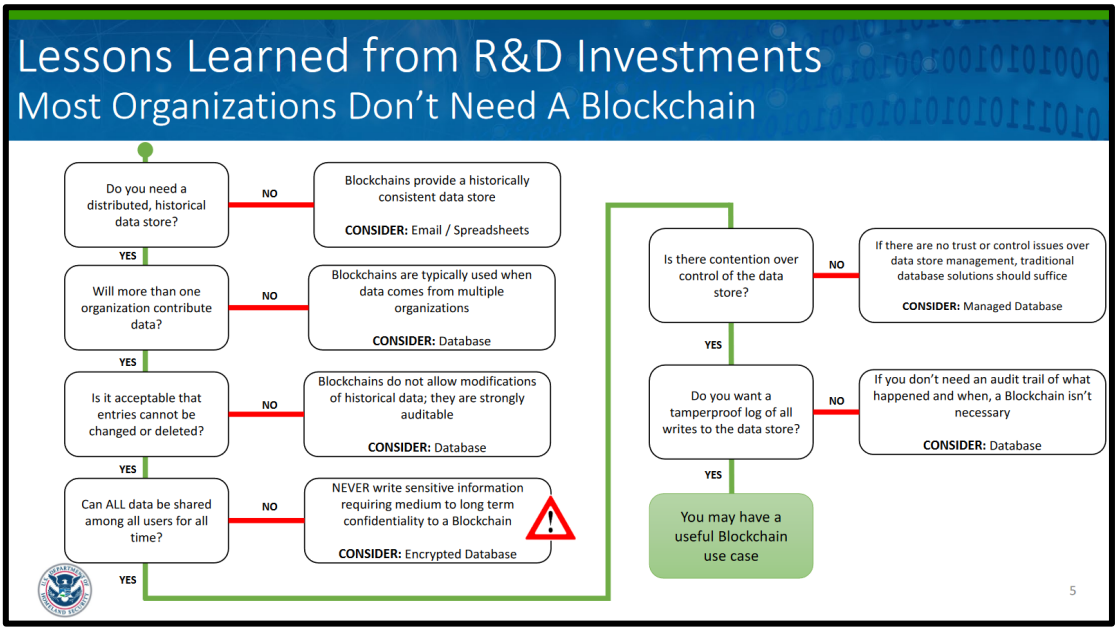

Figure 3.1: When to use Blockchain[17]

If only one of the answers in Figure 1 is "no", there may still be a case for the use of Blockchain—for example, if a tamper-proof log is a key asset or those with read access do not trust those with write access. In addition, in some cases a database solution could do the job well, but a Blockchain solution may be quicker and/or cheaper to implement, so it is important to also look at time and cost.

It is important to remember that the use of Blockchains implies a type of authentication and not all transactions require such a high level of reliability. The UNCITRAL "Model Law on Electronic Commerce" of 1996 underlines that the chosen method of authentication should be "as reliable as appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement."

The implied computational cost of this technology should also be considered. Even when such technology is offered free of charge, there is a cost which will be borne later in the supply chain which may, depending on a variety of factors, increase the final cost to the consumer, so the benefits and costs need to be carefully analyzed. It is also important to ensure that the use of Blockchain technology does not create barriers for Micro, Small and Medium-sized Enterprises or developing/transition economies.

Today, while many organizations have concluded that there is a potential for process improvement using Blockchain in their industry, they are not moving into immediate implementation—but rather are taking an exploratory approach. If there is no existing Blockchain application that an organization can use "off the shelf", then this is probably the

[17] Mr. Anil John, Technical Director, U.S. Department of Homeland Security, Science and Technology, "Beyond Blockchain Basics", at the Annual Computer Security Applications Conference, 5 December 2018, https://www.acsac.org/2018/openconf/modules/request.php?module=oc_program&action=page.php&id=42 (as of February 2020).

best approach because of the newness of Blockchain technology and because it remains untested in the context of many processes. In addition, organizations sometimes want to test Blockchain approaches internally, to gain experience and identify any needed internal procedural or structural changes, before deciding whether or not to join one of an increasing number of sector-wide Blockchain platforms that are being developed and which offer "off the shelf" solutions or promise to do so in the near future.

An exploratory approach typically consists of implementing a proof of concept (PoC) project and, if that is successful, looking at how to implement a larger pilot project and then an organization-wide roll out of the application.

Even if unsuccessful, a PoC can help a company to better understand the uses and pitfalls of the technology and its implementation, which will help them to better evaluate its eventual use in other areas in the future.

If, after going through the above analysis, an organization decides to go forward with a PoC and eventually implementation, the next step is to decide which Blockchain to use. Not all Blockchains are equal. They vary depending upon the consensus method used, the cryptography implemented, the size of the network and whether or not it is a private or permissioned Blockchain (see earlier descriptions). Some of the key characteristics to look at are:

- **Vulnerability**: to hacking and other system failures;
- **Robustness**: how well they handle problems such as flawed code or being hacked;
- **Cost**: transaction cost, sometimes referred to as gas;
- **Speed and ability to scale up**: to large transaction volumes; and
- **Degree of Privacy**: no anonymity vs pseudo anonymity vs total anonymity and conformity with privacy legislation.

In order to evaluate these characteristics, it is important to first determine the specific needs and concerns of an organization in the above areas. Then, in the light of these needs, an organization can evaluate existing Blockchain options. For example, the need to protect against hacking (vulnerability) is probably less if an organization is tracing cucumbers than if it's tracing diamonds; on the other hand, there would probably be much larger volumes of cucumbers to trace than diamonds, which makes scalability important and the low value of cucumbers increases dramatically the need to focus on costs.

As a final note, be sure when doing this last step to use information that is less than twelve months old. This is a rapidly developing sector with many people working on research to solve specific issues in different Blockchain models. As a result, what was true two years or even eighteen months ago, may not be true today. Consulting with programmers that have accumulated experience with Blockchain implementations can also be very useful as there are often work arounds to different issues, especially for public Blockchains where the contributing community of experts is larger.

3.2 Implementation challenges

3.2.1 Alignment of stakeholder interests

The strength (and therefore the value) of a Blockchain is determined by the data registered on the Blockchain in which users have the lowest level of confidence, just like the strength of a chain is determined by its weakest link.

There are many reasons to doubt the veracity of information captured in a Blockchain where the party entering it has reason to enter inaccurate or fraudulent data. Consider a farmer who has been selling four times more volume of an organic crop than his farm can actually produce. Under the current process he may be able to purchase produce from uncertified farms in order to resell it at the premium he has negotiated with a client. In 2017 buyers only had that farmer's word for it, albeit backed by certification or independent audits, the reliability of which has been questioned by some. At present, cross-referencing that farm's total output to all customers is not a cost-effective proposition for any individual customer. Using the automatic reconciliation capabilities of Blockchain technology, and appropriately designed systems, within a few years it will be possible for a farm or production facility's total shipped output across all of its customers to be readily visible to approved users and quickly cross-referenced with the production capacity of the accredited unit. As a result, suppliers who sell more than they can physically produce will risk being exposed.

Suppliers who are currently playing a fair game will likely show significantly less resistance to participating in such a fully transparent system, leaving implementation costs aside for the moment (see Costs below). Those who have been profiting unethically in the past may be harder to align with such new supply chain requirements.

Banks are major players in supply chains and will need to be brought along to ensure that they can continue to support their clients' businesses. Fortunately, banks are among the earliest adopters and most aggressive investigators of Blockchain applications for international trade and payment management. Some crypto currencies have been designed specifically for this purpose.

Blockchain systems are often envisaged to provide services upon which other, more complex, services can be developed. These range from the tracing of maritime containers to the provision of reliable information upon which insurance contracts can be based to the clearing of letters of credit. A number of these services are only workable, financially and even practically, if they are undertaken by a consortium that provides sufficient economies of scale. In these cases, traditional competitors need to learn to work together in new ways, based on the principles of, competitive cooperation sometimes referred to as coopetition. In addition to requiring new mindsets and adjustments to corporate culture, this also requires careful attention to legal issues related to anti-competition legislation in each partners' jurisdiction(s).

3.2.2 Standards

Blockchain has ignited the imagination of thousands of people for whom it offers the potential to solve many problems. Many businesses are actively pursuing pilots and proofs of concept (PoCs) for applications that would allow them to reap the benefits from "lowest hanging fruit" solutions.

But what happens when the PoCs are implemented in the real world? How will the different Blockchain implementations talk to one another to transfer their data? For example, how can supply chain applications communicate invoice information to banks and banks communicate payment information to supply chain applications? Without adherence to standards such as those suggested in this paper, each Blockchain system will thrive in isolation but will run the risk of meeting with frustration, confusion and a large erosion of the deliverable value should it need to interact with external agencies and/or other Blockchains.

Entities seeking to implement Blockchain applications should therefore plan to exist in a broader Blockchain ecosystem regardless of whether or not the initial implementation can be fully coded as only an in-house application.

A key term in supply chain management is the fluidity of information. This refers to the ability of data to flow quickly between parties without alteration. Traditionally this has been achieved in two ways: by reducing the number of parties involved in order to reduce the number of data transfers required; and by adhering to standard protocols and data definitions and formats. For example, use of the data definitions developed by UN/CEFACT could support such information fluidity and the use of UN/CEFACT's standardized data exchange processes and reference data models[18] could support the design of appropriate systems and interfaces. The successful adoption of robust Blockchain standards could have the effect of making the number of parties involved irrelevant because the opportunity to corrupt it would be reduced to zero.

3.2.3 Data integrity from source – e.g. traceability

Similar to the alignment issues noted above and the cost issues mentioned below, the trustworthiness of the information carried by a Blockchain depends on verified inputs occurring as early in the chain as possible. Therefore, it is important in the design of Blockchain systems to focus on when and how data is to be verified. In some cases, this may require the registration on the Blockchain of "certifications" (for example for organic farming) that can be checked against the identity of the supplier or against the goods.

In supply chains where value is added through aggregated production processes such as furniture manufacture, food & beverage production, etc. each raw input would ideally be verified and then captured on the Blockchain prior to its arrival at the production facility. Failure to do so will limit the verifiable claims that manufacturers can make regarding the finished product. We can, therefore, expect that consumer demands/expectations will evolve and drive the need for measures to ensure accurate data inputs to Blockchain systems as far up the supply chain as possible.

3.2.4 Data collection

Data collection needs to be automated in order to maximize the efficiencies that can be achieved. Although the technology to achieve this already exists today (RFID, QR Codes and respective scanners as well as IoT sensors), there have been implementation challenges with accurate or incomplete readings when they are deployed at scale. These issues will have to be addressed to ensure 100 percent accuracy at each stage in order to support full reliance on the data that the Blockchain collects. Any discrepancies in accuracy will undermine the usefulness of the system and therefore the adoption of Blockchain technology.

3.2.5 Anomaly management

The strength of a Blockchain is its un-changeability. A weakness of a Blockchain can be its un-changeability. What happens if data is inadvertently entered incorrectly (e.g. a sensor malfunctions)? How can users discern an amended entry[19] with positive intentions from one with malevolent intentions?

The answers to these questions need to be designed into the rules governing a Blockchain system. When doing this, the ability of the network to recognize nodes with the authority to make correcting entries to original data will be critical to prevent hacking.

[18] See for example: http://www.unece.org/uncefact/mainstandards.html (as of February 2020)
[19] The original entry is not changed, it is corrected/amended via a new entry according to rules set out in a smart contract.

3.2.6 Regulation

One of the headline features of Blockchains is the potential for anonymity that they offer. Although anonymity is something that can be engineered into or out of any specific Blockchain, the potential for hiding or obfuscating important information is of concern to governments. Without regulation it is possible for entire economies to operate out of sight, thereby avoiding taxes, fees and financial laws such as those on money-laundering. For example, using crypto-currencies to transfer value across borders could allow for cross-border shipment of goods at lower values attracting lower taxes or tariffs with a secondary payment being made via anonymous crypto-currency to compensate the seller for the true value of the shipment.

Because of these concerns, governments are likely to be slower than commercial entities to embrace Blockchains using cryptocurrencies until clear and enforceable regulations are in place. Other Blockchain systems, such as those designed to support the traceability of products or the veracity of shared information, many of which could support government regulatory objectives, will probably be more welcome.

At the same time, governments are under pressure to establish clear regulatory frameworks for Blockchain systems, especially in the financial sector where there is a great deal of work and research on Blockchain applications.

In order to minimize such frictions, governments will need to be actively engaged in the development of open and international standards to support Blockchain applications. In that way, businesses and governments can evolve in their understanding of the processes and risks at the same time.

Governments that lag behind and create or maintain barriers to the use of technologies, such as Blockchain, that can improve the efficiency and effectiveness of business and government processes risk losing the competitive advantage of their national businesses and eventually the revenue that flows from these businesses. To that end, good businesses and good governments are entirely aligned on the motives for the adoption of Blockchain and should be able to work out their differences when it comes to their competing agendas.

That said, businesses can anticipate many of the likely needs of governments with regard to Blockchain applications (such as meeting Know Your Customer and Anti Money Laundering requirements) and can work towards meeting those without external prompting.

3.2.7 Costs

For some stakeholders the benefits of Blockchain may be indirect at best. In theory, and in aggregate, the total volume of trade may increase[20] based on increased trustworthiness and falling costs due to Blockchain-related efficiencies. However, as a result of the transparency afforded by Blockchains, those businesses that are currently – maybe unwittingly – engaged in the transport of counterfeit goods, conflict minerals or goods produced using forced or child labour may see their volumes fall off. In addition, small and medium-sized enterprises, especially in developing countries, may also be reluctant, or unable, to make the investments needed for participating in trade-related Blockchain networks. Therefore, keeping the cost of implementation low is critical to removing the most obvious barriers to implementation by reluctant or doubtful parties.

[20] For estimates of the World Economic Forum, see https://www.weforum.org/agenda/2018/09/Blockchain-set-to-increase-global-trade-by-1-trillion/ (as of February 2020).

The cost of sensors and computing power is falling to the point where installing the required hardware is unlikely to be a barrier to implementation in most regions. What is more likely to offer an implementation challenge is the provision of reliable, secure Internet connections at all of the required points. What may prove to be equally difficult is the provision of local technological support to maintain it. In some regions, the security required to protect hardware from damage or theft may also disproportionately increase the real costs.

A combination of Wi-Fi, mesh[21], broadband, cellular and satellite communications offers a solution to the communication needs at almost any location on earth. However, the installation and running costs of such solutions in remote areas may not be justifiable under a standard business case. In these instances, local, national, and even multi-national government agency support may be required in order to prevent suppliers from being forced out of or denied entry to markets by their inability to contribute essential information to relevant Blockchains.

Other costs which may accumulate along a Blockchain and/or place an inordinate burden on users such as small farmers (who are the upstream suppliers in many supply chains) include: the costs for certification (needed in many traceability systems), the cost of an Internet connection when none was previously needed (in some countries this can be 20 percent or more of the average person's income), the cost of labelling goods (with QR codes, RFID tags or other markers), and the cost of scanning the goods. In order to ensure their full participation, these costs need to be balanced with benefits for each stakeholder, from the farmer through to and including the customer.

Many Blockchains, including Bitcoin, currently use proof-of-work algorithms, in order to verify blocks of data. These algorithms require a great deal of computational power (and electricity) and the nodes that undertake this work (often referred to as miners) recover the cost of this expensive work through transaction fees and the issuance, by the Blockchain itself, of "awards" (which is how new crypto-coins are put into circulation in these systems). Due to fluctuations in the value of cryptocurrencies and, therefore, of transaction fees, many businesses find proof-of-work Blockchains unsuitable because of the inability to predict costs and/or the simple accumulation of transaction fees in applications that require multiple transactions of low or no inherent value such as in traceability systems). In addition, the large amount of electricity used in proof of work systems has been heavily criticized because of its impact. For this reason, many public Blockchains that use proof-of-work, such as Ethereum, are moving toward the use of other consensus mechanisms for the verification of data blocks.

3.2.8 Securing the Blockchain

The security of Blockchains is typically achieved by having the risks or costs associated with a malicious act far outweigh any likely benefit from its successful execution. Specifically, they seek to make the costs associated with being caught very large and the likelihood of success very low.

In order to achieve this, Bitcoin has become infamous for the amount of energy that it requires to secure and process its transactions. Similar proof-of-work protocols are unlikely to find favour in supply-chain Blockchain implementations given that the environmental and economic costs, as explained previously, are simply too high.

Other protocols such as Proof-of-Stake (POS) are more appropriate in the Blockchains envisaged for most supply-chain applications. Private and semi-private Blockchains are formed

[21] https://computer.howstuffworks.com/how-wireless-mesh-networks-work.htm (as of February 2020).

by groups of businesses, each of whom has a legitimate interest in protecting the validity of the data being handled. POS protocols allow honest actors to keep attackers at bay by making an attack economically unviable at a very low cost to the honest actors.

Blockchain designers will also have to consider the trade-offs between speed and security required for their Blockchains. Individual supply chains will likely move slowly enough to accommodate the long latency (processing delays) that can accompany the highest levels of security protocols. Aggregations of chains into a holistic system for an entire business or group of businesses will potentially introduce a transaction frequency that demands further examination. Designers will need to take into account the maximum latency that the system can handle and engineer in ways to meet increasing data volumes and the tolerance of users for delays.

It is also important that Blockchain designers create future-proofed security solutions for their systems in order to avoid forks[22] and updates to systems that fundamentally change stakeholder experiences once they have been enrolled in the process.

3.2.9 Privacy and liability

Strong permission-based access protocols offer a theoretical level of privacy that should meet the most exacting standards of business and governmental agencies. Any user's access to information within a private Blockchain can be restricted by their permissions. However, as anyone who has worked within a large organization will attest, changing the permissions for access to even privately-held data is not an instantaneous or friction-less process. In order to verify approvals and action changes, several levels of approval may be required, and resources have to be made available, and paid for by someone.

Extrapolate these checks and balances across a supply chain that covers multiple users in multiple organizations, across multiple time zones, speaking multiple languages and you could have an access-to-information nightmare.

While predictable changes in user permissions could possibly be addressed by smart contracts, the infinite variety of requests that may be created by any Blockchain that deals with a large number of users will inevitably lead to the necessity of human interventions.

Even when the process for giving and restricting access to information is solved to the satisfaction of all participants, the issue of liability remains. To whom are appeals made when confidential information is stolen by a malicious actor or shared with an unauthorized user? Who actually owns the data? These are complicated questions that will need to be answered, possibly in law, before Blockchains can capture all the information necessary to unveil the full power of the technology.

[22] A fork occurs when there is a major update to a Blockchain, these may be compatible with the previous version (soft forks) or, if they are not compatible, they become hard forks. Both kinds of forks require a majority consensus of users to be implemented. This becomes complicated, if one group of participants does not agree with the changes so they continue with the original governance and rules while another (majority) group accepts the changes in the update. The result is two Blockchains that fork out from the original at the time of the implementation of the update. As a result, the history of data recorded on each fork is identical until date X (when the fork occurs) and then, after that time, the data registered on each fork is different. This can be very disruptive since transactions cannot be implemented "across" the two forks.

3.2.10 Smart contract coding

As further explained in the second section, in a Blockchain "smart contracts" are self-executing computer programs that encode business logic and execute when pre-defined conditions are met. What sets them apart from other computer programs is that they are copied across hundreds or thousands of Blockchain nodes and cannot be changed (unless originally coded to, for example, branch to another newer program under pre-defined conditions). In order to maximize the efficiencies that could be created using Blockchain technology, it will likely be necessary to deploy smart contracts that perform a range of functions including transfers of ownership (based on payment or performance), the payment of funds and application of rules to transactions such as the rules governing the registration of data (for example, a smart contract can enforce rules which only allow certain data, such as certificates, to be written to the Blockchain by parties with a specific permission level).

There are two main challenges with smart contracts:

- First, smart contracts are still in their infancy and getting accurately coded contracts that mimic real life expectations may be time consuming and even require the reengineering of some processes and the resetting of expectations. It is also important to have smart contracts audited for security flaws as these can provide opportunities for hackers.
- Second, smart contracts for funds transfers require that money is effectively placed in escrow until the smart contract terms are met. Even if operating in a fiat currency, this would likely create significant cashflow issues for some businesses that might not be offset by faster payments by their creditors. Cashflow challenges can be further complicated by the fluctuation of cryptocurrencies during the holding period, unless cryptocurrencies which are pegged to fiat currencies (called stable coins) are used or the values of cryptocurrencies stabilize.

These challenges are not entirely within the control of any Blockchain application and may need to be solved at a macro level before many parties are persuaded to fully embrace Blockchains.

3.2.11 Conclusions: Implementation Challenges

Blockchain-based systems can support more reliable (more "trustworthy") data, traceability of digital goods and physical goods (if good digital twins can be identified) across complex supply chains, and the reconciliation of many complex, related transactions. These support functions are built upon the characteristics of a successful crypto-currency (the original Blockchain application) replacing the currency with data. In other words, crypto-coins (i.e. the data) cannot be copied or falsified, all of the transactions using a "coin" (a data token representing a digital or physical good) can be traced back to its creation, and the balances of all owners of that cryptocurrency (data token) are known at all times.

These features have a wide range of uses. At the same time, it is very difficult and, for most individuals and organizations, impossible, to use Blockchains in isolation. Like other ICT tools such as databases and the Internet, Blockchains need to be embedded into a "system" with user interfaces, interconnections to reliable external data sources and, in many cases, external controls and procedures.

Blockchain features also require that special attention be given to ensuring the quality of data and to designing "exception handling" into a system where data cannot be changed once it is written. Special attention also needs to be given to data privacy and regulatory issues given the

difficulty in making “ex-post” adjustments. This is discussed in more detail under, “Data Security and Regulatory Issues”

The new features provided by Blockchains also come at a cost. This cost is going down as more and more Blockchains and “Blockchain ecosystems” are developed, but they still cost more than many other options, so it is important to look closely at costs when making system design decisions and to carefully weigh the benefits to be gained from using a Blockchain against the costs.

Caveats aside, Blockchain technology provides important opportunities for increasing efficiency and reducing risks through greater information trustworthiness and improved capabilities for tracing information and reconciling transactions.

4 Data security and regulatory issues

4.1 Introduction

Electronic business often involves transactions between parties where there is a need to establish reliability in the exchange and transparency. Blockchain can provide highly trustworthy (i.e. highly tamper-proof) digital transactions. At the same time, the degree of trustworthiness varies between Blockchains depending upon their characteristics. Therefore, this section seeks to develop an understanding of the data-security characteristics of Blockchains.

In addition, while Blockchain networks are designed to be trustworthy once data is registered on them, there is still a need to establish the identity of participants which is a prerequisite for establishing the legality of their Blockchain transactions. This is particularly true of cross-border trade where identity and identification mechanisms may be different in different countries, and a common framework related to Blockchains must be defined and adopted if the resulting records are to be legally accepted by the countries on both sides of the transaction in question.

Laws and regulations and/or the parties using Blockchain data for authentication, often define the level of risk assurance, accuracy, integrity and privacy required for data stored on a Blockchain to be accepted. This drives considerations for data design and mechanisms for authentication, authorization or consent that need to be put in place for the legal recognition of transactions on a Blockchain system. As a result, data security and regulatory issues are closely related and are treated together in this section.

Like other systems, to ensure security within a Blockchain, user roles and access rights must be specified in detail during the system design stage as it may be difficult to change access rights later (for more on access rights, see section 2.3.2 of the whitepaper, Overview of Blockchain in Trade).

Since Blockchains rely extensively on cryptographic techniques, the development of quantum computers[23] will require changes to the cryptographic technologies used in Blockchain systems. Quantum computing will render many existing and often used cryptographic algorithms useless[24]. For example, the United States' National Institute of Standards and Technology produced a report on post-quantum cryptography, which showed that three well-known encryption technologies (Rivest, Shamir and Adelman algorithm [RSA], Digital Signature Algorithm [DSA] and Diffie-Helman) will no longer be secure and the Advanced Encryption Standard (AES) and Secure Hash Algorithm-2 (SHA-2) and SHA-3 standards will require larger key sizes and output to be effective.[25] As a result, developers may want to already consider implementing "post quantum" cryptographic techniques as being developed by a wide range of standards organizations including the IEEE and ISO[26].

This section focuses on various security and legal aspects related to Blockchain that should be kept in mind when designing an application using a Blockchain-based distributed ledger. These include -

[23] Foreseen to be available within the next decade, see https://www.scientificamerican.com/article/how-close-are-we-really-to-building-a-quantum-computer/ (as of February 2020).
[24] https://cointelegraph.com/news/quantum-computing-vs-Blockchain-impact-on-cryptography (as of February 2020).
[25] https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf (as of February 2020).
[26] https://pqcrypto.eu.org/deliverables/d5.2-final.pdf (as of February 2020).

- Identity and Identification
- Authentication and Authorization
- Data Accuracy, Integrity and Time Stamping
- Privacy, Confidentiality, Accessing and Sharing Information
- Legal Aspects Relating to Use of Blockchain

At the same time, it is important to keep in mind that there are many more aspects than those described in this chapter. These include standards, transaction rules, technology assurance and audit trails. All of these may be critical to the cross-border acceptance of exchanged trade documents. The cross-border exchange of legally accepted records may also require the definition of a common technical framework and/or a common governance/design framework.

4.2 Identities and identification

We increasingly need to prove our identity to third parties, each with different authentication assurance requirements. Despite the move towards digital transactions in both the private and public sectors, we continue to rely on physical identity documents (which can be counterfeited with increasing ease) and username-password authentication processes (susceptible to breach given their centralised nature). Consequently, the need for reliable digital identity solutions is increasingly pressing and is critical to enabling inclusion and a digital transformation of society as a whole.

It is estimated that 1.1 billion people live without an officially recognized identity.[27] As a result, they are unable to participate in commerce, financial markets and have no access to services such as healthcare. An accurate and accessible identity system allows for inclusion and participation in global trade.

Blockchain holds promise in this regard and could be used to create and verify digital identities, for individuals and organizations. These identities could be based on one or more indicators, which might include, for example, community endorsements, past transaction histories, and/or biometric data.

There are multiple types of identities that we use today in online and offline transactions. These identities range from

- Social ID's (social media) – No Proof of Identity Guidelines and completely digital
- Private ID's (e.g. employee ID) –Proof of Identity Guidelines are defined by the issuing party (e.g. employer) and are mostly physical
- IDs issued by Government Authorities or Regulated Entities (National IDs, Bank IDs, Tax IDs, Driver's License, Telephone Numbers) – Strong Proof of Identity Guidelines often defined by law/regulation

The second and third IDs typically require entities to go through an in-person enrolment process which require the entities to establish their identity through a Proof of ID/Existence and/or Proof of Address. These generally form part of "Know Your Customer" (KYC) guidelines defined by regulatory authorities or those who use a service, such as a Blockchain, to authenticate others.

[27] The World Bank, 'Counting the Uncounted: 1.1 billion people without IDs' http://blogs.worldbank.org/ic4d/counting-uncounted-11-billion-people-without-ids(as of February 2020).

Several countries have created digital ID systems that can be used by citizens to identify and authenticate themselves for transactions. These electronic IDs can take the form of a Smart Card (for example: Estonia and some other EU countries) or can be completely digital IDs (e.g. the AADHAAR ID in India).

There are a number of globally accepted systems, which are used for organizational identities such as proprietary systems, jurisdictional registration/incorporation number, tax registration number, etc.

These systems offer reliable means of verifying an organization's identity in online transactions. While some of these identity systems are based on voluntary registrations, others also include an independent verification of public data that is available about an organization, thus making the identity more reliable.

Identity verification "Know-Your-Customer" (KYC) guidelines and background checks are critical in establishing reliable digital IDs that can be used when creating Blockchain transactions that may require legal recognition. Since practices and rules regarding identity verification differ across countries, a common intergovernmental framework may need to be adopted to ensure cross-border acceptance of identity systems and documents implemented using Blockchain technology.

A Blockchain system could leverage digital ID systems which have appropriate authentication mechanisms. By combining decentralized Blockchain principles with identity verification and cryptography, a digital signature can be created and assigned to every online transaction affecting an asset. This has several potential benefits for consumers, businesses and regulators alike.

First, creating an identity on a Blockchain over who has their personal information and how they access it. Blockchain identity management platforms could also simplify procedures associated with burdensome, costly and time-consuming KYC obligations as well as better complying with data collection and privacy regulations. For businesses, this could lead to stronger regulatory compliance, lower costs, reduced fraud[28], and a more seamless experience for clients. Similarly, for regulators, a Blockchain based process could allow for prompt auditing and increased efficiency in compliance control, monitoring and quality. Taken holistically, improved means of verifying and managing digital identities and personal information based on Blockchain technology could increase transaction efficiency and further facilitate trade.

From a development perspective, digital identity secured by Blockchain technology applications has the potential to give those 1 billion unidentified individuals access to a safe, verifiable, and persistent form of identity. More broadly, by reducing costs for financial institutions it could give access to financial services to the 2 billion people who are unbanked.

Blockchain can facilitate immutable and secure sharing and validation of digital attributes for consumers and businesses while respecting privacy. When multiple parties across different jurisdictions want to verify the same identities using Blockchain, (for example authorities in an importing country and an exporting country may both want to verify the identity of the same

[28] In Australia, it was found that the e-commerce merchants currently lose between one and five per cent of revenue to fraud and that across all sectors, compromised security contributes to 2.4 billion Australian dollars in fraud every year. See, Australia Post, 'A Frictionless Future for Identity Management: A practical solution for Australia's digital identity challenge' (December 2016).

manufacturer) a standardized, intergovernmental framework may be required with standardized entity information.

4.3 Authentication and authorization

Authentication very often takes place using electronic signatures. A "signature (manual-ink or its electronic equivalent) creates a link between a person (physical or legal) and the content (document, transaction, procedure or other). This link can be considered as having three inherent functions: an identification function, an evidentiary function and an attribution function. More information about these functions can be found in UNECE Recommendation 14, "Authentication of Trade Documents."[29]

The identification function of authentication "confirms or allows the establishment of the identity of that signatory[30]". People can be identified by one or more means. When more than one means is used this is commonly referred to as Two Factor or Multi Factor Authentication. The technologies used for identification and authentication are constantly evolving, a few are listed below. More detailed descriptions and additional typologies can be found in Recommendation 14 and its annex B2 on "Typologies of means of electronic authentication."[31]

- ID/password;
- Something I know (questions, grid cards, images, knowledge bases, etc);
- Biometric methods (typically, fingerprints or IRIS scans);
- Devices (for example, a one-time pin sent to a mobile number); or
- Third-party verification (which could include digital certificates or social network-based access)

Blockchain-based authentication can leverage any of the above authentication methods based on the level of reliability required by those parties using the Blockchain network for authentication.

Blockchain-based distributed ledgers store data in a trustworthy manner. On the other hand, a Blockchain does not provide an interface for users to interact with it or – with the exception of some smart contracts – decide what transactions or data are written to the Blockchain. Therefore, an application layer is needed such as wallet software or other domain-specific applications in order to allow user interactions with a Blockchain. This means that authentication in a Blockchain-based system starts with the application software, with the possibility for a second layer of authentication coded into the Blockchain through the use of smart contracts. Both levels of authentication may be designed using any of the authentication methods indicated above.

Public and many private/permissioned Blockchain systems have nodes in many countries and can be accessed from anywhere, therefore, while users may be subject to recognized governmental or intergovernmental authorities, the same is not the case for the Blockchain system itself. As a result, an intergovernmental framework may be needed for the cross-border

[29] See UNECE Recommendation 14: Authentication of Trade Documents, 2014: http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec14/ECE_TRADE_C_CEFACT_2014_6E_Rec14.pdf (as of February 2020). Also see UNCITRAL "Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods", United Nations, Vienna, 2009, page 5: http://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf (as of February 2020).
[30] Op. Cit. UNECE Recommendation 14 – see annex B.2, "Typologies of means of electronic authentication" at http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec14/ECE_TRADE_C_CEFACT_2014_6E_Rec14.pdf (as of February 2020).
[31] Op. Cit. UNECE Recommendation 14 – see annex B.2 for a more complete list.

acceptance by authorities (for example courts) of Blockchain data. Such a framework could, for example, define required levels of authentication, reliability and accountability in cases where credentials (i.e. means of authentication) may be compromised.

Authorization refers to the process of obtaining the consent of a user prior to implementing a transaction. This could be a payment transfer or an action as part of a business application that could be coded into a smart contract.

This consent is typically given using a clickable "OK" or "I accept" box as part of an application workflow. To establish transaction integrity, Blockchain-based systems can also make use of digital signatures that use asymmetric key-pairs where a public key is used to encrypt the hash of the data which is decrypted using the private key[32]. This technique is used to ensure that data cannot be altered during its communication as any change in the data will result in an invalid transaction signature.

4.4 Data integrity and time stamping

From a data, integrity and redundancy standpoint, a centralized ledger (database) can be lost or destroyed and it must be regularly backed up. Transactions recorded in a ledger must be validated and users must have confidence that the ledger has recorded all valid transactions completely, accurately and only once. If historical transactions are altered, users must be able to ascertain that changes were made for bona fide reasons and there must be an audit trail so that transaction integrity can be verified.

Because of their characteristics (see second section) many Blockchain systems fulfil the requirements for a ledger in a way that is considered more trustworthy than what can be achieved with centralized databases.

Data authenticity on a Blockchain ledger is further ensured through the use of digital, trustworthy timestamps which can prove the date and time when data was registered on the Blockchain Timestamps are typically added to data by a Blockchain using a reliable external time source such as an atomic clock.

A transaction is normally saved on a Blockchain with both a time stamp and the digital signature of the entity or process initiating the transaction. The time stamp is hashed and digitally signed by the time stamping authority's private key.[33] Such timestamps can be verified, with a very high degree of trustworthiness, to ensure that the document was not backdated.

Since transactions in a Blockchain system can be processed from any participating node/server (which could be located anywhere), there is no single centralized server which can impose censorship or apply prioritization rules to transactions, thus providing additional protection from political and malicious interests.

While Blockchain-based distributed ledgers provide transaction immutability, there is also almost no way to remove inaccurate data if it was erroneously entered in the first place. For this reason, it is important to put logic into Blockchain-based applications and smart contracts which allows for new transactions to be entered that will, in effect, erase the impact of previous inaccurate entries (even though the inaccurate entries remain – just like in a paper-based ledger accounting system). In other words, this would not change the data (which would require a fork

[32] https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work (as of February 2020).
[33] These processes are defined in the Internet Engineering Task Force standard RFC 3161 and the ANSI ASC X9.95 standard

in the Blockchain as explained in section II), rather it is a "reversing entry" as would be made in an accounting ledger.

While in theory Blockchains are vulnerable to cyberattacks including Sybil (51 per cent attacks and distributed denial of service, the combination of decentralized database architecture, cryptography and the principles of immutability and consensus make Blockchain-based distributed ledgers relatively resilient to cyber-attacks (see section 2 for further explanations). The types of attacks that a Blockchain is susceptible to depend upon a range of characteristics. For example, Blockchains with fewer nodes are at a greater risk for 51 per cent attacks, while permission less Blockchains may be more at risk of identity theft than permissioned Blockchains where access is more restricted.

Another vulnerability that will probably arise in the future is the development of quantum-speed computers, and their possible use for hacking, given the extensive reliance of Blockchains on cryptographic techniques. Quantum computing will render many existing and often used cryptographic algorithms much less secure or even useless[34]. For example, the United States' National Institute of Standards and Technology produced a report on post-quantum cryptography, which showed that three well-known encryption technologies (Rivest, Shamir and Adelman algorithm [RSA], Digital Signature Algorithm [DSA] and Diffie-Helman) will no longer be secure and the Advanced Encryption Standard (AES) and Secure Hash Algorithm-2 (SHA-2) and SHA-3 standards will require larger key sizes and output to be effective.[35] As a result, developers may want to already consider implementing the "post quantum" cryptographic techniques being developed by a wide range of standards organizations including the IEEE and ISO.[36]

4.5 Privacy and confidentiality of information

Confidentiality refers to the protection of data so that it is disclosed only to authorized parties and is protected from access by unauthorized third parties[37]. Privacy refers to a person's right to control access to his or her personal information. Digital innovations, including Blockchain technology, may have the potential to protect the rights of citizens to privacy and confidentiality.

In many cases, confidentiality and privacy are enforced by legislation (e.g. EU or national data protection legislation), regulation (client confidentiality) or contract (commercial confidentiality). As such, it is critical to understand how Blockchain technology impacts these protected rights.

The design of any digital platform for trade facilitation using Blockchain technology must be done so as to store and transmit data in a way that safeguards the right of individuals to confidentiality and privacy. To achieve this, it may be necessary for developers to only record hashes of personal data on the Blockchain (or perhaps even only a hash of the data's location/address) and to not store any private data on the Blockchain. Instead, private data can be stored off-chain and only exchanged as needed and in peer-to-peer communications.

For example, an individual who claims to have a valid driver's license for the purposes of employment can have their claim verified by an authorized third party (e.g., the relevant motor

[34] https://cointelegraph.com/news/quantum-computing-vs-Blockchain-impact-on-cryptography (as of February 2020).
[35] https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf (as of February 2020).
[36] https://pqcrypto.eu.org/deliverables/d5.2-final.pdf (as of February 2020).
[37] https://www.techopedia.com/definition/10254/confidentiality (as of February 2020).

vehicle licensing department) which would produce a cryptographic hash of the verified claim and save it on the Blockchain. The employer could then compare the hash to a copy of the claim with the electronic signature (to ensure that it is valid and not a forgery). This allows an individual to assert they have a driver's license without revealing any other personal information. The use of zero-knowledge proofs[38] can add further privacy to personal data, by using mathematical proofs to demonstrate the validity of information without revealing the underlying personal data.[39] For example, zero-knowledge proofs can show that an individual is over 18 without revealing their specific age, or that they live in Paris without providing their address in Paris.

The following rules should be considered when designing Blockchain systems that need to safeguard privacy and confidentiality:

- Transacting parties cannot be identified by an unauthorized third party from the information stored on the Blockchain (including metadata)[40], unless the party(ies) to be identified has/have chosen to reveal that information;
- Other transaction details are not visible to unauthorized third parties and to the open public unless one of the transacting parties has elected to disclose that information; and
- Transaction details cannot be collated, analysed or matched with *off-Blockchain*[41] meta data to reveal any information about the transacting parties or the details of the transaction.[42]

Blockchains do not inherently respect privacy and confidentiality.[43] Indeed, the two largest Blockchain systems, Bitcoin[44] and Ethereum[45], are public (permission less), open, transparent, and pseudonymous. They are open in the sense that there are no restrictions on participation, and they are transparent because all transactions and all transaction information is visible to anyone on the Blockchain. In addition, on the Ethereum Blockchain the code and execution of smart contracts is also visible.

In both Blockchains, transacting parties are pseudonymous and identified by public keys generated using mathematically derived algorithms (known as Bitcoin addresses or Ethereum

[38] A zero-knowledge proof is a cryptographic technique which allows two parties (a prover and a verifier) to prove that a proposition is true, without revealing any information about that thing apart from it being true.
[39] See Daniel Augot et al., 'Transforming face-to-face identity proofing into anonymous digital identity using the Bitcoin Blockchain' (International Conference on Privacy, Security and Trust, 2017) https://arxiv.org/pdf/1710.02951.pdf (as of February 2020).
[40] This includes the time the transaction was executed.
[41] Off-Blockchain transactions are transactions that are recorded on an internal ledger which are periodically synchronized with the Blockchain. For example, Coinbase, a cryptocurrency exchange service, maintains an internal ledger for its clients as they make transactions and later broadcasts those transactions to the Blockchain.
[42] See Danny Yang, Jack Gavigan and Zooko Wilcox-O'Hearn 'Survey of Confidentiality and Privacy Preserving Technologies for Blockchains' R3 Reports November 2016 https://www.r3.com/wp-content/uploads/2017/06/survey_confidentiality_privacy_R3.pdf (as of February 2020).
[43] See, generally, Primavera De Filippi, 'The Interplay between Decentralization and Privacy: The case of Blockchain technologies' (2016) 7 Journal of Peer Production 1, https://hal.archives-ouvertes.fr/hal-01382006/document. See also Morgan Peck, 'Cheat Sheet: The trade-offs of Blockchain privacy tools' 8 March 2019 American Banker https://www.americanbanker.com/news/cheat-sheet-the-trade-offs-of-Blockchain-privacy-tools (as of February 2020).
[44] Satoshi Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008, Bitcoin White Paper): https://bitcoin.org/bitcoin.pdf (as of February 2020).
[45] Vitalik Buterin, "A Next Generation Smart Contract and Decentralized Application Platform" (2015, Ethereum White Paper): https://github.com/ethereum/wiki/wiki/White-Paper (as of February 2020).

accounts). This provides only a very limited amount of confidentiality, because it is possible to connect the identity of an individual with their public key.[46] For example:

- Some people share their address publicly so that other parties may transact with them and, as a result, none of their transactions using that public key (past or future) can be confidential.
- Cryptocurrency exchanges[47] require the verification of physical identity documents in order to join, allowing them to link one's real identity with their public key.
- There are companies making a business from linking identities to addresses and creating commercialized databases that track all Bitcoin activity in an effort to de-anonymize Bitcoin.

