Co-financed by the Connecting Europe Facility of the European Union

# Report on technologies and requirements

Blockchain & Distributed Ledger Observatory

# TABLE OF CONTENTS

# 1. Introduction

The SCALES Project aims at evolving the existing e-Invoicing system in an integrated platform in which e-Invoicing, eProcurement and other services used in the post-award phase are connected. The research conducted by the Blockchain & Distributed Ledger Observatory of the Politecnico di Milano wants to show benefits and technical advantages of a potential SDI architecture system evolution brought about by the Blockchain and Distributed Ledger technologies. Indeed, the application of these technologies could result in a shift from an architecture based on a centralized registry and repository to an architecture based on distributed registries and repositories. The research involves both national and international case histories of Blockchain and Distributed Ledger Technologies applications in several fields. The main objectives are to depict the as-is maturity framework of the usage of this technology and to highlight advantages and disadvantages of the choices in terms of possible platforms.

# 2. Blockchain & Distributed Ledger technologies

Distributed Ledgers are technologies based on distributed append-only data structures in which all the nodes* in a network have the same copy of a database*. The database can be independently read and modified by the individual nodes. In Distributed Databases, all nodes have a copy of the database and can consult it, but they must go through a central entity (or several validators*) to modify the data. In Distributed Ledger technologies, however, changes to the Ledger are regulated by consensus algorithms*. These algorithms are used to achieve consensus between the different versions of the ledger, even if they are independently updated by members of the network. In addition to consensus algorithms, Distributed Ledger and Blockchain also make widespread use of cryptography* to ensure security and immutability of the ledger. Blockchain is a technology belonging to the family of Distributed Ledger Technologies whose distributed ledger is structured as a chain of blocks containing transactions.

Moreover, Blockchain and Distributed Ledger are the technologies behind the Internet of Value, which is the set of applications and platforms based on digital and trustless networks of nodes transferring value through a system of algorithms and cryptographic rules that allows to achieve consensus on the modifications to a distributed ledger keeping track of the transfer of value by means of unique digital assets.

## 2.1. The evolution of the technology: past and present

Blockchain and Distributed Ledger are attracting increasing media attention and are considered among the most exciting digital trends for the coming years. Blockchain technology is a relatively recent invention, dating back just over 10 years to the creation of Bitcoin and cryptocurrencies. Indeed, the innovative idea of a virtual, decentralized, p2p currency was first brought about in 2008, when the white paper by Satoshi Nakamoto was published. However, Bitcoin was soon associated with the illicit market, it was snubbed by banks and media and considered a niche product. At the same time, legislators developed a conflicting approach towards cryptocurrencies. In some cases, Bitcoin was considered a currency, while in others it was prohibited or not recommended. Despite the daunting framework, other platforms were created, based on the very same founding principles of Bitcoin, e.g. Ethereum, Corda, Hyperledger. In 2016 something changed, all of a sudden Blockchain was all over the media as one of the potentially disrupting and revolutionary technology of the future. Media attention, however, has always been closely connected to cryptocurrencies, instead of the technology behind them. The boom phase of the cryptocurrencies market, characterized by a swift rise in capitalization in 2017, was suddenly followed in 2018 by a sharp drop in their value: the so-called Cryptowinter. However, there was no winter for Blockchain, which, if anything is enjoying another spring, as it continues to mature and evolve, gaining strong interest from companies all over the world.

* The terms marked by the asterisk are in-depth defined in Appendix 1 - Glossary

So why is this technology attracting so much attention? What is the real innovation introduced by Blockchain? It is the achievement of effectively integrating well established technology solutions (such as cryptography, hash functions, design mechanisms, distributed systems) to create an irreproachable transfer of “value”, independent of central guarantors and potentially anonymous. The revolutionary significance lies in this paradigm shift that would lead to the creation of the Internet of Value: a system that enables the exchange of goods of value without an intermediary, and in a programmable way using what are known as smart contracts. However, the technology is still not fully mature, and there is a lot of confusion and instrumentalization surrounding what it can and cannot do.

## 2.2. The pillars of the Internet of Value: some definitions and technical features

Blockchain and Distributed Ledger are the technologies behind the Internet of Value, that is, systems that allow to exchange value over the Internet as easily as we currently exchange information.

Distributed Ledger systems can be distinguished according to three fundamental characteristics: network type, consensus mechanism and structure of the ledger. Solutions that are more correctly described as Blockchain, inspired by the Bitcoin* platform, have two additional characteristics that are not necessarily part of Distributed Ledger systems transfers and assets.

