United Nations ECE/TRADE/C/CEFACT/2019/9

Economic and Social Council

Distr.: General
17 January 2019

Original: English

Economic Commission for Europe

UNECE Executive Committee

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

Twenty-fifth session
Geneva, 8–9 April 2019
Item 1 of the i.an introduction to blockchain and trade facilitation
White Paper Overview of Blockchain for Trade

White Paper Overview of Blockchain for Trade

An Introduction to Blockchain Use in Trade Facilitation

Summary

Summary

Blockchain technology and Distributed Ledger Technology (DLT) in general have the potential of bringing great benefit to the trustworthiness of international commercial transactions. This White Paper presents the main aspects of blockchain and its functioning in an attempt to create a common understanding and basis for all future work on the topic within the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT). It concludes with guidance on when blockchain technology is appropriate for a transaction, and when it may not be.

Document ECE/TRADE/C/CEFACT/2019/9 is submitted by the UN/CEFACT Bureau to the twenty-fifth session of the Plenary for noting.

GE.19-00825(E)

* 1 9 0 0 8 2 5 *

I. An introduction to blockchain and trade facilitation

A. Introduction

1. 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 the second White Paper, which looks at how blockchain technology could be used to facilitate trade and related business processes.

2. As described further below, the term "blockchain" is being used throughout this document, although it is interchanged with the term Distributed Ledger Technology.

3. 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 access by all participants to all data in a blockchain; and
- The guaranteed implementation of smart contracts (programmes) that automatically execute once a set of agreed conditions are met.

4. 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 exporter to 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 such as invoices, shipping notices, bills of lading, certificates of origin and import/export declarations lodged with regulatory authorities.

5. This description highlights the interest of UN/CEFACT in blockchain technology. 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.

[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.

6. 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.

7. This layer of trust between economic operators determines which technologies are needed in order to achieve a desired level of reliability in electronic exchanges. Where high levels of trust exist between partners, authentication methods with lower levels of reliability are appropriate. Where such trust has not been established between trading partners, authentication with higher levels of 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.

8. 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.

9. Both DLT and blockchain have the potential to deliver significant improvements and automation in this layer of trust. For the rest of this paper we will refer only to blockchain with the understanding that it is a DLT.

10. 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 main areas of work. The impact on UN/CEFACT electronic business standards is examined in the first White Paper (ECE/TRADE/C/CEFACT/2019/8) and this White Paper looks at the impact of blockchain technology on trade facilitation. Many trade sectors have been studied because different sectors have different needs for trust and over time, have developed different mechanisms to address these needs. Therefore, it is not possible to examine blockchain use in all types of trade as though they were facing identical challenges and needs. A list of the sectors examined can be found below, and the results of the studies can be found in the document "Blockchain in Trade Facilitation: Sectoral Challenges and Examples" (ECE/TRADE/C/CEFACT/2019/INF.2). This paper is presented with the following horizontal sectors and vertical sectors:

- Horizontal Sectors
    - Blockchain security, legal and regulatory issues; and
    - Blockchain supporting the United Nations Sustainable Development Goals (SDGs).

- Vertical Sectors
    - Supply chains, traceability and blockchain;
    - Maritime transport and blockchain;
    - Non-Maritime transportation and blockchain;
    - Agricultural trade and blockchain;
    - Financial services and blockchain;
    - Government Services and blockchain;
    - Tourism and blockchain;
    - Music and arts and blockchain; and
    - Healthcare services and blockchain.

11. In addition, information on use cases and actual implementations have been collected using the template found in the Annex I.

B. Next steps

12. 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 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 promotion discourse of those promoting specific blockchain solutions.

13. To build upon this, the project team proposed the development of a forum for the discussion of blockchain use in the international supply chain and expanding it to include 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.

14. 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 by UN/CEFACT.

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

II. What is blockchain and what are the different types of blockchains?

A. History and background

15. 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.

16. 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.

17. 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.

18. 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).

19. 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.