Because transactions made on Blockchain are fully traceable[48], once a person's identity has been linked to their public key it is possible to infer and monitor an individual's spending patterns (such as where they spend, how much they spend, and how often), their wealth and income, and with whom they undertake transactions. It is also important to remember that the data written to the Blockchain is immutable and irreversible, meaning it is permanently accessible and visible. As such, incursions on one's privacy or confidentiality cannot be reversed or corrected at a later time.

Some Blockchain developers, having recognized the issues associated with privacy and confidentiality, have taken steps to address them by creating platforms that do not make publicly available transaction details, thereby retaining transactional privacy (most of these being permissioned Blockchains).[49] Indeed, the lack of guaranteed privacy has been identified as hindering the broad adoption of decentralized smart contracts because parties to financial transactions, such as the trading of insurance contracts or company shares, require that those transactions be kept private.

At the same time, for international cross-border transactions, it remains important to engage with intergovernmental bodies in order to secure harmonized systems that are accepted from a legal standpoint.

4.6 Legal aspects

4.6.1 Admissibility of electronic evidence

Legal systems expect a certain degree of authenticity, immutability and auditability of the material or data presented in order for courts to consider them as admissible evidence. In the case of a public Blockchain ledger, although the technology provides for the immutability and auditability of transactions, the network allows anyone to participate, using pseudonyms, which

[46] See Elli Androulaki et al 'Evaluating User Privacy in Bitcoin' (2012) 7859 Lecture Notes in Computer Science 1 https://eprint.iacr.org/2012/596.pdf (as of February 2020). In this study, it was concluded that the profiles of almost 40 percent of Bitcoin Blockchain users can be determined even when users adopt privacy measures recommended by Bitcoin.
[47] Popular exchanges include Coinbase https://www.coinbase.com/ (as of February 2020)., Kraken https://www.kraken.com/ (as of February 2020) and Gemini https://gemini.com/ (as of February 2020).
[48] Indeed, a bitcoin is defined as the history of its custody - "an electronic coin as a chain of digital signatures". Satoshi Nakamoto, above n 30, 2
[49] See, generally, Danny Yang, Jack Gavigan and Zooko Wilcox-O'Hearn, Survey of Confidentiality and Privacy Preserving Technologies for Blockchains' R3 Reports November 2016 https://www.r3.com/wp-content/uploads/2017/06/survey_confidentiality_privacy_R3.pdf(as of February 2020). https://z.cash/static/R3_Confidentiality_and_Privacy_Report.pdf (as of February 2020).

makes it very complicated to assess the legal identity of the person(s) participating in a transaction. Thus, unless the person(s) participating in the law suit are mandated (and are able) to identify the true identity of the participant(s) in the transactions on the public Blockchain which are in question, the courts may have concerns about Blockchain-based transactions being admissible evidence.

In the case of private or permissioned ledgers, Blockchain technology can provide immutable and auditable transactions[50] entered by authorized parties (who can be identified) and, thereby, can satisfy the requirements of legal systems for considering digital evidence as being valid. In addition, the tamper proof nature of data recorded using Blockchain technology, usually in a chronological order and/or with time stamps further enhances the reliability of and authenticity of the recorded transactions, thus lending credibility to, and increasing the admissibility of, the electronic data being submitted as evidence.

However, in some countries evidence law prescribes specific conditions for establishing the legal validity of electronic data, such as the authentication of electronic transactions using certified electronic/digital signatures. Blockchain, in general, uses cryptography key technology that is similar to Public Key Infrastructure (PKI), the technology used in digital signatures. Therefore, the digital signatures used in Blockchain may already be compliant with local laws[51], thus making Blockchain transactions legally valid for the purpose of admissibility.

4.6.2 Non-repudiation

The evidentiary function of a signature involves legal implications and can include integrity, consent, acknowledgement…[52] Non-repudiation refers to the author of a statement or a signatory to an agreement not being able to successfully deny the authorship of the statement or the validity of a contract they previously agreed to and/or signed.

The process of establishing non-repudiation depends on the local laws of countries and their recognition of what constitutes a framework under which an electronic record can be considered secure and, therefore, cannot be repudiated. Some of the security procedures that concerned parties could undertake in order to better establish a status of non-repudiation include the ability to:

- Verify that the electronic authorization used in a transaction is unique to the user performing the transaction and it is capable of identifying such user
- Validate the fact that the electronic authorization was created in a manner or using a means which was under the exclusive control of the subscriber
- Verify that the method of electronic authorization is linked to the electronic record to which it relates in such a manner that if the electronic record was altered, the method of electronic authorization would be invalidated

As for any system, the admissibility of electronic evidence from a Blockchain will be based on the ability to establish the non-repudiation of transactions which in turn depends on the security measures in place under which data integrity, confidentiality, privacy and authenticity of transactions can be established.

---

[50] The degree of immutability and auditability provided by private/permissioned Blockchains depends upon their design and governance rules. This is also the case for public Blockchains, although the larger and older ones have had these features well tested.

[51] This needs to be verified on a case by case basis

[52] Op. cit. UNECE recommendation 14, page 5

4.6.3 Dispute Settlement and Enforcement

At the transaction level, the applied consensus mechanism used by a Blockchain allows participants, as a group, to challenge the correctness of outcomes from smart contracts and transactions (based on the rules set out by the Blockchain and the recorded transactions). On the other hand, there is no method available for a participant to challenge the business outcome arrived at by a smart contract if, for example, the outcome (after a correct execution of the contract) is not what the participant expected when agreeing to the original terms of the smart contract.

A contract is a legally enforceable agreement. Smart contracts are computer programs that execute when previously agreed upon conditions are met. In spite of their name, this does not, necessarily, mean that they represent a legal contract. They are only contracts if and when they are the source of an obligation that is clearly understood and agreed upon by the parties involved. On the other hand, they are not a contract if they are only a method for executing an obligation that has its origin elsewhere. For example, a smart contract is not a contract if it implements the terms of an insurance contract which was signed on paper and may cover thousands of instances of smart contract execution (for example an insurance policy covering all the containers shipped by one multi-national). Once written onto a Blockchain, a smart contract cannot be changed, and its execution cannot be stopped (once the pre-defined conditions are met). Therefore, if a smart contract is well designed and coded correctly, the non-performance of the contract is not possible. However, there could be problems linked to incorrectly coded smart contracts, changing circumstances, etc.

A contract is an agreement and legally requires parties to the contract understand clearly what they have agreed to. Where consumers are involved, particularly Micro-, Small- and Medium-Sized Enterprises (MSMEs), interaction with a smart contract usually takes place via a user interface which is likely to have been developed by the creator of the smart contract in question. Therefore, courts are likely to consider the legal agreement as being the offer presented via the user interface by the creator of the smart contract. The smart contract itself is code that cannot be easily understood by humans (and which may or may not correspond to the information presented by the user interface).

Even when a smart contract is not a contract (which is most of the time), it can still have a legal impact or meaning. Among these other legal acts or meanings are:

- Execution of a contract;
- Suspensive or dissolving condition in a contract (i.e. if X is true, then the contract will not execute);
- Unilateral legal act;
- Decision under public law;
- A means of evidence;
- Obligation of compliance with a (fiscal law); and/or
- Others, depending upon the jurisdiction in question.[53]

One novel issue related to the use of smart contracts is what happens when an agreement cannot be enforced or its enforcement cannot be stopped by public law enforcers, but only through the terms and mechanisms set forth in a computer program (i.e., smart contract) that cannot be

[53] The Legal Aspects of Blockchain, UNOPS, 2018, Page 90

changed. The typical legal action for breach of contract involves an aggrieved party going to a court of law or an equivalent, for example a mediator, to demand monetary damages, restitution, or specific performance. With a smart contract, the aggrieved party will need to go to the court to seek a remedy to a contract that has already been executed or is in the process of being performed. Therefore, the remedy will need to come after the fact in order to undo or alter the agreement in some way.

Assuming the parties to a given smart contract are known, courts could require the parties to create a new transaction to reverse the undesirable outcomes of the coded and executed smart contract under dispute. This is a possible solution because courts will not be able to affect the initial outcome of a disputed smart contract transaction and a retroactive change in a Blockchain is not possible, at least from a practical standpoint.[54]

The ability to enforce the agreements represented by smart contracts via traditional legal means is limited. First, disputing a smart contract with traditional means (in court, arbitration, mediation, etc.) is only possible when the identity of the parties involved is known. Because of the anonymity[55] of most public Blockchain transactions this may not be possible. Moreover, while smart contracts are coded as self-executing contracts, if the end result requires actions that cannot be taken directly by the smart contract using the Blockchain network or the Internet, but rather requires human intervention (for example, the physical transfer of property), the smart contract does not provide effective mechanisms for enforcement if one party breaches his or her obligations. While, semantically, it might be argued that breach of a smart contract is not possible because the contract simply will not execute if a parameter is not fulfilled – this may depend upon the smart contract being able to finish execution without any human intervention which may not always be the case.

When a smart contract replaces an existing legal contract, in the majority of circumstances, the smart contract will be governed by the same legal principles as would the similar paper-based legal contract – if the smart contract is a commercial transaction and all of the parties to the smart contract are known. Even when all of the parties are not in the same legal jurisdiction, there exist well established principles in international commercial law for establishing the applicable jurisdiction and law. If the identities of the contracting parties are not known to one another and the Blockchain in question is a private or permissioned one, the operator of the Blockchain platform should have a legal obligation to identify who the breaching party was in a dispute scenario where a breach can be shown to have taken place.

In anticipation of possible disputes, the operators of permissioned Blockchain systems may want to establish governing rules for their Blockchain and specifications for dispute resolution. However, these specifications would have to be disclosed upfront and agreed upon by the parties to the smart contract in order for them to be enforceable.

Courts may be substantially challenged in interpreting smart contracts. Unlike the interpretation of a contractual dispute in the existing legal infrastructure where courts assess what the contentious language in a given contract may mean to a reasonable human observer, smart contracts are not coded for a human observer. Rather, they are intended for execution by

[54] As discussed earlier, it is theoretically possible to change information (including smart contracts) on a Blockchain, but in practice it is nearly impossible

[55] As discussed earlier, some public Blockchains offer complete anonymity but the most important ones offer only the privacy provided by "pseudonyms". While the owners of pseudonyms can be identified (but not always), it is still difficult to do so. As a result, most transactions are, in practical terms, anonymous.

computers on a network of Blockchain nodes and in the future, they may even be created by artificial intelligence.

To the extent that consumers interact with smart contracts, the graphical user interfaces which they use for this purpose should provide courts with information about what the consumer could have reasonably expected from the execution of a smart contract. From a business standpoint there are also communications between business actors and programmers regarding what a smart contract should be developed to do. This second context, however, opens up thorny questions regarding the legal liability of programmers for the consequences of mistakes, even if they are honest mistakes, in smart contracts – and of businesses for mistakes which may be made by artificial intelligence systems that they deploy, and which may develop smart contracts.

The basic premise of smart contracts is computer programming, not human interaction, and, in the future, some smart contracts may be developed by automated systems to regulate interactions between inanimate objects (for example, between solar panels and electrical grids). Because of the emphasis on computer programming and artificial intelligence, courts may not be able to evaluate for themselves the quality of smart contracts (i.e. evaluate if they were developed with appropriate due diligence). Courts may also be limited in their ability to consult programmers to interpret code in a given case because the meaning and logical reasoning of computer code is substantially different from human language.

In the cases where the identities of the participating parties to a smart contract are not known, from an identification perspective, it is unclear who would own the output/data created by the smart contract in question and whether there would need to be any applicable protections, such as for work products or confidentiality. Without knowing the ownership rights for a Blockchain transaction, it is also unclear who would be able to claim privileged information or how discovery would operate via existing laws.

However, when the parties to a smart contract choose to reveal their identities, arguably privileged information and/or discovery laws should apply as if the smart contract was a written contract, despite the fact that the contract/agreement takes the form of computer code.

While international commercial law would normally be applicable when the parties are known, not all contract law remedies may apply to smart contracts which raises possible enforceability issues. If a transaction in a smart contract fails to be completed (for example because some required input cannot be given) or is only partially completed, it is unclear how liability will be allocated if those eventualities have not been taken into account in the development of a smart contract's code and/or any associated agreements. Because of the decentralized nature of Blockchain, it may be unclear who or what is accountable for the failure of the contract. Guidelines for the application of existing contract law to disputes involving Blockchain smart contracts may be useful. As jurisprudence is developed, the need for additional legislation may also be identified. Without such guidance, the liability for failed transactions or conflicts between parties to smart contracts will present unique challenges to judicial systems.

The rest of this section aims to address four aspects of contract law in the context of Blockchain-based distributed ledgers

1. Formation;
2. Performance;
3. Breach & remedies;
4. Input error issues.

4.6.3.1 Formation

A smart contract executes when specified conditions are met and what is executed may range from debiting/crediting an account to issuing an instruction to another system that is "off-chain". Therefore, as stated earlier, many smart contracts are not "contracts" at all. Before any smart contract can be considered to be a "contract", the parties must agree to a set of conditions (contract terms) that initiate the program. This will come through an offer and acceptance.

In the realm of smart contracts, unlike traditional contracts, acceptance can come through performance (i.e. if a party knows that doing X will cause a smart contract to execute, then doing X shows acceptance). For example, Ana individual trader (buyer or seller) can initiate a smart contract by posting the relevant code to a Blockchain. However, until the program initiates (is accepted by a counter party), there is no contract. This smart contract code which has been posted to a ledger can be seen as being an offer. Once an action is taken to accept the offer, such as a party transacting in a way that gives the code control over a certain amount of money, the contract is formed.

Smart contracts can be of particular value because they bind the hands of the executor, which is, in effect, the smart contract, to the original will of the contracting parties, with little room for deviation. Although ambiguity certainly exists in programming languages, these ambiguities are less than in the real world. Thus, the problem of ambiguity is reduced in the smart contract context.

4.6.3.2 Performance and modification

A contract can be performed, modified, or breached. The performance phase is made easier with smart contracts as they offer a tool to reduce ambiguity as discussed above. However, there is a problem with regard to imperfect performance. Courts do not demand perfect performance for a contract to be recognized and enforced. The common-law doctrine of substantial performance sometimes permits a contract to be recognized even if the performance does not fully conform with the express terms laid out in the contract. This is the kind of leeway that a computer program cannot recognize because it involves an outcome that was not contemplated and specified by the parties. One way that parties can deal with this is by incorporating a certain degree of discretion/flexibility into the terms of the contract initially – or by simply not using a smart contract if the ability to respond to unforeseeable circumstances is a necessary part of the contract.

There is also the problem of contract terms which diverge either accidentally or on purpose from what the law recognizes. In this case, the law would have to decide between ex ante and ex post solutions to the problem. Again, ex ante solutions will be difficult to implement because of the immutability of smart contracts.

For example, the law recognizes certain circumstances that will absolve a party from performance or require some sort of modification to a contract. Impossibility and impracticability are two such circumstances. In addition, when a contract becomes illegal after it is formed, then the parties can be excused from performance and there is generally no remedy for an aggrieved party.

This poses a problem for the smart contract. For example, suppose that at the time of contract formation, the time a debtor needs to be in default before the creditor can repossess the goods in question is 30 days and this is written into a smart contract. Then, after the contract is executed, the law is changed so that the required time period is 90 days. There are numerous ways of addressing this potential situation, ranging from state-backed to purely private. One method could be a system in which the relevant jurisdiction creates a publicly available

database, with an application programming interface (API), containing relevant legal provisions related to the contract terms. The smart contract would call upon this database, using the API, and would be able to update those terms in the smart contract based upon the jurisdiction's update of the database.

Another method would be through ex post policing by the parties; this puts the burden on the parties or their agents to update the code. This can only be done in a smart contract by defining some terms as being variable and identifying the conditions under which they can be changed. For example, implementing a change might require electronic signatures from all parties involved. The benefit of this option is that there is no need to rely on a third-party government office to create a new infrastructure. The downside is that this requires parties to foresee the need for possible changes and for a smart contract to be designed in such a way that the parties must agree on changes and it is not possible to unilaterally change the terms of the contract. Such design also reduces the predictability/reliability of smart contract results, which is one of the principle benefits of using smart contracts. This reduction in predictability could be reduced by having certain terms of the contract be modifiable, while restricting others so that they cannot be modified. For example, the requirement for payment could be an immutable term, whereas the length of time a debtor has before he is in default could be modifiable.

Still another method, if the possibility of the change in question was not at all foreseen when the smart contract was developed, is to create a second smart contract that, in effect, reverses the action of the first contract. This would of course require all participating parties to agree.

Finally, computer programs and thus smart contracts can be written with the option of inserting code later. However, this raises all of the issues mentioned above concerning when and how such changes could be made without destroying the principle rationale (predictability and reliability) for the use of smart contracts.

4.6.3.3 **Enforcement, breach and remedies**

The central problem for smart contracts in the context of contract law is: what happens when the outcomes of the smart contract diverge from the outcomes that the law demands? It is possible, and hopefully probable, that smart contracts will diverge less than written contracts from the desired legal outcomes, not the least because of reduced ambiguity and increased difficulties in breaching a contract because participants cannot influence the smart contract after it has been established. Courts will probably be more likely to enforce smart contract terms because the courts will have more certainty as to the parties' intent because the parties had to explicitly lay out their terms in advance. Because of their inflexibility, smart contract drafters are going to be more likely to write smart contracts that conform with existing law and to write smart contracts with terms that are variable in order to accommodate future changes in the law or use of the same smart contract by participants in different jurisdictions. The terms of a lease, for instance, will change to accommodate the property law of the jurisdiction where the property is located. Additionally, it is possible that torts will emerge for negligent coding or negligent updates which would further ensure that future smart contracts are drafted in accordance with existing legal standards.

4.6.3.4 **Input error issues**

Like other systems, Blockchain-based systems cannot attest to the accuracy of input data and errors in this data would influence the outcome of an autonomous smart contract's execution.

While errors can be handled between parties using a reversal transaction, as in a paper-based accounting ledger, courts of law may also need to have provisions to handle issues related to erroneous input to smart contracts.

4.6.4 Mutual recognition

As the number of use cases for Blockchain expands, the number of parties using the same Blockchain-based applications and smart contracts who are located in multiple jurisdictions will also grow. As a result, complications will also increase which are related to enforcement in different jurisdictions where identification, authentication and non-repudiation standards are driven by local laws and regulations. Many of these can be resolved on the basis of existing international commercial law practices, especially when the parties to a transaction are known. At the same time, while Blockchain applications provide increased certainty in some areas such as contract execution, they can also increase ambiguities and create new problems in other areas such as the identity of smart contract participants on public Blockchains or, in some cases, applicable law. There will also be cases where international commercial law cannot be applied (for example, when Blockchain use involves business to government communications and/or assets, such as land, which are covered by local laws).

To give electronic transactions which are used across jurisdictions or involve participants from different jurisdictions the same effect as paper-based transactions, mutual recognition frameworks need to be created which will allow parties in different jurisdictions to execute valid contracts on a Blockchain or using other electronic technologies. These mutual recognition frameworks are especially needed for government to business communications. and.

Depending on the content of a contract and applicable law, mutual recognition frameworks may allow parties to a contract to decide what constitutes a valid transaction. Member states may also mandate guidelines or rules defining the process and procedure to be followed when validating and accepting a transaction from another jurisdiction. These guidelines and rules may take into account the functions of authentication: identification, evidentiary and attribution and should be based upon, or drawn from, existing work, such as the UN/CEFACT Recommendation on the Authentication of Trade Documents[56] and including treaties and agreements between member states. The UN/CEFACT White Paper on Trusted Transboundary Environment may provide such a framework.[57]

4.6.5 Legal aspects – conclusions

The above discussion on the legal aspects of smart contracts highlights the need for foresight and careful planning in order to avoid possible legal pitfalls. Among some of the more important actions that smart contract developers and implementors should consider are the following:

- Identification of variables that might change and methods for changing the variables without undermining the predictability and reliability of the underlying smart contract

[56] Op. Cit. UNECE Recommendation 14.
[57] See UN/CEFACT "White Paper on Trusted Transboundary Environment: Ensuring legally significant trusted trans-boundary electronic interaction," 2018: http://www.unece.org/fileadmin/DAM/cefact/cf_plenary/2018_plenary/ECE_TRADE_C_CEFACT_2018_7E.pdf (as of February 2020).

(for example, the requirement of multiple electronic signatures in order to make changes);

- Identification of inputs where the possibility of errors exist and a plan for identifying and fixing them;
- Identification of where, at some point in time, a selected oracle might cease to exist or fail due to government re-organization, bankruptcy, etc., and backup plans for their replacement if needed;
- Identification of any instances where a smart contract might not finish execution (for example because a required input is not received or not received within allowed time limits) and how such situations should be resolved;
- Identification of the legal circumstances under which it would be necessary to identify the parties to a transaction and if, for example, this requires that the smart contract be implemented on a permissioned Blockchain
- Designation, in advance and in a document separate from the code in the smart contract, of the
    - Applicable law;
    - Jurisdiction under which disputes should be settled;
    - Method of dispute resolution to be used;
    - General terms and conditions.

Part II

Blockchain can have many applications, however the implementation within each supply-chain sector may imply a different approach. During the Blockchain project, the project team identified potential uses of Blockchain in different sectors; these were then organized into the sections which constitute this document. Each section was authored by a different team.

Each of the sections looks at how Blockchain technology could be potentially applied to that specific sector of activity.

5 Supply chain transparency

5.1 Introduction

At the time of its inception, over two thousand years ago by Alexander the Great, the supply chain was a revolutionary idea designed to provide a military advantage to troops that were better supplied. This concept was then much further refined and developed in parallel with the development of assembly-line manufacturing in order to improve the visibility and control of goods and products as they moved from point A to point B.

But the old concept and its related technologies can no longer support today's production and supply cycles, which have become extremely fragmented, complicated, hard to manage and geographically dispersed as well as being increasingly time sensitive due to the development of just-in-time manufacturing.

The business networks supporting supply chains include many participants, including customers, suppliers, banks, partners and others. Supply chains are also linked to communications, energy, transportation, finance, manufacturing… there's almost no limit especially for cross-border supply chains which involve cross-border regulatory management processes by agencies such as Customs, Agriculture Certification Agencies etc.

Business networks, whether they involve buying something, getting goods shipped, manufacturing or maintaining assets, involve a network of participants cooperating with some shared objectives for agreed upon transfers and record keeping.

Goods, services and documents/information are exchanged daily on these networks, however, keeping track of these transactions is a complicated and paper-intensive process, in large part because businesses have multiple ledgers for the multiple networks in which they participate.

Historically, these records are on paper and are handled manually. Today, many of these records are electronic, however, they often rely on physical data entry by different parties and are located in different computer systems in different companies and departments. As a result, these records, still, often require time consuming and, sometimes, manual interventions to ensure that records are properly reconciled (for example to ensure that all goods ordered were shipped; all goods shipped were invoiced and all goods invoiced were paid, etc.).

The problem with paper records and dispersed, multi-party manual data entry and reconciliation is that the information becomes subject to a relatively high error rate. Therefore, existing systems look inefficient, expensive and vulnerable even though they have been in use for decades.

In addition, the volume and complexity of supply chains today can no longer be supported by existing paper-based systems and IT systems based on disbursed multi-party data entry and reconciliation. According to a 2018 article published by Supplychain247.com[58], the total value of goods shipped annually has reached 4 Trillion United States dollars. Approximately 80 percent of this occurs in supply chains that require cross-ocean transportation. Although supply chains have embraced technology to achieve improved levels of efficiency, accuracy and value creation, they are by no means as efficient, accurate or value creating as most stakeholders would like. Some suggest that the global supply chain has not experienced significant disruption since the introduction of the standardized shipping container in the 1950's. A

[58] http://www.supplychain247.com/article/maersk_ibm_to_form_joint_Blockchain_venture(as of February 2020).

commonly cited figure in supply chain costing is that documentation costs can exceed the costs incurred in physically moving the products – in other words, documentation management can double the cost of the process.

In a whitepaper written for the 2017 World Economic Forum[59] in Davos, Switzerland, BVL International states that 85.5 per cent of the surveyed logistics business predicted a positive impact to costs, revenues, or both, from future digital transformation. It is expected that Blockchain implementations could play a significant part in that digital transformation.

How can Blockchains help supply chain stakeholders to save money and drive revenue? In one word, trustworthiness. Even a brief examination of current supply chains exposes the reliance on third parties (e.g. notaries, brokers, agencies, banks, certifying bodies) to establish trustworthiness between parties that cannot implicitly trust one another without such support. The need to establish trustworthiness creates inefficiency and waste. Where trustworthiness is weak or broken there is the potential for and, therefore, very often the reality of fraud. With 3.2 trillion United States dollars' worth of goods being shipped over extended supply chains these inefficiencies and risks become significant.

There are a wide range of stakeholders in a typical international supply chain that need access to information at some point during the movement of the traded goods between seller and buyer. For example:

- Those directing the transport and cargo processes (freight forwarders, shipping agents, forwarding agents, consignors/consignees);
- Transport operators (maritime, road, rail, barge, airlines);
- Port operators (terminal operators, warehouse storage keepers);
- Government agencies (customs, veterinary, police, ministry of transport/health/ environmental protection, port authorities, emergency services, etc.);
- Inspection authorities (surveyors, pest control, phytosanitary); and
- Supporting financial services (banks, insurance companies).

Blockchain offers the potential for improving the dependable accuracy of information, for speeding up and controlling access to that information.

Trustworthiness between parties can be strongly supported by ensuring the availability of trustworthy information which focusses on two main components of the transaction: the transparency with which business is conducted and the traceability of the product throughout its lifecycle.

- Transparency allows stakeholders to see into the process easily and accurately in order to receive accurate information in a timely manner; and
- Traceability allows stakeholders to know with confidence the relevant sources of any product in the process.

The two are intimately linked but are not synonymous. The use of Blockchain technology to increased transparency and traceability in the supply chain would allow stakeholders to realize the following benefits without, necessarily, incurring commensurate increases in costs:

[59] http://www3.weforum.org/docs/WEF_Impact_of_the_Fourth_Industrial_Revolution_on_Supply_Chains_.pdf (as of February 2020).

- Improved data security and reduced fraud
- Speed, for example accelerated payments;
- Accuracy;
- Efficiency, for example through simplified claims settlement and, in some cases, the elimination of middlemen;
- Increased granularity of historical data;
- Real time monitoring;
- Proof of provenance through improved traceability and trackability;
- Increased transparency in prices, ownership and the entire process;
- Increased compliance with reduced costs; and
- Consumer/Customer engagement.

The World Trade Organization has estimated that reducing the friction in current systems, especially at the borders could increase global GDP by 0.5 per cent and increase international trade, with particular benefits to developing countries.[60]

Because there are other sections which look, in depth, at Blockchain use in transport, this section focusses on the opportunities offered by Blockchain technologies in addressing gaps in transparency and how it can support meeting the United Nations Sustainable Development Goals (SDGs) through improved traceability of materials.

5.2 Current challenges faced by modern supply chains

The following are examples of challenges faced by modern supply chains and how Blockchain technology could support their resolution.

5.2.1 Proof of provenance

At present, many transactions take place on the basis that the goods supplied are of a reported quality or are of a specific provenance. Currently, buyers have no cost-effective manner of verifying the authenticity of the suppliers' claims. This increases reliance on long-term and large contracts with established players and creates natural barriers to entry for new and smaller suppliers – and this, in turn, damages true competition.

Despite this, fraud based on passing off non-organic food as organic or even manufactured food (e.g. rice) as naturally grown is a big business. Food fraud is estimated to cost the world's economy 30-40 billion United States dollars per year.[61] Other sectors where fraud is expensive and even life endangering include pharmaceuticals and replacement parts while the fashion industry suffers from products labelled organic cotton or legally farmed crocodile skin which are not always what they proclaim to be.

Blockchain technology can be used to increase traceability whenever it is possible to create a link between a product and a digital identifier that is verifiable and cost effective. Such digital identifiers are referred to as "digital twins" These solutions have varying costs and levels of

[60] https://www.wto.org/english/tratop_e/tradfa_e/tfa_factsheet2017_e.pdf (as of February 2020).
[61] https://fas.org/sgp/crs/misc/R43358.pdf (as of February 2020).

reliability, depending upon the technology and the system within which they are used. For more on Tokens and Digital Twins, refer to the section 2.4.3.

With respect to the UN's SDGs, below are some examples of where increased traceability would have a long-term positive impact on the goals:

- SDG 1 – No Poverty. Items can be traced back to source and each stakeholder can be required to prove that they are not using child labour and/or are paying their workers a living wage. Not every supplier will be able to prove this. These gaps in traceability will help authorities and buyers to identify bad or slow actors in this regard. Suppliers who are unable to meet the certification/traceability requirements should, in theory, begin to see less demand for their products.
- SDG 6 – Clean Water and Sanitation. At present, once it has entered the supply chain, a leather hide that was tanned in a tannery that does not properly manage its waste cannot be differentiated from a more responsibly tanned hide. In the future, buyers may be able to view the environmental credentials of the tannery even when the hide has been incorporated into a finished product. As supply chain traceability becomes more ubiquitous, market forces will likely bring about behavioural changes in business operations by rewarding good actors and removing market share from bad actors.
- SDG 12 - Responsible Production and Consumption. Supplies of rare woods are limited and it must be sustainably and transparently logged. The Blockchain allows for trees to be uniquely identified and tracked throughout their life and post-logging. This ability to control the supply of lumber in order to ensure that it is legally produced will help to reduce the black market for illegally and unsustainably logged lumber. At present, buyers remain wilfully, or innocently, unaware of their part in the illegal logging trade by relying on the word or certification of an intermediary who may be unethical. In the future, lumber will come with an authenticated passport, proving it is genuine and came from a sustainable source. Lumber without that certification will have a limited market and will find it harder to reach distant markets because shipping lines and customs departments will more easily be able to detect and impound illegal shipments.[62]

5.2.2 Customs delays

Customs and Excise officials at any border are reliant on the information provided to them for making their decisions. The opportunity for unscrupulous actors to alter or fabricate information adds risk and distrust into the process. This risk and distrust then become delays, costs and uncertainty for all supply chain participants, irrespective of whether they are good actors or bad.

Like any IT system, those based on Blockchain need to put in place controls and procedures for ensuring the quality of data. However, once information has been captured by a well-designed Blockchain system, it could present a more reliable data set to customs officials, thus requiring fewer controls. This would, theoretically, allow them to both process goods through ports faster and, also, recover revenues owed more efficiently – even automatically.

[62] http://www.foodsafetynews.com/2014/10/foodborne-illnesses-cost-usa-15-6-billion-annually/#.Wmeuua3MzEY (as of February 2020).

5.2.3 Visibility

One of the greatest inefficiencies in many supply chains is the time and effort required to gather accurate information on the location, condition and estimated-time-of-arrival (ETA) of goods within the supply chain. When used for traceability and, in particular, when combined with IoT devices, Blockchain systems can provide a relatively easy to implement data pipeline that allows real-time access by all authorized stakeholders to the same, accurate information. This, in turn, facilitates faster, and better decision-making by stakeholders all along the supply chain. As in other systems, access to information can be controlled via user profiles that specify the access permissions for each participant in order to ensure that competitive information is not shared with the wrong stakeholders.

5.2.4 Incident management

When a supply chain breaks, it can often be very hard to recreate it in order to understand the root cause of issues. For example, a listeria outbreak in the UK may have been caused by contaminated vegetables from a foreign country. Rapidly identifying which country and which farm is responsible is key to maximizing the effectiveness of responses. According to the United States Department of Agriculture (USDA), food borne illnesses cost the US economy close to 16 billion United States dollars per year. Of course, globally this figure is even bigger. Being able to prevent and react smartly to these incidents has an enormous impact on the costs and efficiencies of businesses even outside of the supply chain.

Producers who receive returned parts because of defects could have a much more accurate and reliable source of data to use for identifying the root causes of quality issues. A well designed Blockchain identification and traceability system could allow them to identify the sources of the raw materials used, as well as the operators, supervisors and managers on shift during production and any other information that may be helpful in pattern recognition and root cause identification. This useful information could also include the history of the item after it left the factory.

Transport authorities who need reliable access to plan for and react to incidents involving the transport of dangerous goods could benefit from clear and immediate data from appropriately designed Blockchains.

5.2.5 Errors in payment processing and auditing

Occasionally, auditing may not identify all potential over and under billings or payments. Blockchain technology can help in reducing these errors using smart contracts for reconciliation and by providing a trustworthy and defined information-trail. This can then support the quick identification of where a problem has occurred. As a result, the company concerned will be able to verify the operating systems that were affected and make changes to prevent the problem from occurring again.

5.2.6 Data-based fraud

Even the most detailed audits can overlook indicators of fraud hidden in thousands of pieces of data. However, Blockchain technology is already enabling today's supply-chain entities to reduce and identify attempted fraud more easily.

For example, the simple use of Blockchain will deter attempts to change data because both the responsible party and the change to the data can be quickly identified on a Blockchain, so no secret changes. Indeed, any attempt to change data which has been already registered on a

Blockchain will normally be rejected as part of the consensus process for adding new data. This would both prevent fraud from occurring and allow companies to recognize the parties attempting to make unauthorized changes, driving down costs from potential fraud.

5.2.7 Dispute resolution

Similar to "Incident management" discussed above, disputes that arise for reasons of timing, quantity or quality could be simpler to resolve if reliable data on these questions (for example delivery time and date) was recorded on a Blockchain. In theory, some disputes could also be avoided by using a suite of smart contracts that self-execute, based upon conditions that are previously agreed by all parties, thus reducing administrative overheads and legal bills. See "Smart Contracts" under "Implementation Challenges" below.

5.2.8 Information ends at POS

Under current supply chain arrangements, with the limited exception of warranty-related items, the supply chain ends at the final consignee. Contact is lost with the product and important information on its usage is not captured. Using technologies such as quick reference codes (QR codes) and radio-frequency identification (RFID) together with Blockchain technology, the use of items during their lifecycle could be monitored with the user/consumer being automatically provided, via a Blockchain, with consumer benefits, product development, on sale/upsale and loyalty programmes, none of which have been practical using current, pre-Blockchain technology

5.3 Key stakeholders in improving supply chain transparency

Key stakeholders in improving supply-chain transparency and some thoughts on how they could benefit from Blockchain technology include:

5.3.1 Governments agencies including customs and excise.

Governments can leverage Blockchain technologies in ways that will help them to streamline and improve the areas mentioned below. It will also make it easier for countries whose border systems are currently not as advanced as other countries to implement best-practices more cost-effectively:

- Revenue taxation – Blockchain data can make auditing companies far simpler and more accurate while speeding up the collection of owed taxes by automating the levying of charges;
- Customs and excise – cross-border supply chains that leverage Blockchain technology will allow customs officials to increase the trustworthiness of the contents of shipments/consignments, allowing them to approve greater volumes of freight faster with less risk to the country's security and/or revenue, either by making selected supply chain data directly available to Customs or through the use of Blockchain to support the mutual recognition of Authorized Economic Operator (AEO) programmes as is already being done in part of Latin America[63]; and

[63] https://mag.wcoomd.org/magazine/wco-news-87/cadena-a-Blockchain-enabled-solution-for-the-implementation-of-mutual-recognition-arrangements-agreements/ (as of February 2020).

- Enforcement of compliance – easily being able to verify the contents of shipments/consignments and the sources of raw materials/finished products helps governmental bodies efficiently and effectively enforce their laws.

5.3.2 Consumers

Using near-field RFID technology and/or QR codes, Blockchains will make it possible for consumers to quickly obtain highly reliable information on individual store items. By scanning the code using an appropriate app, it will be possible to visually display the entire history of the item, showing place and time of production, processing and transit/ storage conditions of the item up to that moment, all based on information in a Blockchain.

5.3.3 Brokers

Much has been made of the potential for Blockchains to eliminate brokers and middlemen from supply chains, by reducing the risk to purchasers of dealing directly with suppliers, so the future may see significant changes in their roles.

5.3.4 Merchants and Brands

Merchants and product brands will be able to manage their supply chains with greater accuracy and lower friction as increased transparency, via Blockchain-based traceability systems, make it possible to view their entire supply chain from any connected device, enabling better decision making, reducing waste and lowering costs.

The falling costs of sensors, Internet-of-Things (IoT) devices and other technologies will allow merchants and brands to cost-effectively protect themselves against counterfeit goods even before full end-to-end Blockchains are implemented. For example: DNA tests can now be processed for under 100 United States dollars. Random samples of meat that are supposedly from a specific herd/strain can be DNA tested and compared to DNA samples which that farmer has previously posted on a Blockchain. This way it will be possible to tell quickly whether the received meat is coming from the expected herd regardless of whether the supply chain between the two parties is fully Blockchain-enabled. This protects both the consumer and farmer from mid-chain substitution of high value meats and produce.

5.3.5 Suppliers (primary and tertiary)

By being part of a Blockchain-linked supply chain, suppliers can add value to their businesses by reducing costs (automated data transfer, transparency of information) and potentially increase margins and markets.

Suppliers can get better quality feedback from stakeholders and consumers about their product. Consumers can be incentivized to deliver private feedback that suppliers can use to improve products. By limiting reviews to only those given by confirmed buyers it will be possible to increase the reliability of the feedback and reduce malicious or time-wasting reviews.

According to the WTO, this has the potential to lower costs in trade, including for lower- and middle-income countries, making them more competitive and opening up new markets.[64]

[64] https://www.wto.org/english/res_e/booksp_e/Blockchainrev18_e.pdf (as of February 2020).

5.3.6 Freight forwarders & wholesalers

By being able to more accurately assess where shrinkage, damage and other events occur, through the registration of changes on a Blockchain as part of product traceability, freight forwarders can be held appropriately accountable only for value-deleting events that occur during their stewardship of the goods.

To the extent that government agencies use Blockchain-based systems to increase transparency and provide more consistent processing speeds for regulatory and administrative processes (see A above), it should facilitate more accurate planning, reduce downtime/waiting time, reduce demurrage costs and allow for greater efficiency in the deployment of equipment, manpower and space. At the same time, it should be mentioned that other trade facilitation measures may need to be implemented in parallel in order to achieve this outcome.

5.3.7 Insurance stakeholders

In some instances, it may be possible to offer more cost-effective insurance via the use of smart contracts, when it is possible to provide a Blockchain with reliable data regarding insurable events. For example, when the temperature of a container with insured, temperature-sensitive, goods can be shown, via sensor data, to have been outside of the acceptable range for a determined time period, the smart contract could automatically pay the owner of the goods.

5.3.8 Finance stakeholders

Smart contracts may allow financial institutions to reduce risks by, for example, being able to provide loans to exporters based on invoices for export sales that have been verified by the importer on a Blockchain.

Using transactions and smart contracts on Blockchains should support reduced costs, for example by allowing the automatic reconciliation of purchases, shipments and payments as well as smart contracts that trigger payments when reliable data on completed transactions is received (for example for a letter of credit).

5.4 Conclusions

We are at the very early stages in an evolution of business practices, and possibly even cultural consciousness, as consumers increasingly see, on a day-to-day basis, the impact of their choices on others and on their environment.