Based on the **network type**, systems can be permissioned, i.e. networks for which users need to register and identify themselves to receive authorization from a central entity or the network itself; or permissionless, that is networks that anyone can access, without need for authorization.

The **consensus mechanism** varies according to the network type. In permissioned systems the consensus mechanism is simpler: when a node proposes the addition of a transaction, its validity is checked, and a majority vote can have it added to the ledger. In permissionless systems, on the contrary, the consensus mechanisms are more complex (based for example on Proof of Work* or Proof of Stake*) to ensure that a malicious individual cannot create numerous fictitious identities to influence the process for modifying the register.

The third characteristic of Distributed Ledger systems is the **structure of the ledger**. In Blockchain solutions the ledger is structured like a chain of blocks* containing multiple transactions and the blocks are linked to each other using cryptography (as it is the case in the Bitcoin or Ethereum* platforms). In other solutions, the ledger is made up of Tangle*, in which transactions are processed in parallel (e.g. Iota) or yet other cases in which the ledger is created by a chain of transactions (for example Ripple).

In addition, Blockchain systems enable users to perform transfers, or more generically, transactions. These **transactions** can be either simple or more complex, depending on the level of programmability allowed by the platform. For instance, the Ethereum platform allows the creation and management of smart contracts*.

Finally, the last characteristic of Blockchain systems is that there is a **unique asset** to be transferred, which can be either a cryptocurrency* or a token*. This asset is essential to the functioning of the platform and is usually used in the rewarding system and to make transactions.

The numerous platforms that enable the Internet of Value share the following characteristics:

- Disintermediation, the platforms facilitate the management of transactions without an intermediary, that is, without the presence of trusted central entities;
- Decentralization*, the information is recorded by distributing it over different nodes to guarantee information security and system resilience;
- Immutability of the ledger, once data has been written to the ledger it can no longer be changed without the consent of the network;
- Transparency of ledger, the contents of the register are transparent and visible to all;
- Traceability of transfers, every element represented on the ledger can be traced right back to its exact origin;
- Programmability, it is possible to program that certain actions are performed when certain criteria are met. Smart contracts, defined by Nick Szabo as "a set of promises, specified in digital form, including protocols* within which the parties perform on these promises", are a fundamental element of some platforms;
- Digitalization, data is converted to digital format.

During the period 2016-2017 it seemed that Blockchain solutions could solve countless problems and increase efficiency in many processes. Various companies, spurred only by media hype, started developing projects and experiments without having fully understood how exactly the technology could really bring value. Efforts to apply Blockchain and Distributed Ledger to unsuitable use cases resulted in little benefit, and the technology per se was blamed, rather than its concrete application. For this reason, the Blockchain & Distributed Ledger Observatory, through the analysis of numerous use cases, has identified some variables that must be taken into account when assessing the suitability of Blockchain and Distributed Ledger to a certain project. More specifically, Blockchain and Distributed Ledger technologies are particularly appropriate when there is a **large number of participants** who do not  trust each other **(lack of trust)** and need a third party or a shared system to guarantee that all the copies of the ledger are updated in the same way. In addition, it is important that these participants **need to share information,** i.e. it is useful to make a certain piece of information visible to a large number of individuals, or they need to **transfer assets** between them, an asset that is distinguishable and unique and, therefore, cannot be replicated **(uniqueness of the asset)**. The asset can either be natively digital or easily digitalized **(digitalization).** Blockchain and Distributed Ledger technologies can also be applied to platforms that allow to program that certain actions are performed when certain conditions are met **(programmability variable).** Finally, Blockchain and Distributed Ledger can be fully and properly exploited if the participants consider as the main objective that the shared information remain **immutable** and cannot be tampered with. It is not necessary for all the conditions to be fully applicable, nor all at the same time. However, the more conditions are present, the more benefits the implementation of a Blockchain and Distributed Ledger based solution may bring.

## 2.3. The type of usage of Blockchain

Blockchain and Distributed Ledger projects can be classified according to the type of usage of Blockchain. **Notarization**, for instance, includes projects that use the distributed register of an existing Blockchain to register the date of a document and the fact that it has not been modified over time (timestamp). The mechanism is guaranteed by the use of hashing functions that allow to create from an entire document or database a single and unique hash (an alphanumeric code of fixed length), which can then be shared on the Blockchain. Other projects, on the other hand, use **smart contracts** and exploit existing networks and their programmability characteristics to digitize processes and create decentralized applications (Dapp). There are then projects that exploit the already existing **cryptocurrencies** to allow the exchange of value between actors who do not know each other and do not trust each other. In these projects the presence of a unique asset within the platform becomes fundamental. These three categories mainly use existing platforms.