20. 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].

B. Blockchain: how it works

21. 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). 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

[3] According to https://bitinfocharts.com/ (as of December 2018).

obligations (counterparty risk) and where third-party guarantors are reluctant to intervene and assume part of that risk.

22. 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.

23. First, some nomenclature:

- *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.
- *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.
- *Fiat or Fiat Currency:* These are currencies backed by a central bank such as dollars, euros, yen, etc.
- *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).
- *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.
- *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.
- *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.

1. Blockchain is a distributed ledger technology (DLT)

24. 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.

25. 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 they remain consistent, using a consensus algorithm of which there are different types.

26. 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. It writes transactions

27. 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.

3. These transactions are written to a cryptographically signed block

28. Blockchains implement two kinds of cryptographic technology: hash functions and 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.

29. 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.

4. Independent nodes must verify the cryptographically signed block

30. There are various consensus algorithms used by different blockchain systems. For example, Bitcoin, a public blockchain, uses Proof of Work algorithms which allow miners to recover the cost of computationally expensive work in exchange for transaction fees 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).

these fees also provide a way to initially put coins into circulation. Permissioned ledgers use a consortium of collectively trusted, but not necessarily individually trusted, 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% of the nodes. A more detailed description of public and permissioned blockchains can be found below.

31. 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% 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% 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 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.

32. 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.

33. 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.

34. 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.

5. The block is written to the ledger after it is verified

35. 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

[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.

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.

6. The new block is linked to previous blocks—creating immutability

36. Recall that a hash is a one-way function that produces a unique fingerprint of selected data. Also note that a hash function produces a fixed-size fingerprint regardless of the amount of data being hashed. 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.

37. 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.

38. 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.

39. 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".

C. Blockchain types

1. Public ledgers

40. 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 behaviour. Bitcoin, Ether and a range of other cryptocurrencies with market capitalizations going up to 59 billion USD[6] operate this way, allowing any transaction that is logically valid between any parties on the network, including anonymous and pseudonymous parties.

41. 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 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. 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 trusted regulator. Public blockchains operate with absolute trust in their algorithms and are designed to avoid any need to trust any counterparties. This is why public blockchains are sometimes referred to as being trustless.

[6] https://bitinfocharts.com/ at 14:00 on 8 December 2018.

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

2. Permissioned/Private ledgers

43. 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. 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, licences, 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.

44. 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.

45. 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 behaviour 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 behaviour but not commit antisocial behaviour themselves.

46. On permissioned ledgers, the level of security, and so the confidence 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 trusted participants are allowed to maintain nodes and participate in verification. At the same time, even trusted 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.

3. Interledger: implementing transactions across blockchains

47. 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).

48. Blockchains have the possibility to reference data outside of that blockchain. This includes data in other blockchains as well as from non-blockchain systems. There are two broad categories of external data references that can occur in a blockchain system: linked data and blockchain-spanning transactions.

49. 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 is a very complete library of trade-related semantics which can be used in this context.

50. Blockchain references which point to external data (also known as anchors) 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. 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.

51. In addition to linking data between two blockchain systems (cross-chain references) and pointing to data that may be used by a smart contract (for example a test certificate) in a more standard database, linked data can also be used to incorporate off-chain big data into a space-constrained blockchain system. Supplementary data can either be in public/open distributed data systems such as the InterPlanetary File System (IPFS)—an open, content-addressable memory that uses standard internet protocols—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. 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.

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

53. 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.

D. Smart contracts, oracles and using the Internet of Things with Blockchain

1. Smart contracts

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

55. 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.

56. 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.

57. 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 insurance.

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

2. Oracles

59. 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.

60. 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 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" come 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.

3. The Internet of Things and blockchain

61. The Internet of Things (IoT) refers to sensors and small computing devices or chips embedded in physical objects 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.

62. IoT devices can collect a wide variety of data. Examples of information related to trade and transport communicated by IoT devices include truck or 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.