Those companies who lead the way in supply chain transparency will not be able to implement fully functioning processes immediately. Blockchain is a new technology, the limitations and full potential of which are still being explored. In addition, there is ongoing, intense research on how to resolve a number of the key implementation issues for Blockchain systems including scalability (handling increasing data volumes with speed) and costs. At the same time, there are good examples of where Blockchain technology has been applied to solve existing problems at a significant benefit to its users. Many of those for supply chains have been outlined above and the list will probably expand with time.

6 Maritime trade

6.1 Introduction

6.1.1 The importance of maritime transport to global trade

With over eighty per cent of global trade by volume, and more than seventy per cent of its value, being carried on board ships and handled by seaports worldwide, the importance of maritime transport for trade and development cannot be overemphasized. In 2018, world seaborne trade volumes expanded by 2.7 per cent, down from a 4.1 percent expansion in 2017, and below the historical average annual growth of 3.5 percent over the past four decades. Despite setbacks, a milestone was set with total volumes reaching 11 billion tons, reflecting the addition of over 300 million tons of cargo, about half of which was attributed to dry-bulk commodities. The rapid expansion of e-commerce, enabled by digitalization and the use of electronic platforms, is a contributing factor to the continuing growth in seaborne trade which exceeded the three percent overall world economic growth in 2018. Projections for the medium term also point to continued expansion, with volumes growing at an estimated average annual growth rate of 3.4 percent up until 2023. Cargo flows are set to expand across all segments, with containerized, dry bulk and gas cargos recording the fastest growth:

- Global containerized trade expanded by 2.6 percent, a much slower rate than the six percent increase in 2017, with volumes attaining an estimated 152 million 20-foot equivalent units (TEUs).
- In 2018, world demand for dry bulk commodities consignments grew by 2.6 percent to a total of 5.2 billion tons.

In early 2019, the number of dead weight tons of capacity in container ships increased by 4.89 percent to 256,668 thousand tons and in oil tankers by 0.98 percent to 567,533 thousand tons. Overall, there was more than a 2.6 percent increase in the world fleet. Efficiency in ports made an impressive increase with the average time in port worldwide is decreasing from an estimated 1.37 days or 33 hours to 0.98 days or 23.5 hours. Container ships boast the best performance at 0.7 days spent within port limits. In contrast, liquid and dry bulk carriers seem to have longer port stays, averaging 0.94 and 2.05 days respectively.

Despite modest improvement in world seaborne trade volumes in 2018, weaker world economic and trade growth and rising cost pressures continued to weigh on the performance of world seaports. While these trends affect all ports, container ports are affected the most. In addition, container ports have been affected by the deployment of ever larger ships, the cascading of vessels from main trade lanes to secondary routes, a growing concentration in liner shipping companies, a reshuffling of liner shipping alliances and growing cybersecurity threats.

6.1.2 Players in the maritime trade industry

The number of parties that play a role in the maritime trade industry is large. On average, both in the country of origin and in the country of arrival, about 40 parties/companies play defined roles in the transport and logistics flow. For one roundtrip, on average, a cargo vessel will call in at 5 load and 5 discharge ports and a total of 1,000 active users will be involved in the total transport and cargo flows.

These parties can be split into:

- Those directing the transport and cargo processes (carriers, ships agents, forwarding agents, consignors/consignees /notify parties, terminal operators, warehouse storage keepers);
- Operational service providers (boatmen, pilots, tugboats, lashers);
- Operational suppliers (provision suppliers, bunkers, waste collectors, repairs);
- Hinterland transport operators (road, rail, barge);
- Government agencies (customs, veterinary, police, ministry of transport/health, environmental protection, port authorities, coastguard, emergency services);
- Inspection authorities (surveyors, pest control, phytosanitary); and
- Financial supporting services (banks, insurance companies).

All these parties play an important role in maritime trade. Without timely information they face issues in their planning which results in inefficiency and additional costs. Proper, correct information is important and, in ports where Port Community Systems are in use, is available for all concerned parties from a central point of contact. Some parties in the maritime trade industry act as intermediaries (ship agents, customs agent, etc.) and Blockchain technology may affect the way they work, so it is important for them to identify this impact and possible new role(s) for themselves in the Blockchain era.

6.1.3 Existing digital solutions in maritime trade

Many describe maritime trade as a very bureaucratic environment that involves large volumes of paperwork. It is, however, important to emphasise that, in a significant number of countries, the majority of processes are now carried out using existing digital solutions, some of these are described below.

Shipping portals[65] are electronic transaction platforms, which provide essential digital processes for booking, tracking and tracing and documentation, and which allow customers to communicate with carriers.

A Single Window is defined as a facility that allows parties involved in trade and transport to lodge standardized information and documents with a single-entry point to fulfil all import, export and transit-related regulatory requirements. If information is electronic, then individual data elements should only be submitted once.[66]

In a regional example, The EU Reporting Formalities Directive (2010/65/EU) that aims to simplify, harmonize, and rationalize administrative procedures and reporting requirements for maritime carriers calling at EU ports requires that Member States implement measures to allow the electronic submission and reception of reporting formalities concerning vessels, their crew and cargo via a national maritime Single Window.

A Port Community System (PCS) usually defines itself as a neutral and open electronic platform enabling intelligent and secure exchange of information between public and private stakeholders in order to improve the competitive position of the sea and air ports'

[65] IPCSA, The role of PCS in the development of the National Single Window, 2011
[66] See UNECE Recommendation 33, 2005:
http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec33/rec33_trd352e.pdf (as of February 2020).

communities. It is usually associated with a single port/airport, or multiple port/airport environments within an economy. Some governments regard the PCS as a private entity while, at the same time, considering it to be critical public infrastructure.[67]

A good collaboration between all the parties involved is one of the success factors of a PCS. Distinctive for all PCSs is the link to customs and port authorities and other institutions such as veterinary offices or the coastguard.[68]

For all parties involved, the core benefits include having a standardised communication platform that links operational, logistical and commercial processes which results in higher efficiency and speed for port processes, particularly through the automation and reduction of paperwork as well as improved punctuality, reliability and costs. Both within PCSs and across PCS systems data standardisation and electronic message standardisation are important to ensure smooth and safe operations as well as to reduce costs. Across the maritime world this need is largely met by data and message standards developed by UN/CEFACT.

By eliminating unnecessary paperwork which can considerably slow cargo handling, PCSs contribute to sustainable transport logistics and support the ambition of meeting global carbon reduction requirements. PCSs also perform as 'Gateways to a National or Regional Maritime Single Window' thereby connecting specific business sector actors to the public sector.

Digital negotiable bill of lading (B/L) providers accommodate the possibility of the digital transfer of titles which is an important function within ports where goods are regularly transferred between parties. Three platforms for the digital transfer of negotiable B/Ls have currently been approved by Protection and Indemnity Clubs.

Each of these platforms acts as an intermediary between various trading partners, with the intent of replacing paper title documents with electronic equivalents. Their scope extends to the financial institutions which finance the transactions in question. These solutions are capable of performing the three functions of a bill of lading namely as a proof of receipt, as a document of title and as a contract of carriage which incorporates the Hague or Hague-Visby Rules.

6.2 Blockchain opportunities for maritime trade

Applications of Blockchain technology can provide the following main opportunities and benefits for maritime trade, including for the logistics activities prior to and after seaborne transportation. These opportunities and benefits can be grouped as follows.

6.2.1 An improved means of sharing, distributing and verifying information

Currently in the maritime world, bilateral messaging is frequently used between a sender and a receiver, leaving out all the other parties engaged in a transaction. A receiver or a sender may also be a community system, relaying information between parties and sometimes even sharing with others. A trader in one part of the world, usually needs to know about and consult a large number of various systems in order to get the status of their traded goods that are on

[67] See UN/CEFACT "Technical Note on Terminology for Single Window and other electronic platforms", 2017, page 5:
http://www.unece.org/fileadmin/DAM/cefact/cf_plenary/2017_Plenary/ECE_TRADE_C_CEFACT_2017_10E_TechnicalNoteSW.pdf (as of February 2020).
[68] See UNECE Recommendation 37 on Single Submission Portals:
http://www.unece.org/fileadmin/DAM/cefact/cf_plenary/2019_plenary/ECE_TRADE_C_CEFACT_2019_06E.pdf

the other side of the world. To help with these challenges, traders can procure a service which gathers the required information on their behalf. In addition, at the moment when a shipper shares information with someone else, that information may already be outdated – or someone else may have better information from a better source.

Efforts to create systems which are a single source of truth, such as the third/fourth party logistics (3PL or 4PL) provided Supply Chain Management (SCM) systems, or carrier portals, are essentially gathering information, copying information from various sources and storing them in a centralized database. However, information is required from intermediary providers (such as carriers) and, by design, a central database can always be altered by someone with such privileges. In addition, the timeliness and authentication of the data provided depends upon the aforementioned intermediaries and their participation in the system.

A Blockchain has the potential to increase transparency and availability of information for all participants subject to commercial data confidentiality. A valid transaction stored in a shared ledger will exist in everyone's copy of that ledger. Transactions are not sent to a receiver but saved to a ledger which is then sent to everyone on the network with its updates. It is, therefore, possible for everyone or everything (i.e. Internet of Things – IoT devices) that produces events in a transport chain to potentially share that information with the world. As one IoT example, the crane of a terminal can report the successful loading of a container onto a ship.

A party having an interest in a transaction, such as the seller, buyer or banks, can simply consult their own copy of a shared ledger to see what the current status is or verify information relating to a transaction. This, therefore, increases trustworthiness between the parties beyond the correctness of the documents.

Blockchains thus provide reliable data, which everyone who has a node verifies and owns (everyone has a copy – even if they cannot read what they do not have permission to access). This overcomes one of the principle obstacles to data pipeline applications (which also provide access to common data) which is answering, who will all parties accredit to hold and maintain the data?

It is up to the design of the Blockchain ledger and the systems around it, to determine how access to this information is granted to parties that hold a copy of that ledger.

> *"According to most study participants, the key advantages of distributed ledgers in comparison to existing systems and database technologies seem to lie in their automated reconciliation mechanisms, their transparent nature, and their resilience. The first removes traditional reconciliation efforts required for 'siloed' databases, thereby significantly increasing processing speed and reducing costs throughout the entire operational process.*
>
> *The second enables traceability of anything represented on the ledger, preventing manipulation through the public auditability of the system. Finally, the third provides higher availability and reliability, as well as protection at the system level against some types of cyberattacks."*[69]

[69] Dr Garrick Hileman & Michel Rauchs, Cambridge, GLOBAL BLOCKCHAIN BENCHMARKING STUDY, 2017 https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-09-27-ccaf-globalbchain.pdf (as of February 2020).

6.2.2 More efficient transfer of digital assets

The Internet as we know it was built around freely copying information from one place to another. This is inherently unsuited to the transfer of assets due to the risk of double spending (selling the same asset twice). The lack of efficient options to ensure the security of assets has hindered the exploration of such options. Prior to Blockchain technology, the secure digitalization of assets required the use of third-party intermediaries to guarantee the uniqueness of digital assets and related transactions which added a cost to these transactions. In addition, the related, centralized databases and intermediaries created single points of failure which prevented the wide adoption of such options.

Blockchain does enable the efficient and immediate transfer of assets. The most obvious transfer of assets, in transport, is the document giving title to the goods, one of the functions of the negotiable B/L. A payment obligation or a letter of credit may be its counterpart.

In their current form, non-negotiable seaway bills of lading, which remove the need to send paper documents to the destination for exchange when the goods are picked-up, still retain one problem: the goods are in the seller's possession until released at the destination to the receiver. The party who contracted carriage remains in control of the goods until just before delivery, and he may change the delivery instructions – including the consignee – as permitted under the terms of the contract of carriage. This provides reduced security for all parties involved. A Blockchain digital transfer of assets could provide the benefits of quick transfer, and security.

With the possibility of efficiently transferring assets, Blockchain technology offers the maritime industry an opportunity to explore other options – everything can become an asset. A space reservation, an allocation agreement, the right to pick up or drop-off a container at a terminal, time-slots in terminals, etc.

Such assets can be securely represented on a Blockchain by data packages called "tokens" which can be bought, sold and traded on a Blockchain, much like crypto-coins. For example:

- A carrier may provide a cargo receiver with a "right to pick up the cargo" token. This token can be transferred to a trucker.
- A trucker may get a Blockchain token from a terminal for a specific time-slot. If the trucker cannot keep his timeslot, he may pass it on to someone else registered on the Blockchain. Or the trucker could trade it to procure a new time-slot for himself.
- A carrier may issue securities for space on a voyage. That security may be traded or exchanged among different parties. Currently, this would require cancellations and re-bookings and is tied to various sub-processes and actions required by multiple parties, making the process very inefficient. Intermediaries, such as freight forwarders have taken on this task in the past, with the recurring issue, that space ended up not being used, even during peak-seasons. Issuing tokens instead could result in final information regarding the "owners" of the space on that voyage being available to all parties at the appropriate time and create a largely simplified process.
- Blockchain also provides the opportunity to separate the function of "document of title" from the "contract of carriage".

6.2.3 Automation of contractual obligations through smart contracts

In maritime transport, current process automation stops at the point where assets and their legal ownership change, which often takes place against a payment and is formalized with

paper documents. This exchange of goods against payment process is handled through separate financial and physical flows. These two flows can be synchronized if both assets exist in (or can be represented by) a digital form. Swapping of assets can then happen through smart contracts. For example, a negotiable B/L may be swapped against the payment obligation of the party financing the trade. Common carriers may likewise execute their right to a lien by swapping a negotiable B/L against payment of charges, at origin as well as at destination.

6.2.4 Increased security

6.2.4.1 Document security related to negotiable B/L

Paper documents today are exposed to various security threats. A negotiable B/L may be issued by one party only, therefore the information it contains cannot be counter checked by other parties. Common fraudulent behaviours are the issuing of fake B/Ls, falsely dated B/Ls or documents containing false information created by switching B/Ls or false descriptions regarding the nature of goods. Negotiable B/Ls are also lost occasionally and then access to goods are usually only granted against bank guarantees exceeding the value of the cargo. While a digital asset can be lost as well, it is up to the party to ensure that their assets are stored and backed-up in a safe way (i.e. they do not have to rely upon a third party).

Blockchain applications mitigate such threats by using multiple sources to validate information. Issuers of documents and contributors of data elements may be identified with keys that prove their existence. The content of a document may be used to calculate a hash value, and that hash can be stored in a Blockchain providing an immutable verification of the content. The content can be checked against that hash to verify if it is the original.

External sources can be used to add additional information and trigger transactions. These oracles may be a port, that verifies a vessel has departed, a terminal that has loaded the cargo onto the ship or even both. It will be possible to have the information verified by multiple parties which will make forgery much more complex to achieve.

Current applications to address these problems require third party, neutral, notarization services, that add transactional costs which many Blockchain applications could eliminate.

In the case of a loss of a negotiable B/L, Blockchain technology allows a carrier to track if an asset (the tokenized bill of lading) was indeed transferred to someone else. This is impossible to track and verify in a paper scenario. Carriers require bank guarantees provided by a seller/consignor or buyer/consignee to release the goods nevertheless. These guarantees often were set at 200 percent of the cargo value over a timespan of multiple years. With the data exchange traceability provided by Blockchains, carriers may be able to very significantly reduce their risk of release without the presentation of the digital asset.

The above observations extend to other documents used in maritime transportation, such as certificates of origin, packing lists, dangerous goods declarations, customs bond documents, phytosanitary certificates etc.

6.2.4.2 Right to access the goods

There are ports where the current release information for goods is sent to cargo receivers through unencrypted e-mail. When pin-codes and container numbers are used to pick-up containers, it is still possible that this information is relayed to a wrong party: a party not authorized by the cargo owner to pick up the container. The same applies for the pick-up of

an empty container or the drop-off of a full container at a terminal where, currently, unencrypted information is transferred by e-mail or paper. If such rights are tokenized and exchanged on a Blockchain, then they exist only once, and the use and transfer of these tokens can be traced.

6.2.4.3 Trade compliance

Regulations and compliance rules are generally enforced by human controls. With additional regulations being implemented worldwide, keeping up to date has become difficult. The increased number of transactions also leads to cognitive fatigue by the users verifying transactions. The review of paper documents by people also tends to be less predictable than the review of digitalized documents by information systems.

Through smart contracts, transport information may be shared with an algorithmic compliance checking system. Such systems can be continuously updated with the most current rules and regulations. In such a scenario, information for a transaction may be accessed by regulators that have access to a ledger, even before the transaction happens. Then, if the compliance check results in approval, the transaction may proceed.

Other compliance checks could be, for example, against IMO rules for the transportation of dangerous goods by sea. It might even be useful, where regulatory verification services exist, to extend the scope of checks, that would allow stakeholders to check not only the IMO rules before the goods are transported, but also specific rules that may apply during the pre- or on-carriage of a containerized transport movement under different rules and regulations (i.e. special rules for inland water ways, country specific laws).

In these compliance verification cases, the advantages of Blockchain over a centralized database system are the ability to ensure that digitalized data is original (and cannot later be changed), reduced risks of fraud, and the ability for companies and regulators or third parties to provide this information without needing access to multiple company or regulatory systems.

Distributed ledger networks provide regulators with the opportunity to monitor, supervise and audit trades and agreements in real time, which would be a drastic improvement over regulatory systems in place today.

6.2.4.4 Terms and conditions

The contract of carriage and its terms and conditions may not be clear to the party receiving the goods. Destination as well as auxiliary charges may apply such as destination terminal handling, demurrage, detention or port storage. With the digitization of the release of goods, applications could require that such charges be registered on a Blockchain and the terms be explicitly accepted by cargo receivers in an efficient way. Currently, these terms are not clearly visible to the receiving party because the terms are not explicitly indicated on the contract of carriage itself. Such an application would provide transparency to the receiving party regarding the charges to be paid when requesting the pick-up of goods, and having the charges registered on a Blockchain would show that they are valid and not “invoice padding” to increase the carrier’s margins. This would also assure the carrier that these charges are accepted by the receiving party.

6.2.4.5 Time and cost reductions

The main time and cost reductions can be achieved where paper is currently the only means to transfer information and title from one party to another because of the need to ensure that documents are unique or unchanged. Wherever there is currently a lot of such paperwork and many different stakeholders involved, efficiency gains can be achieved. In maritime, this is mainly the case where an original negotiable B/L is used. These paper documents travel normally by courier or mail from the issuing office to the shipper, his bank, the buyer's bank, the buyer and finally to the party releasing the goods.

Each of these paper-based transfers takes time to open, verify, and send to the next party. Depending on the distance between the parties, this process can take multiple days if not weeks and multiple courier or postage charges are applied. Undertaking these transfers using Blockchain applications could result in funds being released faster to the seller, and buyers having options for refinancing goods that are in their legal possession, instead of funds being blocked by guarantees.

By using a secure and reliable digital document, each transfer can be done within minutes and is potentially cheaper than paying a courier or postal service. Compliance checks done by algorithms can verify information almost instantaneously. Then, if a regulator has the power to veto a transaction, it can be done in real time. Through such immediate rejection, the regulator can prevent a vetoed transaction from being finalized. This can result in major time and cost saving as compared to correcting after a vetoed transaction has happened.

Registering and tracking information in one Blockchain source, creates a chain of visibility allowing parties to quickly get information that, before, was locked in different information silos. Time intense and error-prone human reconciliation of transactions can be eliminated or reduced using Blockchain applications and the laborious collection of information from multiple sources can become obsolete, thus reducing manual labour and costs. This approach also has the potential to reduce costs by allowing stakeholders to reduce the number of bilateral digital and paper interfaces they need to maintain.

6.3 Challenges to implementing Blockchain in maritime trade

While there are many potential benefits to implementing Blockchain technology in maritime trade, there are also a number of important challenges to its implementation.

6.3.1 Technology maturity

Even though Blockchain technology has been around since 2009, and some of its components have even been used before, the technology is still not mature enough to be used widely in a conservative industry like the maritime trade. There are some more advanced Blockchain platforms, but it is still not clear which platform will last and a wrong decision today may lead to a lost investment so many of the maritime trading partners prefer to wait for a clearer picture.

6.3.2 Lack of expert developers

Maritime trading partners that decide to implement Blockchain technology today will find it difficult to access the needed expertise for implementing because there is a lack of Blockchain talent and educational programs to develop such talent. There are a growing number of Blockchain start-ups, including in the maritime trade sector but they primarily sell standard products/solutions and do not develop tailor-made applications

6.3.3 Long transaction confirmation time

Many Blockchains have transaction confirmation times that are too long for high-volume and time-sensitive transactions. Transaction confirmation times are determined by a range of parameters including the consensus mechanism used, the number of validators, the technology used, etc. Some Blockchains have shorter confirmation times, although faster response time is often purchased at a cost which compromises, to some degree, other desirable Blockchain characteristics.

In some maritime trade applications such delays would cause a serious problem, especially in applications that use real-time IoT devices for monitoring (for example of location, temperature, etc.) where transactions need to be confirmed and validated in a short time window, preferably milliseconds, and where the volume could reach millions per day. This is a key unresolved issue for the maritime sector and the results of current intense research by Blockchain experts and organizations to resolve this issue, if successful, could unleash a tidal wave of applications that will transform trade.

6.3.4 Legal recognition

When looking to transform a maritime trade business process through the use of Blockchain technology, one common concern is the recognition of the new process and its results by legal authorities, for example, in the case of a dispute.

It is, therefore, very important that Blockchain technology be accepted by legal parties and, after thorough analyses, be accepted as a 100 per cent guarantee of the endorsement and reliability of the data.

In 2017, the United Nations Commission on International Trade Law (UNCITRAL) published the "Model Law on Electronic Transferable Records" which considers the possibility of using distributed ledger technologies. For example, one relevant paragraph is:

> *" Certain electronic transferable records management systems, such as those based on distributed ledgers, may identify the signatory by referring to pseudonyms rather than to real names. That identification, and the possibility of linking pseudonym and real name, including based on factual elements to be found outside distributed ledger systems, could satisfy the requirement to identify the signatory."*[70]

This is an important development, at the same time, it will take time for countries to adopt the model law so that it is reflected in national legislation.

6.3.5 Regulatory recognition

Some maritime trade processes are regulated by different authorities: port authorities, customs, etc. and some of them also involve financial partners like banks and insurance companies that are also regulated, but by other authorities.

Some of those authorities are just recently making efforts to move away from paper documents and have made large investments in new IT systems, so it may be politically difficult for them to migrate soon to a Blockchain-based solution. On the other hand, where this automation has been based on international standards, such as the case of the International Plant Protection Convention (IPPC) which is moving the phytosanitary certificate to a digital

[70] https://www.uncitral.org/pdf/english/texts/electcom/MLETR_ebook.pdf (as of February 2020).

e-phyto certificate based on UN/CEFACT standards[71], the future exchange of information with Blockchain-based solutions may be facilitated.

6.3.6 Data ownership, personal privacy, General Data Protection Regulation

Maritime trade community members are sometimes competitors and sometimes may be partners and if they are using one Blockchain network, special care will need to be taken to protect the data and to give Blockchain network members access only to relevant information. In addition, the protection of private information needs to be considered, including user names, contact details and information where users can be identified such as data for the shipment of personal goods. Under the new European Union General Data Protection Regulation (EU GDPR) which came into force in 2018 there is a requirement to protect privacy by design, i.e. it should be part of the design and development of the system. In addition, the law also provides for the right to be forgotten and if one party/individual in a Blockchain requests to be forgotten there are still questions over how, in a Blockchain or archived Blockchain, this can be achieved, although a growing number of solutions have been proposed.

6.3.7 Overlap between solutions

The maritime trade sector is not an isolated island in the supply chain. Many aspects of maritime trade influence and are influenced by other sectors: finance, insurance, land transportation (road/rail), agriculture, etc.

There are Blockchain initiatives in all of those sectors that compete for the resources of their partners and the lack of coordination between relevant initiatives slows down the progress of all the initiatives.

6.3.8 Interoperability of Blockchain networks

Even though there are Blockchain initiatives in the maritime trade sector that aim to provide solutions to all maritime trade members and to all of their needs, we believe that, in the end, there will be a number of co-existing solutions.

If those networks won't intercommunicate with each other, they will be silos of information, not allowing users to see the whole supply chain picture and will reduce the overall effectiveness of each Blockchain network.

6.3.9 Use Blockchain only when needed

"Through 2018, 85 per cent of Blockchain-named projects would deliver business value without using a Blockchain."[72] Maritime-trade participants should study carefully the business processes they want to implement with Blockchain technology and do so only for those that can't be done better using other technologies.

[71] See: https://www.unece.org/uncefact/mainstandards.html#ui-accordion-jfmulticontent_c66452-panel-1 (as of February 2020)
[72] Rajesh Kandaswamy, Gartner webinar, 2017

6.3.10 Multiple players with different technology adoption levels

The maritime trade community has a huge number of stakeholders as detailed above, and a significant percentage are conservative companies or small/medium companies that will not adopt quickly new technology.

To allow the early adopters in the maritime trade sector to use Blockchain technology, while still doing business with the late adopters, there is a need for parties that will supply mediating procedures or bridge technologies that will allow this to happen.

UNCITRAL in the "Model Law on Electronic Transferable Records" mentioned earlier, also discusses the need to handle this situation from the legal perspective:

> *"If the law recognizes the use of both transferable documents or instruments and electronic transferable records, the need for a change of medium may arise during the life cycle of those documents, instruments or records. Enabling change of medium is critical for the wider acceptance and use of electronic transferable records, especially when used across borders, given the different levels of acceptance of electronic means and readiness for their use in different States and business communities."*[73]

6.3.11 Need to change business processes

The following quote from a Cambridge study is very relevant to the conservative maritime trade community: "Another major challenge to DLT that needs to be overcome is the general reluctance of enterprises to change established business processes, which is, in many cases, a necessary requirement for DLT to take meaningful effect."[74]

6.3.12 Missing open standards

Many Blockchain start-ups are using proprietary standards with different data definitions for the same data element, thus causing potential confusion in the marketplace, particularly where data needs to be exchanged between multiple parties. Data definitions and data elements should comply with currently used international standards which in the maritime industry is UN/EDIFACT and thus, by default, with the Multi Modal Transport Reference Data Model[75] which is based on a subset of the Core Component Library of UN/CEFACT.

6.3.13 Cybersecurity threats and risks

Like most trade sectors, the maritime trade sector deals with growing cybersecurity threats. To adopt Blockchain in the maritime trade, its members have to be confident that this technology is safe. The introduction of quantum computers in the future may affect Blockchain security so the development and implementation of quantum proof Blockchain may create more trustworthiness by maritime trade members in Blockchain.

---

[73] https://www.uncitral.org/pdf/english/texts/electcom/MLETR_ebook.pdf (as of February 2020).

[74] Dr Garrick Hileman & Michel Rauchs ,Cambridge, GLOBAL BLOCKCHAIN BENCHMARKING STUDY, 2017 https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-09-27-ccaf-globalbchain.pdf (as of February 2020).

[75] See: https://www.unece.org/uncefact/mainstandards.html#ui-accordion-jfmulticontent_c66199-panel-0 (as of February 2020)

6.3.14 MSMEs' ability to be integrated into Blockchain-based systems

Most Micro, Small and Medium sized Enterprises (MSMEs) that take part in maritime trade lack the technological expertise to implement Blockchain solutions and thus will require support from third parties to implement a solution. This could lead to a two-speed technological change where large enterprises with the technological knowhow start to run Blockchain solutions which affect MSME's but these MSME's require third party support and this could increase their costs when compared to current solutions.

6.4 Use cases

UN/CEFACT have a repository of Blockchain use cases[76], in which authors have identified a number of important case studies that can be divided into the following types of solutions such as:

- Digitalizes a specific paper-based business process that requires transparency and auditability, and is sensitive to the 'double spending' problem (i.e. the same digital file being 'copy-and-pasted' and transferred multiple times)
- Improves business processes that are already digitalized by: making them more fraud resilient and robust to attacks; adding process automation using smart contracts; "monetizing" the business process
- Digitalizes an entire section that is all paper/e-mail based
- Digital solution for a newly identified business requirement

6.5 Conclusions

More than 80 per cent of global trade by volume is carried by the international shipping industry. Any increased efficiency in the maritime trade sector can have significant effects on global GDP. Blockchain may be one of the key drivers for enhancing the efficiency of maritime trade in the future.

As described above, Blockchain can bring many opportunities and benefits to maritime trade:

- Better means of sharing/distributing/verifying information exchanges and for transferring digital assets;
- As a driver for process automation.

This can lead to time and cost reductions, so it is important to keep investigating the opportunities and benefits that it can bring and implement wisely the identified Blockchain-based solutions. Blockchain is not the solution for all problems so it is important to implement Blockchain in maritime trade processes that take advantage of the special characteristics of the technology.

We expect that in the maritime trade sector and at its interfaces there will be a number of Blockchain solutions, and for that reason working on interoperability standards between different Blockchain networks is extremely important and UN/CEFACT can play an important role in this area.

Open, international standards such as those produced by UN/CEFACT will be essential to ensuring the interoperability of Blockchain solutions.

[76] UN/CEFACT Blockchain repository: http://www.unece.org/tradewelcome/un-centre-for-trade-facilitation-and-e-business-uncefact/case-study-repositories.html

Port Community Systems, which are strategic assets for process harmonization and integration, could bring added value to the implementation of Blockchain-based business processes in the maritime trade sector. As one example, Port Community Systems may be able to be the bridge between different Blockchain local/global networks and the different technology adoption levels of users.

Is Blockchain a game changer in maritime trade? We assume it is, the introduction of Blockchain has acted as a wakeup call to this traditional and conservative community that is now very busy running a large number of Blockchain proof of concept and trial implementation initiatives.

Important factors that could delay the impact of Blockchain applications as a game changer in maritime trade is the access to know-how about maritime logistics and the lack of developers with Blockchain expertise as described earlier.

7 Road Transport

7.1 Introduction

Road transport is a crucial economic activity. It brings people together and it carries goods to where they are needed. The vast majority of the daily needs of the population is delivered by road.

Moreover, the provision of road transport services is an important economic sector in its own right. As an example, within the European Union, the road freight industry generates two percent of GDP, provides employment to three million people and generates a turnover of over 330 billion euros.[77] Total inland freight transport in the EU-28 was estimated to be just over 2 438 billion tonne-kilometres (km) in 2017; some three quarters of this freight total was transported over roads. In the 28 Member States of the European Union (EU-28), in 2017, the share of inland freight that was transported by road (76.7 percent) was more than four times as high as the share transported by rail (17.6 percent), while the remainder (6.0 percent) of the freight transported was carried along inland waterways. In 2017, there were over 550,000 companies in the EU providing road freight transport services as their main business.[78]

Customer expectations are increasing greatly. Both individuals and businesses expect to get goods faster, more flexibly, and – in the case of consumers – at low or no delivery cost. In addition, manufacturing is becoming more and more customised, which is good for customers but hard work for the logistics industry. Add it all together and the sector is under growing pressure to deliver better service at an ever-lower cost.

An increasingly competitive environment is another big factor in the mix. Some of the sector's customers are starting their own logistics operations, and new entrants to the industry are finding ways to carve out the more lucrative elements of the value chain by exploiting digital technology or new sharing business models, and they don't have asset-heavy balance sheets or cumbersome existing systems weighing them down.

Manufacturing industries are facing far greater expectations with regard to efficiency and performance than ever before. Their customers expect faster time-to-market, reduced defect rates and customized products.

As in other transport industries, the road transport industry uses a lot of paper, not to say that it uses exclusively paper. However, in the case of road transport, it's even worse than other transport sectors because of historical issues of equipment and Internet access on the road.

On top of the transport document itself, there are other documents which need to be handled by the carrier or carried on board the truck such as a driver's card, mandatory training certification, agreement certificates, licenses, technical inspection certificate, invoices for the goods transported, consignment notes, documents for ports/docks, bills of lading, customs documents if needed, fiscal documents and many others.

In addition, commercial transportation transactions also involve a large number of papers, such as sales contracts, charter party agreements, bills of lading, consignment notes, letters of credit and others, some of which overlap with those which the carrier and truck driver must

[77] Road Freight Market In The European Union, Dora Naletina, https://bib.irb.hr/datoteka/972757.Road_freight_market_in_the_European_Union.pdf (as of February 2020).

[78] Source DG TRANSPORT: https://ec.europa.eu/transport/sites/transport/files/connect-to-compete-growth_2016_en.pdf AND, an Overview of the EU Road Transport Market 2015 (http://bit.ly/2BP61Ya (as of February 2020).

manage. All these documents may need to pass through a long chain of parties with many controls since their importance is high, with various payments as well as the carriage and delivery of the cargo depending upon their existence and accuracy. Look for an example at negotiable bills of lading (B/Ls) and the long trail they follow: starting from the party(s) at the loading port, they pass through several banks until they reach the receiver of the merchandise. This procedure can be so lengthy and time-consuming that it is very common for vessels to arrive at the discharge port before all of its B/Ls are available (and likewise for trucks to arrive at their destination before their related bills of lading).

Another factor to consider is that, today, road transport vehicles are highly connected with many electronic devices which provide information to drivers in real time (i.e., help for economical driving, best routes, how to avoid traffic, toll payments, etc.). They are being equipped with devices that also collect an exponential quantity of quantitative data (i.e., driving and resting times, number of kilometres travelled, energy/fuel consumption, etc.), as well as qualitative data (i.e., styles of conduct, historical or real-time location, video sequences showing the road or the inside of the vehicle, etc.).

This data, collected on-board, can be added to other data, which can be internal to the company (i.e., from purchasing departments, sales, maintenance, human resources etc.), as well as external data, mainly concerning the state of the road network like the traffic, weather forecasts, the impact of big sports or cultural events on road congestion, etc.

If every time a product changed hands the transaction could be documented, creating a permanent history of a product and its journey from manufacture to sale, this could dramatically reduce the time delays, costs, and human error that plague transactions today.

Blockchain technology can support the development of such systems and has the potential to revolutionize the future of trucking and logistics by providing the basis for new systems for completing transactions, authenticating documents, tracking shipments, managing fleets, solving claims and much more. By providing trustworthy information on cargos, transport and related freight payments, Blockchain could provide supply-chain participants with: efficiency gains; savings in terms of document management; better and quicker decision processes; quicker invoicing processes, etc. And via the use of smart contracts, Blockchain systems could also provide better controls on the enforcement of contract conditions and the enforcement of legal requirements in transport by authorities.

Blockchain technology offers many different benefits to the transport and supply-chain sector, and its applications range from simple asset tracking and transparency to real-time feedback from customers. A detailed description of potential benefits from the implementation of Blockchain technology in this sector can be found in the section on supply chains above under challenges and stakeholders.

One potential future use of Blockchain in road transport is improved asset utilization through open forecasting. A 2016 report, “Trust in trade, toward stronger supply chains”, emphasizes the importance of trustworthiness and forecasting.[79] Carriers, for example, almost always receive orders only a few days in advance. This makes it difficult for them to optimize cargo or infrastructure and to aggregate the kinds of data they would need to forecast their transport capacity needs.

With access to better and more trustworthy data, carriers could more accurately predict where capacity will be needed and more dynamically route their vehicles into these areas. This kind

[79] See https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03771USEN& (as of February 2020).

of cooperation could also reduce inventories and ensure that demand for capacity and, as a result, transportation charging rates, reflect actual needs and are not artificial numbers which fluctuate widely. A carrier might not have a trusted relationship with a consignor or manufacturer but participating together in a Blockchain network could change this. Transparency and visibility could open up new partnerships that they hadn't considered before. Drivers too will have an important role in the implementation of Blockchain-based systems, as they add their own data, often automatically, such as times on and off duty, the road conditions, condition of the load and vehicle and much more.

Trustworthy information registered on the Blockchain by drivers and by remote sensors could also help carriers in disputes with consignors, their own sub-contractors about when and where an event, such as a crash or goods damage, occurred – or with regulators about compliance with equipment and workforce regulations. It might also support their opinion about unsafe vehicles or those that require repairs.

More details about benefits that Blockchain technology could bring to specific problems in road transport are described below.

7.2 Theft prevention

Globally, cargo theft costs the road and rail transport industries between 23[80] and 60[81] billion United States dollars per year.[82] Blockchain technology can help in discouraging and nearly eliminating some forms of cargo theft. One common form of theft is for a thief to identify a scheduled pickup time and show up two hours earlier using the excuse that traffic was light. A dock worker, none the wiser, looks at the paperwork and it all appears in order, so the trailer is loaded, or the driver hooks up to a loaded trailer, and no one suspects anything until the real carrier arrives a few hours later. By then, the thief and load are long gone.

Using Blockchain technology, it becomes much more difficult for a thief to perform such a hold up. You can do a much better job identifying who is who because of the ability to easily connect to a Blockchain where information, linked to the goods by a unique digital identifier, has been registered and cannot be hacked. This can provide the dockworker with a verified digital copy of the paperwork and even a photo showing who the driver is.

Carriers can also have a secure record of who accesses the system to obtain information using Blockchain. These same Blockchain characteristics (including the registration of data from remote sensors through the Internet of Things) can reduce theft by providing a continual, and transparent, record of a shipment's status. Digitally verified, information about how many boxes were loaded and unloaded on a trailer can be combined with GPS data and even door sensors that indicate when and where the trailer doors were opened. This data can then be used to quickly identify the exact point of a theft.

In the case of cargo theft, who is trustworthy? A digital record can go a long way toward creating that trustworthiness. In addition to preventing the theft of trailers and cargo by creating easily identifiable indicators to verify legitimate carriers, Blockchain also has the potential to prevent theft of even a single package from a trailer.

[80] https://www.securecargo.org/news/cargo-theft-and-supply-chain-disruption-cost-56bn-last-year-and-theres-more-to-come (as of February 2020).
[81] http://www.tlimagazine.com/sections/columns/1829-cargo-theft-today (as of February 2020).
[82] Also see https://www.ttclub.com/fileadmin/uploads/tt-club/Documents/BSI_TT_ClubCargoTheftReportH1_2018_FinalRev.pdf (as of February 2020).

To address this issue, one approach is to use encrypted microchips to track goods and prevent counterfeiters.[83] For instance, a microchip can be attached to artwork, sneakers, wine or anything else that is frequently faked so that the buyer can verify the item's authenticity. The same technology could, potentially, be used in the supply chain by adding microchips or GPS trackers onto individual boxes, pallets or trailers. Data collected from these devices could be added to the Blockchain all along the steps in the supply chain, using GPS data. Doing so would identify where and approximately when any item or container disappeared, thus ensuring that every box and pallet arrives at its destination in good shape. Today, this is economically feasible only for very expensive goods, but the continuing miniaturisation of sensors and falling costs will eventually enlarge the selection of goods for which such tracking is cost effective.

The section on supply chains contains more information on the use of Blockchain for tracking the provenance and movement of goods.

7.3 Fleet and asset management

Today's container-based logistics systems requires the management of very complex processes for matching goods with available containers and transporters, moving across multiple transport modes to a range of global destinations and very commonly using multiple logistics service providers for individual shipments, resulting in complex networks of partners and contracts. Just to give an idea of the volumes of data concerned, the numbers of containers shipped via maritime ports during 2018 was over 150 million[84] with 5 percent growth predicted for 2019.[85] The vast majority of these containers were brought to or picked up from ports via road transport (and some via combinations of road and rail or inland water barges). Many of these containers contain consignments from multiple consignors, going to different final destinations. These statistics do not include the many containers that stay on trucks and do not change transport modes, or which travel via only road and rail. In addition to managing these consignments in one direction, transport companies need to reduce costs and carbon emissions by keeping their trucks and containers filled on return trips.

Blockchain could support this planning. One example is in-vehicle tracking systems which could supply data to the Blockchain allowing the verification of a truck's route, its speed, and any delays. This would provide verifiable documentation for fleets to justify delays, for example. Because each entry in a Blockchain is also time-stamped, these entries could also be used to justify/explain detention billing.

Another approach being considered to these complex planning, billing and reconciliation processes is Blockchain-based bidding processes for managing containers, trucks and other assets such as pallets.