On the contrary, there are some projects that rely on new platform created ad hoc. It is the case of **Distributed Ledger Permissioned** and **Distributed Ledger Permissionless**. These projects involve the creation of a network of nodes and an immutable and distributed ledger where information is shared among numerous actors who do not trust each other. This also allows to digitize processes and exploit the programmability of smart contracts, without however introducing unique assets for the management of transfers.

# 3. The research on the Blockchain & Distributed Ledger environment: some evidence from the international market

The analysis has been structured in three phases. The first one consisted in a scouting of use cases on several secondary sources and led to a total of 1050 national and international use cases, running from 2016 to October 2019. These cases have then been analyzed carefully by the Blockchain & Distributed Ledger Observatory, to select only those related to the B2B and Supply Chain (SC) field, i.e. only those involving an exchange of information between two or more subjects. Finally, the remaining 288 cases have been analyzed according to three macro-areas: **stakeholder**, **technology** and **project**. These areas have then been narrowed and divided in sub-areas. More specifically, we considered geographical distribution and area of interest as stakeholder-related variables; type of network, protocol and type of Blockchain application as technology-based variables; state and date of announcing, process of implementation and expected benefits among the project-related variables.

We tracked the **geographical area** in which each case has been developed or is going to be developed. We considered two levels of classification: the continent and the country. The continent is not defined according to its real boundaries, but in order to delimit a specific zone in the world. For example, Russia and Switzerland have been considered as Europe because of their location and because considering them as single continents would have added little value to the analysis. Similarly, Turkey has been considered as Asia. When a case is not related to a specific continent, but it is meant to be applied worldwide, it is classified as “global”. According to our analysis, US is the first country for use cases, with 37 projects (13%), followed by China (19, 7%), Italy (13, 5%), Germany (12, 4%) and Australia (12, 4%). However, the majority of the projects is carried out in Asia (78, 27%) and Europe (75, 26%). Finally, 77 (27%) cases involved more than one continent.

The categorization in **areas of interest** is aimed at understanding which field the Blockchain technology has an impact on and, therefore, where companies, governments and Public Administrations foresee the maximum gain of benefits and advantages. Ten areas of interest have been identified:

- **Agri-food** regards the agricultural production, industrial transformation, distribution and consumption of food products. It combines the term agriculture and food to represent a holistic view of the activities involved around the food production. It is composed by four major segments: Crop Producers (including production for crops for fuel and fiber); Fishers and animal producers (including livestock raised for fiber); Food Manufacturers (e.g. companies that process and package food products); Food and Beverage Retailers (e.g. grocery stores, meat markets, fruits and vegetable markets, GDO).
- **Automotive** comprises a wide range of companies involved in the design, development, production, marketing and selling of motor vehicles, towed vehicles, motorcycles and mopeds.

- **Finance** is a broad category, comprising everything regarding financial services, professional services involving the investment, lending and management of money and assets. The firms involved are banks, credit unions, credit-card companies, accountancy companies, consumer-finance companies, stock brokerages, investment funds. In our classification, the insurance industry is not englobed in the finance sector because of the large number of cases registered.
- **Government** concerns all the initiatives having as subject or object the solution for the following entities: all the units of central, state or local government; all social security funds at each level of government; all non-market non-profit institutions that are controlled and financed by government units (OECD Statistics Directorate, 2019). This sector does not include public corporations, even when all equity of such corporations is owned by government units.
- **Healthcare** comprises the sum of activities performed either by institutions or individuals pursuing, through the application of medical, paramedical and nursing knowledge and technology, the goals of promoting health and preventing disease, curing illness and reducing premature mortality.
- **Insurance** represents the industry in which firms consisting of incorporated, mutual and other entities whose principal function is to provide life, accident, sickness, fire or other forms of insurance to individual institutional units or groups of units operate.
- **Logistics & airline** includes activities like planning, execution, storage, wares management, managing clients and suppliers, transportation, and it includes also all those cases regarding the management of the whole supply chain; the category comprises also the business of transporting paying passengers by air, usually through scheduled routes, typically by airplanes but also by helicopters.
- **Luxury** is a peculiar category because it is not defined according to the nature of the product like in the other sectors, such as cars in automotive and food in agri-food. Rather, it can include all kinds of products and services. It includes all those products which are pleasant to have, exclusive, not necessary and accessible to a small part of the population (Cambridge Dictionary, 2019).
- **Media & telecom** is the group of organizations which share the collection, distribution and creation of media contents. In this sector we include products and services pertaining to the so called “old media” which existed before internet like radio, newspaper, TV, videogames, film, and “new media” like social networks, streaming platforms, blogs, on-line games, web sites and so on (BBC Bitesize, 2019). The category also includes all firms which make communication possible on a global scale, whether it is through the phone or the Internet, through airwaves or cables, through wires or wirelessly. This sector includes also those firms which created the infrastructure enabling the population to communicate and to send data in all sorts of format (video, images, text, video...). Here we can find telephone operators, satellite companies, cable companies and internet providers.
- **Utility** includes the companies which are involved in providing basic goods such as water, electricity, natural gas, sewage, dams.

