|  |  |  |
| --- | --- | --- |
|  | WIPO-E | **E** |

**WIPO Blockchain Whitepaper**

*Document prepared by the International Bureau of World Intellectual Property Organization (WIPO)*



Getty Images Plus / ipopba

Table of Contents

[I. INTRODUCTION 4](#_Toc82791125)

[II. BLOCKCHAIN AND THE FOURTH INDUSTRIAL REVOLUTION 6](#_Toc82791126)

[BLOCKCHAIN TECHNOLOGY AND ITS POTENTIAL 10](#_Toc82791127)

[BLOCKCHAIN BASICS 12](#_Toc82791128)

[BLOCKCHAIN IMPACT 16](#_Toc82791129)

[Value creation with blockchain applications 17](#_Toc82791130)

[PROMINENT USE CASES OF BLOCKCHAIN 18](#_Toc82791131)

[Digital Identity and its management 18](#_Toc82791132)

[Traceability 19](#_Toc82791133)

[Transparency and Fraud prevention 20](#_Toc82791134)

[Smart contracts 21](#_Toc82791135)

[Tokenization and Non-Fungible Tokens (NFTs) 21](#_Toc82791136)

[BLOCKCHAIN TECHNOLOGY SWOT ANALYSIS 22](#_Toc82791137)

[Strengths 22](#_Toc82791138)

[Weaknesses 23](#_Toc82791139)

[Opportunities 23](#_Toc82791140)

[Threats 24](#_Toc82791141)

[BLOCKCHAIN IMPLEMENTATIONS AND CONSORTIUMS 25](#_Toc82791142)

[Main blockchain implementations 25](#_Toc82791143)

[Main blockchain consortiums and Industry alliances 27](#_Toc82791144)

[III. POTENTIAL USE CASES OF BLOCKCHAIN IN IP ECOSYSTEMS 28](#_Toc82791145)

[IP ECOSYSTEMS AND POTENTIAL USE CASES 29](#_Toc82791146)

[IP Ecosystems and IP Value Chains 29](#_Toc82791147)

[Potential blockchain use cases along IP value chains 31](#_Toc82791148)

[INDUSTRIAL PROPERTY RIGHTS 33](#_Toc82791149)

[Blockchain application from a private sector perspective 33](#_Toc82791150)

[Blockchain application from a public sector perspective 38](#_Toc82791151)

[COPYRIGHT AND RELATED RIGHTS 42](#_Toc82791152)

[DATA PROTECTION AND ACCESS 46](#_Toc82791153)

[IPR ENFORCEMENT 48](#_Toc82791154)

[IPR enforcement before judicial courts and administrative bodies 49](#_Toc82791155)

[Alternative Dispute Resolution systems 51](#_Toc82791156)

[Counterfeiting and Piracy 54](#_Toc82791157)

[IV. CONSIDERATIONS 56](#_Toc82791158)

[INTEROPERABILITY AND TECHNICAL STANDARDS 57](#_Toc82791159)

[Interoperability among existing blockchain platform networks and consortium projects 59](#_Toc82791160)

[Interoperability with external and internal blockchain data 59](#_Toc82791161)

[GOVERNANCE 61](#_Toc82791162)

[Four foundational elements of governance 62](#_Toc82791163)

[Governance framework: aspects to address 62](#_Toc82791164)

[REGULATORY FRAMEWORK 67](#_Toc82791165)

[Uncertainty in relation to the general aspects of blockchain 67](#_Toc82791166)

[Uncertainty in relation to some applications of blockchain 69](#_Toc82791167)

[Ongoing works on the regulatory framework adaptation 72](#_Toc82791168)

[SECURITY 73](#_Toc82791169)

[SUSTAINABILITY AND SCALABILITY 74](#_Toc82791170)

[TECHNOLOGY GAP AND CAPACITY BUILDING 74](#_Toc82791171)

# I. INTRODUCTION

Since the mid-1990s the Internet has revolutionized how society provides and accesses services and information in real-time online communication between users, beyond geographical barriers. Although the social and economic benefits that this digital system has enabled are unquestionable, the Internet is lagging behind in some key areas, mainly related to data privacy and identity management.

Currently, with the Fourth Industrial Revolution or 4IR, a new suite of emerging technologies, such as blockchain, Artificial Intelligence (AI), Internet of Things (IoT) and robotics, among others, are increasingly merging with human lives and creating a radical shift for employees, organizations, and society as a whole. These emerging technologies are capable of significantly affecting the way that businesses operate and revolutionize the ecosystem of innovation and creativity by improving the automation of tasks with yet unseen capabilities.

In the context of this paper, blockchain can be defined as a distributed, immutable (append-only) ledger encompassing related solutions, such as distributed identities, smart contracts and tokenization. This ledger is realized as a distributed database storing a permanent and tamper-proof ledger of data. The key features of the technology which bring trust to users are: (i) the potential of decentralization, avoiding the role of traditional intermediaries (trusted third parties) and providing transparency to the participating blockchain nodes; (ii) immutability of the records, for once a transaction is recorded it is almost impossible to alter; (iii) and encryption, allowing for peer-to-peer transactions between untrusted parties via a decentralized and autonomous trust verification model.

Blockchain technologies could offer new ways to handle physical assets and their digital representation, exchange value, run business and implement trust mechanisms. The main insights in relation to the blockchain landscape within the Intellectual Property (IP) ecosystem show that the IP industry started only recently to explore blockchain technologies, and there are already some operative solutions. However, there is still a generalized lack of understanding and adoption. The few blockchain applications already at the productive stage only cover some specific and small use cases combined with traditional solutions or other disruptive technologies.

Although expectations on blockchain applications are still high, the hype has passed and current interested parties understand that blockchain is not the golden solution to all problems and prefer to take a conscious step-by-step approach to explore the potential of blockchain to solve particular, meaningful challenges.

The Member States of the World Intellectual Property Organization (WIPO) established the Blockchain Task Force under the Committee on WIPO Standards (CWS) at its sixth session, held in 2018, with the following mandate:

* Explore the possibility of using blockchain technologies in the procedures for providing Intellectual Property Rights (IPR) protection, and processing information about IP objects and their uses;
* Collect information about IP Office (IPO) developments regarding the use of, and experience with, blockchain, assess current industry standards on blockchain, and consider its merits and applicability to IP Offices;
* Develop reference models for the use of blockchain technologies in the IP field, including guiding principles, common practices, and use of terminology as a framework supporting collaboration, joint projects, and proofs of concept; and
* Prepare a proposal for a new WIPO Standard supporting the potential application of blockchain technologies within the IP ecosystems.

In order to support the work of the Blockchain Task Force and bridge the gap between the IP and blockchain communities, a workshop on blockchain and IP was held in April 2019 where participants sought WIPO’s leadership in exploring blockchain-enabled applications for the IP ecosystems, particularly in relation to the type of governance that the technology could provide. The workshop noted that WIPO should provide guidance for interoperability among the different applications of blockchain, in addition to recommendations on how to use blockchain-based solutions within the IP space.

In order to produce this whitepaper, the following main activities have been carried out:

* Desk research where – with the use of big data analytics tools – a team of researchers utilized publications, bibliographic references, projects and ideas related to blockchain, IP ecosystems, and blockchain within the IP ecosystems. The findings of this research were analyzed and the identified projects and initiatives were categorized by their perceived level of interest for IP ecosystems;
* An online survey sent out to more than 500 potential participants currently playing a role in the blockchain industry and the IP industry; and
* Interviews with relevant actors in IP and blockchain industries with experience in implementation of IP systems using blockchain technology.

Most stakeholders, who have answered the surveys or interviews, identified decentralization as one of the main benefits and key characteristics of blockchain solutions. However, decentralization may be difficult to achieve. In the studied use cases, organizations created their own platform and expect others to subscribe to it or join a consortium while the maintenance and control of the network usually is handled by a controlling entity. The appropriate governance of decentralized networks still needs to be developed. The survey result is summarized in Annex II to this paper.

As this whitepaper aims to describe how blockchain can impact IP ecosystems, besides an overview of blockchain, a comprehensive outline of IP ecosystems and the IP value chain have been included in this whitepaper for reference purposes as Annex I to this paper. This overview and reference models of IP ecosystems and the IP value chain are generalizations for illustrative purposes and may require further development in order to describe the IP ecosystems with the required granularity.

From the activities mentioned above, a number of potential or prominent use cases of blockchain within IP value chains were found. It is noted that blockchain adoption is a steady trend that could be part of the future operational environments of the IP community. Both start-ups and established industry players in the field of IP have started projects that are promising and evolving into production-ready solutions. It is noted that this technology is at an early-adoption stage in IP ecosystems and there are some initiatives taking relatively small but steady steps in implementing blockchain, starting with the development of niche, focused capabilities while envisioning more complete future solutions. A wide variety of use cases have been identified in the preparatory activities explained above and are described to illustrate the potential applications of blockchain and related technologies. Some of these projects and initiatives are explained below and the use cases are described in detail in Annex III to this paper. This document, however, excludes the aspects of cryptocurrency, which is one of the applications of blockchain technologies. It is noted that the evolving linkages between cryptocurrencies on the one hand, and the valuation and monetization of IP on the other are highly dynamic, but lie beyond the scope of this paper.

This document also explores the strengths, weaknesses, opportunities and threats that blockchain technologies present and how they could be applied in IP ecosystems and provides considerations for IP authorities and the private sector – especially for developing countries – on the use of blockchain in their work.

Additionally, this paper proposes several points to consider for the adoption of blockchain in the IP space. Interoperability seems to be the main operational challenge to solve in multiple areas such as data, architecture, transaction and regulation. Currently, enterprises are *de facto* using industry standards provided by respective blockchain platforms and following general blockchain technical guidelines, while lacking recommendations on a global level. Regarding regulations, there is rising demand for creating specific regulations for blockchain-related technologies and new ways to manage relationships between entities in a distributed environment.

WIPO is perceived as a neutral organization that can facilitate discussions on blockchain and IP among interested parties and establish platforms to explore potential blockchain-based solutions in the IP space. WIPO is also perceived as a body, which can establish appropriate governance linkages and coherence between the intergovernmental governance processes of international IP legal systems and the technical processes of blockchain governance models for IP ecosystems. WIPO, in close collaboration with its Member States and other stakeholders, could analyze the impact of the technologies on the IP space and legal systems, and foster standardization, interoperability and complementarity by creating guidelines and recommendations for the entire IP ecosystems.

# II. BLOCKCHAIN AND THE FOURTH INDUSTRIAL REVOLUTION

The Fourth Industrial Revolution or 4IR is currently enabling a new digital economy, Internet 3.0 and the Programmable Economy. It is based on the fusion of technologies such as blockchain (including encryption, digital identities, smart contracts, cryptocurrencies and tokenization), big data, biotechnology, artificial intelligence, robotics, Internet of Things (IoT), 3D/4D printing, the dematerialization of natural physical resources, such as genetic and biological resources, through digital transformation and characterization and the promise of 5G and their interaction across the physical, digital and biological domains.

The concept of the 4IR was coined in 2016 by Professor Klaus Schwab, Founder and Executive Chairman of the World Economic Forum, in a book by the same name “The Fourth Industrial Revolution”.[[1]](#footnote-2) This revolution creates a world in which physical, virtual and biological systems of manufacturing cooperate with each other in a flexible way at the global level. As Mr. Schwab points out[[2]](#footnote-3), it is in the biological domain where he sees the biggest hurdles for appropriate regulation and consequently biological and genetic resources assume a pivotal role and relevance in many 4IR innovation processes. A similar role and relevance of these resources and associated traditional knowledge (TK) also exists in IP ecosystems and the International Bureau of WIPO have conducted extensive work on the subject.

The difference between 4IR and the previous industrial revolutions is the velocity by which this is impacting the transformation of the current systems in every industry.[[3]](#footnote-4) The average annual growth in patenting inventions related to 4IR between 2010 and 2018 at the European Patent Office has been close to 20%.[[4]](#footnote-5)

All scientific and technical revolutions bring advantages and disadvantages, challenges and opportunities. The scope and complexity of the impacts which such historical transformations have on all domains of society and the economy is far too large to be addressed exhaustively within the scope of this paper, but a few aspects, which are particularly pertinent from an IP perspective, may be briefly noted to provide context for the consideration of blockchain technologies in the IP space and ecosystems. In the case of 4IR, the advantages are evident and include *inter alia*: process quality improvement, productivity increase and enhancement of the decision-making process with data-based tools.

When we think about drawbacks, these include *inter alia* a digital gap due to the lack of knowledge and qualified professionals, and the acceleration of change processes requires flexibility and rapid adaptation.