For example, a company in Finland is working on a Blockchain solution to enable smart tendering across supply chains in order to manage the use of pallets.[86] Pallets equipped with Radio Frequency Identification (RFID) tags publish their need to get from point A to point B on the ledger. Carrier applications then place bids to win the move. The Blockchain awards the job to the bidder with the most suitable conditions and the transaction is registered on the

[83] https://chronicled.com/ (as of February 2020).
[84] UNCTAD Maritime Transport Report 2018, figure 1.5 - https://unctad.org/en/PublicationsLibrary/rmt2018_en.pdf (as of February 2020).
[85] https://www.mdst.co.uk/changing-lanes (as of February 2020).
[86] https://www.forbes.com/sites/stevebanker/2016/06/05/building-a-secure-transportation-tendering-and-tracking-application/#232f537a4e5c (as of February 2020).

Blockchain. The shipment/pallet will be progressively tracked as the tag moves down the supply chain and pallets that are available for re-use can be identified and, possibly, recycled.

Each of the trucks and railway wagons involved in goods transportation need to be properly maintained, so their mileage and repairs need to be tracked. One potential maintenance application could be management of information from Driver Vehicle Condition Report (DVCRs) that a driver fills out before and after the completion of a trip. Currently this is a very paper intensive process that should convey the condition of transportation equipment to operations, safety and maintenance. If automated and incorporated into a Blockchain, all the inspection and maintenance information could travel with the equipment throughout its lifecycle, including through changes of ownership – where there is typically a lack of trust between buyer and seller regarding the quality of used vehicles.

Information that needs to be verifiable, such as for inspections, maintenance performance records and recall information could all be part of this Blockchain. This would ultimately simplify asset management and utilization tasks.

Most truck Original Equipment Manufacturers (OEM) have introduced remote diagnostic capabilities whereby vehicles can send codes, back to the maintenance shop for diagnosing and repair. These would be registered in the above described system for tracking all inspection and maintenance on trucks, but what if that repair code is tied to a recall, could this be identified? Also, maybe only some trucks in a fleet are affected by a recall because the part has already been replaced on others. Using the reconciliation and traceability functions of a Blockchain, identifying affected vehicles could take seconds because each repair for each vehicle would have already been entered into that vehicle's Blockchain data.

Another example is on-road repairs which are a necessary evil, but fleets don't always have their own repair shop in locations where their vehicles are. In those situations, a Blockchain application that tracks repairs and service providers could be a trustworthy source of information for identifying which repairs the local repair shop has performed, the quality of the work and whether the parts used have been genuine.

Thus, a Blockchain could maintain a visible and reliable record to hold each person who performs maintenance on a vehicle responsible for their work. That kind of detail provides increased visibility into the supply chain, making everyone more confident in the movement of goods while increasing safety and on-time performance.

7.4 Proof of regulatory compliance

One area where Blockchain technology could provide a major boost, is in proving regulatory compliance and chain of custody to enforcement authorities. For example, Blockchain records could help guarantee precise and fair road checks by inspectors for cabotage (the regulated transport of goods or passengers between two places in the same country by a transport operator from another country).

The integrity of a document, such as a consignment note for road transport[87] (called a CMR[88]), could be established by its issuance, handling and exchange on a Blockchain in a digitalized

[87] The CMR is a document prepared by a consignor and countersigned by the carrier as a proof of receipt of a consignment for delivery at the destination. Used as an alternative to a bill of lading (especially in inland transport), it is generally neither a contract of carriage nor a negotiable instrument (i.e. it cannot be used for transferring the ownership of the goods).

[88] CMR stands for 'Convention relative au contrat de transport international de Marchandises par route,' the French name for the convention that governs its definitions and application. ; UN/CEFACT has developed an

way, and this would perfectly fit the authorities' requirement that the document provided to them be the sole and only version/copy, thus avoiding the current practice of multiple CMRs being handled for the same load which makes efficient controls difficult to perform. It would also simplify the checks of consignment notes and make them quicker.

Another highly regulated sector, where the use of Blockchain would make sense, is the transport of food products. The everchanging regulations for the transport of this kind of goods, have tightened the rules around the transportation of food products and have even gone so far, in some countries, as to stipulate when and how often trailers must be cleaned. All this information, including the cleaning and maintenance of vehicles as well as temperature verification inside the trailer, can be digitalized and easily transferred to a Blockchain as trustworthy data for access, as needed, by authorities, transport companies and shippers. More on the use of Blockchain in agricultural trade can be found in the section on agriculture.

7.5 Additional benefits of Blockchain technology for road transport

Some additional benefits of Blockchain technology specific to road transport can be summarized into the following major categories, which complement the very specific benefits described above. As an integral part of most supply chains, road transport will also profit from many of the benefits outlined in the section on supply chains under challenges and stakeholders.

7.5.1 Better tracking of orders and assets

Since Blockchains, when combined with other technologies, can allow the trustworthy tracking of goods throughout their entire life-cycle and related processes, companies using Blockchain technology will be able to more readily produce detailed information about a product, including supplier information, manufacturing details and logistics information. Examples of benefits to road transport include the ability to: identify quickly the party currently in possession of the goods; allocate costs to specific consignments; prove time and place of delivery; and undertake complex accounting, for example for determining carbon footprints.

7.5.2 Building trustworthiness

If a customer has trustworthy information about where a product originated, they are more likely to develop a longer-term relationship with a given supply-chain entity.

This extends beyond supplier information, Blockchain-based applications could also collect trustworthy information about a company's services; for example, in the logistics industry, on-time delivery, percentages of lost or damaged cargo, quality of warehousing and other services.

7.5.3 Possibilities for increased cooperation

With trustworthy information registered on a Blockchain, the various actors of the transport network could interact with each other in a transparent and real-time way. This could be based, at least in part, on smart contracts that are aligned with the needs of the sector and the regulations in force within the transport industry. The data shared as part of this cooperation,

---

eCMR standard; see (as of February 2020): https://www.unece.org/uncefact/mainstandards.html#ui-accordion-jfmulticontent_c66199-panel-1

and registered on a Blockchain, could be traced, secured and timestamped, without any intervention by a trusted third party thus helping to secure the integrity of the information shared. This supports new business models, based on cooperative competition, which can be advantageous to all when used to pursue common objectives and could support optimization in the transport sector in areas which are still to be discovered.

7.6 Conclusion

As a distributed ledger that ensures both transparency and security, Blockchain technology shows promise as a tool to address some of the current problems in road transport as a part of wider supply chains. With a world of transport that is becoming more connected every day, Blockchain technology will, by nature, develop a symbiotic relationship with the Internet of Things and today's advanced logistics and supply-chain management systems.

8 Agricultural, fisheries and food trade

In order to understand the potential for the use of Blockchain technology in the agricultural, fisheries and food trade sector (8.3 below), one needs to first understand the role of information in food integrity and the challenges to food integrity. These are covered below in sections A and B, respectively.

8.1 Introduction: the role of information in food integrity

In general, agricultural and fish products have 3 destinations:

- The first and most important destination is fresh food and processed food;
- Second, a substantial quantity serves as a commodity for industry, especially fibre and oil products;
- Third destination is as an input for agricultural and fish production, such as animal feed and soil fertility maintenance.

Information integrity is an important issue in agriculture, fisheries and food. This is because of the health implications related to food safety. Society requests and expects safe food and safe products. For agricultural and fish production the supply chain is very complex; it involves multinational companies as well as many small and medium processors and traders in addition to small farmers and fishermen. Sometimes, supply may be limited to a local production chain; but, on many occasions, it is a complex global production chain.

Food and animal feed are high-risk products; as such, the information about the product must maintain high standards of integrity. The level of product information integrity varies, depending on the person or organisation involved, the activity performed, the processing of the product, the information about the product and the exchange of information between parties.

Food and feed safety are dependent on:

- Product characteristics;
- Animal and plant health (sanitary issues);
- Environmental conditions;
- Process and hygiene; and
- Inputs with reliable characteristics.

Food integrity is related to the following product attributes

- Substance;
- Origin/provenance;
- Quality; and
- Other characteristics.

The EU General Food Law and the World Health Organization's (WHO) Hazard Analysis and Critical Control Points (HACCP) guidelines are among the many legislative texts that provide for basic levels of food and feed safety. Regulations usually require that the food and feed producing parties have a legal identity and be registered and licenced. In most cases, farmers are not considered to be a food or feed producing party and as a result, are not required to be registered. However, due to programs to assist farmers, most farmers are registered.

In the case of electronic information exchange, parties must also have an electronic identity.

Because livestock is particularly vulnerable to disease contamination as well as to carrying diseases harmful to human health, many countries have established mandatory rules on the labelling and registration of livestock. In this regard, cattle, sheep and goats are identified as individual animals; while pork and poultry are usually identified in batches. Even in countries where the identification of animals is not mandatory, animals for export or for export products usually must have a unique identifier.

In addition to safety issues, there are other aspects to consider when producing and marketing food, some of which are also defined in legislation. These include product quality, environmental footprint (CO2, H2O), social conditions, origin and pricing. Furthermore, private business partners can also demand additional specifications. Often these specifications are defined in the form of private standards.[89]

The integrity of the product can be verified by a physical or administrative inspection, which can result in the product being given a certificate. However, an inspection or a certificate does not prevent all food and feed incidents.

In this regard, two types of incidents can still occur:

- Product treatment resulting in hazardous products, harmful to health or the environment; and
- Fraud and counterfeiting, where the product is not what is claimed in the documentation (and due to the false product information, there is no guarantee that the product is safe).

The supply chain for food, feed and agricultural inputs is very complex for the following reasons:

- It includes many small producers, traders and processors;
- Most of these commodities and products are bulk products;
- There is a many-to-many relationship between products and between parties (for example retailers purchase products from many producers and producers sell to many retailers); and
- The original producers / suppliers (for example, the farmers) are usually unknown to the processor or trader.

As a result, both the consumer and the retailer have limited information about the product and related production processes.

To provide all parties involved in the supply chain – including the consumer – with reliable information, there is a trend towards more transparency and traceability in the supply chain. Although transparency and traceability often go together, they are not necessarily the same. However, both transparency and traceability are required in order to evaluate whether the product is compliant with food safety regulations and other requirements. As mentioned above, if compliant, a certificate can then be issued.

[89] An overview of private standards is available at the International Trade Center's Standards Map web site https://sustainabilitymap.org/standardidentify/ (as of February 2020).

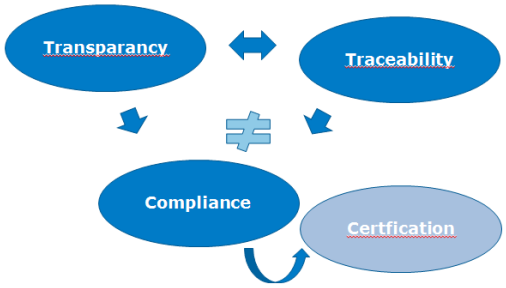

Image 8.1: Transparency and Conformity traceability

Transparency indicates that specific information in the production and supply chain is shared, with whom, and under what conditions. Transparency can include information necessary for traceability, but it may also cover other product aspects such as quality, social conditions, prices and costs.

Conformity traceability indicates that specified aspects of an individual product or product batch can be followed or traced back through its supply and production chains (for example, the location of the farm where the product originated from, or the fact that no pesticides were used in its production, etc.). This includes production processes, storage and transport and the parties involved at each stage. Conformity traceability also requires transparency about events in the production and supply chain, in other words information about the what, where, when, who and why, which will vary depending upon the product. Conformity traceability is defined as the ability to identify and locate: 1) the entry point of an asset (product) into the traceability chain, 2) the traceable asset events which occur after entry, and 3) the exit point when the asset leaves the traceability chain.

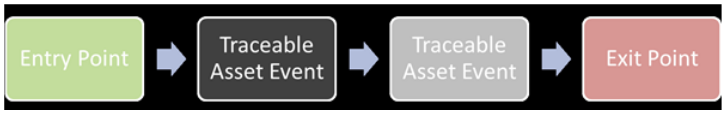

Image 8.2: Steps of conformity traceability

Theoretically, it is straightforward to integrate the traceability chain into product supply chains using a distributed database system such as the Blockchain. In reality; however, the situation is more complex.

In the food supply chain one-dimensional supply chains do not exist. This means that, in most cases, instead of a chain structure there is, a network structure which can vary in time and over product batches. There can also be many entry points and many exit points. This creates two difficult questions:

- What is the main entry point? The chicken or the egg? Or the chicken feed, or the harvested crop used for the feed?
- What is the end point? The egg on the shelve, the chicken meat in the soup, or the chicken dung which is input for the harvested crop?

In answering these questions, the best option is to consider the supply chain as a supply network in which supply chains constantly merge and separate, and which includes circular networks.

8.2 Food integrity challenges

8.2.1 Conformity traceability

Depending on the characteristics of a product there are different traceability models.

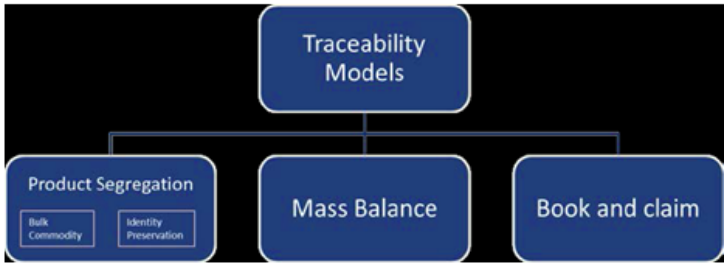

Image 8.3: Conformity traceability models

The product segregation model is used in two situations.

- In the case of bulk commodities, certified material from different suppliers can be mixed. This is used for fruits and vegetables.
- In the case where there is both certified and non-certified products, these should be segregated throughout the supply chain, and the product must be traceable from grower to retailer. This is used for fair trade in bananas.

Using mass balance methods, the policy claim is disassociated from the physical tracing of assets. In this method, the policy claims are validated for each asset before it is aggregated into a larger quantity and, as a result, the policy claim is also valid for the mass balance (i.e., accumulated assets), even though individual assets cannot be traced. The aggregated quantity must, therefore, have a well-defined state, linked to the relevant policy claims such as "organic", "fair-trade", etc. This is used for cotton, sugar, cacao, tea.

In the book-and-claim method there is a free flow of certified and non-certified assets, and no segregation of assets. Instead, a certifying organization sells certificates for X quantity of goods to companies who can then label their product as supporting the good practice in question. The money from the sale of certificates is then used to provide a premium over the market price to growers who are certified as using the good practice, thus providing an incentive for other growers to be certified. The certified product is placed on the market where it is mixed with non-certified product and it is the mixed product that is actually sold. This method is typically used when the production and market conditions make it impractical to sell certified product that has been segregated from non-certified product. At the same time, this method requires audit trails in order to demonstrate that for every certificate sold, certified growers have been compensated for the associated quantity of certified goods. This method is used for soy and palm oil.

Product segregation requires advanced Information and Communication Technology (ICT) implementations, in which the farmers and Micro-, Small- and Medium- Sized Enterprises (MSMEs) participate. It is used for high-risk and delicate products, such as fresh food. Mass balance and the book-and-claim, on the other hand, require less advanced ICT systems. This is because they are based on a set of rules and require only periodic auditing by stakeholders. As a result, one factor that must be taken into account is the ICT capabilities of participants in agricultural, fisheries and food supply chains – which vary greatly.

Conformity traceability also requires information about the assets, information about the what, where, when, who and why. To specify the asset and link it to events, each of the

following must have a unique identifier: the product, party, location, transport and process. Each event that affects the traced asset should thus be registered, and the registered data must be accessible for authorised partners in the chain or network.

The production and supply chain can be very complex and the evaluation of product data, in order to establish if policy or practice claims are correct, requires a high level of expertise in a given production stage or a product domain. Because evaluation is a time consuming and expensive process, it is common practise to use certificates to prove the characteristics of a product. These certificates can be of actual products or of specified stages in the production process and/or the supply chain. The certificate states that the product meets the specified characteristics.

In general, on-farm production is considered and analysed as a separate stage, outside of the supply chain. This production stage includes the on-farm growing, raising or breeding processes, and all the inputs used including: fertilizers, chemicals, medication, seeds, labour, water and energy. In plant production, the end of the production stage is the harvested crop and stored plant produce. In animal production, the end is the delivered raw milk, egg or wool. In animal husbandry for meat production, the end of the production section is the killing of the animal.

The supply chain stage for plants includes the processing of the plant produce, packing and transport up until arrival at the retailor. For animal products and meat from animal husbandry, this includes the processing of milk, eggs or wool, the slaughter and further processing of the animal, and the packing and transport up until arrival at the retailer.

Along the supply chain, many agricultural products and by-products leave the food supply chain (i.e., leather, corn used for methanol, etc.) or are not part of it at all (i.e., wool, cotton etc.). Many plant and animal products and by-products are thus used in non-food sectors. Some of these also require traceability (for example, cotton that is labelled “organic” or clothing that is “fair trade”) and parts of these traceability information chains that go back to the producer of the goods may incorporate information that is also used in food supply chains (for example for palm oil which is used both in food and cosmetics).

8.2.2 Identifiers for producers and products are a prerequisite for traceability

In order to implement traceability, all parties involved in the production and supply network must have a unique electronic identity with a unique identifier as either a person or as a legal entity. In addition to this very basic condition, it is better and often required to give unique identifiers to the products or produce being traced and to their location(s) (i.e., farm, field, storage, processing plant, etc.).

8.2.3 Primary production registration (of farm processes)

The buyers of a farm product require a large set of production data from the farmer including which inputs were used, why and when. Buyers need this product information in order to show, or even prove, that a product meets the required quality standards and is safe for its intended use. Information is also needed for logistics and process planning. This results in a large amount of data with a complex structure. For electronic exchange, several standard electronic messages are used, such as the UN/CEFACT messages eCROP, eDAPLOS or eLAB, or nationally agreed business messages.

These messages are exchanged between the farmer and the first buyer. When information is needed for use further on in the supply chain, a product is typically given one or more certificates.

Between the farmer, the farmer's suppliers and the buyers, four types of information are important:

- Inputs, processes and output data;
- Certificates (of quality and/or characteristics) for the inputs, processes and/or resulting produce;
- Logistics for production inputs and outputs; and
- Financial aspects such as payments, insurance, wages.

8.2.4 Industrial processing registration (for animal products, fish, meat, dairy or non-food and plant products, food, feed, non-food seeds, fibers)

The input for the processing industry is bulk commodities. Even in the case of slaughtering individually identified animals, the slaughter process is handled in batches.

One characteristic of the processing chain is that many partners in the chain purchase from multiple suppliers and sell to multiple customers. All production batches are identified, and production data is recorded. Depending on the type of product, products and batches are kept separate (i.e., individual identification) or are traced with either mass-balance or book and claim systems (as described earlier). In food supply chains, all parties comply with the relevant track and trace regulations.

The first processors who obtain raw produce from a farmer or trader demand all the relevant product information from the farm. However, the output from these first processors is usually no longer linked to this detailed raw product information, except for some product class/status information (i.e., organic, Fairtrade, MSC, etc.), usually supported by a certificate. Based on these certificates, product status can be maintained as the product moves through the whole production – supply chain).

In the case of products presenting possible health risks, the processors can or must be licenced. For example, in New Zealand, only licenced parties may produce and process meat for export.

Process information is usually not shared in the supply chain, except basic information such as processing / packing date, "best before date" and obligatory information such as ingredients, allergens, and the packing station. Product traceability does not guarantee that all product information is available in the supply chain or network.

The above results in low transparency in the product and supply chain about the product's characteristics, source of origin and other qualities. In turn, low transparency creates opportunities for unfair, illegal or even dangerous practises, as well as for keeping these practises undetected. These opportunities introduce food and feed safety risks, environmental risks, and economic risks through fraud, illegal competition, etc.

These risks can be partly eliminated or reduced by using certificates. One approach is to have a well-structured production and supply chain with known and safe partners which have an agreed level of transparency. At the same time, these partners' characteristics are often confirmed through certification. Another approach is to undertake inspections at various stages in the production processes and supply chain or network. This involves physical and administrative inspection activities, and often results in certificates as well.

In all these solutions, certification is an important key to food and feed safety, and to fighting unwanted or illegal practices.

Certification has four aspects:

- The certification process;
- The issuance of the certificate;
- The exchange of the certificate between parties; and
- The link maintained between the certificate and the physical asset.

8.3 The Potential of Blockchain

8.3.1 Certification

The certification of an agricultural product requires inspection. The subject of the inspection can be the product itself, the production location (i.e., the farm, field, warehouse, processing plant) and/or the identity of the producer (i.e., farmer, organisation). It may include a physical inspection and/or an inspection of documents. A physical inspection results in a report, which can be used further in the certification process. An inspection may also be only of documents. All the documents used in or resulting from the inspection process result in questions such as: Are these documents reliable? Which party has created or issued the document? Does the document cover the related assets? Is it the original document?

The use of paper documents requires special procedures to guarantee the value of the documents. These procedures can be time consuming and expensive. The use of paper documents also provides many possibilities for improper handling and fraud.

Instead of paper documents, electronic documents can be used. When electronic documents are generated by the automated recording of activities or by a fully automated administration, the abuse of documents can be greatly reduced or eliminated. The transfer of paper and electronic documents between different parties is still a point of risk. In the transfer of data, the history of a document can be lost, and with it the possibilities for verification of the document.

Therefore, Blockchain technology, and processes which take advantage of this technology, can increase the reliability of all documents used in the certification process. Blockchain applications can also provide possibilities for verifying the actions of involved parties. The table grapes pilot (see UN/CEFACT Blockchain repository[90]) shows the possibilities of a private Blockchain implemented with a smart contract.

In such a structured supply chain the participants can have assigned roles based on defined credentials. For example, based on what their credentials allow:

- A farmer can upload his product documents to the Enterprise Resource Planning system (ERP), which uses Blockchain technology to implement validation;
- The auditor can inspect and grant a certificate;
- Traders and retailers can retrieve product information and certificates from the ERP.

[90] UN/CEFACT Blockchain repository http://www.unece.org/tradewelcome/un-centre-for-trade-facilitation-and-e-business-uncefact/case-study-repositories.html

The exchange of certificates is a critical process. A certificate is a valuable document which is vulnerable to errors and fraud. To prevent fraud, additional measures are typically required. These vary from authentication marks on paper documents, to encryption, hash totals and digital signatures for digital certificates – sometimes in combination with secure process arrangements such as the use of designated send and receive stations. Even then, there are possibilities to misuse a certificate in other business transactions or in other supply chains.

In a supply chain where this information is shared using Blockchain technology, the validity of the certificate issued on the Blockchain can be verified and the certificate cannot be re-used outside of the specified supply chain.

8.3.2 Track and trace

There are standards available for track and trace, such as ISO EPCIS (ISO/IEC 19987:2015) and the UN/CEFACT T&T standards for track and trace of animal traceability and traceability of primary natural products. Based on solutions like those using these standards, many systems for track and trace are used in the agricultural business today.

The question remains: what is the added value of Blockchain technology for the track and trace process? One issue in the track and trace of a product, is the reliability of the track and trace data. This has two aspects:

- a continuous chain with no missing points where data should be captured and
- the quality of the data recording and data processing of each data capture point.

For both of these issues, Blockchain technology can help.

For real traceability, a continuous track and trace chain is required. Every relevant event should be recorded, regardless of the type of traceability model used. A Blockchain itself cannot enforce continuous tracking and tracing in a supply chain. On the other hand, Blockchain technology can verify when, where and the content of each event that is recorded, so when used at each data capture point in the supply chain, the Blockchain can verify the track and trace record of a product from the supplier to the last point where data was recorded, which could be the final customer.

For the second aspect, the quality of the recorded data and data processing, Blockchain technology can provide a key solution. In a standard track and trace system it is not necessary to provide business partners with the track and trace data for a product in real time or even near real time. This provides opportunities for the hidden correction or manipulation of the data. In other words, the administration of the track and trace system can be used to cover up fraud through the manipulation of recorded data on processes and products.

With Blockchain technology, data corrections can be possible; but these corrections are transparent to all users of the Blockchain who will see both the original data and the changes.

Blockchain technology does not prevent poor data quality. Also, fraud is not eliminated with Blockchains. But within a supply chain supported by Blockchain, fraud will be difficult – provided that all conditions are fulfilled, such as proper identification of the product, location and parties together with the proper authorization of parties.

8.3.3 Sensors and Internet of Things

Sensors are very important in agriculture, fisheries and food production. They are used everywhere: on farm equipment, feeding robots, milking robots; on animals to monitor animal conditions, health and location; in storage to monitor climate conditions; in processing; and

in transport. Sensors can produce large amounts of data. Blockchain technology is not very well-suited to securing and storing substantial amounts of data.

The amount of sensor data can be reduced if only sensor values that meet triggering criteria are registered (such as bypassing a minimum or maximum temperature, if a container has been opened, if electric power has been interrupted, etc.). Also, it is possible to register certificates on a Blockchain for a product or process based on recorded sensor data sets (for example, to certify that, during transportation, goods were never exposed to temperatures outside of a specified range). This results in a small amount of data to be recorded in the Blockchain.

8.3.4 Transport

The movement of goods and a product's condition during transport are critical issues for track and trace, for food safety and sanitary reasons. Based on transport events, the next step in the transport, storage, production process or administrative process can begin. With Blockchain technology, the integrity of this event recording can be improved.

8.3.5 Process improvements

Sensor results and event records can be used for the automation of both technical and administrative processes. This is already common practice for processes within a location or within a single production entity or enterprise. The exchange of sensor results and event records between business parties can contribute to enhanced business and process automation. A key element is the trustworthiness of the exchanged data. With Blockchain technology this trustworthiness can be greatly increased. As a result, it is possible to use this data to trigger the next physical and/or administrative business step with the next partner in the chain. In particular, the linkage of an administrative process, such as a payment, with a sensor result and an event record can reduce payment delays in the supply chain. To take advantage of these opportunities, the use of Blockchain technology in combination with smart contracts is required.

8.3.6 Smart contracts

A smart contract is a small programme (algorithm) which defines business rules to be executed when a Blockchain transaction is performed when predefined criteria are met. With a smart contract, you can register basic information in the Blockchain which cannot be altered. Examples of such information includes product characteristics and product certificates. This data can then be used for validation and evaluation purposes and can be input for the automated next step(s) which are triggered by another smart contract when it processes a transaction. With Blockchain technology, transactions as well as the smart contracts which process them and the specified in advance processes which they trigger, are auditable by all parties that have the appropriate consultation rights.

Examples of automated processes that can be based on smart contracts are:

- Automated sorting and grading of coffee beans, resulting in automated pricing and billing of the coffee batch.
- Fast payment for eggs to the farmer, when the batch of eggs has been delivered to the retailer, thus eliminating manual administration by several intermediate parties (i.e., packer, gross trader).

- A fair price payment to coconut growers, which can be verified by the consumer of the fresh coconut.
- The certification process and the verification of the certificate (i.e., global gap and organic) of table grapes.
- Automatic payment of some farm support – animal events (i.e., birth, dead, transport) have to be declared via animal event registrations according to legislation. Based on this event registration, automatic payments can be made in accordance with farm-support programs (i.e., subsidies for holding sheep, premium payments for holding traditional cattle species; in the dairy industry premium payments for milk originating from certificated organic dairy farms, etc.).

8.3.7 Data ownership and data rights

Data ownership, data access, and other data rights are an important issue in all industries that use information technology, including agriculture. Blockchain technology supports the development of applications that clearly differentiate between data ownership, data access, data use and other rights. In the agriculture industry, the standard is that the producer of the data is the owner. For example, in the plant and crop case, the farmer is the data owner. The owner decides who has access to the data and what permissions are granted (for example, permission to read, process, forward, etc). Blockchain can provide additional, trustworthy tools for managing data ownership and rights. In a Blockchain it is possible to govern the rights to data on the Blockchain, by assigning different roles to Blockchain participants and to also record each time a participant's data is accessed, by whom and how it was used. This is also possible for the combination of a Blockchain with linked, off-chain data.

Blockchain's impact on markets, opportunities to use Blockchain for trade

With Blockchain technology, transparency in the food supply chain can be improved. It provides the possibility for supply chain partners to have detailed and reliable information about product specifications, qualities and pricing. In addition, consumers may have access to this product information. Of course, whether or not this information is shared, and with whom, depends upon the data permissions that are defined for each stakeholder in a Blockchain. The possible benefits of Blockchain technology for supply chains is outlined in the Supply-Chain section above.

A smart example in the agricultural sector is the result of a project pilot run by FairFood to support fair pricing and tracing of fresh coconuts from the Indonesian small coconut growers up until the consumer in Europe. In this pilot, the consumer can trace the coconut he purchases back to the individual grower, and the consumer can verify the fair price payment to the grower. This is done using individual identification (i.e., tagging) of each coconut and a Blockchain with smart contracts. Using this system, all the processes and transactions in the supply chain are registered, monitored, verified and, if necessary, corrected.

Although Blockchain technology may be complex, once trade agreements are set and reflected in smart contracts, it is easy to implement, as evidenced by different pilot projects. For example, in the coconut pilot, even in a remote area this Blockchain transaction could be done. For the grower the only requirement was to have access to a smart phone and to have an e-identity.

Blockchain technology can also enhance the opportunities provided by sustainability networks and other initiatives to promote fair trade and environmentally responsible agricultural practices. As sustainable networks provide information about the grower and his

farm, Blockchain technology can add secure transactions and provide verifiable information about products and transactions.

9 Energy trade

9.1 Introduction: Changes in the energy industry

The energy industry is passing through a seismic shift. Several things illustrate this, including the ratification of worldwide agreements to reduce the effects of climate change; cheaper solar panels and batteries now encouraging consumers to become producers; new technologies like the Internet of Things (IoT) enabling intelligence in households; and, also, hyper-connectivity with the Internet and other devices. A report from the World Energy Council has identified topics of critical uncertainty for the energy industry such as the global climate framework agreement, energy access, energy affordability, extreme weather risks, corruption and terrorism, among others.[91] In order to provide a simpler schema of the changes and challenges in the energy industry, the following three concepts can be identified:

- De-carbonization;
- Decentralization; and
- and Digitization.

These are also known as the 3D's of energy Grid 2.0. The disruptions caused by Blockchain technology intensify the need for changes that the energy industry is already going through.

9.1.1 De-carbonization

The Paris Climate Agreement which entered into force on 4 November 2016, has now been ratified by 185 countries as of February 2019. Among other objectives, this agreement aims to mitigate the effects of global warming; and, even though each country determines its own level of contribution, the Agreement is expected to discourage the use of fossil fuels for energy production on a global scale.[92]

9.1.2 De-centralization

Centralized energy production is inefficient because this leads to losses incurred during transmission and distribution. Furthermore, this issue affects, in a higher proportion, low income economies (18 percent loss) as compared to high income countries (6 percent loss).[93] In addition to wasted energy, the lack of resiliency is an even more important problem because natural disasters challenge the stability of electricity grids as seen in 2017 with Hurricane Harvey[94] and Hurricane Irma.[95] In fact, it was the disruption caused by Hurricane Sandy which motivated the authorities from the State of New York to encourage the construction of

[91] World Energy Council. (2017). *World Energy Issues Monitor.* London: World Energy Council. https://www.worldenergy.org/publications/entry/world-energy-issues-monitor-2017-exposing-the-new-energy-realities (as of February 2020).
[92] *Paris Agreement*. (2017, 09 04). United Nations Treaty Collection: https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXVII-7-d&chapter=27&clang=_en (as of February 2020).
[93] OECD/IEA. (2014, 09 09). Electric power transmission and distribution losses (percent of output). *Electric power transmission and distribution losses (percent of output)*. The World Bank Group. (as of February 2020).
[94] St. John, J. (2017, 08 28). *Hurricane Harvey Is Putting Texas Grid Resiliency to the Test*. Green Tech Media: https://www.greentechmedia.com/articles/read/hurricane-harvey-is-putting-texas-grid-resiliency-to-the-test (as of February 2020).
[95] Pounds, M. H. (2017, 09 10). *More than 261,000 homes, businesses without power from Hurricane Irma*. Sun Sentinel: http://www.sun-sentinel.com/news/weather/hurricane/fl-bz-fpl-irma-power-outages-20170908-story.html (as of February 2020).

micro-grids with the aim to improve resiliency.[96,97] One result has been the inception of a Blockchain-enabled project which is described further below. Finally, the emergence of micro-grids will require different network configurations in order to compensate for the lack of central distribution. This includes the interconnection of micro-grids and, given the nature of such network structures, they will probably also include cross-border micro-grid interconnections, thus blurring national borders and the grid's sovereignty, in exchange for a more efficient flow of electricity and stronger resilience.

9.1.3 Digitization

It has been said that Alexander Graham Bell would not recognize the telephone systems of today, but Thomas Edison would fairly easily identify his contributions in today's energy grids. This is not entirely true as described by[98] but it does say something about the perception of breakthroughs and innovation in the corresponding industries. While telecom companies have been disrupted multiple times in the transformations leading from the telegraph to wireless 5G, during the same period, energy companies have continued doing business based on the same principles. They have been relying on long Return on Investments (ROIs) and stable regulations reflected in computer systems that are highly customized with hard-to-change business rules. This is easy to understand because the digitization of utility infrastructure is a double-edged sword. On one hand, it brings affordability and transparency to financial and administrative processes, and, on the other hand, it makes them an attractive target for highly sophisticated cyber-attacks.

9.2 Blockchain features with direct impacts on energy markets

The following is a list of Blockchain features that have the potential to directly impact energy markets.

- **Peer-to-peer (disintermediated) access to electricity trading orders on local, national and international markets**: Energy trading involves multiple actors and multiple consecutive steps, each transaction involving different terms and conditions that enable partners to work together. Having no central authority that controls the network makes business more efficient and cost-effective. It also makes it difficult for members to make secret agreements that would result in the Blockchain making transactions that are in their favour and to the detriment of other participants. This is because the majority of participants need to agree to each transaction and, at least in the most popular public Blockchains, this would require obtaining the agreement of thousands.
- **Fault tolerant network and automatic replication of critical trading data and information**: There is no single unique server, therefore the network is more resistant to being taken down. This is necessary for the national security of every country in

[96] Jones, K. B., Bennett, E. C., Wenhui, F. J., & Kazerooni, B. (2017). Beyond Community Solar: Aggregating Local Distributed Resources for Resilience and Sustainability. In F. P. Sioshnasi (Ed.), *Innovation and Disruption at the Grid's Edge: How distributed energy resources are disrupting the utility business model.* (Kindle ed., pp. 64-79). Walnut Creek, CA, USA: Elsevier

[97] Lacey, S. (2014, 06 10). *Resiliency: How Superstorm Sandy Changed America's Grid*. Green Tech Media: https://www.greentechmedia.com/articles/featured/resiliency-how-superstorm-sandy-changed-americas-grid (as of February 2020).

[98] Bush, S. F. (2014). *Smart Grid: Communication-Enabled Intelligence for the Electric Power Grid.* Chichester, West Sussex, United Kingdom: Wiley - IEEE.

order to ensure the availability of electricity to vital infrastructure such as road traffic management and hospitals.

- **Smart contracts that automate the processing of electricity trading data, production/consumption data, price agreements, administrative and legal paperwork**: This feature alone has the potential to reduce the administrative cost of trustworthy syncing between partners and should result in a streamlined, simplified service to the end-customer.
- **Cryptographically secured identities to ensure legally binding agreements**: The combination of cryptographically secured identities so that no one can pretend to be someone else, with the immutable nature of Blockchain records should bring a solution to the legal nonrepudiation problem. In other words, "Alice cannot send a message to Bob, and then later deny ever sending it."[99] This function will be used primarily to make sure that traders and consumers of the end-product really are who they claim to be and that their commitments are authentic.
- **Tokens that commoditize energy production/consumption**: Tokens can represent (i.e., act as a proxy for) a standard unit of something, such as energy, which can then be traded. The cryptographic techniques embedded in the network, help to avoid the double-spending of such digital assets, protecting users from bad actors that intend to defraud the system in order to obtain an unfair advantage in the trading, production and consumption of energy units. More on tokens can be found in section 2.4.3.

9.3 Opportunities to use Blockchain for energy trading

Within the context of the energy industry and taking into account the previously described features of Blockchain, the following are realistic opportunities to use Blockchain in energy trading.

9.3.1 Blockchain-enabled Internet of Things and smart contract-enabled peer-to-peer energy marketplace

In April 2016, two related projects were launched in Brooklyn, New York in the United States for the installation and setup of a local community micro-grid, and the establishment of a decentralized trading application platform. These were, possibly, the first real-world pilot projects for Blockchain managed micro-grids. They have since moved past being proofs of concept and continue in operation.

These two projects demonstrated the use of Internet of Things (IoT) devices like Blockchain-enabled smart meters, to track the energy production of solar panels, upload this data onto a public network (Ethereum) and then trade the energy in question on a Blockchain network in a local energy market.[100] This concept allows neighbours to purchase electricity produced in their community creating a local energy economy. It is important to note that the realization of such a project was only possible due to the de-regularization of energy trade. This de-regularization and incentives to construct micro-grids in the state of New York were

[99] Bruce, S. (2004). *Secrets and Lies: Digital Security in a Networked World* (Kindle ed.). Indianapolis, Indiana, USA: Wiley Computer Publishing.
[100] LO3 Energy. (2017). *LO3 Energy Projects*. https://lo3energy.com/ (as of February 2020).

motivated by the events following Hurricane Sandy.[101,102] Similar services are now being offered in Australia and New Zealand.

9.3.2 Blockchain-enabled Internet of Things and smart contracts to enable a machine-to-machine energy economy

This case is similar to peer-to-peer energy markets but instead of performing transactions among households, this application would allow a single smart device to purchase its own electricity from another device (Machine to Machine – M2M). The purchase would be made based on forecasts of the smart device's own consumption and would be negotiated with another smart device (i.e., a smart battery) that can fulfil the forecasted demand in the desired period. This transaction may occur without any human intervention; however, the history of such transactions can still be registered on the Blockchain and later accessed by human auditors.

9.3.3 Establishing the foundations and infrastructure for future energy applications

As the energy sector starts to modernize, and technology start-ups start to enrich the ecosystem, it will be necessary to provide a testbed and a launch platform that can host digital innovation in the form of pilot projects. Additionally, compatibility will become an increasingly hot topic because applications and technologies developed in different parts of the world need, increasingly, to interact. The fear of Blockchain islands will hopefully be addressed by new technologies to interconnect completely different Blockchain networks. The development of standards such as those developed by UN/CEFACT at the data and process level will also support compatibility and interconnectivity. The Web Energy Foundation is a private consortium of energy companies and Blockchain start-ups founded in Zug, Switzerland with the aim to develop and open-source IT infrastructure and Blockchain technology that is specific to the energy sector[103] and there are also private sector Blockchain network initiatives.[104]

9.3.4 Blockchain smart tokens to record, transfer and avoid double spending of carbon credit on energy trading markets

"The Paris Agreement includes provisions that can advance carbon markets in two ways: by ensuring there is no double counting when countries engage in emissions trading, and by establishing a new mechanism to facilitate trading."[105] Blockchain could support these enforcement provisions. For example, they could be written into smart contracts to automate cap restrictions on energy trading. Additionally, regulators and society in general are

---

[101] Woyke, E. (2017, 04 19). *Blockchain Is Helping to Build a New Kind of Energy Grid*. MIT Technology Review: https://www.technologyreview.com/s/604227/Blockchain-is-helping-to-build-a-new-kind-of-energy-grid/ (as of February 2020).
[102] Cardwel, D. (2017, 03 13). *Solar Experiment Lets Neighbors Trade Energy Among Themselves*. New York times: https://www.nytimes.com/2017/03/13/business/energy-environment/brooklyn-solar-grid-energy-trading.html (as of February 2020).
[103] Rocky Mountain Institute. (2017, 05 08). *Energy Web Foundation Launch*. https://rmi.org/insights?query=&fwp_stream=news (as of February 2020).
[104] PowerLedger. (2017). *Powerledger Whitepaper.* Powerledger. https://powerledger.io/ (as of February 2020).
[105] Mansell, A. (2016, 02 19). *What's ahead for carbon markets after COP 21*. International Centre for Trade and Sustainable Development: https://www.ictsd.org/bridges-news/biores/news/what%E2%80%99s-ahead-for-carbon-markets-after-cop21 (as of February 2020).

demanding transparency through guarantees of origin for carbon that is traded. As with any other certification, it is important to ensure the genuineness of such attestations.[106] One possible solution would be the creation of a digital asset that can be implemented using Blockchain smart tokens in order to attest to, track ownership of, as well as avoid double spending of carbon credits. This use case is different from projects which reward solar energy producers with "solar credits" which can then be used as virtual currency and exchanged for its equivalent value in fiat money (United States dollars, euros, etc.). This last kind of token/coin can also be used as a means of payment to buy electricity back from a network of prosumers (consumers who are also producers of electricity).