The finance sector is the first one by importance, covering the 26% of the considered SC cases. It is important to stress that Finance is the main sector promoting Blockchain projects and applications in all the fields other than SC, one of the reasons is because it is the field in which Blockchain was born in the first place. Projects in logistics and agri-food are relevant too, representing a countertrend with respect to the total cases, where they count together just for 13%. When looking at the SC field, their product-centricity fits very well with the Blockchain characteristics, leading to several potential benefits and advantages. The majority of projects and announces are related to a private-level, mainly companies and consortium.

The first technology-based variable is the **type of network,** which has been classified according to the consensus mechanism and the platform governance. Two types of networks can be distinguished:

- **Permissioned,** i.e. networks in which users need to register and identify themselves to receive authorization from a central entity or the network itself. In permissioned systems the consensus mechanism is simpler: when a node proposes the addition of a transaction, its validity is checked, and a majority vote can have it added to the ledger.
- **Permissionless,** that is to say networks that anyone can access, without need for authorization. These types of Blockchains need univocal assets like cryptocurrencies to guarantee incentives to validators and to manage the consensus mechanism. In permissionless systems, the consensus mechanisms are more complex (based for example on Proof of Work or Proof of Stake) to ensure that a malicious individual cannot create numerous fictitious identities to influence the process for modifying the register.

From our analysis a sharp prevalence of permissioned platforms emerges, i.e. the 89% of the analyzed cases. This evidence is coherent with the results we get by analyzing the whole projects, not just those related to the SC environment. The higher efficiency of permissioned Blockchains along with the fact that the permissionless platforms are still evolving in order to gain a stronger technological maturity could explain this result. However, permissionless platforms are useful in those cases in which a simple timestamp of data and documents is needed (notarization).

We detected also the **type of protocol** used in each case history. Blockchain platforms indeed could be built on various Blockchain protocol. For the purpose of the research, we registered the Blockchain protocol at the lowest level, e.g. Quorum, a Blockchain protocol developed by JPMorgan Chase, is built on a permissioned version of Ethereum and the protocol would be categorized as Ethereum. Otherwise, a new protocol can be developed. Most of the cases (59% out of 178) rely on existing protocols, such as Hyperledger (59, 33%), Ethereum (33, 19%) and Corda (12, 7%). The advantages of choosing an existing protocol are interoperability, standardization and a greater chance of involving a big number of actors and developers. Despite that, one fifth of the projects (38) develops a new protocol in order to maximize the personalization of the platform.

The last technology-based variable is the **type of Blockchain application**. Three types of Blockchain solutions have been identified in the analysis:

- Notarization;
- Smart contract/DApp;
- New Distributed Ledger (permissioned).

We analyzed the type of Blockchain application only in the operative projects, because it is frequent that the Blockchain chosen in the announcing and PoC phases changes while implementing the project. For this reason, only 32 cases out of 288 have been analyzed according to this specific variable. Most projects (22, 69%) choose to develop a new distributed ledger, that allows a higher level of personalization and a good capacity of managing complex processes with several actors of different types. Smart Contracts and dApps on existing platforms (6, 19%) are mainly used in the Supply Chain Finance projects by exploiting their main features (programmability and the chance of automatically exchanging value fulfilling a contract, even in a trustless environment). Notarization is used in 4 operative projects (12%), when the goal is to register timestamp of static data or documents (such as sales data and production capacity, performance assessment metrics, critical events for SC management, ...). Finally, note that with respect to the classification in the introductory part, “Cryptocurrencies” and “New Distributed Ledger Permissionless” are missing, since we have found no cases related to those categories.