The biggest challenge that 4IR will likely cause is the impact on employment. In 2017 McKinsey reported that due to automation, between 400 and 800 million jobs will disappear by 2030.[[5]](#footnote-6) However, this may also be an opportunity, because new professional skills will be requested, thus creating millions of job opportunities in new sectors.

In the next few years, the combination of blockchain and other disruptive technologies will have a direct impact to various industries, acting as a facilitator of the Programmable Economy that smart things act for themselves. Within IP ecosystems, blockchain has great transformative and disruptive potential, which should be adequately assessed so as to clearly target its beneficial impacts, manage related risks and avoid speculating on inaccurate theories. The key questions are to (1) identify and analyze the governance, legal and operational implications of blockchain applications for existing IP systems, both in terms of opportunities and challenges, and (2) based on this analysis to provide guidance for the appropriate development and deployment of blockchain applications that will add value to IP ecosystems as well as its existing governance processes.

While it had been previously noted that the pace of innovation and creativity is experiencing a constant and exponential increase, the challenge of the COVID-19 pandemic has further accelerated this phenomenon. A few illustrative examples of COVID-19 related innovation acceleration where blockchain might make a conducive contribution for even more effective IP ecosystems may thus illustrate the potential, which blockchain applications or their sub-functions could have for even further improving our innovation ecosystems.

The crisis triggered by COVID-19 has forced companies and organizations, small and large, to accelerate their digital transformation permitting the continuation of their activities during an exceptional situation which changed the habits of the public in general, and consumers in particular. The world has quickly turned digital. Business needs to rapidly adapt to this new scenario where communication channels are now different from those that the industry and citizens used when 2020 began.

The 4IR disruptive technologies are playing a key role in supporting the COVID-19 response and recovery efforts in emerging markets, opening up new opportunities for an accelerated blockchain adoption of blockchain technologies. For example, the so-called “maker community” addressed the shortage of face masks by distributing 3D templates which could be manufactured at home and by small businesses equipped with 3D printers. The same technology provided rapid-response possibilities for the production of alternative oxygenators. The possibility to digitally share blueprints allowed manufacturers and logistic distributors to adapt to the situation. All of a sudden, households became the center of productivity and economic activity, resulting in a surge in the adoption of homeworking and remote working technologies. Companies with advanced digital transformation facilities and programs in place adapted faster compared to those who still were traditional “brick-and-mortar" businesses. Finally, the pandemic fostered adaptability, imagination and creativity across many cultures and businesses, both in private and public circles. It created opportunities for new and emerging business models and potentially a new generation of IP assets, paving a pathway for an accelerated adoption of blockchain and other emerging technologies.

Innovative niche players in the medical and biotech device market teamed up with larger manufacturers and were funded via government initiatives to quickly find answers in treating the victims of the pandemic. 3D printing was used to quickly evaluate prototypes and effectively scale up production. AI allowed for the effective tracking and tracing of research, detecting possible remedies and following up in real-time on the spread of the virus and its variants as well as enabling an early detection of possible hot spots so that effective measures could be taken. This agility is key when it comes to evaluating the applicability of blockchain in various domains. It should be noted that all these players operated in an open network in which information was exchanged, and thus, a collaborative approach could be the cultural change required to better exploit the network capabilities that blockchain offers.

Open exchange and innovation networks were also key factors for innovation ecosystems responding to COVID-19 when it came to optimal availability and disclosure of genetic sequence data for the development of diagnostics, therapeutics and vaccines. COVID-19 showed the importance of such disclosure for any concerted innovation response to the pandemic. Through the availability and real-time exchange of such data, globally effective diagnostics and vaccines could be developed at unprecedented speed. Innovators need strong legal certainty and incentives to disclose their sequence and related research data. Data management practices of scientific databases and repositories, however, presently do not always maximize legal certainty from an IP perspective, because when such data are disclosed most often four critical elements of IP information could be lost: (a) the date of disclosure; (b) the scope of disclosure (i.e., the original disclosed sequence) (c) the version of the sequence data (sequence data are continuously optimized and annotated); and (d) the nature of disclosure (i.e., data on nucleotide sequence vs. natural biological function vs. technical use). The absence of such information has been found to create legal uncertainty and disincentives for innovators to disclose data for public health uses. Solid processes would enable a more vibrant innovation ecosystem for accelerated public health responses and in such narrow use cases certain sub-functions of blockchain applications might provide improved legal certainty, disclosure incentives and thus public good inputs for vibrant innovation ecosystems.

Despite uncertainties concerning the post–COVID-19 economic outlook, emerging markets are expected to experience an acceleration in the adoption of disruptive technologies and a proliferation of online business models and platforms, offered by blockchain and related technologies. Furthermore, the need for more cloud computing capacity and a surge in demand for electronic devices, both for professional and leisure use, caused a shortage in electronics and may cause a long-term effect in several industries, which is undergoing a major transformation. The result is that the major players are making significant investments in increasing their production capacity spread around the globe designing scalable and low-energy consumption components. Given the fact that blockchain may require an investment in scalable and sustainable computing, these investments are potentially going to give a boost to blockchain and related technologies in various aspects like tracking and tracing components, IP and logistics. The increase in capacity will also allow for the scalability and sustainability of blockchain solutions.

The opportunities presented by 4IR are far-reaching. Organizations, businesses, and individuals that hope to take advantage of 4IR in the post-pandemic scenario will need to rethink their strategic approach to leveraging technology and digitalization. In adapting to 4IR, they will have to reposition technology as a critical component for each sphere of specialization and learn the relevant digital skills to become creators and users of these tools.

This rapid digital adaptation brings new challenges in many sectors and social activities. Retail industry has seen how stores need to coexist with the digital channels to be able to continue operating, impacting their logistics and their relationship with their customers or investors. Leisure industries, like cinemas, theaters, events, trade fairs and concerts got canceled; allowing for the home entertainment business such as Netflix and Microsoft Xbox to become household names and forcing an entire industry to revise its distribution strategies and explore new technologies like virtual and augmented reality.[[6]](#footnote-7)

The logistics sector has become a key player in the new business model ensuring traceability and real-time information on the delivery of products purchased on e-commerce platforms. All documents related to the delivery are no longer in paper format but digital. Consumers have become more and more reliant on online shopping, even for basic goods. Customer experience now includes ensuring that the provenance of goods is safe, environmentally sustainable and fairly traded and supply chain traceability makes this possible, making it easier to choose on which marketplace to purchase the goods. Both local and global logistic chains were affected by the pandemic. Local businesses, especially restaurants and groceries, had to adapt and provide home-delivery services using social media and online stores as a means of ordering. Large corporations had to revise their supply lines and look for alternative regional and local sources for procurement and production of goods as globalization got affected by the pandemic. Blockchain can be used to track and trace goods and innovation inputs, and prove their authenticity, preventing fraud and counterfeiting.

Payment methods should be adapted to the new business models. Many companies do not have any physical relationship with their customers and they only accept electronic payments, which require boosted electronic identification systems, such as the use of electronic signatures, electronic certificates or seals and third-party verification systems. This can facilitate direct and completely online transactions for intangible goods based on IP.

With the pandemic came also a surge of cybercrime activity. Several large companies and hospitals everywhere became subject to cybercrime attacks requiring rapid responses. This revealed major flaws in the security system of the digital supply line of software updates and patches. Blockchain and smart contracts could provide elements of solutions to ensure the authenticity of software versions and patches.

The rapid transformation of the business processes towards remote working and home-working technologies is increasing the necessity of protection against cyberattacks, and personal data is more accessible. Furthermore, as remote consultation in industries like banking and medicine is becoming more and more frequent, secure and reliable tools and technologies are required to address privacy and remote diagnostics. Blockchain could be an effective solution in order to fight identity fraud.

Numerous contractual relationships between companies still require that contractual transactions, which are to be documented in writing be verified by the physical signature of documents in the presence of a notary. In fact, physical signature and paper still takes precedence, otherwise doubts arise over the legal certainty and reliability of the generated electronic evidence. In numerous legal and administrative steps that are necessary for the acquisition and exercise of IP rights over data, such notary verification is required. The volume and velocity of data generation by digital transformation, however, makes such notarial confirmation impractical. This applies, for example, when IP owners seek to document their trade secrets or prior user rights over sub-patentable research results, lab notebooks, genetic sequence data or other biological characterization data. Blockchain could be ideally suited to fill the resulting gap of proof of existence and timestamping by acting as a digital ledger.

To summarize, the global digitalization of the supply chain has cut out many middlemen in distribution and supply chains. Both global and local players are required to reposition themselves, e.g., by setting up online stores and participating in digital marketplaces, fostering creative and innovative ways of doing business in a post-pandemic world. As organizations are adapting and accelerating their digital transformation strategies, blockchain can provide a value-added potential building block for increasing legal certainty, operational efficiency, effectiveness, accessibility and inclusiveness of global IP ecosystems.

## BLOCKCHAIN TECHNOLOGY AND ITS POTENTIAL

Bitcoin is the most famous use of blockchain technology, but as an enabling technology, blockchain is far more than just Bitcoin. To understand the Bitcoin creation, not only as a currency, but as a technology and protocol for the exchange of digital assets, we must first understand its philosophical nature. In 2009, numerous scandals related to the banking world, together with the severe economic crisis that hit practically all developed countries, reduced the certainty that many citizens previously had that their money was safely secured. The mistrust generated by the banking systems caused Satoshi Nakamoto (pseudonym of a person or group not yet identified) and other experts in technologies and mathematics (among other disciplines) to start looking for a decentralized solution, that is, one that did not need a banking intermediary, through which people or entities could make and transact value exchanges.

In a viral [TED Talk](https://www.ted.com/talks/mike_schwartz_the_potential_of_blockchain#t-21530) on the potential of blockchain,[[7]](#footnote-8) specialist Mike Schwartz praised “blockchain for enabling an economy between machines”, redefining our world just like the combustion engine, the telephone, the computer, the internet did – each at their own time. Blockchain also has numerous applications: all kinds of assets can be stored like tokens, from cryptocurrencies to computer programs or smart contracts, as well as any other type of information. Such new technical capabilities in the digital environment have massive implications for the management of all kinds of intangible objects, including especially those which are the subject of IP protection. Therefore, the emergence of blockchain as an enabling technology has extensive implications for the future functioning of the existing IP systems.

The birth of blockchain supposes the discovery of a new system that allows participants who do not trust each other to maintain a consensus on the existence, status, timing and evolution of a series of shared events. In other words, blockchain applications can create an immutable record of transactions, linked to participants, that does not give rise to opportunities for fraud, given the characteristics of the technology on which the record is based. The possible mistrust between participants is resolved through the existence of a global network of computers, characterized by nodes that consensually validate all the transactions taking place on this network and therefore managing the distributed database.

The difference with respect to the systems used extensively at present lies in the fact that these usually involve a higher operating cost due to the security systems they use and are not guaranteed to execute in an idempotent way on remote systems creating conflict or dispute risks. Contrary to these, blockchain provides a secure and resilient system, but at the same time relatively cheap and flexible, which makes it possible to build applications that connect with the blockchain system in real time with greater dynamism.

The fact that a blockchain database is unalterable is due to its cryptographic and decentralized nature, since its information is distributed in multiple nodes that contain an updated copy of it, which at the same time is protected by cryptography. Structurally, a blockchain database is organized in blocks of transactions that are mathematically related to each other in a chained way, so that modifying a block would be impossible since it would generate a discrepancy in the system with respect to the rest of the blocks that would invalidate the transaction.

The participants of a blockchain do not authenticate themselves through a user session (login with username and password, as in traditional systems), but rather they use pairs of signature private keys (cryptographically related) that are generated automatically. These signature private keys provide access to modify ‘owned-by-signer’ assets in the ledger database, allowing the smart contract and network consensus to check the validity of a transaction carried out within the network.

When applied in real-world applications, blockchain enables users to maintain and control the use of their own data such as personal data, contents and transactions by ensuring that this information cannot be altered, copied, or otherwise manipulated during transmission thanks to the immutability that blockchain provides. Furthermore, by using smart contracts to facilitate trade across the blockchain, users can undersign transactions via smart contracts and receive tokens, i.e., coins, representing a certain value or the right to use a service/asset as agreed via the smart contract.