9.3.5 Blockchain smart contracts for auditable, automated pricing and billing in energy trading

Electricity has some very distinctive features:

- First, it cannot be stored, which means it either must be consumed immediately or it must be converted into a different state using chemical batteries;
- Second, the quality of the product (i.e., electricity) is exactly the same no matter how it was produced; and
- Third, the cost of production depends on the geographic location, distance to points of consumption, time of the day in which it was produced/consumed, source of production (i.e., renewable, fossil fuels), etc.

These factors make energy pricing and trading a relatively complex process compared to the trading of other assets.[107] It is obvious that traders have a strong desire to eliminate costly errors produced by miscalculations, and consequently attempt to automate the market as much as possible. Blockchain has already been used in a similar case for cash settlements in the financial industry.[108] One possible approach would be the research and testing of a national or supra-national energy market that processes pricing and billing, using smart contracts to manage the process in an automated way. At the same time, such a market could create transparency for traders and auditors both ex-ante via the auditing of smart contracts, and ex-post via auditing of Blockchain transactions.

9.3.6 Blockchain smart contracts to reduce administrative costs of self-consumption energy communities and encourage zero-net-energy buildings

Many countries have started initiatives to encourage so called Zero-Net-Energy Buildings. These are buildings that can produce the same amount of energy as they use during a set period of time, thus effectively netting to zero in their metering. In Switzerland, a new law was passed in May 2017[109] in which tenants of a building can establish a self-consumption

---

[106] Mansell, A. (2016, 02 19). *What's ahead for carbon markets after COP 21*. International Centre for Trade and Sustainable Development: https://www.ictsd.org/bridges-news/biores/news/what%E2%80%99s-ahead-for-carbon-markets-after-cop21 (as of February 2020).

[107] Sioshansi, F. (2017, 08 18). *How electricity will be priced in the future*. Energy Post: http://energypost.eu/how-electricity-will-be-priced-in-the-future/ (as of February 2020).

[108] Neghaiwi, B. H. (2017, 08 31). Six big banks join Blockchain digital cash settlement project. (J. Gaunt, Ed.) Reuters: https://www.reuters.com/article/us-Blockchain-banks/six-big-banks-join-Blockchain-digital-cash-settlement-project-idUSKCN1BB0UA (as of February 2020).

[109] Confédération suisse. (2017, 03 21). *Promouvoir les énergies renouvelables*. Retrieved from Confédération Suisse - Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC:

energy community recognized by the local electricity retailer. This allows a producer (i.e., the building owner) to install solar panels and sell this energy to the tenants for a price that is attractive to both the tenants (i.e., cheaper than the grid) and the solar producer (i.e., higher price than feed-in tariffs). Once the community has been created, the community manager oversees the electricity billing for each community participant. The related administrative costs can affect the profitability of such ventures, therefore, products and services are now being offered in the Swiss market to help reduce these costs using Blockchain.[110]

9.3.7 Blockchain-enabled Internet of Things and Smart Contracts to cooperatively manage responses to demand and increase the flexibility of the grid

A fundamental principle of electricity grids is that energy production must respond proportionally to demand. The challenge for grid operators is to manage the high level of uncertainty on demand throughout the day as well as within seasons. This challenge forces grid operators to develop complex but imperfect forecast models for demand, and to accept additional costs that give them the flexibility they need in order to compensate for unexpected fluctuations in demand. Such costs include having excess capacity available to meet unexpected peaks in energy usage and having the ability to shut down generators to prevent damage in the case of unexpectedly low usage. The massive adoption of IoT devices within households[111] will enable bigger, better and faster data collection. This will make it possible to synchronize disparate household consumption patterns and to better manage demand in order to reduce the levels of flexibility and related costs required by the grid. Specifically, the future smart home will also be able to send data produced by home appliances to a smart contract, which then coordinates with other households in order to automate schedules of electricity use. Each smart contract will act according to the economic incentives provided by the electricity grid.

9.3.8 Scalable fast, Internet of Things-friendly Blockchain networks to allow pay-as-you-go energy financed by micro-transactions

Developing countries, and especially African countries have demonstrated a remarkable growth in the last ten years. This has been propelled by their leapfrogging others by implementing the most recent technologies in a world with rapid technological advancements. In the case of energy, the preferred solutions implemented by businesses and consumers are wireless, solar and mobile. These solutions compensate for inadequacies in the infrastructure of these countries. However, in spite of all these improvements, a lack of transparency, corruption and abuse of power are still major issues[112] and make it difficult for investors to do business in these regions. Within this context, sustainable business models that enable access to electricity in the poorest regions of the world are being developed.[113] Given that developing regions often suffer from corruption, including in civil law courts, the inclusion

---

https://www.uvek.admin.ch/uvek/fr/home/detec/votations/votation-concernan-la-loi-sur-l-energie/energies-renouvelables.html (as of February 2 020).

[110] Alvarado, J. L. (2017, 05 31). *Using Blockchain to accelerate the creation of self-consumption energy communities in Switzerland*. Slideshare: https://www.slideshare.net/JorgeAlvarado87/31052017meetupBlockchainjorgealvarado (as of February 2020).

[111] Gartner. (2017). *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016.* Egham: Gartner. http://www.gartner.com/newsroom/id/3598917 (as of February 2020).

[112] Transparency International. (2016). *Corruption Perceptions Index.* Berlin: Transparency International. http://files.transparency.org/content/download/2089/13368/file/2016_CPIReport_EN.pdf (as of February 2020).

[113] M-Payg. (2017). *Our Vision*. http://www.mpayg.com/#story (as of February 2020).

of IoT-enabled Blockchains could lead to the creation of a transparent, persistent, immutable source of records that supports such business models. Blockchain applications could be designed to keep the transaction costs very low (for example, due to disintermediation there is less room for bribes and extortion). Automation is also important for controlling costs since the monetary value of transactions will be relatively low, while the number of transactions will be very high. Automation comes at the cost of needing an Internet connection, but this can be partially solved with the use of batch synchronization. Such a technology solution could provide a stronger level of confidence for the legal enforcement of agreements to companies. At the same time, this could also reduce the operating cost of performing transactions on a global, secure network.

9.4 Challenges of using Blockchain for energy trading

This section discusses general concerns in the energy industry, which are a result of the inherent characteristics of Blockchains. These are also a concern for many other industries.

9.4.1 Governance and regulatory frameworks for national and cross-border energy trading

Energy trading is most frequently carried out across a complex network of electricity highways physically crossing borders. As a result, industry stakeholders are concerned about how Blockchain can realistically enable/enforce good governance when code is executed as is and the transmission of electrons involves multiple countries, legal jurisdictions, languages and foreign financial exchanges.

9.4.2 Electricity consumption and customer data: data ownership, personal privacy, the General Data Protection Regulation.

Customers and users are increasingly aware of the sensitive information that Internet companies obtain from consumer data that is gathered from the use of their services. The smart meters commonly used to provide intelligence to energy-trading platforms further enable the gathering of massive amounts of data produced by the electricity consumer. Privacy legislation laying out the rules with regard to individual's rights to privacy, such as the EU's new General Data Protection Regulation[114] must be taken into consideration.

9.4.3 Intellectual property, partner and energy price agreements embodied in smart contract code

Business transaction data on products, clients, sales volumes is often the basis of differentiation or pricing strategies, including for energy trading actors. If all data used in business transactions is open to competitors, the commercial or technological advantage disappears. Additionally, there is other sensitive data in energy networks that should be accessed only by authorized parties (for example, for national security reasons). On public Blockchains, access to such data can be reduced using encryption and the storage of data pointers rather than actual data. At the same time, strong encryption has associated costs, and few of these methods are fool-proof solutions when faced with determined hackers. Currently there are two ways to address these issues in a more secure way:

[114] European Union. (2017, 09 04). *General Data Protection Regulation*. https://gdpr.eu/ (as of February 2020).

- First, on a political level by creating a consortium that scans potential partners before granting them access to a permissioned network, and
- Second, on a technical level, by creating a permissioned Blockchain which consists of privately-owned computer networks and Blockchain nodes, which use traditional information technology security design and architecture.

9.4.4 Electricity trading transactions and the need for interoperability between Blockchains

The trading of energy does not work in isolation from the rest of the economy. In fact, the results (i.e., the cost of electricity) are reflected in all other trading and economic activities across the globe – except the most primitive forms of barter where neither the product production nor the trading requires the use of electricity. As a result, as more and more economic activity is performed on Blockchain networks in all sectors, including electricity, it will be increasingly necessary to establish norms of communication and exchange between Blockchain networks. Moreover, the surge of the token economy will bring along new possibilities for exchanges of value across all industries and globally. To support Blockchain interoperability and compatibility at both the technical level of data exchanges and the business process level, inter-disciplinary, inter-industry standards, such as those developed by UN/CEFACT, must be in place in order to allow a seamless exchange of tokens and the execution of smart contracts so that these can be performed in symphony across organizations, industries and geographies.

9.4.5 Transaction costs, micro-transactions and the problem of scalability for energy retailers and the end consumer

Given the mechanics required for the confirmation of transactions on public Blockchains, it is very difficult to use them for micro-transactions in a secure, reliable and economically viable manner. Currently, there are no good public-Blockchain alternatives that address the cost issues for micro-transactions as well as the speed and volume issues that are often, also, associated with micro-transactions. There are some public distributed ledger solutions being developed to address these issues, that do not use Blockchain technology, but instead a method called Directed Acyclic Graph (DAG).[115,116] This technology is still in its infancy compared to Blockchain technologies and, therefore, has not been widely tested. Otherwise, the solutions for scalability and transaction cost tend to push organizations and consortiums into the use of private/permissioned Blockchain networks that interact with traditional IT infrastructure and, invariably result in trade-offs between security, speed and transaction volumes.

[115] Popov, S. (2016). IOTA whitepaper. https://iota.org/IOTA_Whitepaper.pdf (as of February 2020).
[116] IOT chain. (2018, 03 25). Whitepaper. https://iotchain.io/ (as of February 2020).

10 Finance

10.1 Introduction

10.1.1 Blockchain in Finance processes: innovations and expectations

Fintech companies use Blockchain technology and will use it even more in the future, since it seems to hold great potential, for example for supply chain finance, e-payments, foreign exchange (FX), financing and more. By all appearances, we are on the verge of a major technological revolution. At the same time, there are still many unanswered questions, including how governments should oversee Blockchain applications, how regulations should be designed and enforced in order to prevent mis-use of this technology and, also, on how oversight powers can be exercised when dealing with distributed, de-centralized networks that have nodes around the world and no central control. Although the crucial issue of regulation is still unclear, in the final analysis, as always, governments will need to play a major role.

The trend of disintermediation is continuing to gain traction, with Blockchain contributing significantly towards this end. As a result, the roles of banks, central banks, market infrastructure and other clearing houses has now been cast into doubt, and it is still unclear whether this is positive or not. However, it is important to recognize the role that Bitcoin has played in in triggering radical change within the modern world of finance. It has shifted the boundaries and forced everyone in the finance industry to rethink their business models and review their operating methods, failing which they risk disappearing completely.

The digitization of the economy has become an unescapable fact. Since the 2008 global financial crisis, all finance functions, corporations and jobs, have been facing challenges, changes and evolution. The financial crisis was a catalyst for change, one could perhaps even say a revolution. There are a few major changes and key elements which explain this new situation: a new regulatory environment which is more stringent, the complexity of the new International Financial Reporting Standards (IFRS) for accounting combined with technological developments and new IT solutions, the technological evolution of fraud and cybercrime, high market volatility, the increasing complexity of (doing) business and, as a whole, an obvious acceleration of developments.

Looking beyond its use for payments, Blockchain can also facilitate the use of other information where security and trustworthiness are essential (such as land-registry data, registers of works of arts, patents, etc.) and reduce or eliminate the need for third parties in these sectors. Building upon these features, new applications of this technology should allow settlement cycles to be shortened drastically, perhaps even to a few minutes. Although these changes will not happen overnight, they are inevitable and should be a cause for concern to many financial institutions given that the majority of traditional intermediary structures, including some that have been present for centuries, will need to change in order to demonstrate their value added.

10.1.2 Blockchain technology for which financial processes?

Blockchain for financial services is still at an early stage of development. At this time, the hype for Blockchain is cooling off in the global financial industry as the "*development of the*

technology enters a hype-meets-reality phase."[117] One concern at this stage is highlighted by Alistair Milne, *"understanding of the technology lags well behind the hype [… It] seems to promise major change for capital markets and other financial services, but few can say exactly how or why."* [118] This observation indicates that there is an unmet need for specialized skillsets in order to adequately comprehend and utilise Blockchain given that it exists at the crossroads of game theory, cryptography, computer networking, data transmission, economic and monetary theory.

Instant clearing and settlement are probably the most appealing promise of Blockchain in finance. In a world of nanosecond financial transactions, one could ask, why is this not yet possible? Instant clearing and settlement are elusive mainly because of the consensus by reconciliation process. This process is a framework of checks and balances based on the independent reconciliation of multiple autonomous ledgers and, during that process, the implementation of required regulatory prescriptions, corrections, and restrictions. In order to shorten the time required for these processes, progress could be made by using cryptographic tools to improve existing database technology and automation practices. However, at present, the analysis of the regulatory and operational feasibility of alternatives to consensus by reconciliation has been neglected – and this is where Blockchain technology could, potentially, contribute to revolutionary new approaches. However, the only widely accepted opinion is that any alternative to the current process would need to provide a recourse mechanism and have rules subject to the review, management, and approval of some intrinsically centralized higher court – requirements that may be difficult to reconcile with Blockchain technology. There are also some other, very technical examples of clearing and settlement that pose additional issues not described here.

Even more difficult to successfully implement would be Blockchain technology in derivative transactions. The collateral amount for derivative transactions is correlated to the risk of the outstanding portfolio between two counterparties, a crucial calculation that is model-dependent and computationally intensive. In a Blockchain environment, without intermediaries it is not clear how this collateral amount would be determined: which models would be used, by which agent and with what economic incentive.

Another important aspect of Blockchain implementation, which must be taken into account, is the cost of integration with existing ICT applications and infrastructure, which are extensive and important to the functioning of the financial industry.

On the positive side, notarization services are an often neglected and useful Blockchain application for financial markets. These services are further explained later, however, it is worth stressing that they are at the core of the financial world's fascination with the idea of a shared ledger. This is because all participants can be sure that what they see is trustworthy and the same as what everyone else can see. In other words, the shared ledger can be used as authoritative reference, reducing the need for costly reconciliations between multiple private ledgers. In addition, to obtain such a level of certainty, a shared ledger must be based on highly secure governance rules which also ensure the quality of the data that is registered. This can be done in a variety of ways, including being secured by a single authoritative central counterparty or by the distributed consensus of a public permission less ledger such as the Bitcoin or Ethereum Blockchains.

---

[117] https://www.reuters.com/article/us-banks- fintech-blockchain/wall-street-rethinks-blockchain-projects-as-euphoria-meets-reality-idUSKBN1H32GO (as of February 2020).
[118] The Impact and Potential of Blockchain on the Securities Transaction Lifecycle, Mainelli and Milne. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2777404 (as of February 2020).

So far, Blockchain has generated unrealistic expectations, for many reasons, including: the technology itself which has potential for some use cases but also has limitations (such as for data storage) that are not always recognized; Missing and needed standards; the lack of many basic IT tools for Blockchain applications that still need to be developed such as application programming interfaces (APIs) and user interfaces; and the inadequate number of medium and large-scale implementations that test its limitations.

At the same time, financial services are also realizing that Bitcoin and other cryptocurrencies are increasing their relevance as an investment asset (e.g. futures contracts for Bitcoin are now traded at Chicago Mercantile Exchange and Chicago Board Options Exchange) and that transfers of value can be achieved both instantly and securely using Bitcoin and other cryptocurrencies. However, there is still much work to be done on assessing how this will affect the financial industry.

All of the above being said, there are an increasing number of application use cases in finance that have been identified and which are generating work in the form of both exploratory proof of concept projects and actual implementations.[119] The rest of this paper will look at these use cases, with a particular emphasis on those related to trade.

10.2 Blockchain's potential application to local, regional and cross-border payments

Payments form the foundation for trade and are a network business, like many other banking business areas. Their effectiveness depends primarily on some specific factors, including:

- A pervasive network of Payment Service Providers
- The ability to reach Beneficiaries' banks
- The reliability of clearing and settlement mechanisms
- The speed of clearing and settlement, which determines the speed of payment finality.

Although most of the terms used in this section are also used by many regulators[120] and other players in the field, a brief set of definitions is given below.

- **Payment transaction**[121] means an act of placing, transferring or withdrawing funds, initiated by the payer, or on his/her behalf, or by the payee, irrespective of any underlying obligations between the payer and the payee;
- **Local payment** refers to a payment denominated in a single, specific currency exchanged by two banks/Payment Service Providers[122] located within the same country;

[119] For information on best practices for use case identification and on implementation challenges, please refer to the chapter on "Implementing Blockchain for Trade Facilitation" in the first part of this Whitepaper which covers horizontal, cross-sectoral issues.

[120] For instance, the European Commission, the European Parliament and the European Central Bank. One of the main sources is represented by Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (amending directives 2002/65/EC, 2009/110/ EC and 2013/36/EU and regulation (EU) n. 1093/2010, and repealing Directive 2007/64/EC). Such Directive is also known as Payment Services Directive 2 (PSD2), being issued after Directive 2007/64/EC, the first EU law issued for regulating many remarkable aspects of payments services within EU and other countries adhering to the same rules.

[121] Art. 4, (5) Directive (EU) 2015/2366.

[122] The term Payment Service Provider represents a category of payment providers, including, beyond Credit Institutions, Electronic Money Institutions and the so-called Payment Institutions (please refer to art. 1(1) of

- **Regional payment** is a payment denominated in a single, specific currency exchanged by two banks/Payment Service Providers located within a specific geographical area which includes different countries. In this document for regional payment we're going to refer mainly to payments denominated in euro within the Single Euro Payments Area (SEPA[123]);
- **Cross-border payments** refers to payment transactions involving at least two banks/payment service providers located in two different countries. From a technical standpoint, SEPA payments between two banks located in two different countries in the Eurozone are cross-border payments, but, after the launch of SEPA, they are now considered regional (as an extension of local) because of the common rules and regulations governing payments within SEPA.
- **Cross-border and cross-currency payments** are payment transactions involving at least two banks/payment service providers located in two different countries or in the same country, where at least one currency conversion is executed.

10.2.1 Payment execution time: brief framework description

In order to make it clearer how Blockchain could be used in an evolutionary framework, the following paragraphs will provide a very brief picture of payment systems, both traditional (mainly provided by banks, Automated Clearing House (ACH) and Central Banks) and innovative (provided by some Fintech/Tech companies). It is important to note that this paper intentionally considers only the execution time perspective, both for purposes of limiting scope and, also, because execution time is one of the most important features of a payment service.

Due to actions by the European Commission and the Banking Industry[124] as well as competition from Fintech companies, in the last decade banks have improved considerably the quality of local and regional payments, particularly in Europe.

The EU Payment Services Directive 2015/2366 (PSD2) obliges banks to execute payments denominated in euro by the first working day after payment order is received (the execution time can be increased by one banking business day for paper-initiated payment orders).[125] It is important to note that payment execution time has been reduced because of European Commission Directives[126] and because of the competition brought by some fintech companies and, in particular, fintech companies that are able to handle payments on their platforms (closed-loop solutions). Solutions such as these allow for payment finality in a very short time. This is usually real-time/near-time as the debtor party and the creditor party are on the same platform and their sources of money are usually immediately available on such platforms (e.g. PayPal). It goes without saying that payments coming from traditional banking systems towards closed-loop solutions (e.g. PayPal) and vice versa will use the execution time defined

---

the mentioned Directive 2015/2366 (PSD2) for the complete list of institutions that can be labeled as Payment Service Providers.

[123] The Single Euro Payments Area includes 36 countries: 28 UE countries, 4 EFTA Countries (Switzerland, Liechtenstein, Iceland and Norway) plus Andorra, Vatican City, Monaco and San Marino.

[124] In Europe especially, but not exclusively, with the action of European Payments Council (EPC) and European Credit Sector Associations (ECSAs).

[125] Art. 83 e 87 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (amending directives 2002/65/EC, 2009/110/ EC and 2013/36/EU and regulation (EU) n. 1093/2010, and repealing directive 2007/64/EC).

[126] Starting with Directive 97/5/EC of the European Parliament and of the Council of 27 January 1997 on cross-border credit transfers until the previously mentioned Directive (EU) 2015/2366 (PSD2).

by laws (e.g. the PSD2 in Europe) and by banking schemes (e.g. SEPA Credit Transfer in Europe and SEPA Credit Transfer (SCT) Instant Scheme for transactions denominated in euro).

As customers have clearly demonstrated their great appreciation of real-time payment services and considering that technology allows payments to reach a real-time/near time execution, a SEPA Credit Transfer Instant Payment Scheme has been defined and implemented at the EU level (in November 2017) by the European Payments Council (EPC). The EPC Credit Transfer schemes (SEPA Credit Transfer scheme – SCT and the Instant SCT Scheme) allow SEPA located Banks to provide different levels of payment services to their customers ranging from instant to one day execution time[127], both for local and for regional (intra-SEPA) payments denominated in euros.

It must also be highlighted that before the creation of the Instant SCT Scheme in the EU, some national communities created local instant payment schemes, able to compete with fintech solutions. In Italy for instance, a local scheme named "Jiffy" was created in 2014 and it was able to put together the major banks and to reach the vast majority of Italian customers, holding an account or a payment card with an IBAN. In addition, other countries such as Sweden (SWISH), Denmark (NETS), Norway (VIPPS), the UK (Faster) Singapore (G3) and the US (Zelle) also had instant payment schemes in place before 2017.

As a consequence of these developments, the execution time for local and regional payments denominated in the local/regional currency can be assumed to no longer be an issue in many countries, especially where instant payment implementations have taken place during the last four to five years.

The situation is different, however, when looking at cross-border and cross-currency payments. In relation to EU/SEPA, a distinction must be made between:

- Payments within the EU Payment Services Directive (PSD2) scope, where the execution time is set to:
    - **one business day** when EU currencies other than the euro are involved (with an additional business day for paper-based orders);
    - **one business day** for non-euro transactions different from the ones mentioned under the previous bullet point, unless differently agreed between the payment service provider and the customer, and in no more than **four working days.**[128] A typical use case is illustrated by a credit transfer made in US dollars and ordered by a customer of a bank located in an EU country to a beneficiary with an account held in another EU country;
- Payments outside the scope of PSD2, for which, in Europe, no limit is set for the end-to-end execution time. This is in specific reference to one-leg transactions, these being transactions where only one bank (the payer's Bank, or the beneficiary's bank) is located in the EU since it is clear that the European Commission can only regulate the part of the transaction executed in the EU. A typical use case is illustrated by a credit transfer made in a non-EU currency and ordered by a customer of a bank located in the EU to credit a beneficiary with an account held in a non-EU country (or vice versa). As a result, the execution time cannot be determined and may take a long time, due to differences in time zones, payment systems and Central Banks.

[127] Two banking business days for paper-initiated payment transactions.
[128] Please refer to Section 2, Execution time and value date and, in particular, to articles 82, 83 and 87

This problem with execution times also exists in countries outside of the EU and in other use cases. This is especially true for cross-border and cross-currency transactions of the kind mentioned above (with banks in different countries), due to the cross-jurisdictional nature of the credit transfer. Even when considering only the execution time, without taking into consideration other aspects of a credit transfer, such as fees, it is clear that the use cases described leave room for greater efficiency. This is especially true in a world that is always connected and for the vast majority of people who are unaware of all the processes needed to ensure a smooth execution of cross-border and cross-currency payments.[129]

10.2.2 Permission-less (Bitcoin-) Blockchain based cryptocurrency payments

Bitcoin has been selected for making a comparison between Blockchain and traditional payments, it is currently the most important cryptocurrency used for payments, although it is not the only permission-less Blockchain network.

The execution time of a bitcoin payment should be considered to be about an hour on average, as the addition of four to six blocks to the chain[130] are judged to be a sufficient number to consider final (confirm) a bitcoin payment. In 2009, when the Bitcoin Blockchain was created, its execution time presented a great advantage over traditional payment systems, especially in the case of regional payments. However, in Europe, the introduction of instant payment schemes has made Bitcoin not faster than local and regional SEPA euro payments. However, from the perspective of execution time, Bitcoin still has an advantage in cross-border and cross-currency payments, and, particularly, for those transactions with, and between, banks outside of Europe.

For a complete comparison, consideration must be given to other characteristics of the Bitcoin Blockchain as a payment service system, with a specific focus on current limitations, from a banking perspective, in comparison with traditional payment systems:

- **Scalability**: The current number of transactions per second on the Bitcoin Blockchain is about seven, which is significantly lower than traditional payment systems. Solutions are being developed[131] (some of which also work with other Blockchains), but these are still in early stages of development and are not easily accessible by individuals without technical backgrounds who want to make payments
- **Privacy**: Permission-less Blockchain transactions are public by design. Therefore, even though addresses are not immediately attachable to a natural or legal person, they are pseudonyms which can, with skilled forensic research, be linked to the real identity of a party and, in addition, any third party with an Internet connection can see the transactions made by an address.
- **Traceability**: for compliance reasons, payments must be traced at end-to-end level, from the payment order to the credit entry in favour of the beneficiary, by having a complete track of all the parties (customers and Payment Service Providers) that have been involved in the transaction. The Bitcoin Blockchain, and some other Blockchains,

[129] We can mention for instance clearing, settlement, Know Your Customer, creditworthiness, funds availability, processes.
[130] In the Bitcoin network a new block is added every 10 minutes
[131] https://cointelegraph.com/lightning-network-101/what-is-lightning-network-and-how-it-works#cons (as of February 2020).

but not all, use an accounting method based on features which are called UTXOs.[132] This model adds another level of complexity which can make it more difficult to trace payments.

- **Bitcoin price**: the volatility of the price of Bitcoin makes it very difficult to guarantee the transfer of a fixed fiat currency value using a Bitcoin payment because of exchange rate differences that could occur during the transaction as well as fluctuations in the fiat value of the Bitcoin transaction fee.[133] For example, if a bank decides to use Bitcoin to transfer a (main) fiat currency (like euro or United States dollar), there would be Bitcoin volatility during both currency conversions, (i.e. from fiat currency to Bitcoin and from Bitcoin back into a fiat currency) and fluctuations in the fiat value of the transaction fee – all of this further complicated by the related rules to be applied to these costs for fiscal and accounting purposes.

As a result of the above-mentioned limitations, banks believe that, currently, Bitcoin cannot be scaled for use at a large-scale global level for payments. At the same time, Bitcoin and other Blockchain cryptocurrencies also represent an extraordinary innovation because they make possible the transfer of digital assets between two independent parties in a short timeframe, in a trustworthy manner and without the need of an intermediary. This is in comparison to traditional payment systems (even if more efficient) which require of a number of players (banks, Automated Clearing House (ACH), Central Banks, etc.) in order to guarantee a payment's completion.

10.2.3 Payments executed with a permissioned Blockchain

Taking into account the limitations described above and the negative attitude of many regulators towards Bitcoin and other cryptocurrencies[134] which use public Blockchain networks, it is easy to understand the search for alternatives. As a result, many important financial institutions have looked towards permissioned Blockchain networks. With this technology, financial institutions are trying to obtain the advantages of Blockchain technology such as higher efficiency and the enabling of new services while eliminating some features of permission-less Blockchains that are not considered useful in a permissioned environment.

The advantages described above which are the key motivations that drive banks and other institutions to invest in Blockchain permissioned networks also exist on permission-less Blockchain networks and, sometimes, are even stronger on such Blockchains – but they most often come with some, or all, of the limitations described above for Bitcoin.

Permissioned Blockchain networks can avoid most of the limitations of the Bitcoin Blockchain. This is because they set their own governance rules and can change them more easily than public networks because they control who is allowed to maintain a node (and all nodes must agree on the governance rules to be used). As a result, and depending upon the governance rules it uses, Blockchain permissioned networks seem to have made possible the execution of

[132] UTXO is the acronym of Unspent Transaction Output. For an explanation see https://coincentral.com/utxo-beginners-explainer// (as of February 2020).
[133] A fiat currency is a currency issued by a National Central Bank, so formally and legally accepted for payments and extinguishing debits.
[134] A warning on the risks connected to virtual currencies was issued in February 2018 "*ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies*" See https://www.eiopa.europa.eu/content/esma-eba-and-eiopa-warn-consumers-risks-virtual-currencies_en?source=search (as of February 2020).

payments without the limitations connected to public Blockchains and especially those limitations related to traceability, privacy and scalability.[135]

With regard to the execution time for payments on a Blockchain-permissioned network, this depends on the governance structure (rules) and agreed upon payment methods. Three of the most common payment cases are described below.

- When a publicly-traded cryptocurrency is used, the end-to-end-execution time (for cross-currency payments) can be greatly reduced with respect to what has been described for traditional payments, even though a prefunding by the banks involved is usually needed in either cryptocurrencies and/or fiat currencies (according to the case).
- Only fiat currencies are used. In this case, the traditional payment mechanisms are used for currency conversion and settlement, which means that the execution time is usually not reduced dramatically (when compared to standard execution times). So, for Blockchain permissioned networks that do not use a cryptocurrency, payment execution (i.e. the real transfer of value) must be implemented off the Blockchain using traditional methods.
- IoUs (a document acknowledging a debt) or tokens[136] representing IoUs are used together with fiat currencies. Blockchain networks can be used to transfer any asset that can be represented digitally, in this case an IoU. In this case, only use of cryptocurrency is to pay generally small transaction fees, so cryptocurrency price fluctuations have a minimal impact.[137]

For the above-mentioned issues and cases there is currently no solution in place for large-scale global use, but it is possible that a winning solution will emerge in the near future. However, considering that considerable attention is being given to this subject[138], as well as anticipated contributions from high-value players, it is plausible that a solution will be found soon. This is also because there are some important signals of a potential cooperation between traditional and fintech players, which is the right combination for creating a new and fully effective solution. In addition, it is important to mention that there are many initiatives (proof-of-concepts and pilots) either completed or in progress which deal with other aspects of the payments value chain that are based on Blockchain permissioned networks[139], some examples of which are given below:

- SWIFT tested nostro/vostro[140] accounts reconciliation (see section on Nostro accounts) with a proof-of-concept in which thirty-four leading international banks participated. In

[135] Please refer to what mentioned on their respective websites for example by two important players like Ripple (with its solution) and JP Morgan (with Quorum).

[136] Tokens are more limited in their use than cryptocurrencies. A token has a specific use in a blockchain network. For example, one could have a token that can only be used for paying transaction fees on a specific network and nothing else or that could only be used for purchasing music on one blockchain, etc. Tokens must be purchased with cryptocurrencies, but you cannot purchase cryptocurrencies with tokens.

[137] The following explain the functioning of one such network. The first is a non-technical explanation and the second goes into more detail. Non-technical: https://medium.com/@jcata018/everything-to-know-about-ripple-part-1-how-ripple-works-f7404aa4a8d1; More detailed: https://www.mycryptopedia.com/ripplenet-and-ripple-xcurrent-explained/ (as of February 2020).

[138] See https://www.ibm.com/downloads/cas/JLDYADKJ and https://bitcoinexchangeguide.com/top-rated-blockchain-bank-payment-systems/ (as of February 2020).

[139] We mentioned only a small subset of initiatives in the payments area to provide some examples, bearing in mind that a much richer list might be provided.

[140] https://www.investopedia.com/ask/answers/051815/what-difference-between-nostro-and-vostro-account.asp (as of February 2020).

particular, Blockchain technology demonstrated that it was able to deliver automated real-time liquidity monitoring and reconciliation;

- Many Central Banks are also testing the capabilities of DLT/Blockchain permissioned networks. For instance, the Bank of Japan (BOJ) and the European Central Bank (ECB) launched a research project called "Stella", which studied the possible use of Blockchain technology for financial market infrastructure. In the first step of their cooperation, the BOJ and the ECB conducted in-depth experiments on whether specific existing functionalities of their respective payment systems could be run in a Blockchain environment in an efficient and safe manner. Specifically, the liquidity saving mechanisms of BOJ-NET and TARGET2 (the Real-Time Gross Settlement (RTGS) systems of the two central banks) were tested in a publicly available application and a number of tests were run.

Consequently, it can be concluded that many processes around payments are being tested by different players, from the liquidity saving mechanism (verified by some Central Banks), to the payment execution and reconciliation mechanism (tested by banks and SWIFT). If the increasing number of tests and players involved are combined with the continuous improvement of Blockchain-permissioned networks, the results could see such technologies soon becoming functional in real-world environments.

10.2.4 Intercompany payments

A large percentage of trade today is intra-firm trade[141] with accompanying intercompany payments; and an increasing number of companies today are experiencing serious issues and financial costs as a result of improper or insufficient intercompany accounting practices. There have been several instances where companies have restated their prior year's financial statements due to error and fraud discovered within intercompany accounts. Many companies have actively attempted to address the weak points within intercompany processes by increasing automation, developing an internal centre of excellence and improving internal organisational alignment. However, according to a recent survey on Intercompany accounting and process management[142] several key challenges continue to exist.

The challenges identified include;

- **50 percent** of respondents noticed a **lack of defined ownership** of the intercompany process and challenges with visibility into the process and key management activities;
- **54 percent** have **manual intercompany processing** with limited counterparty visibility to support reconciliation and the elimination of errors and unbalanced items
- **47 percent** indicated only **ad hoc netting capabilities**
- **30 percent** noted significant **out-of-balance positions**

While intercompany accounting covers a number of processes; a starting point for many large corporations has been to focus on the area of intercompany reconciliations. Intercompany reconciliation is a monthly process within large organisations whereby the accounts between

[141] Lanz, R. and S. Miroudot (2011), "Intra-Firm Trade: Patterns, Determinants and Policy Implications", OECD Trade Policy Papers, No. 114, OECD Publishing, Paris. http://dx.doi.org/10.1787/5kg9p39lrwnn-en (as of February 2020).

[142] Deloitte (2017) Intercompany accounting and process management. Survey results, See https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-intercompany-accounting-survey1.pdf (as of February 2020).

subsidiaries are balanced and any mismatches of transaction data within the group are identified. The various subsidiaries are usually in different locations and offer different products and services, adding to the complexity of the process. The current process, in most organisations, depends on manual data entry resulting in delays between the distribution and receipt of goods and the recording and sharing of related information. This, in turn, creates inefficiencies and added effort in balancing intercompany transactions.

The key pain points within the intercompany reconciliation process can be summarized below:

- **Business Processes**: Manual data entry exists in the process that could be automated;
- **Data Analysis**: Data inconsistency and variation between systems that lead to Out-of-Balances (OOB's) that could be prevented;
- **System Architecture**: A lack of integration and data sharing among systems, resulting in extra work.

The graphic below highlights a sample problem faced in an intercompany reconciliation

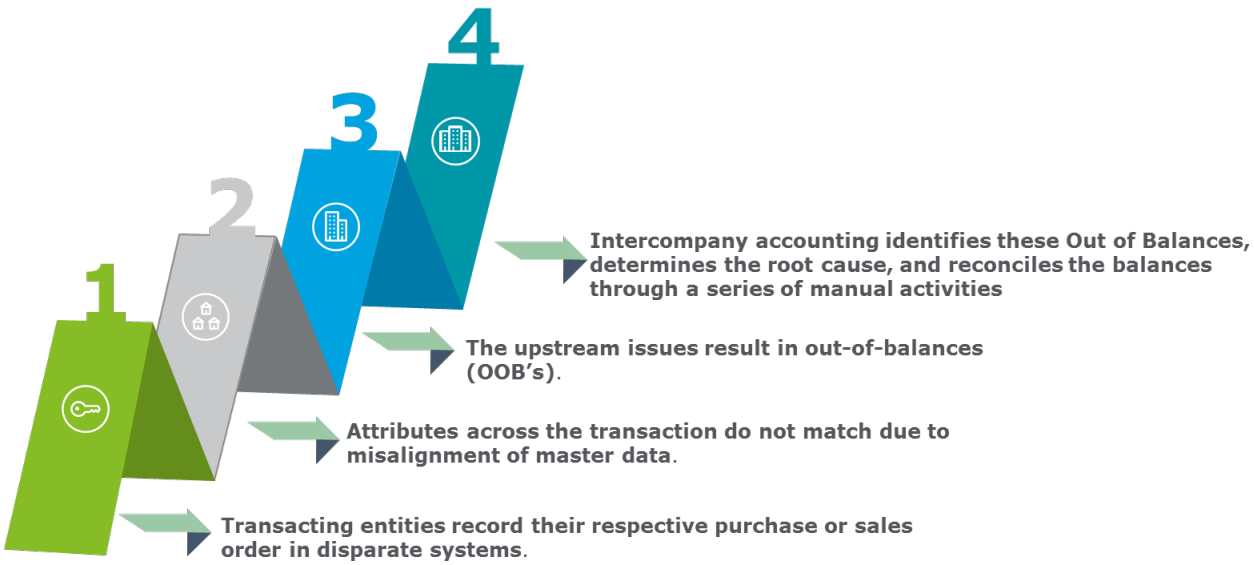

Figure 10.1 - Problem Faced in an Intercompany Reconciliation

Blockchain has been identified as a potential game changer within the accounting space to address intercompany transactions, as highlighted in the article, *"Blockchain Technology; A game-changer in accounting?"* [143] Rather than maintaining separate records based on transaction receipts, a company could write their transactions directly into a joint register. This would create an interlocking system of enduring accounting records. Additionally, due to Blockchain's decentralized network and tamper-proof capabilities, falsifying or destroying data would be practically impossible.

With regard to the intercompany transactions process specifically, Blockchain has three key capabilities which could make a real impact in this space.

[143] Deloitte (2017) Blockchain Technology – A game-changer in accounting See https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A%20game-changer%20in%20accounting.pdf (as of February 2020).

1. **Smart Contracts,** if programmed to do so could:
    - Compare key fields in transaction documents (e.g. sales order, purchase order, goods, receipt, etc)
    - Where key fields do not match across documents, the smart contract could notify parties to take corrective action
2. **Distributed Ledgers** with secure copies of all data on multiple nodes, can increase access to information because:
    - Key stakeholders, who are dependent on or consume upstream transaction data, have access to the complete history of any given transaction.
    - Increased transparency allows near real-time decision making, so issues can be resolved at their point of origination, before month-end, and so occurrences of OOB's can be reduced.
3. **Irreversibility** – An irreversible and immutable record of transactions provides benefits because:
    - By its nature, once information has been posted to the Blockchain, it cannot be altered or removed.
    - This creates transparency which can support or complement existing compliance or audit controls. Entire business processes, spanning multiple departments or companies become easily traceable – providing huge benefits from an accounting perspective.

These Blockchain capabilities can enable a more trustworthy, transparent and secure process which effectively eliminates the manual processes and data errors that impact the process today. The use of smart contracts to execute and validate reconciliations means that the resource requirements and manual hours spent on this process can be dramatically reduced. These cost reductions and efficiency gains can positively impact the bottom line of an organisation and make this use case for Blockchain technology an attractive one.

However, in order to realise the full benefits of Blockchain technology, the solution must function in collaboration with other systems which are external to the organisation. The art of the possible would see an industry-wide platform for payments, transactions and reconciliations across separate organisations, but reality will probably result in a variety of such platforms. The need to exchange information between these platforms will focus attention on the need for data definition standards such as those developed by UN/CEFACT.