63. IoT devices can be a useful way to capture data that is analysed 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 the IoT 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.

64. A classic example of the use of IoT data by a blockchain is insurance for temperature-sensitive goods (i.e. fruit that is supposed to be kept at between 4 and 15 degrees Celsius during shipment). During shipment an IoT device in a 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.

E. When to use Blockchains and when not to

65. 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
- More economical processes and/or implementation.

66. 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.

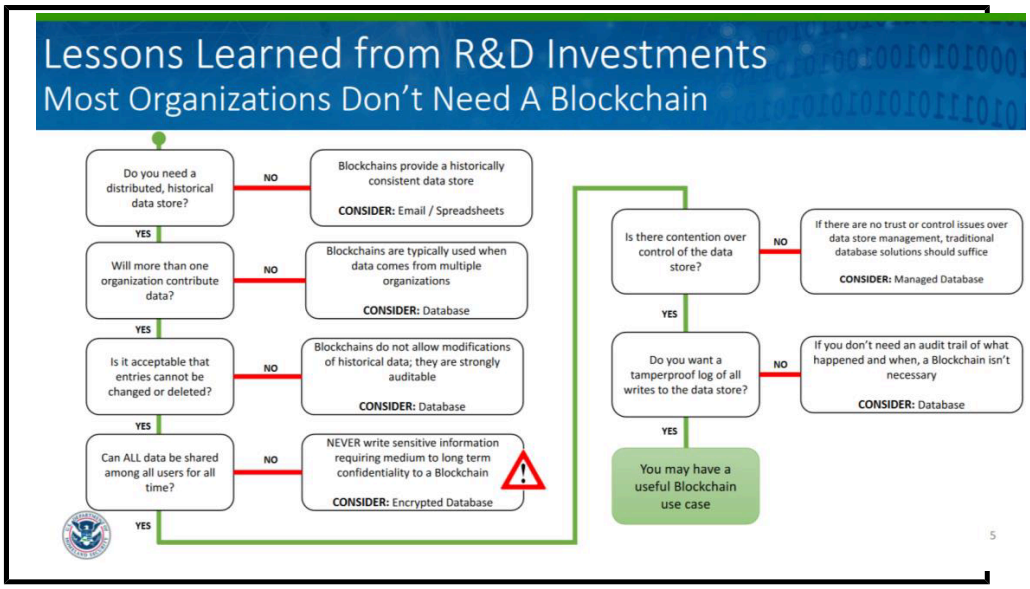

Figure 1 — When to use blockchain[7]

67. 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.

68. 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."[8]

69. 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 analysed. 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.

70. 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

[7] 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 (accessed 24 December 2018).

[8] See also 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

the 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.

71. 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.

72. 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.

73. 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.

74. 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.

75. 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.

Annex I

Sector	*Only enter if more detail is needed than what is given in the chapter title*
Short Description	1-2 sentences or less – 240 characters maximum
Proposing / Implementing /Testing Organization	If not relevant or available enter N.A.
Contact for further information	Name and email address (minimum), also could include • telephone number(s) and/or • mailing address and/or • website
Long description	1200 characters maximum
Description of potential business benefits from blockchain use	Should include only benefits derived from the special characteristics of blockchain, i.e. that could not be obtained using other technologies
Special concerns (legal, technical, etc.)	These could include aspects ranging from the need for minimum response times to the need for legal recognition, to the need for a minimum number of consortium members or network nodes
Blockchain being used/proposed	Bitcoin, Bitcoin Cash, Ethereum, Consortium, Private, etc.
Type of consensus algorithm used (if the blockchain is private or permissioned / consortium-based)	If not relevant or available enter N.A.
Rationale and trade-offs considered when selecting a blockchain	If not relevant or available enter N.A.
Any special hardware or “other” used (IoT, QR codes, etc.)	If not relevant or available enter N.A.
Any open-source software being used/proposed	If not relevant or available enter N.A.
Links to related information, including technical White Papers	If not relevant or available enter N.A.