Blockchain’s inherent main characteristics are summarized as follows:

1. Decentralization: blockchain is characterized by the absence of a central entity that mediates transactions between actors who do not necessarily trust each other. In a blockchain network, the same protocol is shared by all the participants of the network, which has pre-established rules that all must comply with;
2. Distributed ledgers: blockchain is a network of identical ledgers shared and synchronized across multiple sites, bodies or geographies which allows recording the transactions performed in multiple places at the same time;
3. Immutability: once a block has been included at the end of the chain, it is permanently stored in the blockchain without the possibility of modification. This ensures the integrity of the data incorporated into the blockchain. The resolution of conflicts in the network is governed by a series of pre-established rules that are defined in the smart contracts. The integrity and deterministic execution flow of such smart contracts is also guaranteed;
4. Consensus: since the accounting book or ledger-database is kept independently by each of the system nodes in a copy that they store, there are consensus algorithms that regulate the method by which the true state of the network is reached. The objective is that all the nodes agree on which one is the next block to incorporate and subsequently said block is mined; and
5. Encryption: based on public key cryptographic protocols, participation in a blockchain implies that any user on the network has a unique identifier associated with their public key, which could potentially be linked to blockchain-based digital identity solutions.

Blockchain can further be enhanced, among others, with the following features, which are further explained below:

1. Tokenization: in an easy way, tokenization may be defined as the process of converting physical, financial or intellectual assets into a digital token. Normally, one asset is broken down into smaller parts which become many tokens in the blockchain. Once the asset has been tokenized, the owner can trade it in the digital world which could affect the asset complete or partially. The simplest example is to move a bank account with cash to the blockchain where the blockchain infrastructure will replace the bank office and the cryptocurrency tokens are used instead of physical coins. A token is a digital representation of an item reflecting its value.
2. Smart Contracts: the term ‘smart contract’ was originally coined by Nick Szabo and relates to software automating the terms of an agreement which reflects a digitally specified agreement and the protocol performed by the partaking parties on the agreement. Blockchain enables automatic idempotent logic execution replication between machines through them, which are nothing more than code extracts that determine actions to be executed when certain pre-programmed conditions are met.
3. Automation: Blockchain enables numerous possibilities around the scheduling of automated transactions based on predetermined conditions. These conditions can be programmed based on any information that enriches or feeds the database, coming from both internal (on-chain) or external (off-chain) sources. The information received can therefore be used to condition certain actions. This automation is possible or can be further facilitated if the blockchain system is connected to other frontier technologies such as AI and machine learning.
4. Self-Sovereign Identity (SSI): Blockchain enables SSI or the decentralized identity that users should be able to create and manage their own identity, without relying on any centralized authority. SSI is based on the use of the Decentralized Identifiers (DIDs) which are a form of digital identifiers that can be used within a blockchain context to identify a natural person or a legal entity and validate an identity.

## BLOCKCHAIN BASICS

In practice, a blockchain network involves a set of computers or servers (nodes), connected to each other and sharing the same communication system known as a protocol. The main mission of the nodes of the network is to validate the transactions that take place within it and to store the registry of the system information, thus ensuring its integrity. To do this, these nodes have to act under the same rules, that is, communicate through the same protocol, since the evolution of blockchain and the participation in its ecosystem by numerous actors has led to the creation of numerous communication protocols based on this technology and that are usually aligned with the needs of each platform that is based on it.

The blocks are related to each other using cryptographic algorithms that, through hashes, relate each block to the previous one and so on, until reaching the genesis block (the origin of the chain). The blocks are appended to the chain depending on an agreed consensus mechanism. Consensus mechanism defines the security of the blockchain by maintaining consistency across the network and enables the blockchain network to attain reliability and build a level of trust between different nodes, while ensuring security in the environment. Consensus can be achieved through various models and some of these models are outlined below:

1. *Proof of work:* Proof of work (PoW) is notably used as the consensus model behind Bitcoin and a number of cryptocurrencies. The PoW model requires users, who wants to publish a new block be the first one to solve a computational puzzle to demonstrate work has been done to gain the solution to the computational puzzle. The user who first resolves the puzzle will have their solution verified by other nodes on the network. The puzzles are designed in a way that is hard to solve and easier to verify. When other nodes verify the solution to the puzzle submitted, the solution is either accepted or rejected in accordance with established consensus requirements.[[8]](#footnote-9) If accepted, the user submitting the correct solution to the puzzle is rewarded or incentivized for work done adding a new block onto the blockchain. The users, who are solving the puzzle to add a new block onto the chain are often referred to as ‘miners’. As in the case of Bitcoin, with the value of the incentive or reward increasing, the difficulty of the puzzle increases and more compute is required to solve the puzzle/ mine the new block. It is vital to consider the cost of compute and energy consumption when looking at the PoW model.
2. *Proof of stake:* The Proof Stake (PoS) is consensus model is funded on the basis that more stake or investment one has in a network the more likely the investor wants the system to succeed and less likely one would sabotage their own investment.[[9]](#footnote-10) In the design of proof of stake model, stake is held by a facility/ arrangement established by consensus. The ability of a user to succeed in publishing a new block on the chain is proportional to their stake invested in the chain.[[10]](#footnote-11) This model is not as reliant on compute to prove ability to add a new block on the chain. However, the additional complexities are introduced in the design to approach securing the intended proof by stake outcome. One of the ways to achieve such is through Byzantine Fault Tolerance (BFT). BFT relies on the assumption that majority of the nodes in the chain is behaving as intended, a majority of the node could vote to agree an execution, this is seen as consensus. A risk with BFT model is that an agreement may be prevented from reaching when there are a significant malicious attack or faulty nodes.[[11]](#footnote-12) A notable application of BFT is in Hyperledger. As opposed to PoW which necessitates a large amount of energy with miners needing to sell their coins to eventually cover the costs, the PoS grants mining power based on the share of coins held by a miner. The PoS mechanism is more suitable in environments that can work with dependable nodes and may require a more tailored mechanism to assign computational tasks.
3. *Proof by authority*: This consensus model is a commonly used and applicable consensus model to permissioned blockchain networks. For proof by authority to be implement, nodes on a blockchain network must have their identity at least visible to the ‘owner’ or the managing authority of the chain. The node seeking to publish a new block is staking its reputation and/or authority to publish.[[12]](#footnote-13) As a result, a node can lose its ability to publish or access to the blockchain. This application only works on networks where the identity of on-chain nodes to off-chain entities is verified and can be trusted. This model is likely to be used in network arrangements, such as where all nodes are attached to off-chain entities with a high level of public trust and reputation. It is therefore in the entity’s interest to maintain their reputation and trust by following the consensus.
4. *Round Robin*: This consensus model is more suitable to a permissioned blockchain, where the identities of the nodes are known and verified off-chain. Round Robin works by permitting all nodes on a chain to take turns in adding a block to the chain.[[13]](#footnote-14) This ensured that no one node is able to create the majority of the blocks. If a node in line to publish a new block is not available or unable to publish a new block, a time limit set for each interval to publish a new block and a blockage is not be caused, preventing other nodes from publishing their new block when the time is up.[[14]](#footnote-15) It is important to note, Round Robin is not an appropriate model to be used on permissionless networks, as malicious actors could generate unlimited nodes to cause blockage and halt the network.

Depending on the strategic interests of the actors involved, the blockchain can gradually variate from a pure decentralized (permissionless) system – e.g., Bitcoin, to a private (permissioned) one governed in accordance with the interests of a few concerned parties – i.e., closed blockchains. Both types of blockchain present different characteristics. The first blockchain networks were public, mainly due to the philosophy behind blockchain that seeks absolute transparency and ease of adoption by the maximum number of users.

1. *A public/ permissionless blockchain* is one whose access and participation are open to any user, without the need for them to have any specific type of permission. Any user can also be the owner of a network node and help maintain it, provided he has computing power at his disposal. Anyone with internet access can both observe, download, validate and send transactions on a public blockchain. In this type of network, all participants are equal, and therefore have the same rights within the network. The maintenance of the network is ensured thanks to economic incentives that are granted to the owners of an active node that confirms and validates transactions, also known as miners. Furthermore, the solution operates in a fully decentralized governance model using the notion of consensus to write records to the blockchain. The best known public blockchains are Bitcoin and Ethereum, famous for being the first open-source blockchains that serve as the basis for the most widely used cryptocurrencies.
2. A *private/permissioned blockchain* is one created by an entity for internal or restricted use. Access to users outside the process is totally restricted, and it is not possible to have read or written permissions. Each node of the network is controlled by the same entity, which is in charge of its management and maintenance. Essentially, it is operating under a centralized governance model. The characteristics of these types of blockchains make them very valuable tools for a company, since they can make applications based on blockchain for their processes in a completely opaque manner, taking advantage of its attributes like security and immutability of data without the risk of exposing any type of information. Although the infrastructure can be based on an open-source solution, the applications that run on a private blockchain are usually proprietary, being developed specifically for the needs of the specific company, institution or community. Another important feature is the absence of compensations via tokens. Since the process of appending blocks is carried out privately by the infrastructure owner, there is no need to reward the nodes that maintain the network, so more efficient consensus algorithms can be used that prioritize performance and scalability, over the total decentralization that characterizes public blockchains.
3. One can speak of *hybrid blockchains*, also called permissioned, as an intermediate case between public and private ones. Although they are private in nature, in the sense that they are promoted by a private entity or a consortium, they are open to those members who have specific permissions or have a license to operate on the network, factually operating under a centralized governance model. The isolation of the different processes within a hybrid blockchain is guaranteed; an agent can make transactions that are completely opaque to another member who does not have read permissions on those transactions. This type of infrastructure is especially powerful since it promotes the decentralization of complex services between companies, institutions or communities, because different actors can operate on the same blockchain independently, without the need for a central body that governs the infrastructure, eliminating any trust problem that may exist between the different agents that make up the platform. Currently there are different consortia that make use of hybrid blockchain to bring together various companies, institutions or communities in the same sector- or multisector actors with common interests- and thus create a network that everyone can use for their internal processes independently or jointly, depending on the desired configuration. In Spain, the clearest example is the Alastria network, a hybrid blockchain based on Quorum that allows companies from different sectors to operate their applications for the network in a way other than the rest of the members through a system based on licenses issued by the consortium administrators.

|  |  |
| --- | --- |
| Permissionless | Permissioned Lock with solid fill |
| No central authority, implementation of the trustless network concept. | A central authority or special roles are established to regulate the blockchain. |
| Anyone can publish a new block in accordance with the consensus model, without need for approval or authorization from an authority. | Publication of new blocks are regulated or authorized by authority, either through a single trusted party or decentralised authorities. |
| Anyone who has downloaded the software to access the blockchain can read the chain as well as write to the ledger. | Read access to the blockchain maybe restricted and not open to public. |
| Permissionless blockchains often require more or increasing compute to prove the publication of a new block by design through algorithms. | Often require less resource or compute to establish user’s authority to publish a new block. |
| Consensus often focuses on design/ rules on proof, which prevents malicious attacks through increased cost to commit such. | Consensus often establishes roles, permissions, levels of access and authorities for difference users or user levels. |
| Often developed using open-source software and downloadable by anyone. | Network maintenance, including software updates are often a responsibility of the authorised entity or owner(s). |

[Table 1: Permissionless vs. Permissioned]

One of the first questions to analyze when implementing a blockchain system is to decide the type of blockchain to use, whether public, private or hybrid, taking into account their characteristics. Furthermore, it is important to understand what kind of consensus mechanism is required and what kind of “mining” pool may be acceptable – a large number of varying nodes or a small stable pool of nodes.

For example, in case a company, institution or community would want to license an IP right to potential partners, the chosen blockchain implementation should allow for a smart contract to be signed so that both parties can undersign the transaction, register the transaction in the blockchain and exchange and store tokens in a wallet (holding other tokens, proving licenses to other IP assets) which represent the value and proof of the license. In a similar way, should the IP license be used in a product or service and a consumer used that product or service, this could be registered in a blockchain and a token could be used as proof of the same. Depending on the rules set forward in the smart contract, the licensee could then have to transfer part of the value he or she received to the IP asset owner as a role. In that sense, the proof of ownership, the proof of license and the proof of legal consumption of the service can all be represented in different types of tokens having an interchangeable value. Within a fully decentralized blockchain the different users are responsible for storing their identities and tokens safely in a so-called wallet. However, to avoid the risks of losing and tampering these assets, specific centralized wallet services have been developed as part of the blockchain solution landscape. Each time a transaction is carried out, the nodes must validate the block and the information it contains, so that, once this process is completed, the information will be incorporated into the chain and, from there on, it will remain unchanged. This eliminates the need for a trusted third party to supervise and validate the process, if not for it to take the form of tens, thousands, or even millions of nodes.