The first project-related variable considered is the **state of the announcing** with respect to the date. In 2016 and 2017 PoC represented most of the use cases, respectively 13 out of 15 and 36 out of 65. However, the trend reversed in 2018, when the number of announcements almost doubled, going from 26 in 2017 to 56 in 2018. Overall, the number of use cases rose in the period spanning from 2016 to 2019, proof of the increased interest shown by private as well as public actors. It is important to stress that the data are updated up to October 2019. We estimate a total of 120 cases in 2019, having already registered 102 ones.

We considered also the **process of implementation.** In a single sector it is indeed possible to find solutions which are very different because conceived to impact various areas and processes. Therefore, the general processes in the sector impacted by the solution were defined as follows:

- **Advertising management,** regarding those cases which impact the way the firms share their messages to promote products or services. It regards for example the way firms buy physical or digital spaces for advertising or deal with the opacity reduction along the digital advertising process.
- **Capital markets,** regarding those solutions which impact the exchange of value between investor firms, investing in equity or long-term debt, and firms which are looking for capital. The operations in the capital markets are usually divided in primary market, in which the securities are issued and sold for the first time, and secondary market, in which the securities are traded.

- **Data & Document Management,** involving those processes in which documents and data are stored and managed. Here, there are solutions regarding contract or data registration, documents notarization, solutions to integrate data of common interest between firms, certification registration and so on.
- **Identity,** which is a transversal category of processes which is being developed in almost every sector. Identity processes regard concepts such as digital identity, registration and authentication processes, Know Your Customer, decentralized self-sovereign identity.
- **Payment** regards all the solutions which impact the way in which value is sent between an entity to another usually in exchange of goods and services. It doesn't regard only the use of cryptocurrencies as an asset to exchange value between entities, but also the change in the core processes characterizing the payments. Here we can find solutions which impact cross border payments referring to transactions involving individuals, companies, banks or settlement institutions operating in at least two different countries, micropayments, interbank transactions, aid donations, remittances and general mobile, remote and proximity payments.
- **Supply chain finance,** regarding those projects which impact the way firms finance their working capital, that means all the solutions which are drawn to optimize cash flow by leveraging on the role of the working capital along the whole firm's supply chain. Here we can find initiatives such as vendor managed inventories, consignment stocks, factoring, reverse factoring, inventory finance.
- **Tracking and supply chain,** in which the solutions meant to improve the transparency and traceability along the supply chain, both for an internal and an external use, are registered. Moreover, we include solutions impacting the way the supply chain works. Examples pertaining to this category of processes are asset tracking, registration of the whole lifecycle of an asset, tracking of the production process, procurement, post selling, waste disposal, fraud prevention.

Tracking represents the most important process where the Blockchain technology has been applied. Here, 157 cases (55%) are included. Data & Document Management account for the 23% of considered cases. Most cases are aimed at digitizing trade documents, to streamline the process, reduce costs and improve efficiency and security. In fact, risks related to frauds, document losses or document corruptions can be dealt with and reduced using this type of technologies. Supply Chain Finance represents 14% of the use cases. Blockchain technology is used to store, certify and share documents with financial institutes in a safer and more efficient way.

To conclude, we analyzed the **benefits** the players expect to gain from the projects carried on. They are mainly related to transparency of data and documents, security of the shared information and a cost reduction stemming from a higher level of collaboration among the Supply Chain actors. The Blockchain and DLT technologies allow for the creation of new ecosystems in which suppliers, customers, competitors, banks, insurances and Public Administrations could collaborate. The validation process and the impossibility of corrupting information require no trust among participants.

## 3.1. A focus on the Order-to-Payment Cycle

By looking at the case histories considered in the analysis, many of them exploit the Blockchain and distributed ledger technologies in two specific phases of the Supply Chain:

- **Control,** phase in which two or more actors collaborate to monitor and control data and information. Some examples are: the sharing of sales data and production capacity, performance assessment metrics, critical events for SC management (such as the traceability to certify the quality of a product).
- **Order-to-Payment Cycle,** i.e. the order-delivery-invoicing cycle that includes all logistics, commercial, administrative and accounting phases, where the aim is to integrate and automate all the phases at the interface between supply chain partners, using a structured electronic format.