An intercompany-reconciliations use case can be a good starting point for organisations to familiarise themselves with Blockchain technology and to build related technical skills and expertise. It allows the technology to be tested in a safe environment and provides the team with first-hand experience in interacting with Blockchain technology as well as understanding its capabilities and limitations.

10.3 Credit Management (CM) and related Know Your Customer (KYC) requirements

Credit Management (CM) is a composite tool made up of processes to identify and manage the commercial counterparty risk of corporates. In order to identify possible uses of Blockchain technology in CM, significant attention has been paid to relevant innovation and improvement needs, with a focus on the most critical processes.

10.3.1 Credit Management processes

A usual breakdown of CM tasks and activities includes:

- Customer or counterparty setup and evaluation, or better, KYC activities;
- Credit Insurance management;
- Analysis, and Interchange with the insurance company (data exchange, service evaluation, contract definition);
- Definition of credit level and payment terms and conditions;
- Procedures for collection and overdue management;
- Includes reminder emails and interaction with Customer Service and Legal departments;
- Support to Reporting: i.e. the output and availability of data for reporting, accounting and sharing with other internal/external departments/offices.

All of the above activities are required for both the account setup and maintenance/update phases. Below are some interesting areas for possible innovation and some thoughts on the use of Blockchain technology.

10.3.2 Customer setup and evaluation

This process is increasingly evolving into standard KYC and insurance management practices and appears to be suitable for innovation and improvement, both in terms of data flow and performance.

10.3.3 Blockchain technology potential

Most CM phases/tasks analyse data flow and then take decisions, producing and/or forwarding new data. As a result, smart contracts have the potential to be useful tools. In addition, having available a Blockchain notarization service could help to streamline many processes by ensuring the trustworthiness of data integrity, of origin/destination authenticity, and of timestamps.

10.4 Invoice financing

Invoice financing, also known as accounts receivable financing, is a form of short-term borrowing which is extended by a bank or a lender to its customers based on unpaid invoices. Another form of invoice-based financing is factoring, which involves the sale of accounts receivables rather than getting a loan. Invoice financing is often done to meet the short-term liquidity needs of a company. To provide this service, banks offer invoice financing services based upon information exchanges between them and the account owners (e.g. companies).

Currently, invoice financing services are composed of the following main steps:

- The seller provides his products and services to the buyer, and invoices them accordingly;
- The seller then sends his paper invoices to the bank that offers his invoice financing solution; and
- The bank advances up to a defined percentage of the value of the invoices to the seller.

In this process, the credit entitlement (from payment of the invoice) is not transferred to the bank but remains with the seller.

This process can also be electronically offered by banks (ISO standards are available for this); through the use of digitalized services. This enables companies to make their internal processes more efficient and increase the level of automation, while significantly reducing their "paper-based" activities.

The information included in the invoice financing request is primarily general invoicing information which can usually be found on an invoice's header/footer such as buyer and seller information; invoice payment amount; and payment terms and conditions

In order to provide an overview of the current reference model for the process called invoice financing service, a business scenario has been identified. This scenario identifies three main phases, as illustrated in the picture below.

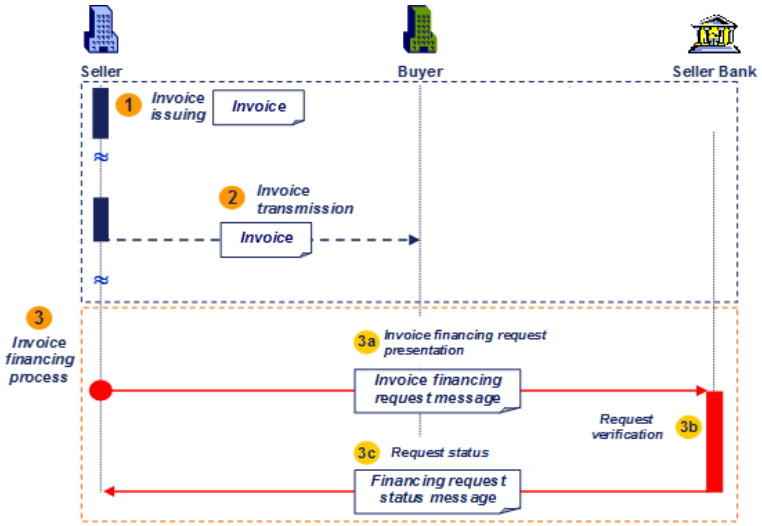

Figure 10.2 - Invoice Financing Service

10.4.1 Invoice Business scenario

The first two phases describe the invoice presentation:

a) Invoice issuing, which includes all the procedures executed by the seller in order to issue the trading transaction invoice (which can be either electronic or paper-based) to the buyer; and

b) Invoice transmission, which is the sending of the invoice from the seller to the buyer.

c) The third phase, which is shown with red lines in the illustration, describes the invoice financing process:

i. The seller sends an invoice financing request message (which can be submitted through several channels e.g. email, private networks etc.) to his bank (Seller Bank);

ii. After presentation of the invoice financing request, the Seller Bank completes verification of the financing request message (e.g. message syntax verification); and according to the results of the verification when it is completed,

iii. The Seller Bank sends a "financing request status messages" (e.g. 'financing request received by Seller Bank', 'financing request rejected by Seller Bank').

The process of how invoice financing could be organized using Blockchain technology is illustrated and explained below.

10.4.1.1 Invoice financing request with Blockchain technology

Once the Seller invoices the buyer, the bank can immediately provide short term financing to the seller, resulting in improved economics of capital allocation and reduced risks of fraud. This would be a result of the ability of Blockchain to make available trustworthy invoice information in real time, including the information that the invoice had been submitted for factoring, thus eliminating the risk of duplicate submissions of the same invoice for factoring. If the smart contract also requires that the buyer acknowledge the invoice as being valid before it is financed, this could even further reduce risks and make factoring more affordable for SMEs.

Discounters (i.e. Banks) could gain multiple benefits from the application of this technology, including:

- An immutable and time stamped record of the existence of every invoice raised by a requesting company;
- An immutable and time stamped record of the requesting-company client's receipt, confirmation and verification of the invoice (against which a discounter would fund);
- If decided upon, an immutable time stamped record of the assignment of a particular invoice to a discounter (for factoring);
- A registered status change of the invoice to indicate that it has been "discounted", and of its impact on the available balance of the requesting company, registered on the permissioned network and shared among (only) financing intermediaries. This would allow the intermediaries to better evaluate, subsequent submissions of invoice financing requests from the same company.

One last obstacle is the size of the accounts receivables balance which is needed in order to obtain invoice financing -a relatively large accounts receivable being needed in order to offset the costs of processing and handling this kind of loan as well as the risk. As a result, this kind of financing may not be a viable option for micro, small and medium enterprises (MSMEs) due to the size of their account receivables. Therefore, by dramatically lowering costs and risk, Blockchain technology could open up new business scenarios, enabling MSMEs to easily access short-term financing through the sale of account receivables on Blockchain, using smart contracts. This would create a digital marketplace for invoices and a credit-rating system for MSMEs in the network (e.g. Populous[144] and Hiveterminal[145] projects).

In the case where the debtor is also granted a letter of credit (guarantee of payment from a financial agent), and this event is registered on the Blockchain, the invoice financing process can also be expedited for the seller of the account's receivables.

[144] https://coinrivet.com/populous-worlds-invoice-financing-platform-is-now-live/ (as of February 2020).
[145] https://www.hiveterminal.com/en/ (as of February 2020).

10.5 Purchase Order Financing (POF)

Purchase order financing (POF) gives companies a short-term solution for working capital, i.e. the funds necessary to manufacture or create the goods/services need to fill orders and thus complete sales transactions. This financing is also tied to inventory. It can be based upon both receivables (similar to factoring) or payables (financing of commercial debts), and it can either be based on purchase orders released/received, or contracts already signed between customer and supplier. POF can either be covered by a banking credit line or by another financial agent/instrument which works via direct payments to suppliers.

Both factoring and POF offer short-term financing solutions. However, the former accelerates cash flow from invoices while the latter allows clients to be in possession of the goods before generation of the invoice.

Companies use purchase order funding to support expansion, handle large orders or surges in business, and occasionally for operating expenses. Some of the reasons for using POF financing include:

- Lack of working capital
- Profit opportunity
- Desire to avoid credit risk (POF is not considered debt)
- Immediate sales.

POF is designed, in particular, for growing businesses that want to fill large orders. The types of businesses that usually qualify include:

- Manufacturers
- Distributors
- Wholesalers/resellers, and
- Importers/exporters.

The creation of a classic working-capital-gap problem occurs when a seller needs to make an up-front payment to a supplier following a large purchase order (PO) from a new or existing customer. This is a problem because the seller will typically receive the payment for their invoice from their customer between 60-90 days after the shipment is received. As a result, in the time between the advance payment to the supplier and the receipt of payment from the customer there is a classic working capital gap. PO financing provides the capital needed for the purchase of supplies, the production of products and the shipping of finished goods.

Figure 10.3 - Purchase order financing

10.5.1 The Purchase Order Financing (POF) process

There are four parties in a POF process:

a) The borrower/seller who seeks the funds;

b) The POF company that provides the funds;

c) The supplier who supplies the goods that are then sold or distributed by the borrower; and

d) The customer to whom the borrower sells the goods.

The buyer makes a purchase order (PO) and sends it to the seller (the borrower). In this case, the assumption is that because the seller/borrower does not have the necessary funds, he seeks some outside financing. The borrower then applies for funding from a POF company, providing the customer's PO as well as a cost proposal from their supplier. When the borrower is approved, the POF company uses a letter of credit to pay the supplier to manufacture and deliver the goods required by the seller. The customer receives the goods either from the borrower/seller or from the supplier and is invoiced by the borrower. The customer then directly pays the POF company, which in turn pays the borrower, but only after deducting their fees for the service provided.

10.5.2 Blockchain to enhance purchase order financing

As is the case for Invoice Financing, POF could be enhanced by the use of Blockchain technology. It may be possible for traders and financiers to benefit from:

a) An immutable and time stamped record of the purchase order;

b) An immutable and time stamped record of the confirmation and verification of the purchase order;

c) An immutable and time stamped record of the assignment of a particular purchase order to a financier;

d) A status change of the 'financed' purchase order on the Blockchain (showing it to be financed) and the registration of the available balance (in the POF account) on the permissioned network and shared amongst (only) the financing intermediaries, thus allowing them to better evaluate other POF requests from the same party(ies).

The Blockchain could also register all the financed trade documents so as to avoid double financing of both invoicing and of other receivables (active orders confirmed). This would all be done while keeping track of all the documents linked to the same contract/payments in a notarized way.

One of the most important risks in the supply chain lies in small suppliers which are often SMEs. This is because they face difficulties in accessing capital to finance their operations. The main problem with extending supplier finance to these small suppliers concerns commercial privacy because most of them would not want to reveal to their customers and partners their cost of goods from sub-suppliers or their operating margins.

Blockchain technology can offer a solution to this privacy issue. As described earlier, Blockchain applications can be designed to let users selectively share information, deciding on a case by case basis what to include or exclude. As a result, transactions can be recorded on the Blockchain and supply chain participants could retain control of their own data, revealing only chosen information to selected parties, who can still be assured of the validity and the

authenticity of the data. Fund providers would thus be able to validate the total amount of purchase orders or invoices without having access to more sensitive information.

10.6 Letters of Credit (LC)

A Letter of Credit (LC) is a tripartite formal agreement involving the buyer (applicant), the bank and the seller (beneficiary). The bank promises 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. This method of payment is frequently used in international trade, particularly when buyer and seller do not have a pre-existing relationship and are located in different countries with different laws and trading rules. From the beneficiary's standpoint, the LC helps to reduce credit risks.

An LC is a complex agreement to be managed, there are many clauses which can be included and many parties and documents that can be involved.

10.6.1 Sales Agreement Between Buyer and Seller

The sales agreement between the buyer and the seller is not part of the LC. The LC includes information from the sales agreement, but it is a completely different and separate agreement. When a buyer and a seller decide to do business together, they agree on quantity and price of the goods as well as other commercial conditions (i.e. method and terms of shipment and method of payment). Part of this agreement may include that the seller wants to cover the shipment with a LC. The buyer sends to the seller orders for goods, the seller agrees to produce them, and then issues an orders confirmation with the description of the goods and the price of the ordered items.

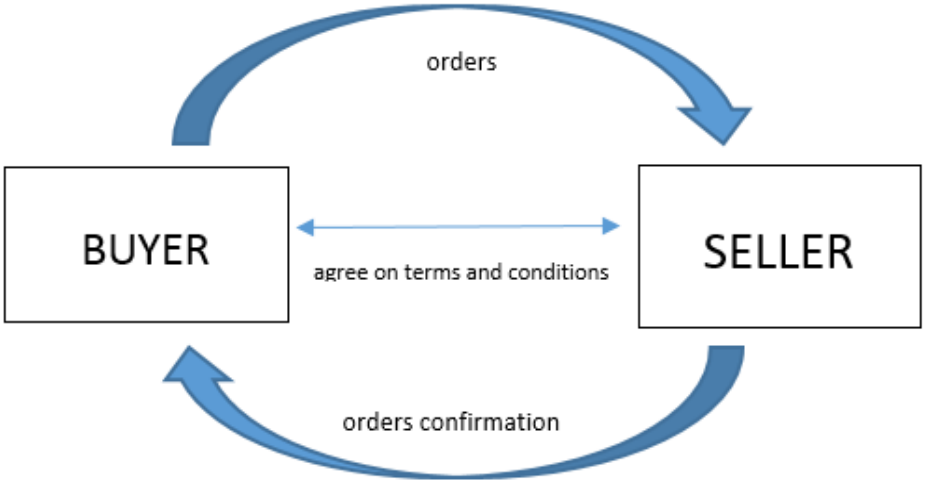

Figure 10.4 - Sales Agreement Between the Buyer and the Seller

10.6.2 Letter of Credit Process

The Letter of Credit (LC) process can be summarized as follows:

- Issuing of LC
- Shipment of goods and sending of documents, and
- Payment.

10.6.3 Issuing of Letter of Credit

The parties involved in the issuing phase are the:

- Buyer (Applicant)
- Buyer's bank (Issuing Bank)
- Seller, (Beneficiary), and
- Seller's bank (Advising Bank).

Once a sale has been agreed, the buyer contacts his bank. Usually the bank operates in the buyer's country and, in most cases, there is a stable business relationship between them. The buyer provides the bank with all the information necessary to open the LC on a bank form which is specifically for that purpose.

- The most frequently requested information concerns the:
- Amount of related sales agreement;
- Name and the address of the beneficiary (seller);
- Latest date for the shipment;
- Date and place of expiry of the LC;
- Presentation period –i.e. the due date by which the seller must present the requested documents to the bank (which is 21 days after the last date of shipment, unless otherwise indicated by the parties);
- Method of transportation;
- Place of departure and destination; and
- Other details (e.g. documents requested, name of the forwarder, INCOTERMS, party in charge of the insurance).

The bank draws up the text of the LC and sends a draft to the buyer/applicant for a formal check and confirmation. If the LC draft includes all the information requested and it is correct, the buyer/applicant authorizes his bank to proceed with the issuing of the LC. The Issuing (Buyer's) Bank opens the LC and sends it to the Advising (Seller's) bank which is typically a bank in the seller's country with whom the seller works. From this moment, the Buyer's Bank promises to make the payment, under the conditions of the LC. After having reviewed the text of the received LC, the Seller's bank forwards it to the Seller. If the text complies with the sales agreement between the Buyer and the Seller, the Seller begins to produce the goods. If the text does not comply with the sales agreement between the Buyer and the Seller, the Seller will ask for an amendment to the LC so that it meets the terms of the sales agreement.

10.6.4 Shipment of Goods and Sending of Documents

The parties involved in this phase of the process are the:

- Buyer
- Buyer's Bank
- Seller's Bank Seller
- Carrier; and

- Others (i.e. Chamber of Commerce if the LC requires a Certificate of Origin, or Customs Operator if the LC requires EUR.1/EUR.2 Certificate).

Generally, the Seller has to:

- Ship the goods by the latest date of shipment agreed;
- Use the method of shipment and the carrier specified in the LC;
- Ship the goods from and to the indicated ports/airports;
- Collect all the documents requested in the LC;
- Submit the documents to the Seller's Bank within the presentation period and before the expiry date of the LC.

The Seller, after the production of the goods, issues the commercial invoice and the packing list. Then he contacts the Carrier who takes the goods and issues the transport documents. Depending on the mode of transport, the Carrier issues a B/L (if the shipment is by sea), an Air Waybill (if the shipment is by air) or a CMR (if the shipment is by truck).

Above all, if the Seller chooses to be paid with a LC, he has to submit to the Seller's Bank all the documents indicated in the LC and these documents must reflect the stated conditions. Typical kinds of documents requested in a LC are:

- Commercial documents (invoice and packing list);
- Transport documents (Bill of Lading, Air Waybill, CMR …); and/or
- Other documents (Certificate of Origin, inspection certificate …).

If the LC requires other documents, the Seller must contact the entity(ies) responsible for producing them. For example, if the agreement between the Seller and the Buyer requires the issuing of a Certificate of Origin, the Seller must contact the local Chamber of Commerce in order to obtain it. If a certificate of inspection is necessary, the entity nominated by the parties and indicated in the text of the LC must check the goods, and issue a document stating that quality of goods is acceptable.

When the Seller's Bank receives the documents, it checks whether they are consistent with the terms and conditions of the LC. The bank performs a formal check and, in the event that a discrepancy exists between one of the documents and what is stated in the LC, the bank refuses the payment. The bank is not interested in the quality of goods nor any other issues related to the business relationship itself.

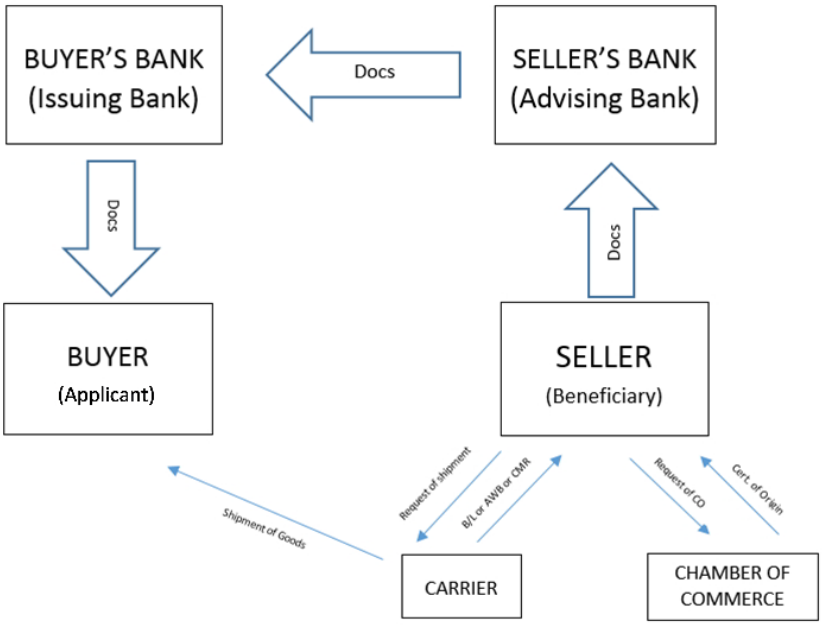

Figure 10.5 - Shipment of Goods and Sending of Documents

10.6.5 Payment of LC

The parties involved in this phase of the process are the:

- Buyer
- Buyer's Bank
- Seller's Bank, and
- Seller.

As a result of the checking of the documents performed by the bank it is possible to have two different situations which are:

a) The documents comply with the terms of the LC (clean documents); and

b) The documents do not comply with the terms of the LC (discrepant documents).

In both cases, the Seller's Bank sends the documents to the Buyer's Bank which then reviews them. If the documents comply with the terms of the LC, the Buyer's Bank sends the payment to the Seller's Bank. This happens if the payment term that is used is at sight. In the event that the term used is deferred payment, the Buyer's Bank commits to pay. Afterwards, the Buyer's Bank forwards the documents to the Buyer, who is able to use them to collect the goods as soon as they arrive at the destination port/airport.

If the documents are discrepant, the Buyer's Bank informs the Buyer that the documents are not consistent with the LC terms, giving the Buyer an option to either accept the discrepant documents or not. If the Buyer accepts the documents, the Buyer's Bank forwards the documents to the Buyer and debits its account. If the Buyer decides not to accept the documents, the bank does not make the payment and gives back the documents to the Seller's Bank. This means that the Buyer will be unable to collect the goods.

10.6.6 Issues in Current LC Process

LCs are evaluated on the basis of trade documents and underlying contracts including sales contracts between the Buyer and the Seller, as well as contracts signed by the Buyer to reimburse payments made by the Buyer's Bank (based on the Seller's compliance with the LC).

Problems can arise in the interpretation of documents' text, and of requirements. Errors may give rise to disputes between the parties, leading to delays in the acceptance of goods upon delivery and, as a result, delays in payments.

According to a Cognizant whitepaper[146], the main issues on LCs are:

- Payment disputes due to contractual ambiguities - 4 out of 5 of the first versions of LC document submissions contain inaccuracies, errors and/or discrepancies
- Payment delays from errors in the contract (including semantic or syntactic errors) – 70 percent of LC documents are rejected on first presentation
- Increases in costs and overhead due to LC amendments - 7-10 days is the average LC issuance time and 250 United States dollars the average issuance cost

LCs are a business practice that has been in use for a very long time. The key point related to the above issues is the need to present documents to facilitate trade payments, thus the risk of fraud and error, and delays. In all cases, it is also a relatively slow and expensive process. An alternative is the use of open account terms instead of LCs. With open-account transactions, sold goods are shipped and delivered before payment is due, which is normally 30 - 90 days. This, together with the working capital advantage for the importer, creates a risk for the exporter. Risk mitigation can be implemented by supply chain finance tools[147], such as: receivables discounting, forfaiting, factoring, payables finance, loan or advance against receivables, distributor finance, loan advance against inventory, pre-shipment finance, bank payment obligation (BPO), etc. [148]

According to Chain Business Insights[147] "the majority of trade [is] now conducted on open account terms", as confirmed by the International Chamber of Commerce in its Global Survey on Trade Finance and Supply Chain Finance 2017. But "traditional trade finance remains…, estimates the ICC – a sizeable chunk of world trade". Therefore, as highlighted by a pilot project of BBVA, "paper-based LCs are ripe for Blockchain-based solutions. Which begs the question: will Blockchain technology halt the decline in the LC, or even trigger something of a renaissance in its use?" [149]

[146] Lata Varghese, Rashi Goyal, "Blockchain for Trade Finance: Payment Method Automation (Part 2)", https://www.cognizant.com/whitepapers/blockchain-for-trade-finance-payment-method-automation-part-2-codex3071.pdf (as of February 2020).
[147] https://www.chainbusinessinsights.com/insights-blog/can-blockchain-revive-the-letter-of-credit (as of February 2020).
[148] http://icc.academy/wp-content/uploads/2016/03/Standard_Definitions_for_Techniques_of_Supply_Chain_Finance.pdf (as of February 2020).
[149] https://www.bbva.com/en/bbva-and-wave-carry-first-blockchain-based-international-trade-transaction-europe-and-latin-america/ (as of February 2020).

10.6.7 A Blockchain-Based LC

According to the Cognizant analysis cited above, in a Blockchain environment LCs can be structured as smart contracts between the financing institution and the supplier in order to guarantee payment to the latter. This occurs provided that traded goods are delivered to the buyer according to specified conditions. Such smart contracts codify "*the terms and conditions of trade. This is done by abstracting and expressing conditional clauses — regarding the time, place and manner of shipment and delivery, the description and quantity of the goods shipped, and the documentary evidence required for verification — as separate, independent or interdependent functions that provide pass/fail outputs based on the input information. Based on the documents submitted by the exporter, evaluating and verifying that the LC conditions meet specified shipment deadlines can be automated through program logic to indicate compliance or non-compliance for each case*".[146]

A typical LC transaction process, using Blockchain technology, could include the following steps (see IBM[150]):

After buyer and seller enter into sales contract:

a) At buyer's request, buyer's bank sends LoC to seller's bank (Letter of Credit through Blockchain);

b) Seller ships goods to port near buyer (Goods);

c) Seller obtains receipt confirmation documents from port & forwards them to its bank (Documents through Blockchain);

d) Seller's bank reviews the documents and sends to buyer's bank (Documents through Blockchain);

e) Buyer's bank reviews entire transaction and pays seller's bank, which in turn pays seller (Payment Authorization through Blockchain); and

f) Buyer takes delivery of goods from port (Goods).

Thus, the LC can be sequentially reviewed and approved by all participants. The network consensus mechanism ensures there is only one single final version of the LC draft at any given time and that all parties are able to view and work on this version based on their access rights.

10.6.8 Blockchain Benefits for LCs

From the above analysis and design proposal, the most relevant benefits introduced by Blockchain-based LCs can be listed as[151]:

- Reduction of ambiguities and errors in contracts - specifying LC requirements as logical and verifiable conditions in smart contracts requires exactness and precision regarding time, place, value and manner of shipment while drafting the LC.

---

[150] Allen Chan, Paul Pacholski, Ah Hock Teh, and Kim Kiow Tan, "Use blockchain to manage legal documents stored in an enterprise content repository. How to implement a Letter of Credit solution", Published on March 07, 2018, https://www.ibm.com/developerworks/cloud/library/cl-use-blockchain-bpm-manage-legal-documents-letter-of-credit/index.html (as of February 2020).

[151] Allen Chan, Paul Pacholski, Ah Hock Teh, and Kim Kiow Tan, "Use blockchain to manage legal documents stored in an enterprise content repository. How to implement a Letter of Credit solution", Published on March 07, 2018, https://www.ibm.com/developerworks/cloud/library/cl-use-blockchain-bpm-manage-legal-documents-letter-of-credit/index.html (as of February 2020).

- Through smart contracts, each condition can be formalized and evaluated based on the documents submitted by the exporter, effectively removing ambiguities and, consequently, the need for discretion by the issuing bank.
- All trading and facilitating parties have visibility into the LC issuance and development process on Blockchain (clear oversight into the status of the pending actions), thus easing the identification of possible discrepancies and errors, and in all cases taking required actions, including digital authorizations.
- A digitized workflow eliminates the need of physical presentation of documents and reduces LC amendment costs and time.
- Payments:

    a. early and quick resolution of issues regarding identification and amendment prevent or reduce possible disputes;

    b. payment automation by smart contracts reduces internal workflow time.

In short, the Blockchain multilateral process vs the LC bilateral one generates a pervasively better quality of trustworthy information and shorter action time in the financial, logistics and compliance aspects of trade. A BBVA pilot project[36] resulted in the reduction of a full LC process from between seven and ten days, to only two and a half hours.

10.6.9 Next Possible Evolution

LC process improvement (dealing with current information exchange, authorizations, payment issues) leads to more efficient trade finance payment methods that are reliable and profitable for all trading parties, and also increases risk mitigation in international trade. In essence, Blockchain technology reduces process inefficiencies by digitizing the documentary evaluation of LCs in the short term. In the long term, to the extent that Blockchain-based processes become widespread and result in a decline in the need for document-based evaluation and financing, LC evaluation and financing could be based on asset movement and other contractual milestones

10.7 Financial supply chain

In this era of just-in-time global supply-chain operations with shorter times-to-market, many supply-chain actors are under increasing pressure to create higher levels of efficiency; and these actors are often based in different countries with different currencies and legislation. This is because competition is increasing significantly and so corporate departments are always expected to do more with less: fewer resources, reduced budgets, etc.

In addition, accounts-receivable managers have to ensure that credit risk is at the lowest possible level and corporate treasurers need to improve efficiency through the automation of cash management, accounting and reconciliation processes.

Traditional financial supply-chain structures rely on traditional payment tools, guarantees, insurance, letters of credit, etc. In this context, Blockchain can break these traditions through an innovative digital technology that grants transparency, security and traceability to the whole supply chain, especially when quality and digital identities play an important role in a process.

According to experience and requirements therefore, two important examples of financial supply-chain processes to examine are:

A. Agricultural goods production, quality control, tracking, delivery, payment

B. Suppliers' credit status cluster management

For process A, monitoring of the supply chain is a key success factor because it creates some level of mutual trustworthiness between the participants in the supply-chain. For example, this can be in terms of recognized quality of the raw materials on one side and creditworthiness on the other side.

Without Blockchain the players involved in agricultural supply chains need many confirmations such as proof of payment, advance payment, bank guarantees, quality controls, and many other documents. Blockchain enables all these checks to be better integrated into an easy process.

Often the farmer in the supply-chain is a small or medium-sized company for which the collection of invoiced amounts is crucial and insolvency unsustainable. For this reason, the farmer often delivers the wares only after having collected the money. This can result in complications such as the:

- Customer having to pay in advance and facing the administrative complexity coming from advance-payment management,
- Supplier having to find a way to get information about the collection of the goods in real time, because this ensures the invoice collection,
- Invoice following sometime after the delivery, obliging the customer's administrative department to keep the advance (payment) open until the booking of the invoice, or
- Customer's administrative department having to immediately process the payment once the wares are delivered to them, and after a quality check. Given that many farmers can deliver in a day, this can result in the administrative department having to spend lot of time on payment processing on a daily basis.

The shared and known reputations of participants inside the group, and supply-chain information registered on the Blockchain, can help ensure that the quality of products is in line with the customer requests. For example, if the production process is monitored from the beginning and results of the monitoring are made known to all participants via a Blockchain, then additional quality control actions are not necessary prior to payment. On the other hand, farmers can be reassured that the customer will pay based upon their history of on-time payments in previous transactions. This can, in turn, eliminate the need for advance payment. The two main advantages are thus an easier quality control process and an improved collection process.

In **process B**, suppliers' credit status cluster management, a corporation allows a cluster of selected suppliers to supply transactions, and benefit from their corporate credit status with a specific (group of) bank(s).

In general, the main steps could be:

a) Proposal of prospective supplier cluster, meaning:
    - Identification of external criteria (geographic area, supply scope of concerned corporate branch/factory)
    - Preliminary list of suppliers according to external / supply history information

b) Agreement with the interested bank(s) on the granting of a corporate credit status to suppliers (economic conditions, impact on corporate credit levels, suppliers' assessment process, …)

c) Assessment and inclusion of individual suppliers

- Corporate interaction
- Banks' interactions

d) Release of credit status allowance terms & conditions to each supplier and drawing-up of an agreement

e) Codification of the terms and conditions into a smart contract

f) Automatic allocation and reimbursement of credits based on the registration of reliable information on the Blockchain system, by the corporation; for example, of purchase orders and product deliveries

g) Monitoring, via the smart contract, of supply operations as regards compliance to cluster terms and conditions

10.8 Nostro account management – improving cross-border money flows

This section outlines the main elements of an application of Blockchain technology for bank to bank Nostro accounts reconciliation which could reduce the costs for cross-border money transfers and currency conversions. (This information has been largely drawn from SWIFT's Final Report dated 8 March 2018 and titled; Global Payments Innovation (GPI) real-time Nostro Proof of Concept: "Can Blockchain pave the way for real-time Nostro reconciliation and liquidity optimisation?".[152])

10.8.1 What is a Nostro Account?

For those who are not familiar with the finance industry, in order to understand this section, it is important to first understand what a Nostro account is and how they are used. The following explanation comes from Investopedia.[140]

> "*A nostro account refers to an account that a bank holds in a foreign currency in another bank. Nostros, a term derived from the Latin word for "ours," are frequently used to facilitate foreign exchange and trade transactions. The opposite term "vostro accounts," derived from the Latin word for "yours," is how a bank refers to the accounts that other banks have on its books in its home currency….[Therefore,] A nostro account and a vostro account actually refer to the same entity but from a different perspective. For example, Bank X has an account with Bank Y in Bank Y's home currency. To Bank X, that is a nostro, meaning "our account on your books," while to Bank Y, it is a vostro, meaning "your account on our books." These accounts are used to facilitate international transactions and to settle transactions that hedge exchange rate risk….Most large commercial banks worldwide hold nostro accounts in every country with a convertible currency. Major examples of convertible currencies are the U.S. dollar, Canadian dollar, British pound, the euro and the Japanese yen*."

[152] "Final Report. gpi real-time Nostro Proof of Concept. Can blockchain pave the way for real-time Nostro reconciliation and liquidity optimisation?", SWIFT, February 2018, https://www.swift.com/news-events/news/swift-completes-landmark-dlt-proof-of-concept (as of February 2020).

10.8.2 Basic business situation

A key priority for banks is the improvement of operational efficiency together with the reduction of transaction costs related to international payments. According to one Industry Report,[153] "on average, 34 percent of the cost of an international payment is related to Nostro trapped liquidity, caused by the absence of real-time data to optimise intraday liquidity management … while 9 percent of the cost is linked to investigations or exceptions mainly driven by a lack of standardisation in the end-to-end payment's process"[31].

The key actions to improve visibility and timeliness, therefore, are "monitoring intraday liquidity usage by means of real-time confirmation of each entry on Nostro accounts, and …improving… intraday forecasting by systematic early identification of incoming movements."[154]

10.8.3 Issues and action areas

As highlighted by the 2016 Sibos[155] Survey, the main issues preventing the implementation of actions for improving operational efficiency[156] include important data gaps which result in the following challenges[157] :

- Too few transactions reported on a real- time basis
- Lack of timeliness of the reporting
- Lack of granularity in the information provided including the required time stamps, and
- Limited business practice for the usage of credit notifications in support of intraday liquidity.

The underlying reasons are related to:[158]

- The lack of data centralisation and integration of Nostro accounts management across e.g. different legal entities of a Group, and/or "treasury and reconciliation systems … across regions and currencies;
- Exceptions and investigations, due to the above, lead to increasing transaction costs, including delays in reconciliation, non-optimized funding and manual processing.

---

[153]https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/A%20mixed%202015%20for%20the%20global%20payments%20industry/Global-Payments-2016.ashx. (as of February 2020).

[154]https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/A%20mixed%202015%20for%20the%20global%20payments%20industry/Global-Payments-2016.ashx. (as of February 2020).

[155] Sibos is the annual conference, exhibition and networking event organized by SWIFT for the financial industry

[156]https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/A%20mixed%202015%20for%20the%20global%20payments%20industry/Global-Payments-2016.ashx. (as of February 2020).

[157]https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/A%20mixed%202015%20for%20the%20global%20payments%20industry/Global-Payments-2016.ashx. (as of February 2020).

[158]https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/A%20mixed%202015%20for%20the%20global%20payments%20industry/Global-Payments-2016.ashx. (as of February 2020).

10.8.4 Objectives and scope for the proof of concept

The SWIFT proof of concept, while introducing a real-time Blockchain solution, aims to verify the possible achievement of business objectives, as well as a technical objective which is to assess the suitability of Blockchain and specific implementation modes.

10.8.5 Business objectives

The aim of the Proof of Concept (PoC) is to demonstrate whether a real-time Blockchain solution could help resolve the identified issues which include:

- Less than optimal funding positions across Nostro accounts due to a lack of real-time visibility of the account's entries, and monitoring of the related intraday expected and available balances;
- Operational savings through increased efficiency of Nostro reconciliation.[159]

Such objectives imply:

- End-to-End Nostro account entries workflow

The following summarises the results and findings of these various activities.

Conclusions

1. Assessed adequacy of the DLT [Blockchain] based Nostro solution as defined by the functional requirements.
2. Value of DLT solution will depend on bank's liquidity management capabilities, level of automation and centralisation.
3. A one size fits all DLT solution will not work.
4. New hybrid DLT architectures bring significant progress but it is still early days.

10.9 Insurance processes

An early-adopter of Blockchain has been insurance-service providers. Blockchain technology is particularly suited to the insurance industry as distributed ledgers can speed the issuance of complex international commercial policies. Historically, these have required the transfer of multiple paper agreements with complex verifications across borders, all of which has been manual and resource intensive.

The use of Blockchain technology can address issues in the insurance environment linked to having a huge network of suppliers and providers, which all have complex relationships and authorisation steps to follow, and the need for streamlining processes from beginning to end. In addition, it creates a powerful and flourishing (particularly in the supply-chain space) horizontal industry integration model where insurance can then span multiple industries. Furthermore, Blockchain technology enhances collaboration and provides end-to-end tracking which creates transparency and has the potential to open up new revenue streams and create more efficient, automated processes. It is clear that Blockchain technology has emerged as a way to bring about a transformation in the insurance sector including in client onboarding, underwriting, and claims processing.

[159]https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/A%20mixed%202015%20for%20the%20global%20payments%20industry/Global-Payments-2016.ashx. (as of February 2020).

10.9.1 Client onboarding

To satisfy compliance requirements such as know your customer (KYC), insurance providers must collect, validate and verify key documents to prove customer characteristics such as name, address, birth, health and economic status. Various third parties and internal departments review this data to complete their due diligence processes, making delays common. In addition, companies spend vast resources fixing errors that occur when records are being reconciled with KYC proofs.

A Blockchain network can facilitate the secure sharing of information across an organization as well as appropriate sharing with third parties. Furthermore, if customer identities[160] are already secured with Blockchain, insurers can efficiently verify their eligibility without needing to go to multiple sources.

10.9.2 Underwriting

Throughout the underwriting process, insurers evaluate the risk of furnishing a client with a policy in order to determine how much coverage the client should receive, and how much they should pay for it. Although insurance poses risks, insurance companies rarely involve themselves without thoroughly looking at the data and making sure the odds are favourable. In some cases, the period required for weighing the risks versus the rewards can range from months to a year for larger corporate policies.

On Blockchains, external data can be included to decrease liability risks and provide semi-automatic pricing. This can help to automate and shorten the underwriting process, reducing the cost of operations. Blockchains also bring transparency and improve trustworthiness in the underwriting process by enabling shared visibility in complex multinational programmes. For example, last year the first multinational insurance policy to use Blockchain and smart contracts in order to allow visibility into underwriting coverage and premiums at the local and master level was pilot tested.[161]

10.9.3 Claims processing

For a policy holder, making an insurance claim can be a long and confusing process. This is because, in most cases, the process includes waiting for insurers and reinsurers to locate and verify contracts, as well as to track payment records and accounting ledgers. This process can be time consuming and even more so if extra time is needed to adhere to tighter regulations for combating fraudulent claims.

At this point of the discussion, another question arises; what if Blockchain could be used to get information about insured goods and events? Everledger[162] which is an example of such an initiative, is making this possible by putting diamonds on a Blockchain network. Each diamond's characteristics are registered onto the Blockchain and every time there is a transfer a record is created, and this chain of linked records allows the diamond to be traced back to its origin. *Provenance*, or knowing where something came from, can be very helpful in discerning counterfeit items. With less risk of fraud, claims can be handled in a timelier manner.

[160] https://www.ibm.com/blockchain/solutions/identity (as of February 2020).
[161] https://www-03.ibm.com/press/us/en/pressrelease/52607.wss (as of February 2020).
[162] https://www.everledger.io (as of February 2020).

Another example in insurance is a Blockchain proof-of-concept (PoC) [163]where a multinational policy which was controlled by a master policy written in the UK together with three local policies in the US, Singapore and Kenya, was converted into a "smart contract" that provides a shared view of policy data and documentation in real-time. The PoC also gives visibility into coverage and premium payments at the local and master level, as well as creating automated notifications to network participants following payment events. The pilot also demonstrates the ability to include third parties in the network, such as brokers, auditors and other stakeholders. For all stakeholders, the PoC provides, based on what information they are allowed to have, a customized view of policy and payment data and documentation.

10.10 Notarization services

Notarization (also known as timestamping) services are a powerful non-monetary Blockchain application, consisting of the trustworthy timestamping of documents or the provision of verification fingerprints (also called anchoring) for arbitrarily large data sets.

A generic data file can be hashed to produce a short unique identifier that is equivalent to its digital fingerprint. The immutability of this *hashed commitment on the Blockchain* provides the data file owner with a robust means of non-reputable timestamping, in other words the ability to exhibit a file later and prove, without a doubt, that its contents have not changed. This is done by comparing the hash of the exhibited file to the hash that has been notarized on the Blockchain – if they are the same then nothing has changed. This generic process is already available as a service[164] in order to achieve third-party auditable verification.