## BLOCKCHAIN IMPACT

The fact that blockchain has the potential to fundamentally transform a wide range of industries and markets has led international and regional organizations to launch projects or adopt guidelines in the fields. For examples, the Blockchain Policy Centre and Forum of the Organisation for Economic Co-operation and Development (OECD)[[15]](#footnote-16) where policy aspects, like standardization and governance, are debated and information and opinions exchanged; the United Nations Conference on Trade and Development (UNCTAD) issuing a paper on “Harnessing blockchain for sustainable development: prospects and challenges”[[16]](#footnote-17); the Joint Inspection Unit (JIU) of the UN Systems publishing a paper titled “Blockchain applications in the United Nations system: towards a state of readiness”[[17]](#footnote-18) which contains eight recommendations for either the governing bodies or the executive heads of the UN system organizations; the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) Blockchain White Paper Project[[18]](#footnote-19); and the European Union (EU) Blockchain Observatory aiming to accelerate blockchain innovation and the development of the blockchain ecosystem within the EU[[19]](#footnote-20). Initiatives in the private sector are also multiple, such as the International Chamber of Commerce (ICC) projects on blockchain-backed Incoterms[[20]](#footnote-21) and the creation of the International E-Registry of Ships (IERS) which is the world’s first blockchain-backed digital shipping registration and renewal system. These initiatives are leading the way on how societies will interact with the governing bodies.

While some of the above mentioned projects focus on expanding the potential benefits of blockchain technologies to developing countries, certain developed economies are already implementing their own projects. This is the case of the UK government’s project to use blockchain and other Distributed Ledger Technologies (DLTs) to verify the provenance of goods; the project of the US Department of Agriculture to use blockchain to streamline the functioning of complex agricultural supply chains; or the case of Estonia, where citizens have full access to a suite of e-government services and interact fully digitally with public instances. Furthermore, a number of governments around the globe have established Blockchain guideline and roadmap documents that lead the direction and benchmark considerations required of government entities prior to engaging in blockchain implementations or provision of service aided by blockchain technology. For example, the National Institute of Standards and Technology of U.S Department of Commerce has published Blockchain Technology Overview[[21]](#footnote-22), in 2018, which serves a comprehensive survey of Blockchain technology and identifies that the use of blockchain technology is not a silver bullet and considerations must be paid closely to dealing with malicious users, control and particularly for government entities the considerations of operational and governance.

According to Gartner´s 2020 reports on blockchain,[[22]](#footnote-23) enterprises are beginning to deploy blockchain-inspired solutions, requiring that the implemented architectures and technologies be reconsidered to allow for optimum exploitation of blockchain with the least possible business friction. However, blockchain is still at an early stage, lacks standardization and has a variety of divergent implementations. As the technology further matures, leaves the enterprise perimeter and can be used to facilitate and automate business transactions such as by using the smart contracts, public institutions and governing bodies should be ready to govern and regulate the usage of blockchain in a wider business-to-business context. They should facilitate standardization and ensure legal certainty when using blockchain in a digital economy. This also applies with paramount importance for the public institutions and governing bodies in the IP ecosystems, who should facilitate adequate Member State driven governance, systemic coherence, standardization and legal certainty of blockchain applications for IP.

The fact that industries are not yet widely adopting blockchain has more to do with the big changes it implies (e.g. sunk costs and switching costs) than with the learning curve of its technological complexity. Blockchain is forcing industries to rewire their brain around major concepts – transactions, interactions, and money will no longer be the same. In fact, trade is undergoing the biggest change since the shift from barter to the emergence of the money form as a general equivalent for the exchange of economic value. Furthermore, we get to experience a new level of freedom and trust due to the transparency it offers and the removal of middlemen. Therefore, it has been maintained that blockchain is more than a technological change: blockchain adoption implies a cultural change.

Gartner believes the market will climb out of this ‘Trough of Disillusionment’[[23]](#footnote-24) over the next two to three years as pragmatic use cases are deployed and the technology evolves. Market analysts expect that de facto standards (especially for data formats) will become more apparent, enabling better interoperability with less complex and costly integration. Moreover, leading software vendors, like Microsoft and IBM, will increasingly integrate blockchain technologies as a feature in their enterprise software.

While it is true that the speed of evolution and diffusion of blockchain and other DLTs) is overwhelming for many stakeholders, it is still a technology that is at its early stage of development and adoption. We should also bear in mind that blockchain, compared to other emerging technologies, has a much higher speed, given the revolution that it represents and the amount of diffusion it has had, thanks to Bitcoin and other cryptocurrencies being implemented and supported by open-source communities.

### Value creation with blockchain applications

Blockchain has the potential to advance an internet of value, in which a value chain of digital assets can be realized using blockchain, governed by smart contracts, represented by tokens, and run by distributed and self-sovereign identities without intermediaries in transactions. Such new value chains will disrupt current value chains and requires revised or even new sets of standards, regulations and guidelines.

Blockchain itself has been a Bitcoin enabler. In a similar fashion, blockchain can offer a technological basis and act as a common enabler for new innovative value chains. The self-sovereign identity can be implemented on a blockchain, removing the need for an intermediary to validate identities. Smart contracts, using the DID and the potential of AI can create a completely new way of automating trading, allowing an automated process to gain insights in a trade pattern and optimize purchases and/or selling power for participating parties, creating added value in a specific value chain, which can then be valorized using tokenization. The whereabouts of the assets subject to these transactions can be traced and tracked both in a virtual and real-world setting, understanding who originally owns the digital assets, where they were and are, and whom the assets were transferred to. Given that the underlying technologies are based on established encryption methods and implemented according to the immutability principle, all transactions provide confidentiality, integrity and availability at all times and provide a complete and tamper-proof historical transaction record.

To understand how to apply blockchain to each particular situation, a deep understanding of the different solutions that exist today based on this technology is necessary, identifying the potential for disruption and the process reengineering capacity offered by each one of them. There is an increasing interest in the application of blockchain and related technologies both within private and public organizations. Several organizations have taken their initiatives and experimented with the technologies. However, the outcome of these experiments and early adoptions of blockchain technologies remain inconclusive on its long-term sustainability and scalability.

Blockchain, in addition to encouraging the evolution of companies, institutions and communities towards more efficient and secure systems, enables the creation of new business models that were not possible before this technology, at least in such an efficient, fast and secure way. The ability of blockchain to generate greater interoperability between companies, institutions and communities of practice as well as to digitally represent any asset and carry out transactions with it, generates a new value exchange scenario that allows untrusted and untrusting entities to collaborate in different areas. This, consequently, favors the creation of new business models, products and services. The internet of value, therefore, comes to replace the internet of information, which enables the transmission of information in real time as well as its capitalization in business models with a new ecosystem that enables the transmission of value under the same framework of immediacy and efficiency.

As we already know, blockchain was born with the intention of enabling monetary transactions between users without the need for a trusted intermediary, so one of its main applications falls on the creation of self-regulated business models that do not need intermediaries for the exchange of value among end users or customers. This application generates a new paradigm for companies and institutions when it comes to empowering their customers and evolving towards peer-to-peer models in which the company or institution becomes, on many occasions, a mere provider of technologies and platforms, leaving all the prominence to the user and even rewarding them for helping to build a more efficient model.

## PROMINENT USE CASES OF BLOCKCHAIN

Blockchain as an underlying technology can facilitate several use cases and challenges faced by current technologies.

### Digital Identity and its management

Today, the identity of citizens faces several problems, for example, the duplication or fragmentation of citizens’ identity, even in the form of digital signatures and certificates, depending on the entity or organization with which they relate, the lack of security with respect to the management of personal data and the lack of data control by citizens themselves.

Blockchain technologies open a world of possibilities around the management of personal information and the identity of the users to which it is linked. The capabilities of blockchain to manage identity, represent the evolution towards a new model that is based on and focuses on the empowerment of users with respect to the management of their personal data, as well as the possibility of enabling new business models in which they themselves can manage the information they want or need to share with external agents. This enables the generation of new business models around the exchange of information between companies that previously had isolated information systems, even allowing users to be rewarded for sharing additional data, in addition to eliminating the need for a central body storing or managing such data.

To solve the problems generated by separated information silos for which separate user identities are required, blockchain allows users of the network, such as a natural person, a legal entity or thing, their sovereign identity that could link any information to themselves stored in the blockchain. This identity model is already being defined in different environments such as SSI, a decentralized identification system that allows generating a digital identity for its users using blockchain technologies. According to the DID specification of W3C[[24]](#footnote-25), DIDs are a new type of identifier for verifiable, "self-sovereign" digital identity. DIDs are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority.

Once the information provided is stored in the blockchain database, the owner of such information can choose with whom to share it and to what level. This information, given the characteristics of blockchain, is kept encrypted against forgery. The registration and identity management capabilities offered by blockchain present an opportunity for companies to generate new business models that are based on the provision of authentication and identity management services, as well as the data associated with them.

78. While in the current model, innumerable identity checks are carried out daily by all market players and independently, by using blockchain it is possible to achieve a level of interconnection between databases that would automate this current system to the maximum. For example, that would be possible thanks to a blockchain platform such as the accounting book that records identity transactions and manages the sharing of information necessary to activate each service provided to the user based on what is indicated in the smart contracts. In this way, consequently, the generation of synergies and interoperability between different databases is enabled, facilitating the sharing of sensitive information in a secure manner and without giving rise to fraud.

79. Subject to permission considerations, identity verification and management play a varied level of importance in the design and management of a blockchain network. For permissionless blockchain networks, usually nodes or parties that are participating in the chain remain detached from their off-chain identity, often through pseudonyms. Identity verification plays a relatively small part in providing access to the blockchain, with the exception of public and private key authentication.

For IP ecosystems, there may be frameworks and policy requirements that IPOs are subject to under their national government or legislative directions in managing digital identities. Some of the required assessment that IPOs should consider when implementing public facing blockchain solutions include, an independent privacy impact assessment, and an independent security assessment, ICT penetration test, and treatment plans on privacy protection, security and fraud control and accessibility and usability.

### Traceability

Traceability is the ability to trace the entire lifecycle of an asset within a blockchain from creation to its current state which ensures credibility, efficiency and safety. Blockchain technology makes it possible to ensure the safe storage of the information stored in its database, as well as to program automated actions that are activated based on the data they contain. Thanks to blockchain, we can achieve full traceability of information, people and things, especially if we take advantage of the integration capabilities of blockchain databases with external other technologies or data sources such as IoT. Currently, numerous entities are conducting proofs of concept around the traceability of their resources and products, taking advantage of blockchain to offer their customers true information about what they buy, while optimizing their logistics processes to reduce their time-to-market and operating cost. Under this new paradigm, the opportunity arises for certain entities to assume the role of data management, focusing their value proposition on the intelligent tracking and tracing of assets.

### Transparency and Fraud prevention

Blockchain has the advantage of providing the user with a greater degree of transparency in real time and under a strong layer of security, which can significantly reduce the risk of fraudulent transactions.

The high level of transparency, immutability and the intentional lack of intermediaries, that blockchain offers, means that the information that exists within the network generates a higher level of responsibility over its participants than other databases. This level of responsibility exists in the absence of a trusted third party who has to ensure or validate the veracity of the data, since the guarantee of the same falls on the network itself and its participating nodes. Data encryption and the distributed network increase the security level of the information, have the information unalterable and reduce the risk of fraud. Furthermore, a consensus that should be carried out between the nodes of the network for a transaction makes the blockchain detect and prevent in real time all kinds of fraud and negligence within the network.

Blockchain has the ability to transform current systems towards a more transparent model in which information can be constantly verified throughout the life cycle or value chain of a resource, product or service. Through the use of blockchain, we can verify in real time who is the owner of a good or asset and the information linked to it and transfer its ownership to another participant of the network without giving rise to fraud. In other words, the level of traceability of the information that blockchain provides us in combination with the need for a consensus to exist to carry out any transaction minimizes the incentive for fraud as all the activity can be visible to the public on a public chain.

One of the main uses of the above is the verification of the legitimacy of luxury and second-hand goods, such as diamonds, since blockchain allows the use of physical elements such as cryptochips that are connected in real time to a blockchain database and verify their identity and linked information, allowing the client to confirm their legitimacy through the front-end of an application in a simple way. In this way, for example, users could use their mobile device to read a Near Field Communication (NFC) or QR code that tells them if the product they have purchased has the appropriate certification.

Blockchain does not stop or prevent fraud but makes it harder to commit and has an ability to detect errors within the network. Blockchain also acts as a deterrent as it increases the integrity, traceability, security and transparency of the transactions made by all the parties of the network. The fact that a database is based on blockchain technology implies that verifiable records of every transaction are stored by consensus, leaving a permanent and timestamped evidence for every stage of the transaction, and provides the ability to analyze and detect the veracity of the information in real time so that patterns of fraudulent behavior can be detected and stopped instantly. In addition to the fraud, risks can also include a human error can lead to an incorrect execution of certain processes, as for example in the case of payrolls. Through blockchain, we can ensure the execution of the clauses of a contract automatically without giving rise to error, consequently avoiding the cost derived from claims and legal processes that may arise due to this type of errors. In relation to this, numerous potential business models have emerged, the best known of which consists of automatically refunding the amount of an airline ticket in the event of a flight delay.