However, by considering the characteristics of the Blockchain, the Order-to-Payment Cycle is particularly interesting, since it could take advantage of several benefits of these technologies in a better way than the control phase. For this reason, we ran an in-depth analysis on those cases related to the execution phase.

More specifically, we identified 66 projects related to the Order-to-Payment Cycle. They have been classified according to the specific phase they affect:

- **Order,** that is to say commercial and administrative phase aimed at managing documents such as buying and selling order and order confirmation;
- **Delivery,** i.e. logistic phase;
- **Invoicing,** which represents the administrative and accounting phase that manages the exchange of invoicing-related documents;
- **Payment,** that is the administrative, commercial and accounting phase aimed at managing the payment-related documents (letter of credit, premissory notes, etc.).

Only 11 (17%) cases have been conducted with the purpose to digitize the entire cycle. Most projects are instead using the technology to manage only one phase, especially to notify data and document. Moreover, by looking at the Order-to-Payment Cycle phases, the delivery and the payment represent the two most common applications.

With respect to the area of interest, most of the use cases affect the sectors of Logistic (29 case, 41%) and Finance (21 cases, 29%), which is in line with Delivery and Payment being the most affected phases of the cycle. Finally, there are no big differences with respect to the other SC cases when looking at the technological variables.

# 4. Conclusions and takeaways

### The Blockchain Ecosystem

The analysis shows that the usage of Blockchain and Distributed Ledger Technologies in the Supply Chain environment is mainly related to the Control phase and the Order-to-Pay Cycle. Nevertheless, the characteristics of this technology (described in the first part of this document) in terms of immutability, transparency, traceability, digitalization and programmability fit very well when the counterparts exchange documents or data, especially when there is no trust among the actors. Summarizing the results, there are four cases that are particularly interesting when applying the Blockchain & Distributed Ledger Technology.

Firstly, in the solutions of Supply Chain Finance, e.g. trade finance or invoice financing, Blockchain can ease the management and the execution of contracts where enterprises (small, medium and large) collaborate with banks and other companies. In fact, Supply Chain Finance solutions could face managerial, legal and technological impediments that hinder their adoption. Blockchain technologies can help to achieve a stronger integration among partners and among physical, administrative and financial flows.

Secondly, In the Order-to-Pay Cycle, i.e. Supply Chain execution, Blockchain benefits are at their maximum level when the project involves not just one phase of the process, but it embraces the whole steps. The characteristics of transparency and trustworthiness of Blockchain technology allow for the involvement of all actors in the Order-to-Pay Cycle: not only partners from the same supply chain, such as suppliers and customers, but also third parties from other supply chains. Moreover, when digitizing several phases, a higher level of efficiency is gained.

In addition, In the Supply Chain Collaboration field, the creation of a new platform could cope with the need of managing complex processes with a high number of external actors. Theoretically, these are the most interesting solutions to analyze, even if it is very complex to create a concrete project. Some examples of Supply Chain Collaboration are linked to logistic processes in international trade.

Finally, in the Supply Chain Control phase (tracking quality of products), there is still the need to fully understand how to take advantage of the Blockchain paradigm. The benefits of Blockchain application then also depend on the type of supply chain or products.

### Private Permissioned platform

When choosing the type of platform, it is fundamental to consider which are the objectives in terms of expected efficiency and trustworthiness, together with the nature of the specific case of application. Permissionless platforms rely on existing platforms with consolidated standards. Hence, they could represent a good solution when a simple data/document registration is needed in order to give public proof of their truthfulness (e.g. notarization). On the other hand, permissioned platform can be useful when a higher level of privacy of the data is needed and a higher level of efficiency is required.

As of today, most projects (89%) show the usage of a permissioned platform. This trend is particularly strong when looking at the cases related to the Order-to-Pay Cycle. However, some projects exploit hybrid solutions that combine the efficiency of permissioned platforms with the transparency and immutability features of the permissionless ones. The as-is preference for permissioned platforms can be partially explained by considering that today permissionless platforms still suffer from technological issues. In the next years, this could evolve and, consequently, shift from permissioned to permissionless standards.

### Existing protocol

Most projects choose existing protocols of Blockchain and Distributed Ledger, such as Hyperledger, Ethereum and Corda. The advantages of relying on an existing protocol are interoperability, standardization and chance of involving a big number of subjects and developers. Interoperability is particularly important when technological standards do not exist and neither the market nor the regulator have a clear position on it. The SCALES project takes place in a context in which there is still uncertainty about the future technological platform at the European level. Therefore, it is fundamental to choose a flexible approach that could guarantee interoperability with other solutions. The main solution that must be taken into account is the European Blockchain Services Infrastructure framework (EBSI), that the European Commission and European Blockchain Partnership (EBP) are jointly developing.