One application involves broker-dealers using this notarization process to satisfy regulatory requirements for storing specified records exclusively in non-rewriteable and non-erasable electronic storage media. Write Once Read Many (WORM) optical media has been used so far, but it is quite impractical, especially for large data sets. Instead, compliance could be easily achieved by anchoring rewritable data sources to the Blockchain thus providing accurate, secure and tamper-evident timestamping.[165]

Moreover, Blockchain timestamping can reinforce digital signatures and traditional timestamping. Currently, if a private key for electronic signing is compromised, issuing a private-key revocation certificate does not really help. This is because digital signatures are not timestamped, making it impossible to discriminate between documents signed before or after the compromising incident and the issuance of the revocation certificate. To alleviate this problem, digital signatures are often reinforced using timestamping from a certification authority. Unfortunately, this timestamping is also achieved using a certification authority digital signature. As a result, should the private-signing key of the certification authority be compromised, all its timestamps would be invalid. However, this mess can be gracefully cleaned and solved by timestamping the signed document on a Blockchain. There is no way to achieve Blockchain backdating, therefore, making the issuance of the revocation certificate for a compromised private key completely effective.

These unsophisticated applications are very powerful in their implications.

[163] http://www-03.ibm.com/press/us/en/pressrelease/52607.wss (as of February 2020).
[164] https://opentimestamps.org/ (as of February 2020).
[165] "The Distributed Ledger Technology Applied to Securities Markets", Response to ESMA/2016/773, by F. Ametrano, E. Barucci, D. Marazzina, and S. Zanero.
https://drive.google.com/open?id=0B8tGDTaBY4-NLWhqMXlIbTVfRVk (as of February 2020).

Notarization can be performed on multiple Blockchains at the same time. Public permissionless Blockchains are often better for this purpose than permissioned private ones because the process is reliable and independent from a central counterparty and the larger public Blockchains are also better protected against 51 percent hacking attacks.

10.11 Financial Regulatory reporting

Since the financial crisis in 2008, regulators across the globe have started to focus on increasing financial stability while protecting investors. Additionally, increased levels of political uncertainty have created an environment of financial unpredictability and volatility. For financial institutions, this has resulted in an increasing regulatory burden, more reporting requirements and more complex compliance measures all of which have impacted their internal operations and bottom line.

Regulatory reporting and managing regulatory risk are key concerns and pain points across the financial sector today. A report by Thomson Reuters in 2019 found that 71 percent of firms expected the focus on managing regulatory risk to increase over the coming year.[166] To date, the industry has struggled to find a sustainable solution to managing these tighter and continuously evolving regulatory requirements. Some avenues explored have included: the deployment of additional resources; offshoring functions and teams to lower-cost locations; re-engineering internal processes; and plugging new bespoke solutions into legacy system architecture. However, despite significant efforts, these attempted solutions have failed to effectively address regulatory reporting requirements and the challenges facing financial institutions remain.

10.11.1Current challenges in financial regulatory reporting

The main challenges in financial regulatory reporting include: [167]

- **Operational inefficiency**
  - Manual keying from core systems to reporting tools
  - Reliance on Microsoft Excel as a reporting tool
  - Quarterly and mon-end workload pressures
  - High-cost, low value and non-differentiating process
- **Data management**
  - Questionable data quality
  - Potential for data manipulations
  - Data errors due to manual keying
  - Time consuming extraction, reconciliation and report generating
- **Complexity and change**
  - Increasing requirement for granularity with look through and advanced analytics
  - Changing requirements of domestic and regional regulators
  - High cost of change with legacy applications
- **Cost challenges**
  - Increasing FTE cost burden on fund administrators due to new regulations
  - Large scale IT costs relating to improving existing legacy systems

[166] Thomson Reuters (2019), Cost of Compliance Survey 2019, https://blogs.thomsonreuters.com/answerson/cost-of-compliance-survey-2019/ (as of February 2020).
[167] https://files.irishfunds.ie/1488968245-Regulatory-Reporting-Blockchain-POC-Factsheet..pdf (as of February 2020).

- Adverse affect on the cost income ratio

Regulatory reporting is currently a manual, costly and cumbersome process for financial institutions. It is an activity which has no value added and uses resources, in some cases, even a dedicated regulatory department. In the industry currently, there is a one size fits all reporting process with a poor understanding around aspects of the reporting process such as validations and rules. This is due to basic spreadsheet software being the most advanced reporting tool in most cases. Data manipulation is another key concern due to the manual nature of traditional regulatory reporting processes. This impacts the overall quality of the data that is sent to the regulator. Finally, since the global financial crisis, regulators globally have enhanced their compliance standards and are more focused on rigid risk and reporting processes.

It has become apparent that existing systems in financial institutions are not equipped to meet these continuously evolving regulatory requirements. There is a clear gap in the industry where new, disruptive technologies could play a role in addressing the challenges. As a result, regulation is one of the services that have been the focus of tech treatment in recent times. RegTech solutions are helping firms to better understand and manage their risks. As highlighted in the Deloitte report, "*RegTech is the new FinTech"* [168], RegTech has the ability to enable reporting with increased agility, speed and integration while also providing analytic capabilities that allow organisations to derive real value from the information they hold. This report also details how RegTech provides senior executives with an opportunity to leverage existing systems and data to produce regulatory data and reporting in a cost-effective, flexible and timely manner without taking the risk of replacing / updating legacy systems. In the short term, RegTech will help firms to automate more mundane compliance tasks and reduce operational risks associated with meeting compliance and reporting obligations – and Blockchain is one of the technologies that RegTech can now add to its toolbox.

10.11.2 Blockchain opportunities in financial regulatory reporting

Blockchain technology could play a pivotal role in redesigning the manner in which reports are created, validated and shared with regulators. A report by the Institute of International Finance[169] has highlighted Blockchain technology as having the potential to create more efficient information sharing mechanisms in and between financial institutions. Blockchain's unique characteristics including its data integrity, reliability, data sharing and analytics could provide a solution to improving and enhancing the current process around regulatory reporting in the industry

The key characteristics of Blockchain technology are described in more detail in the first part of this White Paper and are summarized below from the perspective of what is most interesting to the financial sector.

- **Smart Contracts:** The ability to utilise smart contracts to check and validate reports against previous quarter data removes the risk of data errors created by manual input.
- **Data Integrity:** Data input into a Blockchain is extremely hard to alter which makes it a good basis for auditing.
- **Decentralisation:** As every node in the network holds a copy of the ledger, there is no central point of failure and the technology is better able to withstand malicious attacks

[168] Deloitte (2016), RegTech is the new FinTech
[169] Institute of International Finance (2016), RegTech in Financial Services: Technology solutions for compliance and reporting

and recover from disasters (earthquakes, floods, etc.). This additional security and reliability is a key benefit for regulatory reporting.

- **Analytics:** A Blockchain solution can be enhanced through the addition of an analytics layer which enables a financial institution to derive value from the data that is being reported. A dashboard could provide an overview of trends within and across different divisions of a company or, if all parties are using the same Blockchain, an industry.

The capabilities of Blockchain technology enable the data generated by reporting processes to be more available, transparent and secure. For financial institutions, a Blockchain solution can also enable an organisation to have a clear, proactive and transparent communication line with the regulator, which is currently not experienced by either party. For the regulator, the use of a Blockchain network would enable far easier access to reports and a far greater trustworthiness in the integrity of the data. It also could provide a platform for reporting across the industry which would streamline the reporting process and also provide greater insights into industry-wide data on a real-time basis.

The potential of Blockchain technology to provide a solution to regulatory reporting challenges has been recognised within and across the financial services sector. In early 2017, a Proof of Concept was developed with the Irish Funds body[170] where a Blockchain enabled platform was used for the reporting of Money Market Investment Funds (MMIF) which are submitted to the Irish Central Bank on a quarterly basis. In the UK, the Financial Conduct Authority (FCA) is exploring the potential of Blockchain technology for regulatory reporting and as a potential RegTech solution to a number of challenges.[171]

At the same time, despite the numerous apparent benefits of using Blockchain technology to solve the regulatory reporting burden, some roadblocks to adoption remain. Blockchain as a technology is still in its infancy. Ironically, even as the discussion on Blockchain as a solution for regulatory reporting takes place, the regulation of the technology itself is still under review. In addition, there are many outstanding considerations to be addressed including the lack of standards around Blockchain technology and its governance.

As part of the review of its regulatory sandbox the Financial Control Authority (FCA) in the UK released a discussion paper (DP 17/03) on Blockchain[172]. This paper highlights the need for each regulated entity to ensure that due diligence is carried out prior to the adoption of a Blockchain solution in order to mitigate any potential operational risks. In a regulatory reporting scenario, each regulated entity would still hold ultimate responsibility for the information being shared and stored on the platform. Concerns regarding data privacy, compliance with security would also need to be addressed before a regulator could sign off on the technology as a solution.

The use of Blockchain technology within RegTech is in its early stages, at the same time, regulators across the globe are starting to sit up and pay attention to the technology and its potential impact within the financial services sector.

---

[170] https://files.irishfunds.ie/1488968245-Regulatory-Reporting-Blockchain-POC-Factsheet..pdf (as of February 2020).
[171] https://www.fnlondon.com/articles/r3-and-fca-put-regulatory-reporting-on-the-blockchain-20170912 and https://www.ledgerinsights.com/fca-questions-csuite-blockchain-dlt-knowledge/ (as of February 2020).
[172] Financial Conduct Authority (2017), Distributed Ledger Technology: Feedback statement on Discussion Paper 17/03 and 17/04, See https://www.fca.org.uk/publication/discussion/dp17-03.pdf (as of February 2020) and https://www.fca.org.uk/publication/feedback/fs17-04.pdf (as of February 2020).

10.12 Tax compliance and payments

The fight against cross-border tax evasion is receiving increased attention among countries. This is made possible primarily through the exchange of information between tax administrations. The OECD publication, "Offshore Voluntary Disclosure - Comparative Analysis, Guidance and Policy Advice" of September 2010[173] highlights the effectiveness of voluntary compliance programmes adopted by several countries, which facilitate the collaboration of the taxable subjects involved, while at the same time achieving considerable savings, including in terms of litigation (including criminal litigation). In addition, the creation has begun recently of a new relationship between tax administrations around the world, with the involvement of large companies.

Cooperative compliance is a legal tool created to help align, on the basis of collaboration, the perspectives of, particularly, large business entities and Financial Administrations regarding the application of fiscal norms/regulations.

New, innovative technology developments, particularly in Blockchain technology, require legislators to rethink their approach to the formulation of rules and regulations. It is becoming important to focus on creating general rules, in coordination with other countries, that can be enforced but do not go so far as to define technical details, which would risk being already outdated when they come into force. A sample set of references on this issue and possible roles for Blockchain includes:

- EY, How Blockchain could transform the world of indirect tax[174]
- PwC, Blockchain for tax compliance[175]
- Deloitte, Blockchain technology, and its potential in taxes[176]
- European Parliament, Policy Department A at the request of the Committee on Financial Crimes, Tax Evasion and Tax Avoidance, Impact of Digitalisation on International Tax Matters - Challenges and Remedies[177]

The creation and use of internationally agreed guidelines are important for general legislation, particularly in the field of tax, given that markets are now global and not just national. Close attention also needs to be given as to how technological developments influence executive legislative policies which, in the context of fiscal policies, can be closely linked in an indissoluble manner (as in the case of the recent web tax in Italy), in order to avoid issues created by large differences in the past and present technological capabilities of enterprises and individuals.

Blockchain technology can generate and maintain a public register of transactions and of the consent of participants, thus allowing transactions to take place in security with multiple participants, and, if the case allows this, without intermediaries. For tax compliance, Blockchain technology could be used to manage a simple business process such as:

[173] http://www.oecd.org/tax/exchange-of-tax-information/46244704.pdf (as of February 2020).
[174] www.ey.com/en_gl/trust/how-Blockchain-could-transform-the-world-of-indirect-tax (as of February 2020)
[175] https://www.pwc.nl/en/topics/digital/digital-transformation/blockchain.html (as of February 2020)
[176] www2.deloitte.com/content/dam/Deloitte/pl/Documents/Reports/pl_Blockchain-technology-and-its-potential-in-taxes-2017-EN.PDF(as of February 2020)
[177] www.europarl.europa.eu/cmsdata/161104/ST%20Impact%20of%20Digitalisation%20publication.pdf (as of February 2020)

- Presentation of the invoice from the supplier to the customer, - the invoice can be in any format or standard (e.g. UN/EDIFACT INVOIC, UN/CEFACT CII XML, EN 16931: 2017, etc.);
- Provision for simple invoice clearance,
- If the case requires it, third party authorization and/or registration (e.g. a Tax Authority),
- Dispute handling for well-defined possible disputes and their resolution according to defined rules and payments handled as part of the automated process, and/or
- More initial focus on document information presentation (and accuracy)

One question, that is so far unresolved in many jurisdictions, is the taxation of capital gains realized or achievable by the sale of cryptocurrencies. This issue is representative of some of the tax problems linked to the use of Blockchain. In particular, a possible widespread growth of cryptocurrency use may place in front of all financial and tax operators the issue of how to tax capital gains realized (or achievable) from the sale of a cryptocurrency.

Considering today's laws and rules related to the taxation of capital gains realized by individuals, it is important to note that, as of mid-2018, in Italy, there was only one official reference issued by the Revenue Agency[178] This was in response to a request made by a company that wanted to start a Bitcoin currency exchange business.

In other words, currently, at least in Italy, there are no consolidated case laws nor are there general accepted practices on similar topics.

In conclusion, using Blockchain to facilitate the application of existing fiscal regulations concerning off-Blockchain transactions and the application of tax compliance to Blockchain transactions is possible and should be encouraged, provided that it is based on rules that ensure:

- National and cross-border interoperability (discussed earlier in this Whitepaper);
- Transparency;
- The availability and conservation of all the digital data concerned;
- Compliance with international standards;
- Compliance with civil and fiscal laws and rules;
- Correct management of data and processes in relation to their impact on safety, data protection, anti-money laundering and anti-crime regulations.

[178] Resolution no. 72 / E of September 2, 2016

11 Government Services

11.1 Government & Blockchain

Governments carry out two principal tasks for their citizens: Providing security and protection and providing goods and services that individuals cannot provide for themselves. Governments are nothing more, or less, than the collective action of the citizens they govern.

Blockchain technology is very well suited to address several challenges governments are facing in the current and future information society. Blockchains characteristics make it well suited for government applications because governments often have the role in society of providing trusted and authentic information. Until now, that has been delivered using traditional database technologies (or paper documents). Blockchain is not going to replace all of these, but it can provide a secure and decentralized layer of increased trustworthiness that facilitates the work of governments and improves the life of citizens.

Security, continuity and immutability are often important, whether it's for identity, land registry, company registries or other basic government information. Blockchain cannot replace all existing information systems in these areas but it can provide a higher level of authentication and control. From the viewpoints of both security and complexity, the current approach of multiple centralized information silos is not sustainable. In addition, not all information necessary for delivering government products and services is available within the bureaucracy of government. Much of it resides in a network of (semi) public and private organizations as well as with citizens themselves. Currently, most governments try to collect and copy this information/data, which is then prone to errors, results in unsustainable systems and, not infrequently, creates undesirable results. Blockchain can help governments better adapt to the realities of today´s data-filled world and improve their processes.

In a citizen-centric government there is a desire to give citizens maximum control over their own data, and the ability to control it in a granular way. This can include an identity that's not controlled by some central entity but is decentralized, and under the citizen's control (called a self-sovereign identity). Blockchain is a tool that governments could use to make self-sovereign identities a reality.

When considering possible applications, it is important to not look at Blockchain technology in isolation but rather in combination with developments in other fields such as big data, artificial intelligence, Internet of Things and cloud/edge computing. Also, one should keep in mind that it is still developing and is far from being mature. As a result, mistakes can be made, and there is still a great deal of uncertainty about which Blockchain technologies to use, even as this same technology advances. Still, governments need to start developing applications now, in order to learn and improve. The potential for addressing important government challenges is too great to let this opportunity pass.

11.2 Challenges that governments can address using Blockchain technology

At the peak of the hype-cycle it's sometimes hard to see the real potential of Blockchain technology. It's not the solution for everything, and Blockchain-based applications will not replace all current data applications and databases. Still, it can add an infrastructure layer with the potential to dramatically improve the functioning of governments around the world. In many cases, this infrastructure will not, itself, contain application data, instead it will authenticate data by providing reliable pointers to where the data can be found and/or hashes and timestamps to prove that data is unchanged.

The key areas, where there are government challenges that Blockchain could address, are described below.

11.3 Identity

Digital identity is one of the most important assets needed in order to participate in the digital economy. A Blockchain can offer an infrastructure for establishing permanent digital identities for both persons and legal entities (enterprises and organizations). These can be self-governed by the individual or company/entity owning the identity, without the need for control by one central authority. A so-called decentralized identifier (DID) which can be generated at will for various situations can offer privacy protection not possible with traditional solutions in this field. A public Blockchain with DID's makes it easy to digitally sign something and make it verifiable by everyone concerned. Common standards and some governance are necessary, and the technology needs to be developed further, but governments could play an active role in shaping this opportunity for better digital identities that both provide more privacy and are easier to verify. This would support delivering on policy goals like privacy protection and increased security for citizens.

The same infrastructure can be applied within the corporate environment, making it possible to clearly identify the mandate/authority of individuals within a company and the contexts in which the mandate exists. For example, it would allow a counterparty to identify that both Samuel and Elisabeth have the authority to sign contracts up to amount X for their company, but only Elisabeth can sign for larger amounts.

11.4 Safety, Environmental and Social Protection in a connected society

Soon, the majority of physical objects for which it is useful to collect data will be connected to the Internet in some way. This development is called the Internet of Things and it creates a big data challenge for society.

11.4.1 Identity and attributes of things

Just as for natural persons, there exists an identity challenge which regard to things or (virtual) entities. To ensure the accuracy and value of data it's important for every entity that is generating data to have a unique ID and attributes. Attributes can contain information themselves or point/direct to other authentic sources of data. An entity can be anything, a physical product, a contract, a certificate and so on. Once an entity has an identity, and information about it can be registered on a Blockchain, this unlocks many possibilities, in particular for the tracking and tracing of entities throughout a process or a life cycle. For example, if there is a problem with contaminated food, or a defective product, being able to quickly identify the farm and/or the factory where that food or product came from would significantly improve customer safety. Many consumers would also like to identify if the wood in their furniture was sustainably grown and be reassured that the cotton in their shirts was not harvested using slave labor. They may also want to be able to access relevant quality certificates, the inspections that have been done and so on. By providing a trustworthy immutable single point for recording (meta)information about individual products, Blockchain technology can identify the provenance of things and address these issues for both governments and citizens.

11.4.2 State of condition sensing and monitoring

This Internet of Things and its interface with Blockchain applications can provide additional opportunities for support services that protect citizens. For example, sensors attached to critical

infrastructure such as bridges, buses and commuter trains could register the need for maintenance and repairs on a Blockchain, which could then automatically request that this work be done (using smart contracts) – and also record, via sensor results, if a problem was fixed or not. This issue of how to identify and monitor things and their state (such as, "in good condition", or "in need of repair") is also relevant for food, pharmaceuticals, drones, autonomous cars, medical implants and many other devices whose origin, status and functioning impact the well-being and lives of citizens. The vast volumes of data and numbers of stakeholders linked to each product type, means that a decentralized approach is the most likely to succeed and Blockchain is the most suitable technology to provide trustworthiness in the underlying infrastructure.

11.5 Energy

Governments have a responsibility to ensure that citizens have the energy they need, at a price that they can afford and in a way that creates the least possible damage to the environment. In this context, the energy landscape is changing. In the future, large-scale power plants will be less important. New networks of smart and clean energy systems will appear, often using smart grids to maximize their impact. Smart grids allocate energy by matching energy sources with demand and keeping track of energy pricing and charges without human interference. Blockchain-based applications can track these transactions and charges at a much more granular level than existing systems. This will allow, for example, a micro-grid with 10 or 15 apartments or houses, which have solar panels installed, to allocate electricity among one another, based on demand, and to order additional electricity from a main grid when needed while keeping track of who owes who money based on their generation and use of electricity. Current, centralized systems could not handle the volume of transactions and the computing power required to do this on a large scale. The development of this new infrastructure requires efforts by both private and public parties. Governments need to be interested in this future energy infrastructure from the perspectives of continuity, taxation and energy policy. In the energy sector, Blockchain applications are also interesting because of their ability to support a system of carbon credits.

11.6 Managing Government Assets

Even though the total value of the Bitcoin cryptocurrency is limited in comparison with the financial world as a whole, its impact has been big. It was the first use of Blockchain as a technology and created the interest that we see today in this technology.

Using a Blockchain to provide a currency, token or other digital asset can also be a way for governments to support asset and financial management within the complex and multiple management structures that they must internally manage. Such applications can make the use of government funds programmable and traceable. Implementations can range from the use of internal government coins (used for accounting and corresponding to real financial assets) to the automatic execution of simple financial transactions if certain requirements are met. Expenditures when made using a Blockchain-based currency or asset are recorded in a way that creates immutable audit trails, thus increasing accountability in government offices and reducing the expenditures required for auditing.

As one example, the World Food Programme has run a pilot test using Blockchain technology for distributing benefits to refugees. One side benefit was the ability to report, almost immediately and at very little cost, to donors on exactly how their funds were spent and for what.

11.7 Authenticated and Reliable Registries of Key Assets

Reliable, shared basic registries for assets such as property, people, companies, cars, and income are crucial for government services and even more so for digital services. In an age of Big Data, reliable government means reliable government-wide information that is used for providing services to and making decisions about citizens and companies. This is important not only for high quality services but also for fraud detection.

Blockchain technology offers new possibilities for preventing the unnecessary copying (with concomitant opportunities for fraud) of data about key assets by providing a decentralized and secure infrastructure which stores the data itself (for non-personal data only) or provides pointers to authentic sources. Blockchains can also provide reliable logging of data about processes, changes and events that modify the status of a key asset (for example, ownership of land or an automobile).

11.8 Accountability, Audit & Control

Governments face a challenge in being accountable for the complex systems and structures that they finance and manage. There will always be a need to check whether a system is legal, compliant and working properly and these checks are performed by audits.

The use of Blockchain technology changes the perspective of what is examined in audits and has the potential to change how audit work is conducted.

Some of the questions that auditors face when looking at Blockchain applications are: How do you audit a decentralized ledger? How do you evaluate consensus algorithms? How can you assess the quality of a smart contract? Can the "right to be forgotten" be implemented? – And many of these questions need to be answered before a Blockchain application is launched, not after 6 months or a year of operations, thus modifying both the timing and perspective of audits.

On the other hand, Blockchain technology can drastically increase the effectiveness and efficiency of the audit process. Various Blockchains offer technical assurances for security, integrity and immutability which make many existing checks redundant. Also, if the auditor also has a node in the decentralized network, they always have a copy of all registered transactions and, thus, continuous auditing is much easier to implement.

Just as for natural persons, in a corporate or government-agency environment identity and authorizations are essential. Blockchain technology can provide assurance regarding the identity of a company or agency, and the authorization of its employees for all relevant transactions.

Finally, application logic (small programs), called smart contracts, can be added to Blockchain infrastructure, thus making automatic transactions and controls possible. In the future, even the practice of double accounting could become redundant as Blockchain infrastructure can provide verifiable and highly trustworthy transaction data for all parties involved through a single ledger.

11.9 Democracy & Voting

In a digital world, when compared to paper-based processes, governments want the same or better assurances for voting at all levels: local, regional and national. There is lot of worry about the security aspects of e-Voting. Regardless of whether voting in the future is a fully digital process or a mix of digital and physical components; in all scenarios, Blockchain technology can provide additional guarantees with regard to the authenticity, integrity and

security of voting. These range from implementing the electronic logging of votes generated by the traditional voting process to complete digital voting.

11.10 Healthcare

Many governments are struggling with digital medical records. Many public and private parties are involved. At the same time, security, integrity and privacy-protection are crucial aspects that need to be ensured. In this context, carefully designed Blockchain applications can be used to facilitate data sharing with proper authentication while maintaining confidentiality. More details about the use of Blockchain in this sector can be found in the healthcare chapter.

11.11 Fighting fraud & corruption

Because of all the characteristics mentioned earlier, Blockchain infrastructure can provide efficient ways to fight and prevent fraud. Both in developed and less-developed countries it could increase the reliability of information about ownership, identity, certificates, credit rating, funds provided and so on. Blockchain technology offers the possibility to make security, integrity checking and immutability an integral part of any solution/application that is developed. In most cases, with the use of open-source technology which can be audited by any party involved. Simple examples are checking the integrity and validity of contracts, ID-documents, insurance claims or any other transaction registered on a Blockchain network. Blockchain solutions can also contribute to the KYC (Know Your Customer) checks many financial companies have to implement.

11.12 The way forward

The descriptions given above of the various government challenges where Blockchain technology could help provide answers is far from complete. At the same time, it does provide an overview of the potential of this technology. Every government context where transparency, immutability, redundancy and security are important is a possible Blockchain use case. At the same time, governments should be careful not to apply Blockchain for the sake of the technology but only if it brings clear added value in comparison with other technology options.

The most efficient and effective way to learn about Blockchain technology and its possible uses is to start using it for a project or a prototype. Preferably not in a laboratory setting, but in a controlled live environment with real business processes. At its core, a Blockchain implementation should not be a technology project. Instead, ideally, it should be a project where government processes and government services are drastically improved through infrastructure which supports a highly reliable information network for governments, companies and individuals. Blockchain has the potential to make government less about government itself and more about society.

12 Healthcare

12.1 Introduction

Compared to the financial sector where innovative digital technologies including Blockchain and AI are reshaping the landscape, healthcare has been slower to adopt. At the same time, there is an urgent need for change. A rapidly growing and ageing population is putting pressure on the already strained global healthcare industry. Health systems around the world are facing many challenges, including, but not limited to, the overconsumption of acute-care services, poor integration of healthcare across social and health boundaries, inconsistent quality of services exacerbating existing health inequalities, workforce issues and spiraling health care costs putting pressure on economies, payers and consumers. Within this environment, there is significant opportunity for digital technologies to create real impact, releasing some of this strain. However, the cost of failure and the reward for success extends beyond material, or commercial gains because it influences lives and well-being. Therefore, in a traditionally risk-averse sector, the implementation of novel or innovative solutions in healthcare demands critical attention with strict adherence to clinical and regulatory guidelines where available.

One major trend in healthcare is the shift from reactive 'sick' care, towards a more proactive, preventative care focused system, in part due to the growing crisis of chronic disease. Statistics from the World Health Organization have shown the rise in obesity worldwide is unprecedented, having more than doubled since 1980; diabetes has also seen a global meteoric rise, with more than 500 million adults suffering from the condition in 2018, nearly quadrupling since 1980[179]. Unsurprisingly, the startling increase in such conditions produces a critical strain on healthcare services. Despite the introduction of Universal Health Coverage and national health systems in several countries, economies, payers and providers are still struggling with unsustainable levels of consumption and expenditure – leading to poorer patient outcomes. Innovative technologies, such as IoT, wearable devices and Blockchain, are ideally placed to transform the management of both preventable and chronic disease and represent a significant opportunity for digital disruption in healthcare.

Through a combination of Blockchain, IoT and wearable devices, data can flow across existing health and social care settings and be collected and analyzed on a level and scale that was never before achievable. In addition, the emergence of newer platforms using open APIs[180] to create links with between computer programs goes some way toward addressing the interoperability challenges faced by legacy systems. Together, these innovations can provide the inputs needed to catalyze machine learning and adaptive algorithms, thus allowing risk identification in populations, and the delivery of personalized, targeted interventions improving patient outcomes. Furthermore, since other stakeholders within healthcare benefit from these technologies; they can also facilitate greater system efficiencies in the transfer of goods, data and funds.

In particular, Blockchain technology possesses the ability to overcome existing major hurdles in traditional models of care, resulting in a more patient-driven approach. This is because Blockchain can be designed to provide data privacy (for example, through a range of techniques including zero-knowledge proofs which allow data inquiries to be answered without revealing

[179] https://www.who.int/news-room/fact-sheets/detail/diabetes (as of February 2020).

[180] API = Application Program Interface. An API is an intermediary piece of software that makes it possible for application programs to interact with each other and share data. Open APIs are shared freely and are published on the Internet.

private data, such as confirming that a patient lives in Spain without giving their address) and ownership, traceability and accountability of data, secure storage and integrity protection (through the immutability of records) as well as ease of data sharing.

In healthcare systems, Blockchain technology can provide trustworthiness and, separately, incentivize data sharing and/or better health behavior through the creation of digital assets (e.g. crypto tokens). More importantly, Blockchain can provide a bridge, integrating data from multiple sources such as medical devices, wearables and healthcare Internet-of-Things (IoT) devices. This healthcare and lifestyle data can be critical to informing not only the correct diagnosis, but also the appropriate patient-driven intervention.

This section seeks to empower readers with the knowledge of how the implementation of such technologies can impact current business and trade processes in healthcare. For simplicity, this information is presented in three sections looking at: the transfer of goods, the transfer of data and the transfer of funds in healthcare.

12.2 Transfer of goods

12.2.1 Preventing Sale of Counterfeit Medicine

Traceability in the drug supply chain is based on the concept of tracking and tracing every step from the creation of pharmaceutical products until they are finally delivered to customers. The aim is not only to make the whole system more efficient by reducing unnecessary frictions but also to prevent the counterfeiting of medicines. The first aim implies less administrative handling and lower costs using a system that is sufficiently trustworthy to all parties that participate in the current systems. The second aim means that traceability information will have to be available to the consumer as well. The impact of such traceability systems is widely recognized and, as one result, regulatory authorities around the world, including in the USA, EU and Taiwan, Province of China, have issued regulations to make sure that all of the logistical information concerning the drugs supplied to their citizens is recorded.

One specific example of legislative action is the United States' Drug Supply Chain Security Act (DCSA), enacted in 2013. This Act outlines steps to build an electronic system to identify and trace drugs that are distributed in the United States.[181] The system would also aim to improve the detection and removal of counterfeit drugs from supply chains in the country.

As a consequence of these regulatory actions, there is a requirement for systems that generate trustworthiness and transparency among manufacturers, suppliers, governments and consumers.

Tracking and tracing of healthcare products requires a highly complex system that needs to respect requirements in areas like interoperability, scalability, auditability and usability. Therefore, determining an appropriate architecture for such a system is a key step. A suitable system should be able to satisfy the following criteria:

- Resilient, a characteristic strongly supported by decentralization
- Able to avoid a single point of failure
- Interoperable, by design, with existing software based on secure Application Programming Interfaces (APIs)

[181]https://www.fda.gov/Drugs/DrugSafety/DrugIntegrityandSupplyChainSecurity/DrugSupplyChainSecurityAct/ (as of February 2020).

- Open and platform-based, where new features can be easily added to achieve both security and privacy while ensuring that sensitive information is only shared with the right parties
- Auditable, with regulatory compliance reporting capabilities
- User-friendly, providing consumer interfaces that allow quick and easy verification of purchased products

From the above, it is clear need that innovative Blockchain-based systems, together with other new technologies such as IoT, can meet these specification as well as creating a range of new supply chain functionalities. As the keeping track of every pill in a system, in a way that is visible to all involved, is similar to the way the Bitcoin Blockchain tracks the origin of every Bitcoin and its fragments that are scattered in many records over distributed nodes; it is not surprising that there have been a number of research ideas and proposals to adopt various kinds of Blockchains to combat drug counterfeiting.

Despite Blockchain technology's desirable properties, in order to make its adoption a success in preventing counterfeit medicines, one needs a strong policy framework to come from governments around the world, working together. To be able to do this for all medicines, will require the development of substantial data exchange systems spanning across many entities, in both the government and private sectors. In terms of regulations, it means a new set of rules (auditing and compliance) would be needed for operating and monitoring data interchanges at all levels. For all stakeholders, the most effective system would probably be an open framework that allows all participants to contribute to designing the system. It is also crucial that all parties involved agree upon the standards used by the system. As for the technology itself, given the features described above, Blockchain would be a strong candidate for tracing goods such as medicines. However, its maturity still needs to be proven in practice, especially with regard to scalability and performance when processing high transaction volumes.

The use of Blockchain to prevent the sale of counterfeit medicines is discussed in more detail in section 12.6.1.

12.2.2 Serialization

Multi-level packaging and the serialization of pharmaceutical goods require unique and unequivocal identification of each of the individual selling units in the distribution channel. This identification is currently handled via a unique serial number on the individual physical package. The purpose of using Blockchain is to not only physically, but also logically, distribute the data from this multi-level serialization identification throughout the supply chain. Access to this information in a timely fashion, and its immutability, will improve the accuracy and handling of goods, thus reducing the costs and risks associated with mishandling and misidentification.

For example: if a serialization program gave a vial a serial number of "12345," typically the next number would be "12346." This is sequential serialization. With this process, a person could easily make counterfeits and give serial numbers that appear real. However, with Blockchain serialization, the next number could potentially be, "45267" instead of "12346." The first two numbers are the end of the first serial number, the third number is the "content" of the block (created based upon agreed rules), and the last two numbers are determined by an algorithm that is based on the rest of the numbers in the block. The number after that would be "67390." Both of these numbers were generated using the same, very simple, one-step algorithm, and yet it is difficult to guess what the next number in the sequence would be. Because Blockchain requires a person to not only know every serial number in sequence, but

also the algorithm to determine the next set of numbers, it is nearly impossible to guess or create a valid serial number.

In addition, the development and use by Blockchains of standardized definitions of supply chain processes and standardized data, such as those developed by UN/CEFACT will enhance and bring additional opportunities to the industry

Eventually this association between supply chain transactions and products through the use of product identification and Blockchain technology will allow increased tracking beyond the supply chain, reaching out as far as patient consumption and remote patient monitoring (for given cases, where this can be traced electronically).

12.3 Transfer of data

Blockchain technology can provide a next generation solution for collaborative clinical decision making and data sharing in the following areas:

- Verifying the identity and authenticating all participants
- Storing and exchanging data securely
- Granting consistent, permissioned access to data sources
- Applying consistent data formats
- Allowing multi-channel communications

This well-defined and detailed use case has to yet be implemented on a national or international scale, but there are increasing examples of this technology use on a smaller scale.

12.3.1 DIM – Distributed Identity management

One new technology frontier is the migration to electronic identities for individuals as well as corporations through decentralized and distributed identity management (DIM) protocols (based on Blockchain technology) and the need for associated intuitive user interfaces that allow the easy management of those digital identities by their owners. Going beyond that, there is also a need, in many industries and particularly in healthcare, to be able to assign digital identities (DIDs) to products, services and devices using easy-to-manage systems that are not cost prohibitive or exclusive. The methods used for decentralized digital identity management need to be based on standards, emerging standards and/or be compatible with other identity standards. Ideally, individuals and entities should be able to maintain a single trustworthy and private DID for multiple purposes, not just for healthcare, which would accelerate adoption. It is important that DIDs have the capacity to be associated with credentials from trusted third parties (who maintain DIDs and have agreed to implement a rigorous identification framework). For example, a person's DID might have a medical diploma or certificate associated with it. In the case of devices, a DID needs to include details such as the device's origin, current custodian and custodianship history. In the case of corporations or service providers, important details such as location, government clearance/registration, etc. would be useful.

In healthcare there will be three ways to apply Distributed Identity Management according to the type of Blockchain network:

1. **Official with Public Access:** For official and formal identification managed by governments and institutions to uniquely identify individuals and corporations while giving these individuals and corporations control over who accesses their information.
2. **Permissioned:** Managed as an independent and private platform with network providers to enable security, access, traceability and participation.

3. **Hybrid:** Where private, permissioned networks reference or integrate information obtained from an official/public DID.

12.3.2 Custody and trading of personal health data

Patients generate an enormous amount of health-related information through their interactions with healthcare professionals and treatment cycles but whenever this data is shared or sold externally for research purposes, they do not receive any of the financial benefits. Blockchain technology can incentivize patients to share this data for a fee, opening up a new market space. Blockchain-based information management systems could enhance the exchange of and trade in health-related data between patients and institutions who seek data for research, the information coming directly from electronic-medical-record (EMR) platforms. Blockchain technology enables patients to hold their own data, thus bypassing issues created when data is fragmented between treatment centers. General Data Protection Regulation (GDPR) also provides an opportunity for Blockchain technology to come into its own, by creating a system where interaction with each piece of information can be tracked and recorded in order to ensure that the custodianship and processing of personally identifiable information can be controlled by the ultimate owners of this data, i.e. the patients.

12.3.3 Adverse Event reporting

Adverse events are untoward medical occurrences in a patient or clinical investigation subject who has been administered a pharmaceutical product or device, which does not necessarily have a causal relationship with their treatment under the clinical investigation. All genuine adverse events collected by a manufacturer must be reported to health authorities in a secure and immutable manner due to the clinical significance of the data. Blockchain technology provides opportunities to both reduce any data integrity issues in the transmission of such data and also opens up the prospects for multi-party data sharing involving multiple regulatory agencies.

12.3.4 Submission of minor changes to a New Drug Application (NDA)

In areas where regular and near-continuous additional submissions are made to regulators for existing drug approvals (Label changes and modifications are a commonly cited example) many regulators are looking to reduce the administrative burden associated with such submissions. Both the United States' Food & Drug Administration (FDA) and the European Medicines Agency (EMA) are currently investigating the possibility of using Blockchain technologies to assist in these areas.

12.3.5 Laboratory Data Integrity

Laboratory data integrity and the management of raw data has been a common issue for regulators in recent years with many observations and warning letters issued by all of the global regulators in this area. Blockchain's security by design principles can be used to reduce technical risk in this area to near zero by capturing all raw data at the source, thus locking in the original output data taken from lab instrumentation and removing any possibility of manipulation and alteration of the data. Regulators have expressed interest in such technology being explored by the industry to reduce this intrinsic risk.

12.3.6 Clinical Trials

Clinical trials conducted by the private sector (often pharma-related companies and private universities) are a multi-billion-dollar business. The global Contract Research Organizations (CROs) market alone saw a total revenue of 34.5 billion United States dollars generated by the top ten CROs in 2017. This market is growing at a strong rate due to the increased dependence of pharmaceutical, biopharmaceutical and medical device companies on outsourcing R&D activities, increased R&D expenditures, and an increasing number of clinical trials worldwide. The scientific credibility of findings from clinical trials are undermined by a range of problems including missing data, endpoint switching, data dredging, and selective publication; contributing to systematically distorted perceptions regarding the benefits and risks of treatments. Blockchain technology could cut costs, improve performance and increase trustworthiness among stakeholders (e.g. FDA, CROs, pharma, patients) leading to better cost-effectiveness and cost-efficiency.

Blockchain technology allows for a substantial level of historical tracking and data inviolability in the whole document flow in a clinical trial. Hence, it ensures traceability, prevents a posteriori reconstruction and allows for securely automating the clinical trial through Smart Contracts. According to Benchoufi and Ravaud[182], at the same time, the technology ensures fine-grained control of the data, its security and its shareable parameters, for a single patient or group of patients or clinical trial stakeholders.

The impact of Blockchain technologies on clinical trials is discussed in more detail in in section 12.6.2.

12.4 Transfer of funds

There are several areas where Blockchain technology could provide a beneficial platform for the transfer of funds within the healthcare sector. Even the provision of the simplest procedure or therapy within healthcare can initiate a cascade of events fraught with transactional inefficiencies. Taking advantage of the data sharing capabilities provided by distributed ledger technology, the ability to automate transactions using smart contracts and the option of using cryptocurrencies for payments has opened the door to a new paradigm in healthcare payment and multi-party financing mechanisms; making the transfer of funds cheaper, faster, reliable and increasingly dynamic. Examples of how the fundamental characteristics of Blockchain technology can be used to improve current processes for the transfer of funds are outlined below.

12.4.1 Claims processing and prior authorizations

The prior authorization and claims adjudication process currently undertaken by health insurance organizations to verify patient coverage is an area where Blockchain technology could provide great benefits.

Often in the healthcare industry, whether it is prior authorization, claims processing or reimbursement across the supply chain, delays in payment (often caused by a lack of confidence in the trustworthiness of data by the parties involved) can lead to delayed access to healthcare, mismanagement of budgets and a substantial administrative burden for all stakeholders.