### Smart contracts

Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. In 1994, Nick Szabo defined smart contracts as ‘a computerized protocol that executes the terms of a contract’.[[25]](#footnote-26) Smart contracts store the agreement between the parties written into code on a blockchain. The conditions of the agreement are implemented and executed within the networks of computers part of the blockchain. These conditions, including the business relations and payment obligations, are immutable as well as the transactions related to this contract which are stored in the blockchain. Several blockchain implementations, like Ethereum, support a scripting language by which such contracts can be implemented within the blockchain environment.

One of the biggest benefits of smart contracts is that they are a self-executed piece of software with the capacity to act without the intervention of the contractual parties to execute or administer them, helping the organizations to automate certain aspects of their business, while still maintaining legal certainty or improving processes where trust was an issue. Once the process is completed, all the involved parties will receive the results of the transaction as agreed. If the conditional protocols are not satisfied, smart contracts will return the product to their respective owners. Moreover, the smart contract ledger will store the complete details and imposes an immutable feature on it. This means that, once the data is stored, no one can alter/change them.

On a blockchain, the undersigned participants in a transaction within a smart contract may receive tokens to reflect the nature of the transaction (e.g., royalties) and the value that transaction represents. The creation of the smart contract and related tokenization, therefore, implies bringing the discipline of law to the field of programming, facilitating the creation or transformation of business models focused on employees or clients, enabling a high level of automation in the provision of their services. Smart contracts, together with the automation capabilities that blockchain brings, promise to significantly reduce the need for middlemen and thereby reduce overall business cost. Most importantly, they save participants time by disposing of intermediaries. Many use cases can be constructed also in the field of IP and achieve just that.

Automatic and dynamic billing systems based on real-time data could be created to allow provision of personalized services to the customers, based on their data and the conditions previously established in the contract; at the same time as guaranteeing the collection of the amount of the service provided, upon activation of the smart contract after signing the contract. Consequently, the result is a higher level of customer satisfaction, improving the experience and therefore potentially increasing revenue, all while reducing costs thanks to the efficiencies generated due to reduction of the processing time per request.

### Tokenization and Non-Fungible Tokens (NFTs)

The concept of asset digitalization is not new but using blockchain technology allows anyone from anywhere to tokenize their assets in a decentralized system and conduct business using them. Blockchain characteristics such as immutability play a key role in the tokenization because transparency allows to certify the ownership of the asset to all the participants in the blockchain and trace the entire history of the activities performed with the asset. Immutability brings the certainty that the stored data in the blockchain is accurate and has not been changed by any of the participants.

Non-fungibles tokens (NFTs) are a type of cryptographic token that represents assets that can be commercialized in a digital way. They function as verifiable proofs of authenticity and ownership within a blockchain network, bearing several characteristics such as scarcity, uniqueness and non-fungibility[[26]](#footnote-27). In particular, NFTs allow their owner to possess the (digital/virtual) representation of a unique object unequivocally associated to their wallet or user in the virtual space. Scarcity is another crucial characteristic, since it is the direct consequence of uniqueness, as NFTs associated to one digital or physical object they provide scarcity in the market. Finally, fungibility is the last but not the least important aspects of NFTs, which is also contained in the acronym itself (Non-Fungible Tokens). Fungibility represents the possibility of interchanging items, whereas non-fungibility does not. A non-fungible token is not replaceable, whereas a fungible token is. The perfect example can be represented by another type of tokens, such as Bitcoin: two peers can in fact exchange a bitcoin with another bitcoin, since they bear the same value. On the other hand, two peers may not exchange two different Cryptopunks[[27]](#footnote-28) or Cryptokitties[[28]](#footnote-29) or Bored Apes[[29]](#footnote-30), since each one of them is a different item and is, thus, not replaceable. In the simplest terms, NFTs transform digital works into one-of-a-kind, verifiable assets that are easy to trade on the blockchain.

Nowadays NTFs are gaining notoriety in the creative business becoming a popular way to commercialize digital creative works. As a matter of fact, several creative works are currently being sold either solely virtually or both physical and virtual as NFTs, reaching several thousands of dollars’ worth in sales on the OpenSea[[30]](#footnote-31) platform.

## BLOCKCHAIN TECHNOLOGY SWOT ANALYSIS

Blockchain has become one of the disruptive emerging technologies from 2008 when Nakamoto introduced it with the conception of Bitcoin and it is receiving increasing attention from researchers and industries aiming to understand how blockchain can support them to become more efficient. It is easy to get carried away by assumptions that this technology offers a multitude of opportunities to solve a number of situations that various sectors face. However, blockchain also brings drawbacks.

SWOT analysis is a method of analysis that allows to identify blockchains’ strengths, weaknesses, opportunities, and threats, and is important to really understand what blockchain technology has to offer, from an objective perspective, and where it is best placed to help and bring about innovation that truly improves the world. It appears that some of the core features of the technology appear to be incompatible with areas of interest and current practices of several participants. The fact that blockchain is immutable requires due care and control prior to appending a record to the chain, as corrections come at a much higher computational cost than traditional ledgers. This results in compromised solutions being sought and implemented, causing some inherent blockchain features and benefits to be omitted from the implementation.

### Strengths

Blockchain is built upon a set of well-known security features, hence confidentiality, integrity and availability of information is warranted equally for all participants. Due to the immutable nature of the technology, an append-only immutable chain of transactions, there is traceability and transparency towards all participants in the transaction. The network-based feature of blockchain allows to build distributed ledgers across multiple nodes. These strengths should permit several industries, especially the IP community, to develop digital trade solutions whereby various natures of IP are protected, accessible and can be exchanged and traded spanning the entire value-chain.

Additionally, blockchain technology can deliver significant information processing efficiencies. Through enabling peer-to-peer “trustless” trade reconciliation and settlement, for example, blockchain can remove the need for middlemen in many processes for fields such as payments and licensing. In comparison to traditional financial services, blockchain facilitates faster transactions by allowing P2P cross-border transfers with a digital currency.

The blockchain ledger allows each transaction performed in the network to be recorded on the blockchain. This cannot only help improve security and prevent fraud in exchange-related businesses, but it can also help verify the traceability of the supply chain from manufacturer to distributer, or in the creative industry to provide an irrefutable proof of ownership.

### Weaknesses

A perceived weakness of the solution is the lack of centralized control and governance, opening doors to abuse and misappropriation of digital assets and reducing the legal certainty of a business transaction. To overcome such weakness a totally new way of thinking will be required, making the participants in the blockchain more responsible and accountable when assuming their respective roles and responsibilities in the transactional chain. Furthermore, blockchain currently has limitations when it comes to scalability and sustainability as it requires a much higher degree of computing resources and energy consumption while the consensus models are susceptible to different energy consumption and scalability. Furthermore, to some extent, blockchains have dependency to validate data on the blockchains as they are isolated networks and need associated data and services, which are available on off-chain systems. One major challenge is how to ensure, manage and enforce the quality of off-chain data which is inputted into the blockchain. As the technology is still in an early stage, there are many divergent implementations which have a vertical focus and require further focus on interoperability and standardization to ensure a wider degree of adoption.

If blockchains are widely used in the future, evidences proven by the blockchains may be more often used in the legal proceedings or other dispute mechanisms. It is therefore important to consider the issue of legal admissibility and weight of the information recorded and stored on the blockchain. Laws and regulations governing the admissibility and weight to be given to such evidence may differ from each jurisdiction, thus making it difficult to generalize about how such evidence might be treated by the courts, and because of that, uncertainty prevails.

### Opportunities

Taking into account the perceived strengths and assuming the perceived weakness can be addressed by further technical standardization, the implementation of proper data protection and authentication mechanisms, policies, and common governance practices; blockchain opens a wide degree of possibilities in tracking and tracing both digital and physical assets by the implementation of e.g. smart contracts reducing or potentially eliminating middlemen which currently are required to underwrite and validate the transactions. The technology can act as a catalyst to further accelerate the digital transformation in various industries and establish innovative fast-moving digital trade platforms which will create additional value. There is a need for a minimum set of standards and regulations to allow the development of a digital trade ecosystem, within specific “vertical” industries across which to avoid the development of stovepipes which will in the end hamper the wider adoption and interoperability of blockchain.

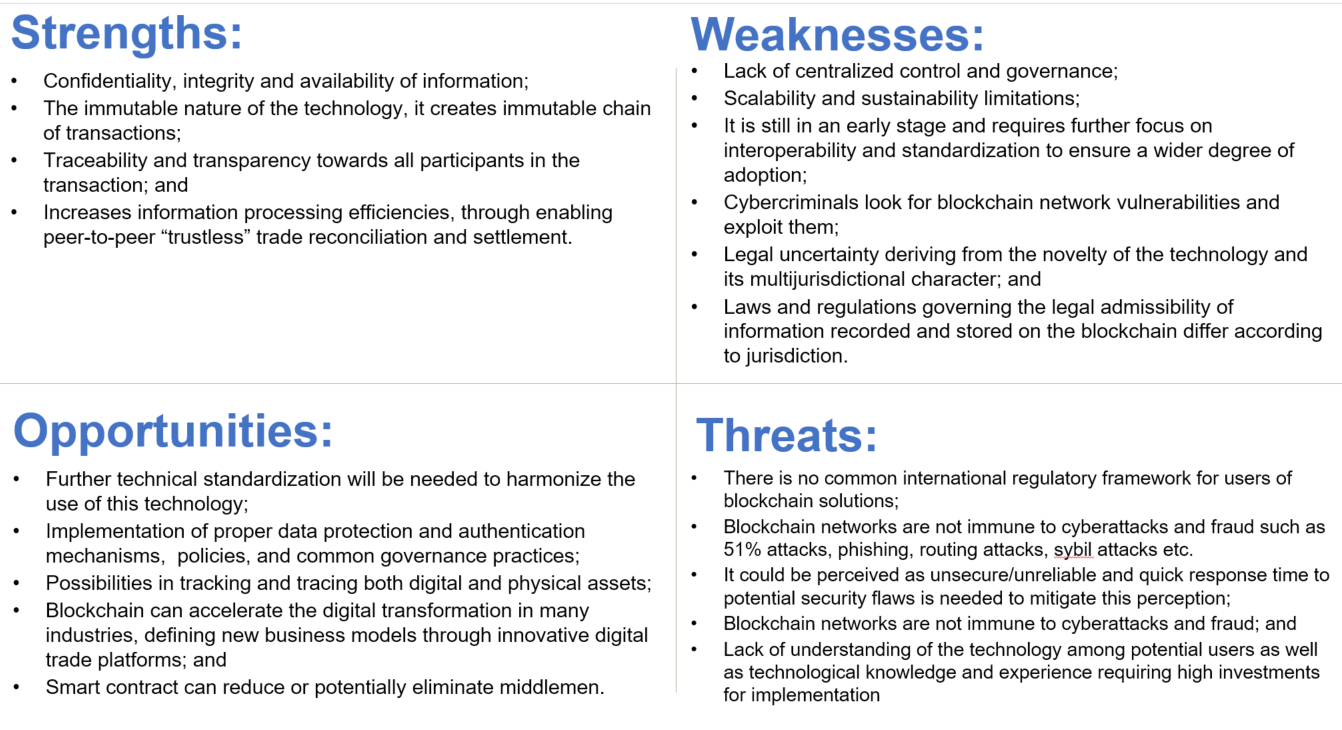
### Threats

As the technology is still at an early stage and evolving at a fast pace, there are many technology-based threats. There is no common international regulatory framework for users of blockchain solutions, which means that there is a lack of appropriate protection in the international environment.[[31]](#footnote-32)

The early adopters need to be able to respond quickly to potential security flaws, respond to emerging trends and hedge their choices when it comes to choosing from competing consortia and blockchain implementations. Many organizations will likely feel threatened by the technologies as it will affect their role and revenue stream within the existing value chain, especially those playing the role of middlemen when validating and underwriting transactions. By cutting out the middlemen required to underwrite transactions, however the freed-up resources and expertise can be used for the purpose of creating awareness and education in blockchain applications, in increasing accessibility to compute, to cover cost of compute and support the standardization and enforcement of this technology to establish common standards, policies and governance models.