### Recommendations

On the application-level, we recommend projecting a Blockchain solution that could involve a wide ecosystem composed by several actors, such as suppliers, customers, Public administrations, banks, insurances and so on. We also advise to begin with solutions related to the Order-to-Pay Cycle and include all phases (or at least 3 of the 4). Only after, i.e. in the advanced phases of the SCALES project, the project should be extended to Supply Chain Finance and Collaboration solutions.

On a technical-level, we suggest selecting an already existing protocol with the following characteristics: open-source, reliability, high-performance. It is also important to create a solution that could be interoperable with other Blockchain platforms both permissioned and permissionless, keeping in mind that Blockchain technology is still evolving and changing.

# 5. Appendix A: Glossary

**Address:** information, often presented in the form of an alphanumeric string and linked to a public key, used to identify an entity that can receive and transmit assets on a Blockchain network.

**Bitcoin:** the first cryptocurrency to use Blockchain technology. Bitcoin, created in 2008, and implemented and launched in 2009 by a person or group of people using the pseudonym Satoshi Nakamoto.

**Block:** type of data structure used in Blockchain ledgers to group transactions. The blocks are chained to each other by the inclusion of the hash code of the previous block.

**Blockchain:** the technology behind Bitcoin, Ethereum and other platforms in which the distributed ledger is structured like a chain of blocks containing transactions.

**Consensus algorithm:** protocol used to reach consensus between nodes in a network on a single version of a distributed ledger. These algorithms allow participants in the network to agree on the content of the ledger, even in the event of malicious parties or a breakdown in the network.

**Consensus:** agreement of the majority of participants in a network on the validity of a historical sequence of transactions.

**Corda:** open source Distributed Ledger platform, created in 2016 by the R3 banking consortium for use by financial institutions.

**Cryptocurrency:** decentralized digital currency that uses cryptographic techniques and incentive alignment systems to guarantee the security of exchanges between users. Unlike traditional currencies, there is no central entity acting as intermediary for transactions and the rules that apply to exchanges are written in an open source software, that can be publicly verified.

**Cryptography:** branch of mathematics that defines methods and algorithms to hide information and render it accessible only if certain conditions exist (for example, knowledge of a certain key). Cryptography is widely used in Blockchain platforms.

**DApp (Decentralized Application):** a decentralized application, similar to a conventional app, that relies on Blockchain platforms and their distributed network to obtain guarantees of non- censurability.

**Decentralization:** transfer of authority and responsibility from a centralized organization to a distributed network.

**Distributed Ledger:** technology in which all nodes in a network contain the same copy of a database, which can be read and modified by each single node independently. In Distributed Ledger technology, changes to the ledger are regulated by consensus algorithms. These algorithms allow the reaching of a consensus between different versions of the register, even if they are updated independently by network participants.

**Double spending:** situation in which a user tries to spend the same digital coin more than once, for example, sending the same payment to two different beneficiaries.

**Ethereum:** platform based on Blockchain technology that allows the writing of smart contracts and the creation of non-censurable distributed applications (DApps). The native tokens of this Blockchain are called ether and are used both for solving computing operations within the network or for exchanging value in transactions.

**Fork:** possible creation of an alternative version of a ledger, as a result of a change to the basic protocol of the network. The two chains can then continue to grow, each developing different ledgers.

**Governance:** set of rules and procedures that control the management of a Blockchain platform and the ways in which changes to how it works can be proposed, and if applicable, executed.

**Hash:** result of a function that transforms data into a unique output of fixed length from which it is impossible to trace back to the input data. It can be considered as the electronic version of a fingerprint, for any type of data.

**Hyperledger:** project started by the Linux Foundation to support the creation of permissioned Blockchains and facilitate the collaborative development of open source Distributed Ledgers.

**ICO:** acronym of Initial Coin Offering, describes the action of generating and selling new tokens to interested investors, with the objective of financing the development of a specific project.

**Internet of Value:** digital network of nodes that transfer value to each other using a system of algorithms and cryptographic rules. These networks enable the reaching of consensus, even in the absence of trust, on changes to be made to a distributed ledger that tracks unique transfers of digital assets.