[182] Benchoufi M and Ravaud P (2017). Blockchain technology for improving clinical research quality. Trials. Jul 19;18(1):335. doi: 10.1186/s13063-017-2035-z.

As an example, the tedious prior-authorization process of verification by the healthcare provider of coverage from the health insurer leaves both the patient and provider frustrated due to its complexity, poor communications and existence of multiple manual steps. The time needed for authorization varies and delays the provision of treatment, which is often critical in healthcare. Approximately 83,000 United States dollars per year, per medical practice, in the United States is spent on prior authorizations and related activities per annum[183]. In addition, again in the United States, around 20 percent of authorization requests are declined the first time they are submitted and 80 percent of those result in appeals, indicating high levels of inefficiency.[184,185]

The possibility of sharing essential patient information, in a trustworthy and confidential manner, among healthcare stakeholders (i.e. entitlement, eligibility and pre-authorization conditions) via the Blockchain network, these frictions in the systems (i.e. data collection, sharing and determination of eligibility) can be reduced to a great extent. The development of smart contracts where the transfer of digital assets/funds is automatically triggered based on pre-set conditions provides confidence in trustworthiness and the ability to save time, resource use and costs to create a faster and more cost-effective payment/reimbursement process. The results of such a process could also prevent delays in claim settlement and revenue cycles, accelerate patient access to therapy, and reduce the administrative burden for all stakeholders involved.

12.4.2 Value-based reimbursement

Blockchain facilitates the seamless implementation of value-based healthcare arrangements between all key stakeholders within the health economy. The tamper-proof nature of Blockchain creates a medical information infrastructure that is transparent and security conscious. As the shift to outcomes-based pricing[186] gathers steam on a global scale, decentralized data management systems allow all peers within a network to have the same understanding and trustworthiness of the outcomes' data that is used to justify payments; crucial for enforcing any outcomes-related payment mechanisms.

When health systems, payers and pharmaceutical companies seek to consider the implementation of value-based reimbursement or any other risk-sharing scheme, they are faced with a substantial administrative burden related to data collection, reconciliation and processing. The shift to personalized medicine also requires corresponding healthcare payment mechanisms to be flexible enough to function appropriately with minimal impact on resource use and without the above-mentioned administrative burdens. Smart contracts offer a unique solution for the trustworthy automation of even complex reimbursement agreements, offering a neutral enforcement of previously agreed upon terms. Using Blockchain technology pricing

[183] Bendix, J. (July 8, 2014). The Prior Authorization Predicament. Medical Economics.
[184] American Medical Association (June 2011). Standardization of prior authorization process for medical services white paper.
[185] Janasik M and Cathcart N, Blockchain and healthcare transactions: The secure, distributed four-party health services ledger. https://www.linkedin.com/pulse/blockchain-healthcare-enabling-data-portability-nicole-cathcart/ (as of February 2020).
[186] Outcomes-based healthcare focuses on reducing variation in how a wide variety of diseases and conditions are treated - a process that requires all clinicians to provide accurate diagnoses and treatment algorithms to improve patient outcomes. Outcomes-based healthcare also targets a more proactive approach to healthcare: creating a healthcare system that strives to *maintain* healthy populations and *prevent* illness. https://www.healthcatalyst.com/Outcomes-Based-Healthcare-Top-Success-Factors (as of February 2020).

agreements for insurance could be customized to match groups of patients who share identified health conditions, thus empowering key stakeholders to no longer worry about whether personalized pricing schemes would be so expensive to implement that any benefits from such schemes would be negated.

12.4.3 Auditability

Blockchain technology and the ability for stakeholders to have a shared, distributed ledger that is a single version of the truth and always in-sync can facilitate the recording of transactions and healthcare payments. This functionality allows all contracting parties to analyze and track the status of patients and of healthcare payments continuously, at the same time and throughout the patient's healthcare journey (from beginning to end). The characteristics of Blockchain technology enable all network participants to have the same payment information available, with confidence that this information is free from manipulation or malicious activity. This is imperative in an environment where business networks are made up of unlinked parties. The ability for key stakeholders within the reimbursement process to have an up-to-date understanding of the payment status of patients/contracting parties can also eliminate the risks of overcharging and consequent financial issues for those paying.

With the availability of Blockchain technology to ensure that reconciliation between the healthcare provided and payments made are correct, auditors could turn their attention to ensuring better quality data, as this is a key element in ensuring that Blockchain-based systems function as intended.

12.4.4 Cryptocurrency for healthcare payments

Up until now, the process of cross-border healthcare has been slow and tedious, involving various banks as intermediaries; with the use of Blockchain technology these payments can be sped up significantly. The cost incurred in the process would also be minimized due to the removal of middlemen. Digital payment mechanisms eliminate unnecessary paperwork and the immutability of the ledger would prevent existing issues in health insurance such as duplicate claims. Confidence in payments via Blockchain is on the rise, as suggested by the entrance of companies such as American express, Visa and MasterCard into the market for payment processing using Blockchain. Digital or Crypto currencies have also been proposed as a means of rewarding or incentivizing patients for the contribution of data to a healthcare network or as rewards for healthy behaviors.

Critically, the use of digital or crypto currencies for healthcare payments is very much in its infancy as concerns around the volatility of this asset class for the transfer of funds and the complexities in converting crypto currencies into to fiat currencies remains a concern.

12.5 Discussion

As illustrated by the examples above, there are several robust uses for Blockchain technology in healthcare, with widespread possible applications across payers, providers and manufacturers providing an opportunity to generate positive patient outcomes. However, although existing use-cases demonstrate the data-driven value Blockchain can add to healthcare, there remain technical, legal, business and reliance challenges delaying its mainstream adoption. For example, several start-ups and larger companies are creating new Blockchain-based solutions, however, in order to be implemented this technology would need to be incorporated almost seamlessly, as well as cost-effectively, with existing legacy systems. Legally, concerns related to the sensitivity of healthcare data transfer, payments and facilitation

processes will need to be resolved. Furthermore, implementation of Blockchain within healthcare systems requires co-operation from multiple stakeholders and the re-writing of operational processes.

At a time when healthcare systems are already resource-stricken and under strain, in the short-term more education is required to build the required confidence for mainstream adoption. That being said, organizations who take on the challenge, and embrace Blockchain in healthcare, will benefit from optimized business processes.

12.6 The Use of Blockchain Technology to Prevent Counterfeit Medicine and Support Clinical Trials

12.6.1 Preventing Counterfeit Medicine via Improved Pharmaceutical Supply Chain Management

One of the earliest vertical sectors determined to be a positive case for healthcare and Blockchain was the pharmaceutical supply chain. This is likely due, in part, to the magnitude of the problem to be solved (i.e. the 200 billion United States dollars global market for substandard and counterfeit medicines) and how well aligned Blockchain characteristics are with the legal and regulatory efforts intended to enhance supply chain management of pharmaceuticals. In the US, the regulatory framework is provided by the Drug Supply Chain Security Act (DSCSA), which was enacted by Congress and mandates an electronic and interoperable framework that allows for identification and tracing of medicines. It was enacted to help strengthen the security of the supply chain, remove dangerous drugs, and reduce Substandard and Falsified (SF) medicines (e.g., counterfeit, grey market). The implementation timeline for the DSCSA spans a ten year period from 2013 to 2023, at which point unit-level traceability will be required. The DSCSA is anchored by its key requirements (e.g., identification, verification, notification, etc.). So, the question then becomes: are the capabilities of Blockchain technology compatible with those requirements? As seen in Table below, Blockchain capabilities map extremely well to all DSCSA key requirements and allow for innovative means to satisfy them.

Key Requirement	Applicability	Compatible
Product identification	Unique product identifier can be required with contributed information validated as a side chain	**YES**
Product tracing	Allows manufacturers, distributors and dispensers to provide tracing information in shared ledger with automatic verification of important information	**YES**
Product verification	Creates system and open solution to verify product identifier and other contributed information	**YES**
Detection and response	Allows public and private actors to report and detect drugs suspected as counterfeit, unapproved, or dangerous	**YES**
Notification	Creates shared system to notify FDA and other stakeholders if an illegitimate drug is found	**YES**
Information requirement	Can create shared ledger of product and transaction information including verification of licensure information	**YES**

Reproduced with permission. Blockchain in Healthcare Today. doi: 10.30953/bhty.v1.20

Image 12.1 - Blockchain capabilities

The entry of SF medicines into the supply chain is not limited to the United States. Efforts in the European Union (EU) to combat these problems include the Falsified Medicines Directive and Council of Europe MEDICRIME Convention. Similarly, Blockchain would support

implementation of Health Canada's Food and Drugs Act (and amendments) as it applies to its four phases – particularly drug manufacturing, drug procurement and distribution and extending to frontline delivery. While countries in North America and the EU are battling these problems, developing countries are especially vulnerable to supply chain disruption as, often, very large percentages of their medications are imported – thus increasing the number of vectors of attack. Regardless of the local circumstances and the varying nature of the vulnerabilities by region, they are linked by the common fact that superior supply chain practices are possible when facilitated by Blockchain technology.

12.6.2 Improving Clinical Trials through better data management

Clinical Trials are becoming ever more complex, distributed and dynamic. The demand for precision medicine is bringing an unprecedented challenge for containing the costs of biomedical research and maintaining appropriate regulatory oversight.

CROs are playing an increasingly important role in clinical trials and are experts in providing the necessary back-office infrastructure, site management, and human resources to undertake trial activities. CROs are now becoming involved in all aspects of clinical trials from design, conduct, reporting, and final submissions to regulatory approval. Recent estimates project that up to 70 percent of all trials will be managed by CROs by 2020.[187] But despite this expenditure and expertise, the vast majority of trials still fail for avoidable reasons.

Blockchain Technologies present the opportunity to transform the management of clinical trials. A great part of the work undertaken by CROs could be substituted with a technological platform that is more transparent and accountable to all relevant parties including trial sponsors, regulatory agencies, trial sites (hospitals, clinics), and patients themselves. Such a platform could prove far more cost-effective at managing safe and effective clinical trials, improving data availability for review and meta-analysis, as well as preventing non-publication and a posteriori analysis.

Blockchain also holds promise for managing the next generation of clinical trials, which will be vastly more data-rich, individualized, and distributed over a global collection of sites to reach the right patient populations. One can imagine a future trial aided by wearable devices providing real-time data over high bandwidth networks to feed machine-learning (artificial intelligence) programs for live statistical analysis. But the management, monitoring, and auditing of such a trial is beyond the current capabilities of any traditional regulator or oversight committee. Hence, we need to think about how to update these structures so that the costs and times to market for life-saving medications can be significantly reduced. We also need to look beyond current management and reporting methods toward automated systems capable of continuous risk assessment and individualized monitoring and reporting.

All of these goals can be supported by an improved data architecture based upon the capabilities of Blockchain technology to maintain tamper-proof and time-sequenced datasets amassed from the contributions of disparate and unaligned parties engaged in a common enterprise. *Totum maior summa partum* – the whole is greater than the sum of its parts. In this case, improved global healthcare outcomes through better medicine is more than just the alignment of pharmaceutical companies, clinicians, regulators, hospitals, and patients.

[187] https://www.pharmavoice.com/article/clinical-services-0615/ (as of February 2020).

However, whether a Blockchain-based platform can truly replace CROs, and whether it can bring greater transparency and efficiency to clinical trials and the rest of biomedical research remains unclear. We need to see groups of trialists and Blockchain companies collaborating to take bold first steps, alongside a forward-thinking regulator.

Finally, while existing clinical trial management systems hold some promise for improving aspects of patient recruitment, data entry & collection, trial monitoring, logistics, remuneration and reporting, these systems are monolithic silos, often deployed as cloud-based Software as a Service (SaaS) without the redundancy, availability, and transparency guarantees provided by Blockchain technology. Blockchain presents us with the opportunity to realize the low-cost, highly personalized therapies of the future through secure, distributed, automated, clinical trials.

13 Tourism

13.1 Introduction: The tourism industry and rapid growth

The rapid growth of international tourism is quite remarkable. The 2018 Annual Report of the United Nations World Tourism Organization (UNWTO)[188] says that international tourist arrivals reached 1,326 million in 2017, the result of a continuous growth of around four percent a year during the past eight years and a seven percent increase over 2016. Tourism is one of the most rapidly growing business domains and will, inevitably, need to make use of the most advanced technologies available in order to accommodate the needs of this growing market.

13.2 The historical evolution of state-of-the-art Information Technologies in the tourism industry since the development of UN/EDIFACT

The tourism domain has played a leading role in the use of innovative Information Technologies (IT) and has been among the first users of state-of-the-art IT at each stage of their evolution.

13.3 From computer reservation systems to Global Distribution Systems

In the 1980s major airline companies competed with each other by expanding their proprietary Computer Reservation Systems (CRSs) through the absorption of other smaller CRSs. This evolution was based on using the power of large-scale computers. Around 1990, the major airline CRSs became Global Distribution Systems (GDSs). With the invention of personal computers (PCs) and the need to interconnect with other travel-product supplier systems (i.e., hotel chains, car rental companies, etc.), they realized the need to standardize their business processes by creating relevant messages and data interchanges.

Such standardization created opportunities for increased functionality and reduced IT development and maintenance costs. It was at this time when the tourism domain became active in the development of the United Nations Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT). The tourism domain involved a range of industry participants from airlines, railways, hotel chains, major car rental companies, ferries, travel agents, etc. Soon after they started these activities, they realized the need for creating Interactive EDI (Electronic Data Interchange) messages instead of the batch EDI messages which, at that time, formed the mainstream of UN/EDIFACT activities.

The tourism domain took the main role of developing the interactive syntax rules for UN/EDIFACT by providing user input for their development. Since then, many data interchange messages based on these rules have been developed and are still in use today by the major IT systems in the domain.

13.4 From the Internet to mobile communications

Around 1995 commercial Internet applications and sites started to come on-line. The United Nations, through its Centre for Trade Facilitation and Electronic Business (UN/CEFACT) supported this movement toward e-commerce with ebXML specifications to make use of XML (eXtensible Markup Language) technologies. Based on these specifications, an entire range of UN/CEFACT SLH (Small-scaled Lodging House) related information process projects were completed by 2012. The output of these projects is now in international SLH

[188] See https://www.e-unwto.org/doi/pdf/10.18111/9789284419876 (as of February 2020).

pilot use, waiting to be commercially used to trade globally traditional, cultural and local lodging houses.

With the growing use of smart phones, mobile technologies have become a prevailing factor in the domain since around 2010 and XML specifications, in general, have been widely implemented to make use of PCs and mobile technologies. The major tourism domain players, (especially intermediaries such as online travel agents) have been using proprietary specification-based XML messages. Their systems have been based around the use of central servers. The architecture of the use of central servers is quite similar to the ones used by GDSs, although they keep the UN/EDIFACT specifications as the basis of the message interchange. Currently, only a few online travel agents and GDSs have a dominant presence in the domain. Their businesses have been so successful globally that it seems to be quite difficult to start up a new business in the domain based on a similar business model.

13.5 And now, Blockchain and related new technologies

Blockchain and related new technologies are being implemented by a number of businesses throughout the world, providing users with the first introduction to these technologies' features and benefits. In the tourism domain, around the world, many proof-of-concept projects to test these technologies have also been initiated. Most of these technologies are in their initial development stage, but there are many parties who have a great interest in the potential benefits that these could provide to businesses and consumers. The UN/CEFACT Travel/Tourism domain is paying close attention to the progression of these technologies in order to identify an appropriate time to initiate standardization activities with domain knowledge experts and business players which will enable them to implement these technologies more effectively.

13.6 Issues in the tourism domain

Even though state-of-the-art technologies have been applied to domain businesses, there still remain some issues to be solved, some of which could be addressed by the use of Blockchain and related technologies. the following are some of the key issues.

13.6.1 High commission rates

Some intermediaries with centralized server systems have been dominating the global travel distribution markets, especially in airline and hotel sectors. They usually require high commission rates from their suppliers, who inevitably increase the costs for end-users in order to cover part of these expenses. As a result, many suppliers suffer from the burden of high costs.

13.6.2 Connecting local travel-product suppliers and customers

In every country, local areas provide a huge number of travel products such as: lodging houses, sightseeing facilities, experience activities, food and eating places, etc., some of which are world-class in quality. Customers for these products are not limited only to immediate, local areas but exist all over the world. Nonetheless, the worldwide or countrywide dominant distribution systems may find it difficult to effectively accommodate the vast number of local travel products and associated providers in their systems. Today, it is also recognized that tourists are more prone to visit rural areas in order to enjoy new experience programs in less crowded places. There is, therefore, a need for innovative methods to meet this demand.

13.6.3 Confidence in the existence of local suppliers and customers

Despite the common use of websites, both international and domestic customers could find difficulty in confirming the real existence of local travel product suppliers, in the same way that finding individual local attractions or services may be difficult. In addition, service providers need to have confidence in the identity of their guests. They also need to be informed of any changes in arrival times in an effective manner that allows them to manage their businesses.

13.6.4 Lack of ability to bear distribution costs

As the size of suppliers goes down, it becomes more and more difficult for suppliers to pay the cost of distribution through the central server systems used by the dominant online travel agents. If smaller businesses were able to make payments based on a sliding scale linked to their supply capacity, they could afford to use centralized distribution services.

13.6.5 Small payment amounts

In many cases, suppliers and buyers have to pay or receive small amounts of money which may be a percentage of a payment (such as commissions). International payments are costlier and take longer to settle in comparison with domestic payments. This is because international payments have to pass through the international banking system. Therefore, when suppliers of rural experience programs or activities, need to settle small commissions with many players and with international parties, the cost and time can either negatively affect them or even make some activities unprofitable.

13.6.6 Personal information

All travel service providers require at least some personal information about their customers. This information needs to be kept securely and be shared safely with other service providers as determined by the needs and conditions of relevant participants and by regulators (if applicable). There are also some cases where service providers (for example a centralized distribution platform) acquire initial customer information successfully but are unwilling to share data with other service providers who need to have access.

13.6.7 Digital divide

The IT capacity of small and medium-sized trade and tourism service providers (SMEs), especially in rural areas, is usually limited. When these SMEs start using IT technology, it is advisable to connect them with useful contacts or organizations who can assist them. This is because rural travel products usually need more detailed information than those in urban areas in order for customers to enjoy their visits. To support rural business players, web sites should be available to them without a large investment in infrastructure. And, at the same time, many rural and remote areas have remained without Internet connectivity for many years and suffer from a shortage of IT technical expertise.

13.6.8 The need for new customer rating systems

The review systems that are provided by some major information suppliers allow customers to review and give public ratings to their travel service providers. Sometimes, these ratings may reflect misunderstandings or even misconduct with purposeful attempts to influence ratings. However, if travel service providers could keep track of the behaviour and special

requests made by customers during their trips, they could obtain more appropriate information from customers on how to provide them with more satisfactory services. This new mechanism could protect travel service providers from fraud or security risks.

13.6.9 Opportunities presented by Blockchain

If distributed ledger technologies could solve some or all of the issues listed above, that would have a great, positive impact on the tourism business.

13.6.10 High commission rates

If suppliers could access end-users without any intermediaries, they could save a large amount of money. This could decrease the cost of distributing and promoting their travel products. Hence, end-users could get their travel products at a cheaper price. Distributed ledger technologies could be used to create direct sales between tourism suppliers and customers while providing both with the guarantees, previously provided by intermediaries, for payments and services provided.

13.6.11 Connecting local product suppliers and customers

The new distributed-ledger technologies could also be very effective in supporting decentralized solutions for the distribution of local travel products. In that regard, customers can emerge from any region of the world. There have already been initiatives, in the form of proof-of-concept implementations, which could show the ability to support this functionality. In the future, as these proofs of concept move into full implementation, the industry will be able to better judge their likelihood of success. Therefore, these new technologies could be expected to provide a wide range of local travel products and information to customers in the future.

13.6.12 Confidence in the existence of local suppliers and customers

Once the suppliers of travel products and information are registered in a distributed ledger environment, this information can be kept there as long as the suppliers are active. In addition, customer information can also remain stored once registered. Parties with authorization to access information regarding tourism business players or customers in a distributed-ledger environment, could also be given access to all registered and relevant information.

13.6.13 Lack of ability to bear distribution costs

As distributed-ledger technologies could allow direct communication between travel product suppliers and their users, this could, depending upon the design of the distributed-ledger networks, reduce the distribution cost to a minimum. Therefore, small-sized suppliers could be accommodated well in such networks.

13.6.14 Small payment amounts

In the tourism domain many players work harmoniously, with a small payment or commission paid or settled quickly and easily between them at the lowest possible cost. The challenge is when there is need for the payment to be settled internationally, with the associated, elevated fees. In this regard, the distributed-ledger technologies could provide solutions, either through the use of cryptocurrencies or tokens that can be exchanged at a fixed rate for fiat currencies (i.e. currencies issued by central banks such as United States dollars or euros).

13.6.15 Personal information

In some cases, tourism transactions also require the use of confidential information (such as personal information covered by privacy legislation or information related to payments). In applications that use distributed-ledger technologies, this information could be encrypted and saved securely either on a ledger or off-chain at an address stored on the ledger (see the section on "Accessing off-chain data" in section 2.3.3). Only authorized participants would then have the cryptographic keys needed for viewing the data. This could very well increase the privacy and security of data for all business participants and clients while also providing adequate access.

13.6.16 Digital divide

This issue is not directly related to distributed-ledger technologies but must be addressed if rural suppliers and customers are to have access to related services and benefits. In some cases, in countries where Internet use is restricted, distributed-ledger technologies could help revitalize travel businesses by offering an alternative. Furthermore, in rural areas everywhere, and especially in developing countries, travel businesses might also lack access to banking systems. They could thus use digital-ledger technologies in order to receive payments from customers or send payments to suppliers without needing to rely exclusively on the banking system.

13.6.17 The need for new customer rating systems

Distributed ledger technologies could allow the cost-effective tracking of historical data on business players and their customers. Thus, illegal or non-suitable behaviour by business players or their customers could also be tracked. Distributed ledger technologies can also be used to safeguard user privacy while simultaneously tracking customers' travel activities and preferences (i.e., to identify trends). In addition, these technologies can be used to track customer reviews of their suppliers or of travel products while paying attention to privacy concerns such as the identity of the customer.

13.7 Challenges to using distributed ledger technologies in tourism

The distributed ledger technologies discussed here arguably have significant merits which should allow them to function well in the future. At the same time, in order to reach this goal, there remain challenges to be addressed, including the following.

13.7.1 Reaching markets as a new tourism domain startup

Due to the extremely large and dominant travel product distributors now operating in the tourism domain, it might not be easy to start up new distribution businesses regardless of the technology used, including distributed ledger technologies. For example, obtaining the attention of a critical mass of potential users so that they try a new service even just once, is a daunting task in an industry where the majority of the public go to only four or five, or event fewer well known, existing online travel service providers.

At the same time, it is noticeable that initiatives have already been started in the domain. In addition, since a large number of travel products are not in the hands of the big players and remain in rural regions, there is the potential to create a niche for products to be handled by applications based on distributed ledger technologies.

13.7.2 Standardization needs

If a large number of separate distributed ledger networks emerge in order to meet the challenges described above, the issue of how they could be interconnected with each other and share information exists. There should be standardized processes and data for exchanging information across distributed-ledger networks and with other, data sources outside of distributed ledgers. This will make it possible to accommodate the need of suppliers and customers to work with a variety of distributed ledger networks and other, linked systems. UN/CEFACT standardization activities should support these interconnections and data exchanges across separate distributed ledger networks so that they function well in the future.

13.7.3 The role of intermediaries

There are a lot of intermediaries in the tourism domain who currently work on distributing travel products. They have been functioning well up to now. But if distributed ledger technologies function much better, suppliers and buyers of travel products could more directly deal with each other. If this happens, then intermediaries will need to re-consider their functions and services and find good solutions in the future. If not, their industry will be profoundly disrupted.

13.7.4 Protecting data securely

The private/secret data of individuals and companies must be kept secure and made available only to those who are allowed to do so by the data's owners. Encryption and decryption technologies support this objective but are not adequate by themselves because of their predictable obsolescence (for example, the secure encryption technologies of ten years ago are easily broken today). Security is essential and must take priority even over reducing the costs of gathering, using, storing and disposing of data. Therefore, as discussed in more detail in in section 4.5, privacy needs to be designed into systems and well-structured and secure infrastructure should be available at all times.

13.7.5 Development costs

There needs to be more public or private channels for raising the funds to start up a business using distributed ledger technologies. In some cases, providers have raised funds by creating cryptocurrencies. However, the technical knowledge and, above all, the increasingly complex legal and regulatory environment for such Initial Coin Offerings (ICOs), make this an unrealistic alternative for the majority of start-ups and SMEs. Therefore, technical, legal and financial assistance to those with good concepts for the use of distributed ledger technologies in the tourism domain would make a big difference.

13.7.6 Long-term certainty

Blockchain is a new technology, and different designs (i.e., protocols) and operating methodologies are constantly being developed. In an industry such as tourism it will be important for both service providers and customers to have a high degree of confidence in the technology and its long-term sustainability. This will require a careful examination of the incentives, financial and otherwise, for their long-term operation.

13.8 The future

The future of the tourism domain is rather difficult to predict. This is especially true when trying to predict who the winners or survivors among the emerging Blockchain systems will be. Businesses with a dominant edge today may, or may not, stay ahead without adapting to the changes that can be brought with distributed ledger technology. It is inevitable to expect the arrival of new players who adapt quickly to these technological changes. However, it is also uncertain whether such models will thrive. What can be said with certainty is that distributed ledger technologies provide opportunities for the development of new tourism services that do not currently exist, and there are an increasing number of initiatives appearing around the globe which look to solve some of the challenges described above. To know the future, we may need to wait and to continue observing the work of current dominant players as well as emerging initiatives. What is guaranteed is that change is forthcoming and that the future will be interesting.

13.9 Use Cases

In UN/CEFACT Blockchain repository, there are two travel/tourism use cases.

One of them is on Winding Tree and describes a public and permissionless Blockchain platform being developed for travel product suppliers and buyers by Winding Tree Stiftung of Switzerland. The second one describes a private Blockchain technology implementation being developed for the booking of travel products and payment by TUI,3 which is a German travel related company and one of the largest ones in the world.

14 Music and arts

14.1 Introduction

Artists, music producers and music fans are going to be amazed at how Blockchain will revolutionize the music and art industry. In the same way that other industries are leveraging Blockchain technologies to cut out inefficiencies and increase profits, the music industry also has a lot to gain from this technology which many believe will revolutionize the way people interact with one another and with organizations.

Many music lovers have hailed digitization as bringing democracy to the music industry. At the same time, many aspects of the global music industry, have, paradoxically, remained the same. In 2017, the music industry had revenues of over 17.3 billion Unites States dollars, 54 percent of which was digital income and reflecting an increase over 2016 of 8.1 percent. On the other hand, it is increasingly difficult for new artists to become known and it remains difficult, if not impossible, for the vast majority of artists to make a living from their work. In addition, those who discover and produce artists are also revenue challenged. Music piracy through illegally downloaded, copied and shared content eats into artists' and music labels' royalties and revenue. Digital streaming services pay artists as little as 0.0003 United States dollars per play (i.e. the artist receives 3 United States dollars after 1000 plays), and the lack of a robust rights management system also leads to a loss of revenue for artists. In addition, it can take up to two years for this revenue to reach the artist.

Another area of concern is unpaid royalties, the payment of which is often suspended at various stages for reasons that include missing information on rights ownership. There is also a lack of access to real-time digital sales data which, if available, could also be used to develop strategies for more effective marketing campaigns.

In addition, artists can also suffer from the lack of transparency in sales information; so even though Digital Service Providers (DSPs) report a huge volume of streaming transactions, artists may end up receiving payment for only twenty to forty percent of these transactions. This has led to several artists choosing to keep their music off such on-demand streaming services, causing notable gaps in the libraries of popular on-line services.

Blockchain can make a significant contribution to these areas by eliminating the need for an intermediary or third party to manage or control information. Blockchains' immutable, distributed and peer-to-peer architecture has immense potential for dealing with the present woes affecting the music industry and its artists.

In other words, Blockchain technology can potentially revolutionize the way music and art are distributed and consumed.

14.2 Some changes that Blockchain could initiate

A primary area in which Blockchain can bring positive change is in the creation of a digital rights database. The identification and assignment of digital rights is one of the key issues afflicting today's music industry.

Identifying the copyright of a song and defining how royalties should be split between songwriters, performers, publishers and producers is difficult, and especially so in the digital space. Often artists lose out on royalties due to the complicated copyright environment. Blockchain's immutable distributed ledger system could register agreed upon royalty allocations, in a manner that prevents them from being altered or claimed by others. In addition to the royalties themselves, secure, trustworthy files can be registered on a Blockchain containing related information such as the creators of the composition, lyrics,

linear notes, cover art, licensing, etc. and the allocation of royalty rights across these parties. Such a system would result in an enormous increase in transparency since this information would be available to all stakeholders.

Blockchain technology can also be leveraged to facilitate the automatic payment of royalties through smart contracts. British singer Imogen Heap's 2015 song, "Tiny Human" was released on a Blockchain powered site where users could purchase the song using the cryptocurrency Ether. The smart contract encoded in the Ethereum Blockchain by this application enabled the proceeds to directly reach the artists as well as the producers, writers and engineers. Such a system removes the need for intermediaries and provides a transparent ecosystem which ensures that all stakeholders receive their fair share of royalties.

In addition, the digitization of the music and media industry has left artists and producers to deal with the rampant problem of piracy, with users finding innovative ways to copy, record and distribute content, without compensating the copyright holders. The highly trustworthy security that Blockchain technology provides can be utilized to find solutions to prevent unauthorized distribution. There are various options for achieving this objective, one would be to create a unique record which results in a payment every time a song is played, thus preventing the content from being ripped off.

14.3 The time for disruption is now

Many agree with Nick Mason of Pink Floyd, when he says, "If Blockchain technology is going to be the future, we need to dig in and make it happen." The music industry, disrupted by digitization, is currently in a struggle due to age-old structures that are unable to cope with present day digital demands. Today, there is an opportunity for Blockchain technology to contribute towards the building of a healthy and robust ecosystem that can benefit both artists and producers

At the same time, however, there are challenges which still need to be met in order to realize Blockchain's potential in this sector.

14.3.1 Challenge 1: Access and distribution

Historically, ownership and access to content has always been an issue. Currently, artists and fans are linked only through major, centralized, music hubs that pass relatively few profits on to artists and charge fans very large fees for access. As a result, artists with smaller reputations suffer and are unable to make a living strictly from producing music. Even the established, big-name artists give up much of their profits to this centralized management. In addition, it is important to note that research shows that playlist makers[189] although driving much of the profit on digital music sites, are never compensated for their research and work.

When you buy a book, do you only buy the one physical copy, or do you own the content you have bought?

When you buy a track on iTunes, do you have the perpetual and immutable right to play that song, and can you copy it onto another media? This becomes more challenging when you consider a subscription service, where you pay for access to the platform but then cannot listen to the track anywhere except on that platform

One approach to this use and ownership issue, is being developed on an Ethereum-based Blockchain. The following is a brief, high-level description of how it works, as an example

[189] For example, see http://playlists.net/charts (as of February 2020).

of the possibilities available. This Blockchain platform creates a global ledger with all the music that has ever been uploaded onto it. Then, this layer of music is always accessible, regardless of location or time, and songs that have been purchased are always available to the user for listening or downloading. The platform is completely transparent with all transactions available for public viewing on the Ethereum Blockchain. Furthermore, 97 percent of the money received goes directly to the artists. Simply put, the system is designed to move funds to the artists who create the music, rather than to the centralized management organizations and systems that, today, act as expensive intermediaries. Playlist-makers are credited for increasing user traffic towards artists' works, as well as fans that actively promote their favourite artists, and they can also earn from their activities on this platform. Therefore, this concept drastically changes the business model of music for both fans and artists, allowing for greater access to more music and in ways that will eventually be simpler than the options offered today.

As more people use Blockchain and better user interfaces are developed, Blockchain-based music platforms could significantly contribute to the digital music industry. In particular, they could make it possible to simultaneously lower costs for users and increase income for artists by reducing the use of large-scale, costly digital music intermediaries through decentralized control and management that is in the hands of artists and producers.

14.3.2 Challenge 2: Commercial viability

One big challenge in distributing creative works is making them commercially viable.

This can be of particular concern to independent or small artists who do not have full control in managing their works. Case in point: it is estimated that major, centralized platforms acting as intermediaries, receive at least eighty percent of whatever listeners pay for an artist's music. The copyright holders (the singers and songwriters, in this case) only get slim pickings.

Big artists might have more clout, and their large sales volumes allow them to make a decent living, but losing a big part of their potential income to the platform can still hurt, considering the effort put into conceptualizing and executing their performance art. By contrast, independent artists often struggle in competition with everyone else in a big platform, unable to raise their profile high enough for listeners to even know that they exist.

By reducing the high cost of intermediaries in the music business, Blockchain technology can increase commercial viability for artists by connecting them directly with their fans and allowing them to earn significantly more revenue from listener payments. For example, in 2015, the artist Imogen Heap used a Blockchain platform to deliver tracks directly to fans, while accepting payments in cryptocurrency. This idea has been considered a proof of concept and is being pursued by a range of start-ups, including one launched by Ms. Heap which is looking at how to "shift from our current outdated music industry models, exploring new technological solutions to enliven and positively impact the music ecosystem."

In the digital visual arts, commercial viability can also be increased by creating digital scarcity. This refers to the use of Blockchain technology to limit the number of legal copies in existence on the digital market (i.e., like a limited-edition print), as well as tracking who owns these copies. This allows a user to verify that there are indeed only a certain number of limited-edition copies of an artwork, that the artwork purchased by the user belongs to them, and that it was created by a specific artist. Another way that decentralized digital art platforms can support the commercial viability of the arts industry, is by giving a portion of the proceeds to the artist whenever a limited-edition digital artwork is re-sold.

Such decentralized marketplaces where limited-edition digital artworks can be bought are already being developed.

Blockchain technology can also support the commercial viability of traditional fine arts by democratizing fine arts investment. As of 2018, one company allows you to own a fraction of a famous painting by artists which include Picasso, Warhol, Monet, and many others. Galleries, museums, and collectors are able to auction works from their collection in order to raise money for the purchase of future works, while keeping the art that has been sold in their collection. Although this is done through art-funds today, Blockchain will greatly reduce the costs by eliminating the middlemen. For example, a gallery could raise funds to purchase a three-million-dollar artwork using a three-year art-secured loan at a 13.5 percent annual interest, or it could raise funds on a Blockchain platform by auctioning some of their art using the model described above for a one-time fee that might be as low as 6 percent. This would represent a savings of over 400 thousand United States dollars for the gallery.

This is great for the gallery and also for investors. Because the cost of transactions goes down dramatically, artworks valued at tens of millions of United States dollars can be transformed into tiny digital units that can be easily bought and sold in real time: essentially a stock market for art.

14.3.3 Challenge 3: Managing assets and digital rights

The multi-billion-dollar movie industry is also ready for disruption by innovative technologies like Blockchain. This industry is currently highly centralized, with the power residing in a few companies In addition, movie production is often mired in legalese and fine print, which sometimes results in people not being adequately compensated for their work and/or not fully understanding the basis for their compensation.

There are three ways that Blockchain technology could support improving this situation.

- Lowering the barriers for obtaining production financing by raising funds through Blockchain platforms via the sale of tokens/coins and lowering distribution costs for the final product by using a Blockchain platform for distribution;
- Improving transparency by receiving and spending funds using cryptocurrency and smart contracts, thus providing a trustworthy, and public, Blockchain audit trail of how investors' funds were spent, and profits were distributed; and
- Improving the way digital rights are managed, through the use of smart contracts, in order to ensure that filmmakers, actors and other stakeholders, including those who have invested through token purchases are appropriately compensated.

14.3.4 Challenge 4: Enforcing intellectual property rights

Enforcing intellectual property rights (IPR) is an expensive and problematic issue for law enforcement and all holders of digital assets, including movie studios, music producers, distributors and artists. In this context there are the problems of piracy and forgery as well as the problem of content creators not receiving the royalty payments which should come to them.

This last issue is particularly complex in the case of movies which include a collection of copyrights and IPR, spanning across screenplays, derivative works from books, designs, technical works, licensing from other works, merchandise, actors' performances and so forth. In addition, there are many content creators who do not have enough clout (or enough

information) to enforce payment of the royalties they should receive because of their participation in the creation of a digital asset.

Blockchain distributed ledgers could help address these challenges by creating an immutable record of transactions involving any asset, idea or creative work, and also on the allocation of IPR across all parties involved. Thus, IPR could be tracked throughout the lifetime of an asset (or the copy of an asset), even when ownership is sold or otherwise transferred or assigned, including when these IPR assets are assigned to players in other industries, such as music, television, and the like.

There are a wide variety of Blockchain initiatives in the arts. Many of these, even if it is not always their principal focus, support the enforcement of IPR as well as the reduction or elimination of piracy, the sale of forgeries and illegal copying. Some additional initiatives which have these objectives as their main focus are described below.

One start-up has launched an application that aims to keep track of, and identify illegal copies of digital assets like movies, music, eBooks and other media through Blockchain technology and the use of an imperceptible watermarking technology. This watermark contains a Bitcoin reward that, if collected, notifies the holder of the IPR that their asset has been illegally copied.

Identifying the use of music is particularly complex because songs can be combined to form new compositions and mash-ups. To address this, one start-up has published a white paper on a solution based on digital watermarking for audio used together with a Blockchain. This solution addresses problems related to licensing and royalty tracking as well as the provision of reliable and accurate indicators (data) for Blockchains to act upon in support of IPR.

The problem with IPR enforcement is that it requires auditing, compliance checking and market surveillance. These requirements can be at least partially replaced by Blockchain's ability to guarantee the trustworthiness of a transaction, before it takes place, including confirmation that the ownership of artwork and the identity of the artist(s) are accurate and remain unaltered. One Blockchain initiative is focussing on this area by creating a convenient and effective way to trade art and track the history of artwork, thus minimizing counterfeit art, building trustworthiness within the art market, improving art trade services and increasing the economic and social benefits to the global art community.

There are also a wide range of initiatives in the area of Blockchain and photography, which incorporate most of the features discussed above (watermarking, tracking ownership, creating IPR supportive marketplaces, etc.).

14.4 Conclusion/Summary: Decentralization helps artists, producers and consumers

By now it should be clear that Blockchain technology has the potential to disrupt, in a positive way, the business of art, especially in those sectors where intermediaries play a prominent role and/or there is a lack of transparency.

At the same time, for this potential to be realized, platforms and implementations need to be developed with good user interfaces and a critical mass of users. This will take time, but the incentives are there to create new paradigms, based on Blockchain technology, that will result in a wider selection of choices in the arts for consumers as well as better livelihoods for artists.

What is UN/CEFACT?

UN/CEFACT, the United Nations Centre for Trade Facilitation and Electronic Business, supports activities dedicated to improving the ability of business, trade and administrative organizations, from developed, developing and transition economies, to **exchange products and relevant services effectively**. Its principal focus is on facilitating national and international transactions, through **the simplification and harmonization of processes, procedures and information flows**, and so contributing to the growth of global commerce.

UN/CEFACT has a global mandate. Participation in the UN/CEFACT Forum is open to all. There are some 300 experts representing every region in the world.

Within the framework of the United Nations Economic and Social Council, the United Nations Economic Commission for Europe (UNECE) serves as the focal point for **trade facilitation recommendations and electronic business standards**, covering both commercial and government business processes that can foster growth in international trade and related services. In this context UN/CEFACT was established, as a subsidiary, intergovernmental body of the UNECE.

Participation in the development of UN/CEFACT standards and recommendations is free of charge.
If you are interested in joining us,
you can register at
https://uncefact.unece.org/display/uncefactpublic/UNCEFACT+Expert+Registration
All resulting deliverables are available online free of charge at http://www.unece.org/cefact

For more information:
http://www.unece.org/cefact
See also: http://tfig.unece.org/

UNECE secretariat:
+41 22 917 1298
Lance Thompson, Secretary UN/CEFACT
lance.thompson@un.org
uncefact@un.org