The emergence of new technology requires time for the developer community to adopt it, and for educational institutions to introduce relevant training. The blockchain landscape is currently in its infancy, and therefore there is a lack of experienced developers. While blockchain technology produces a tamper-proof ledger of transactions, blockchain networks are not immune to cyberattacks and fraud. Hackers have succeeded in various hacks and frauds over the years. Here are the top four blockchain security issues[[32]](#footnote-33):

1. 51% Attacks. A 51% attack refers to an attack on a blockchain by a group of attackers gain control of 51% or more of the computing power on a blockchain and they are able to reverse past transactions that need to be confirmed and double-spend the coins and prevent new transactions from being confirmed. Since attackers can manipulate transactions that are awaiting confirmation, they can use the same cryptocurrencies multiple times as if the previous transactions hadn’t taken place, since they control which transactions get confirmed;
2. Phishing. Phishing is becoming already be a well-known phenomenon through awareness-raising campaigns and online reporting of several big hacks throughout this type of attack: Cyber criminals send wallet key owners emails designed to get user’s credentials and then, the cybercriminals are able to access to confidential data and/ or financials for their personal gain;
3. Routing attacks. A routing attack can impact both individual nodes and the whole network. The idea of this hack is to tamper with transactions before pushing them to peers. It’s nearly impossible for other nodes to detect this tampering, as the hacker divides the network into partitions that are unable to communicate with each other; and
4. Sybil attacks. In a Sybil attack, the same node can be assigned with several identifiers creating fake network identities. During a sybil attack, hackers can take control of multiple nodes in the blockchain network with malicious interests.



[Table 2: SWOT Analysis ]

## BLOCKCHAIN IMPLEMENTATIONS AND CONSORTIUMS

Besides Bitcoin, and various “coin” variants, several general and specific purpose implementations of blockchain have imposed themselves, each with specific features and application domains, based on the original blockchain principles established by the Satoshi Nakamoto’s paper[[33]](#footnote-34).

### Main blockchain implementations

Among others, there are four major blockchain platforms which are currently used: Bitcoin, Ethereum, Hyperledger and Quorum.

#### Bitcoin Network

The Bitcoin network, based on open-source, is the most widespread in the world according to its number of nodes. It is a public blockchain and it was the first to be used massively. Its objective is to create a financial system that is more transparent, secure and independent from central banks. The triumph of Bitcoin raised blockchain technology to the spotlight of large corporations, which since then have focused much of their efforts on understanding the disruptive potential that the technology offers.

There are two types of transactions in the bitcoin network: those of creation or issuance of Bitcoin and those of transfer of Bitcoin between users of the network. The transactions that are issued to the network are grouped into blocks that are incorporated into the chain of blocks once the nodes have reached consensus on which is the next block to be included in the chain.

Both the amount of bitcoin created per block and the value of the commissions corresponding to each transaction are delivered to the node that has managed to resolve the next block to include. As explained before, this is known as mining in a public blockchain, and it is the reward provided by the network to the nodes in charge of validating the transactions, as compensation for the high computational cost incurred when participating in the mining of the network.

Each user of the bitcoin network has an associated public key or blockchain address, which serves as the user's identifier and will allow him to receive bitcoin. On the other hand, each user has a private key corresponding to the public key. This private key performs the digital signature of the transaction and supposes the control of the balance of the corresponding address.

#### Ethereum MainNet

Currently, the Ethereum MainNet, also conceived as an open-source project, has the second largest number of nodes. Proposed in 2013 by Vitalik Buterin, the Ethereum blockchain aims to create a decentralized global computer that enables the possibility of creating decentralized applications on the network.

Unlike the Bitcoin blockchain, in which only cryptocurrency transfers can be made between users, Ethereum introduces the so-called smart contracts, computer programs included in the blockchain that run at the same time in all nodes of the system as they were created by their programmer. Nobody can alter the code of a smart contract once it has been incorporated into the blockchain. The Ethereum network has a new cryptocurrency associated with it, Ether (ETH). This currency is designed to serve as a means for assuming the cost of the commissions derived from the use of the network, as for Bitcoin, but it is also used to pay the computational cost in which the network incurs when a contract is executed. In other words, Ether is used as a means of payment or incentive to maintain the consensus of the network. Smart contracts allow new functionalities regarding the exchange of digital assets. A contract will contain all the clauses in its code, and its execution is guaranteed according to its initial programming once the corresponding cost has been paid.

Like the Bitcoin network, the Ethereum blockchain relies on public key cryptography to identify its users on the network. However, in Ethereum there are two types of accounts: one similar to the one in Bitcoin, and another of the contract type that contains the code of a smart contract. As part of the Ethereum strategy to enable an energy-efficient transaction validation process, Ethereum 2.0 will be moved from a proof-of-work (PoW) consensus algorithm to a proof-of-stake (PoS) consensus model.

#### Hyperledger

Hyperledger is a solution promoted by a consortium of companies mainly promoted by IBM and the Linux Foundation, with the aim of creating open-source tools that facilitate the creation and implementation of hybrid/private blockchain-based solutions in all types of industries. It is a platform or group of modular and interoperable platforms, with different frameworks such as Fabric, Iroha or Sawtooth, dedicated to the creation of blockchains and smart contracts within the framework of a hybrid/private blockchain, which provides a high degree of confidentiality and platform flexibility.

#### Quorum

Developed by the financial services firm J.P. Morgan Chase, Quorum is an open source copy of Ethereum with additional functionalities focused on greater control of privacy and network permissions. This additional layer allows for establishing a hierarchy of roles and permissions within the blockchain infrastructure, providing separate read and write permissions to the desired nodes, resulting in more flexible and scalable solutions than those that can be achieved with public blockchains.

### Main blockchain consortiums and Industry alliances

There are different business consortiums that have been formed with the aim of exploring and creating new solutions and business models based on this technology and thus take advantage of its disruptive potential both in specific sectors and in other ways. There are consortiums formed around specific industries, studying use cases that apply to them directly, but there are also multi-sectoral groups studying transversal use cases focused on the development of generalist products that can be used by any industry for its specific needs.

#### Hyperledger Fabric

Led by the Linux Foundation, Hyperledger Fabric is one of the world's largest blockchain consortia. Based on the Open Source philosophy, Hyperledger Fabric aims to create development tools that allow the introduction of new solutions based on DLT.

This process of product standardization is carried out in a shared work mode: individual developers or those belonging to consortium companies contribute the code to the platform in order to create increasingly complex, robust and scalable products. Based on the Hyperledger development environment, anyone can develop their distributed applications, start studying use cases and potentially migrate their processes to others based on blockchain, taking advantage of all its potential without having to develop a DLT infrastructure from scratch.

#### Ethereum Enterprise Alliance (EEA)

Created in 2016, this consortium was born from the need to bring Ethereum network technology to corporations, providing them with resources so that they become familiar with the technology, learn to develop applications and understand the different use cases that make sense in a decentralized technological infrastructure. Currently the consortium is made up of more than 150 companies from different sectors, including BP, BBVA, Santander, NTT Data, Intel, ConsenSys, Amalto or JP Morgan.

#### R3

Oriented to the financial sector, R3 leads an initiative formed by more than 70 institutions of great importance worldwide. Together, they investigate the development of fintech applications based on DLT and how these solutions can replace or complement existing processes.

#### Blockchain Insurance Industry Initiative (B3i)

B3i is a global consortium made up of insurance companies. Initially formed by Aegon, Allianz, Munich Re, Swiss and Zurich, it is an initiative focused on exploring the potential of blockchain technologies to improve the service provided to its customers and develop new products that are faster, more comfortable and secure. The initiative was created by the software developer PONTON to explore the possibilities of blockchain technology in the energy sector. Among its objectives are the creation of a blockchain consortium in the sector. To achieve this, a two-day working session was held in Berlin with the 17 largest utility companies with the aim of forming a pilot consortium that would have an initial capital of €400,000 (€20-25,000 per participant).

#### Enerchain

Consortium promoted by the software development company PONTON with the aim of studying blockchain use cases oriented to the electricity sector. It has a special interest in exploring possibilities for the market for buying and selling electricity (power exchanges) and is supported by the EFET (European Federation of Energy Traders). Specific cases such as trade in smart energy products, process optimization at the transmission grid level, incident management, P2P trade in electricity or more precise adjustment of response to demand variations are in the focus of the consortium, since blockchain technologies can help create new consumer products or make existing ones more secure and efficient.

#### Alastria

Officially born in 2017, the Alastria network is a non-profit multi-sector consortium that aims to create a blockchain network with legal validity in Spain. Created with the intention of promoting the creation of a new digital ecosystem in the country, the consortium already has more than 250 members, including large companies, SMEs and start-ups. The Alastria network is built using encryption protocols, establishing a hierarchical structure of permissions, to allow isolation between the operations of its different members and provide a unique identity to all participants on the platform. One of Alastria's main use cases is the creation of a sovereign digital identity standard. To do this, a large amount of resources is being concentrated on providing the network with legal guarantees. It is intended to collaborate with the Administration to identify use cases in public bodies.

# III. POTENTIAL USE CASES OF BLOCKCHAIN IN IP ECOSYSTEMS

In a globalized digital world where the free flow of information and creative and innovative thinking is paramount, IP plays a pivotal role. The effective generation, protection, management and commercialization of IP assets, therefore, have been considered as one of the top priorities for business in private and public sectors and at the same time they are in a great challenge. At the same time, the opportunities that the actors have to maximize their benefits with the exploitation of their IP assets have been multiplied. In parallel, competition among participants in the market has become fierce, and risks of IP right infringement and misappropriation have increased as a result of new technological dynamics. Nowadays, the pervasiveness of digital technologies has been accentuated, and with it, the relevance of IP as a means to protect intangible assets has been reinvigorated.

This chapter is to explain how the blockchain applications previously explained may help public and private actors in IP ecosystems to address these challenges and make use of the opportunities that the digital environment opens. This chapter firstly describes the IP ecosystem and its components (in particular, the IP value chain), and then explains the potential applications of blockchain in four different sections: industrial property rights, copyright and related rights, data protection and access and IP right enforcement.

It should be noted that the following analysis aims to address various actors in IP ecosystems, not only IP Offices or international organizations. Needless to say, the willingness of these actors to introduce blockchain solutions, and the type of solutions in particular, will partly depend on the policies established by them. In addition, before introducing any blockchain-based applications, it is recommended that the concerned actors analyze whether they are suited to their business (see below the decision flow, Figure 2., and the value that the solution could add to the existing technology stack in use. In the affirmative, further assessment is needed on which are the most appropriate options, taking into account potential benefits and challenges of respective solutions, and their cost-effectiveness. The potential applications provided in this document should be perceived without any prejudice whether or not blockchain is the most appropriate solution to those cases. In this sense, sharing experiences by those stakeholders already introducing the technology, the promotion of collaboration and joint projects, and launching pilot projects are initiatives that may provide relevant information to all stakeholders in the IP ecosystem to adopt these decisions.

## IP ECOSYSTEMS AND POTENTIAL USE CASES

### IP Ecosystems and IP Value Chains

Intellectual property, broadly, means the legal rights which result from intellectual activity in the industrial, scientific, literary and artistic fields and it has traditionally been divided into two main branches, “industrial property”[[34]](#footnote-35) and “copyright”.[[35]](#footnote-36) It is also to be noted that there are branches of IP law and practice, which lie beyond the distinction between the two main branches, and which are therefore referred to as *sui generis* rights (rights “of their own kind”). Examples include the *sui generis* protection of new varieties of plants, non-original databases, software and traditional knowledge (TK) and traditional cultural expressions (TCEs). With the digital transformation of the 4IR, intangible assets that may fall beyond the classical branches of IP, ie., industrial property and copyright, such as big data sets, algorithms, TK and TCEs, are assuming increased significance and, because they are not direclty and fully protected by the classical main branches of IP system, they have been discussed as subject matter of potential use cases for blockchain applications.

An IP ecosystem can be understood as a network of various actors (e.g. creators, inventors, enterprises, Collective Management Organizations, IP Offices, enforcement authorities) that interact with each other in collaborative and competitive ways in the IP environment[[36]](#footnote-37) using resources to generate, protect, manage and/or commercialize intellectual assets. These interactions are highly diverse, context- and case-specific and often discontinuous. However, when they form continuous interactions taking place over a continuously evolving intangible (set of) asset(s), they have been described as value chains of IP, i.e. IP value chains. Such IP value chains are highly diverse and rapidly changing in the context of the technological, legal and commercial transformations that are currently reshaping IP ecosystems and are therefore demanding to generalize. Nevertheless, when simplified for illustrative purposes into a single generic model, they could be described in the following generalized model of an IP value chain.

IP value chains are sets of activities that add value to IP assets. The value chain can be represented as a lifecycle model with four phases:

1. Generation. This phase includes all steps from the initial idea with potential IP value to the existence of an intangible asset eligible for IP protection. It may include the following sub-phases: ideation, exploration, conception, production of creative works and development of an IP protection strategy.
2. Protection. This phase includes all the activities involved in obtaining legal protection for an intangible asset in the form of IP rights, including voluntary ownership registration. In general, these activities may be grouped in three sub-phases: ownership registration, IP maintenance and IP enforcement.
3. Management. This phase refers to the activities that the IP right holder may undertake in order to develop and raise the value of the IP right portfolio. It may include sub-phases such as IP audit, IP portfolio analysis, IP lifecycle analysis, Competitive Technology Intelligence and IP landscape.
4. Commercialization. This phase includes all those activities directly involved in generating revenue from the IP rights portfolio. It may be subdivided in IP finance (valuation, collateralization, securitization and fundraising), collection and distribution of creative works, and monetization (licensing, franchising, joint ventures, collection and distribution of royalties).