**Lightning networks and State channels:** so-called second-layer protocols used to make transactions faster and resolve scalability problems. They work using one-to-one channels between nodes, which are updated outside of the Blockchain, to which they are periodically updated.

**Mining:** process by which bitcoin transactions are verified, grouped in blocks, validated and added to the Blockchain. This process is done by resolving cryptography problems that require effort of time and energy and are paid for with a fee and the issuing of new value for the validating node.

**Node:** computer on the network that manages a copy of the Blockchain ledger.

**Off chain:** expression that refers to transactions that are not registered on the Blockchain but are validated separately. Usually, such systems are used to increase the speed or privacy of transactions.

**On chain:** expression that refers to traditional Blockchain transactions, validated by the network and registered in a block on the main network.

**Open source:** software with source code that is accessible and modifiable by users.

**Oracle:** agent in charge of providing the Blockchain with information coming from the "real" world that is of interest to the functioning of the smart contract. The information may also be provided in conjunction with a cryptographic test that guarantees its provenance.

**Peer-to-peer:** IT network architecture in which the nodes are at the same hierarchical level and govern themselves based on certain protocols, without the need for a central entity.

**Prediction market:** market created with the aim of providing predictions on future events. These markets are based on predictions made by users that speculate on future events, betting on the result of a specific event. Based on the betting odds you can identify which event the users consider to be most probable.

**Private key:** information, used in asymmetric cryptography systems, that allows, among other things, the "signing" of a document in a verifiable, non-repudiable way. In cryptocurrencies, it is typically used to arrange transfers from one account to another. The safekeeping of private keys is one of the most sensitive elements of using cryptocurrencies.

**Proof of Concept:** develop a sample or a prototype of a specific project to confirm its feasibility.

**Proof of Stake:** consensus algorithm in which changes to the ledger are not validated with computing effort, but in which the users guarantee the validity of transactions by putting at stake, therefore committing, a share of their own cryptocurrencies. In this way, the validators are incentivised to behave honestly so as not to lose their stake.

**Proof of Work:** consensus algorithm that requires users to resolve complex mathematical problems to verify transactions. Whoever resolves the problem, and thus demonstrates proof of work, usually receives a reward.

**Protocol:** set of rules that determine how data is exchanged and transferred.

**Public key:** can be used by anyone to encrypt a transaction, which can then only be decrypted using the corresponding private key. In cryptocurrencies, the public key is typically used to identify an account to which assets are associated, that can be verified only with knowledge of the corresponding private key.

**Side chain:** a new Blockchain that is linked to another reference Blockchain with a bidirectional link that allows for assets to be exchanged between the two networks. The original Blockchain is usually referred to as the “main chain”.

**Smart contract:** set of instructions expressed in computer language and visible to all. It is executed automatically by a Blockchain network once certain predetermined events occur. Once a smart contract has been activated its execution is guaranteed and cannot be stopped. In some platforms smart contracts are also able to send and receive transactions.

**Stablecoin:** digital assets that enjoy the guarantees and the properties typical of cryptocurrencies, but with a stable price linked to a reference asset which may be a fiat currency, such as the dollar or Euro, a commodity such as gold, or a price index.

**Stealth Address:** in the Monero cryptocurrency, stealth addresses help to hide identity, making it impossible to find any links between a transaction and its beneficiary.

**Tangle:** a particular type of ledger based on Directed Acyclic Graphs (DAG). Tangle’s greatest innovation is that transactions are processed in parallel, which enables greater scalability and a reduction in validation costs and time required.

**Token:** a particular type of digital asset that can be exchanged on a Blockchain. Tokens are often used to represent other digital or physical assets or a right, such as ownership of an asset or access to a service.

**Turing Completeness:** characteristic of a programming language that indicates the maximum possible degree of expressiveness, that is, the ability to describe every accessible logic with any other programming language.

**Validating Node:** node in a network that is part of the group of validators who are responsible for creating blocks and transmitting these blocks to the network. To create a new block, the validators must follow the rules specified by the consensus algorithm.

**Wallet:** system for safekeeping private keys linked to cryptocurrencies and that can communicate with the respective Blockchain. The wallet can be online, offline or on a physical device.

**Zero knowledge proof:** family of techniques that allow demonstration of the existence of certain conditions (for example, the availability of funds sufficient to complete a transaction) without revealing any other information. This makes it possible, for example, to guarantee the integrity and correctness of economic transactions, without revealing information such as sender, beneficiary or amount.