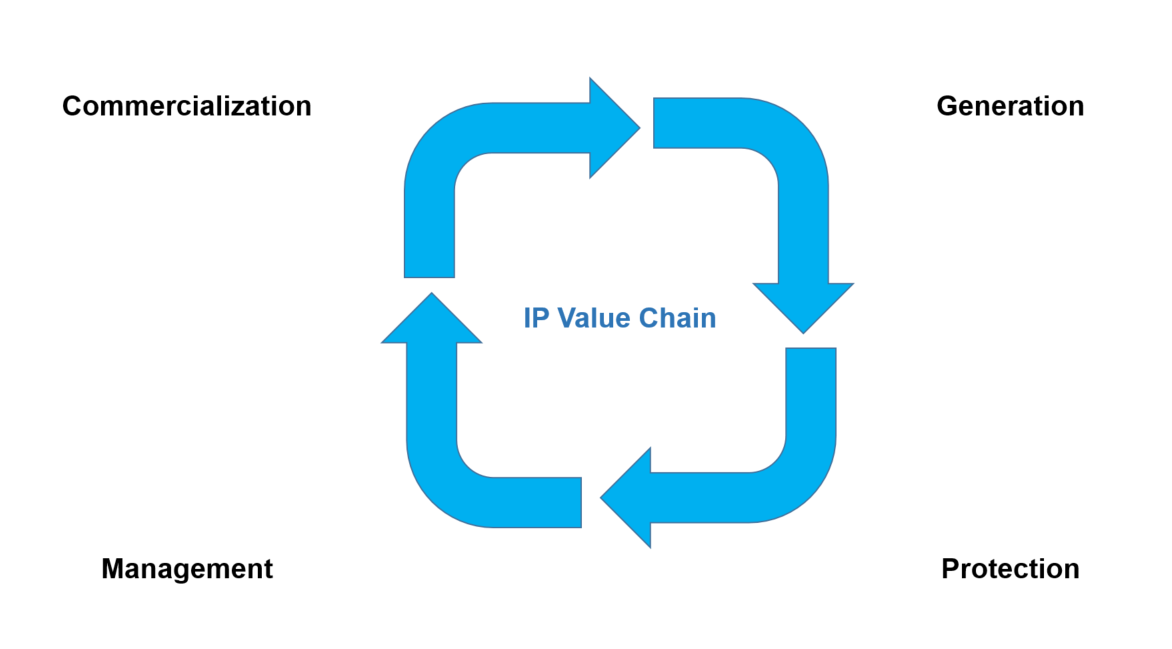


Figure 1: IP Value Chain

Describing the ecosystems of all IP assets in a single framework is a challenging and highly complex task, given the diversity of IP assets and IP systems at national, regional and international levels. A more comprehensive and differentiated description requires additional work and further development effort could be undertaken in due course, as required.

There are a number of important qualifications to be kept in mind when referring to this simplified and generalized representation of the IP asset life cycle in this paper. First, the reader should bear in mind that activities identified in each phase of the IP value chain are not necessarily sequential. Second, the distinctions between the different phases of the life cycle are not hard and fast and in practice they may overlap. Third, not all phases take place for all IP assets and not always in such a sequential manner, especially in the case of unregistered IP rights. In particular, enforcement actions (before judicial courts or administrative bodies) will usually be adopted once the IP is in the commercialization phase. Fourth, the processes may differ between different branches of IP systems. This would be the case in copyright, since the Generation phase usually coincides with the Protection phase, because a work is usually protected upon creation; while registration is available, IP Offices do not play a role in the protection of copyright as the one played for industrial property rights; the management phase may be often mixed with the commercialization phase, especially when a copyright is managed and at the same time licensed by a Collective Management Organization (CMO).[[37]](#footnote-38) As opposed to industrial property rights, copyright data is mostly held by private parties and not by IP Offices or public entities. Finally, the illustrative and simplified IP value chain, which is used as an abridged generalization in this paper, reflects a value chain within an IP ecosystem of IP assets which are intended for formal legal protection and commercialization. There are - at the same time and in parallel within the ecosystem - also other, complementary value chains of intangible assets, which are equally important for a vibrant ecosystem and which are not destined for commercialization and legal protection through exclusive rights. Within well-functioning IP ecosystems, these complementary value chains constitute a corresponding, equally important ‘other side of the coin’ of commercialization and the grant of exclusive rights. Different branches of IP law and practice refer to this aspect by a range of terms, such as the prior art and the public domain, with the general function to provide important inputs for innovation and the protected IP assets in the ecosystem. These value chains relate, for example, to technical public disclosure, the recognition of prior art, the maintenance of research commons, the public domain, which provide inputs for further innovation in the ecosystem. Further detailed description of IP ecosystems and IP value chains referred to in this paper is explained in Annex I to this paper.

### Potential blockchain use cases along IP value chains

While blockchain and DLTs have become a widely discussed topic recently with their potential and their use cases in almost every industry, this paper focuses on the implications and use cases of these technologies within IP ecosystems and the next section explores potential use cases which might be relevant to IP value chains. There are obstacles and challenges associated with the applications of the technologies, including regulations, interoperability, governance, data security, and privacy concerns. Nevertheless, blockchain and related DLTs offer positive prospects, e.g., for IP protection and registration, and as evidence either at the registry stage or in court.

While certain blockchain solutions only have potential applications in a single phase of the IP value chain, others have applications in several. In this regard, uses cases can be classified as horizontal – i.e. applicable in all the phases of IP value chains; and vertical – i.e. applicable in specific phases of the IP value chains. Following is the summary of some potential or prominent use cases and an exhaustive explanation of these use cases is provided in Annex III to this paper.

Horizontal use cases include:

1. DIDs - The creation of DIDs for IP ecosystem actors enables faster interactions along the different phases of the IP value chains.
2. Timestamping - A digital timestamp is the proof that a document, file, or any type of relevant digital content existed or was set in a digital place, like attaching it to a blockchain, at a particular date and time.
3. Arbitration and Dispute Resolution (ADR) Services - Blockchain in ADR can be used in increasing security with respect to evidence relating to the dispute and communications between parties, maintaining confidentiality and automation through implementation of smart contracts.
4. Transactions via Smart Contracts - If smart contracts are used to facilitate trade across the blockchains, actors can undersign transactions via smart contracts and receive tokens (coins) representing a certain value or the right to use a service/asset as agreed via that smart contract.
5. Version management - Many IP assets are continuously and rapidly transforming (e.g. ongoingly reannotated, value-added data sets) and thus transparent and trusted version management is important to maximize legal certainty regarding IP rights in such assets.
6. Proof of existence – blockchain can fundamentally improve the legal certainty around intellectual assets by providing immutable proof of the existence of these assets as a horizontal use case. This horizontal use case can be implemented in vertical applications of proof of existence for intellectual assets which are subject of IP protection, such as the vertical use cases of trade secrets or creative works, and intellectual assets which are not to be subject to IP protection, such as the vertical use cases of technical public disclosure, recognition of prior art, public prior use and prior user rights.

Vertical uses cases include:

1. IP Register (Generation / Protection phase) – Entering creative or innovative assets and the details of its generation into a blockchain would create a timestamped record and trustable proof of generation that owners could use to manage and commercialize their intangible assets, while additionally safeguarding against misappropriation or infringement. Blockchain can create securely interconnected IP registers of registered IP rights such as patents, trademarks and industrial designs, and unregistered IP rights such as copyright and unregistered design rights as it can easily provide evidence of the time of generation, rights management information (if applicable) and jurisdictional requirements.
2. Evidence of Generation (Generation) – Uploading newly generated IP assets and the details of its generation to a blockchain would allow the registration of a timestamped record and trustable proof of generation. The owners can use this to safeguard it from the potential misappropriation and infringement, for example complex data sets, such as sequence data generated by genomic sequencing.
3. Track and trace of source of origin (Protection / Commercialization) – Blockchain can be used to fight against counterfeiting of goods by tracking the routes and recording all the stakeholders involved in the final delivery of the products to the customer.
4. IPR Enforcement (Protection) – Blockchain technologies allow for the creation of a decentralized platform where all parties involved in the protection of IPR (enforcement authorities, right holders, IP Offices, and other parties) have access to relevant product-related information. This platform would allow the enforcement authorities and IPR holders to share (confidential) data securely, thereby contributing to support the fight against counterfeiting.
5. Priority Document Exchange (Protection) – IP Offices may create a common infrastructure for exchanging priority patent documentation among them. This will allow all IP Offices to have the same level of control and security over information, in addition to end-to-end traceability, and greater automation. Furthermore, applicants might be relieved of the need to submit documents to the Office of First Filing in the process of patent approval request in the IP Offices of different countries.
6. Certification Mark (Protection) – This use case refers to the creation of a distributed register of certification marks in which the marks and the information related to each of them including the owners, the certification authorities and the approval process, as well as the management of the application received for the use of the mark are stored.
7. Evidence of trademark use (Protection). Blockchain may provide reliable and timestamped evidence of actual use and frequency of use of a trademark in trade, both of which are relevant in proving first use, genuine use, acquired distinctiveness/secondary meaning or goodwill in a trademark. Similarly, it could be used to publish technologies for defensive publication as prior art to prevent others from obtaining a patent over such technologies.
8. Prosecution of plant variety protection application (Protection) – Blockchain solution could create an immutable record of “events” in the life of a protected variety, globally. It could include the moment when a Plant Variety Protection (PVP) application is filed, examined and granted. It might also resolve the practicalities of collating, storing and providing such evidence. It could be also relevant for the PVP matters after grant (e.g. keeping the rights in force, nullity and cancellation).
9. IPR Transfer (Management) – Blockchain has the potential to support all parties involved in this process, making it easier to create and manage the evidence of the agreement between the assignee and the assignor for the transfer of the IPR.
10. IP Licenses (Commercialization). Blockchain could bring a secure, reliable, and scalable distributed transaction processing to licensing IPR. It could introduce traceable and verifiable ownership and an accurate distribution of royalties, allowing the possibility to pay the right holders directly, reducing the use of middlemen.

It is also to be noted that horizontal uses such as proof of existence can find multiple vertical applications, such as trade secret protection, prior user rights, recognition of prior public use or prior art and others. In some areas the use of DLTs could offer additional benefits to implement long-standing proposals. For example, increased legal certainty in the recognition of prior arts concerning TK or related GRs has been proposed and accomplished through establishing conventional off-chain databases.[[38]](#footnote-39) Conventional national electronic databases for GRs and TK have been created by Member States, while a centralized international one-click system has so far not been possible since holders of TK wished to themselves control primary data on the disclosed knowledge for cultural, conservation, equity or other reasons. Distributed ledgers or blockchain could offer additional benefits and further improve the ability of patent examiners to take into account such prior art.

Keeping in mind that some use cases are horizontal and others are applicable in more than one phase, the following sections explain the potential use cases in industrial property rights, copyright, data protection and access, and enforcement.

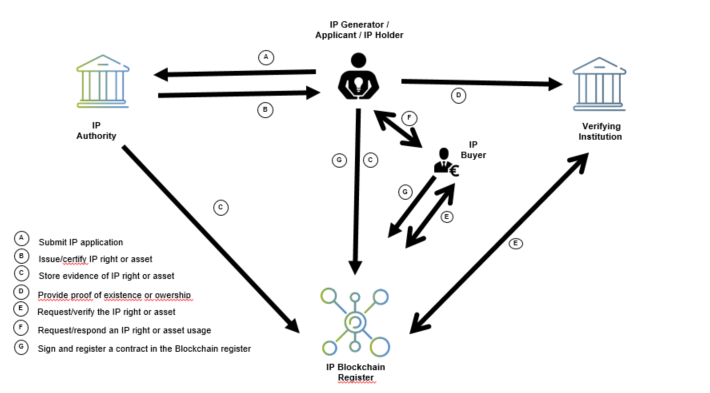


Figure 2: Overview of Blockchain use in IP ecosystems

## INDUSTRIAL PROPERTY RIGHTS

In the context of industrial property rights,[[39]](#footnote-40) blockchain brings the potential of enabling actors in the IP ecosystems to identify and record their intangible assets, providing a clear, dated and accurate proof of ownership. Other potential benefits are the constitution of blockchain-based networks for IPOs, the digital identification of right holders, the traceability of products and the digital recordation of documents. In light of the aforesaid, blockchain needs to be thought in the context of industrial property rights from a twofold perspective: on the one hand, private sector perspective – intended as the usage of this technology by private actors in IP ecosystems; and on the other hand, public institutional perspective - as in the implications of blockchain in a public system such as IPOs.

### Blockchain application from a private sector perspective

Blockchain may constitute a strategic tool to reduce costs and increase transparency as well as efficiency by providing timestamped and secured evidence from the right holders’ perspective. As a matter of fact, blockchain solutions are relevant in all stages of the IP value chain: from the early stages of the Generation phase all the way to the commercialization of the final product.[[40]](#footnote-41)

To begin with, blockchain can certainly be used in the context of generation of tamper-proof documentation bearing a precise date and time, and attributable to a specific individual or entity. Some platforms integrating this utility are already available from relevant and established providers like Bernstein, MyTitle, Creativity Safe, Origin Stamp or Zertifier, as well as services developed by law firms specifically for clients.[[41]](#footnote-42)

The digital recordation service provided by these entities is usually divided in three steps: upload, certification and verification:

1. Upload. This Phase consists in uploading a specific digital item of any kind – e.g. research notebooks, confidential information, etc. - in an encrypted cloud service connected to a blockchain through an Application Programming Interface (API), he outcome is to obtain the creation of a transaction recorded on the blockchain, bearing relevant date, time and owner. Such a transaction is localized with an ID, which is the hash, associated with the encryption of a particular document. Said document is usually encrypted adopting the so-called “*zero-knowledge technology*”, meaning that the provider offering the API service which connects the end consumer with the blockchain does not have access to the uploaded document. As a matter of fact, only a digital fingerprint of the document, translated into the hash, will be recorded onto the blockchain.
2. Certification. Once the document is uploaded on the ‘digital cloud’ and encrypted on the blockchain, the blockchain network operator issues ownership certificates that bear all the relevant information either to be submitted to the competent authority or even simply for personal record attesting the possession of a specific document in a particular moment in time. The relevant information may consist of name of the owner, date and time of the encryption, transaction ID (hash) and all accessory and additional information that may be customized and filled in with (e.g. – there could be a section on the blockchain certificate called “*notes*” or “*comments*”, whereby IP owners can describe the characteristics of the encrypted document).
3. Verification. As mentioned above, since the services are often offered following a zero-knowledge technology, the certificate may only prove the existence of a specific content/document that has been encrypted on the blockchain and that bears a particular transaction number (hash), meaning that the document is not contained in the provided certificate. Therefore, there remains the issue of authenticity verification. In order to verify the authenticity of the document encrypted on the blockchain, and not a modified version of it or a copy, this solution requires a tool to verify which specific document was uploaded generating said transaction. For these purposes, in order to verify the authenticity of the transaction, two factors need to be checked: the existence of a transaction associated to the hash; and the possession of the original document uploaded:
   * Existence of the transaction. As per the localization of the transaction, blockchains such as Ethereum and Bitcoin already offer free specific services that allow searching for a transaction in their whole blockchain,[[42]](#footnote-43) thus the end user and/or the authority who received the blockchain-based evidence will be able to determine and localize a transaction by inputting the hash on such platforms. If the service is provided via a different blockchain, the provider must grant third parties to have access to the transaction ID in order to localize it.
   * Document match. On the other hand, in order to determine whether such transaction contains a specific document and not a modified or subsequent version, providers have enabled a service normally called “*verification tool*” (the commercial name of such tool may vary from provider to provider), which, through the upload of the same original document initially encrypted, will confirm the match with the blockchain transaction by recognizing the same identical digital fingerprint uploaded beforehand. Should the original document be different in even the smallest details such as a comma or a space, and should that posterior altered version be uploaded on the verification tool, this latter will reveal the lack of match and will not confirm it.

These applications may help to create and submit evidence to the IP Offices or courts during IP-related proceedings enforcing both registered and unregistered rights. As a matter of fact, dated and tamper-proof documentation attributed to the rightful holder may significantly facilitate the work of authorities, allowing IP asset holders to create a trail of records with blockchain that enable the existence of evidentiary documentation throughout the lifecycle of IP assets.

A timestamp proves the existence of a document, but there is no need to reveal this information unless required in a legal dispute. Blockchain technology can provide up-to-date advanced timestamp services for IP rights and related IP data covering multiple participants and multi-step timestamp workflows. This service coupled with intrinsic immutability can provide higher quality evidence and legal value.

In the context of trademark proceedings, these applications might be useful to provide the proof of trademark use requests in the context of opposition or cancellation for non-use actions as well as acquired distinctiveness claims. IP Offices may require opponents or trademark holders to submit documentation such as invoices, promotional material, annual turnovers, sales figures, advertising investments, social media interaction and so forth. All such evidence, in order to be accepted, has to show use of the trademark for a period of time in relation to the goods and services for which it sought protection and must bear a relevant date within the requested timeframe. The same applies to trademark applicants in the context of acquired distinctiveness claims, whereby the Office requires the applicant to show that the filed trademark has been used in the market to such an extent that the average consumer will be able to determine the commercial origin of any product bearing such sign. Many right holders faced inconveniences due to undated evidence, which may have also led the IP Offices to decide unfavorably due to lack of secure, immutable and solidly dated evidence. It has to be borne in mind that such process will only work if IP holders carry out a periodical blockchain timestamping, so that evidence is always dated in case proof of use requests arise. Blockchain evidentiary documentation cannot be created after having received a proof of use request, but exactly the opposite: the IP holder will be able to submit such duly dated documentation in the relevant period only if he/she has performed the corresponding generation of evidence during the five-year timeframe of interest.

Collecting information on the use of a trademark in trade or commerce on a blockchain-based official trademark register would result in reliable and timestamped evidence of actual use and frequency of use of a trademark, both of which are relevant in proving first use, genuine use, acquired distinctiveness/secondary meaning or goodwill in a trademark.

Through the use of blockchain for the generation of evidence, IPR holders can provide tamper-proof evidence to be submitted before IP Offices in case of disputes concerning trademarks, patents, designs, enforcing both registered and unregistered rights, vis-à-vis subsequent applications for registrations. Such evidence may prove to be useful in IP proceedings, potentially valid and acceptable before offices worldwide, even though local regulation will certainly need to be complied with. In relation to the aforesaid, please see the IPR enforcement section below.

As per the patent realm, the generation of timestamped evidence offers inventors and patent holders protection from their preparatory documentation all the way to their patent application filing. This would simply work as a digital notary, with the difference of being fast, discrete, confidential, and available 24/7. In this regard, debates have already been generated regarding what the role of this tool would be. Such is the case of a document prepared for the European Parliament, in which the development and role played by the blockchain in the protection of innovation is discussed.[[43]](#footnote-44) This report assesses to what extent blockchain technology can be useful in this field of industrial property; with the encryption and proof of existence, it would be possible to prove by inventors or applicants that the registration existed at any given time, without revealing its content.

Similarly, in the patent field, another potential application of blockchain solutions is referred to defensive publications. Defensive publications are strategies that use the publication of a technical development as a tool to create prior art and thus prevent patents from being granted on such invention.[[44]](#footnote-45) Blockchain solutions can also contribute to the publication of prior art where databases may be difficult to create, for example for natural genetic resources or related local indigenous knowledge. As a matter of fact, defensive publications guarantee freedom to operate by preventing third parties from patenting the invention. However, in order to successfully determine such defensive publication as prior art and include it within the current state of the art, such content must be accessible by patent examiners and it must bear a specific date, both points equally well-fitting in a blockchain-based solution combined with IPFS (*InterPlanetary File System*).[[45]](#footnote-46)

Blockchain can also be very helpful in relation to industrial designs, in particular unregistered designs, that will be used in the market for short timeframes, such as in the fashion industry. It is widely known, in fact, that the fashion industry is constantly moving, with trends that may last a few months, if not less, meaning that applying for protection over the aesthetic appearance of a product (i.e. a design) may often be too slow and ineffective in comparison to the market speed. In fact, in light of the above, unregistered designs in the EU regulation are protected for the period of three years (non-renewable) without the need of being registered. Such figure, however confers protection only against identical designs, differently to Community registered designs, which furthermore confer protection over a period of five years, renewable until a total of 25 years. Even in the unregistered design cases, however, the main issue of unregistered designs, however, revolves around the *dies a quo* from when protection starts to apply since no registration is required, no precise date is established by an authority and the enforcement action relies on the evidence filed and provided by the affected party. Through the use of blockchain, IP holders will notice a reduction in expenses that they may incur in providing such evidence.

Another blockchain use case in relation to industrial property is the traceability of goods protected by geographical indications (designations of origin, geographical indications, traditional specialties, named as PDO, PGI and TSG, respectively). Taking as an example the European Union system of Geographical Indications or Appellation of Origin, among their requirements, one can find the quality control on behalf of the appointed entity. In this regard, if quality controls are not carried out, geographical indications may be subject to revocation. Certainly, a tool that can be used by user associations, consortia and whichever entity, private or public, in charge of quality control in the jurisdiction from which the PDO/PGI/TSG originates, could be the traceability of products through a blockchain ledger. This would result in the entity being able to trace every step and every movement of the goods bearing such indication of origin, thus controlling the quality and being able to handpick on any unit that may be suspicious or may contravene the specifications of the quality scheme belonging to the corresponding indication.

Trade secrets holders may also benefit from blockchain applications. In this regard, blockchain can easily be used as a successful tool to guarantee compliance with the requirements set by the law to take the necessary steps to protect the information. This occurs by encrypting the file containing the trade secret in a local IPFS, timestamped on the blockchain and accessed through a “*zero-knowledge platform*”. This provides, on the one hand, compliance with legal requirements concerning trade secret protection – i.e. the owner taking the reasonable steps to ensure the effective protection of the confidential information and, on the other, a time-sealed document securely dated, allowing its holder to establish the exact *dies a quo* from which the corresponding protection starts to apply.

In this line, there are solutions arising nowadays concerning encrypted documentation transfers such as *Zertifier[[46]](#footnote-47)* with their solution *HASH4LIFE,[[47]](#footnote-48)* which may have relevant applications for protecting confidential information. In fact, this solution uses blockchain to send documentation in a safe manner, all based on the use of blockchain. This occurs by encrypting and storing the files in a decentralized IPFS server cluster, where they will be available to be downloaded for a period of seven days (similarly to a WeTransfer[[48]](#footnote-49) application, only using blockchain for further security features). Furthermore, the blockchain-powered service allows, through a verification tool, to verify ownership of the document. This application may be useful in the context of trade secret licenses or assignments, *know-how,* as well as potentially due diligence in relation to IP matters.

Traditional mechanisms do not ensure effective protection of trade secrets in the digital world due to constant and sophisticated cyberattacks. Classical protection systems are expensive and time-consuming to keep the information safely and securely.

Blockchain technologies could drastically reduce time consumption and costs for economic actors owning a trade secret, by providing a simple and inexpensive registry of proof of existence.

These blockchain applications can also help to streamline the activities in the management phase that IP asset holders need to carry out to develop and raise the value of their IPRs portfolio. To start with, interoperability of blockchain solutions introduced in the IP ecosystems can allow the holders to use computer applications that simplify the identification and monitoring of the whole intangible asset portfolio of an entity at a transnational scale. This may help to better secure IP assets and set up an effective IP administration structure at a global scale. In addition, IP holders may obtain easier access to information gathered by public entities on external activities that could affect a company’s business, including technical information available in patent registries and third parties’ rights.

Blockchain solutions can also help to monetize industrial property rights – e.g. authorizing a third party to make use of the IP assets either through licensing, assignment or more complex contractual schemes such as franchising, joint venture, spin-offs or technology transfer. In all these cases, IPR holders may recourse to smart contracts that can be automatically concluded and performed. For example, IPwe[[49]](#footnote-50) provides a blockchain-enabled patent registry and ratings database currently containing basic information on eighty percent of the world’s patents.[[50]](#footnote-51) This company provides a marketplace, allowing patent holders to have exposure with potential licensees interested in purchasing or negotiating a license with such holders.

Finally, blockchain can help companies to securitize their IP assets or to use them as collaterals. Bonds of a company’s IP assets can be issued as tokens with blockchain solutions. Blockchain-based equity funding (or crowdfunding) can potentially allow the tokenization of an IP asset in the results of future research projects (e.g. the invention of a new medicine). In the short-medium term, this will facilitate the funding of research and innovation activities. An example of this could be the tokenization of a patent, which by dividing it into several fragments, can increase monetization and have the possibility of multiple assignments, licenses and so forth.[[51]](#footnote-52) As clear as it is, the aforesaid changes the scenery, by empowering owners and allowing IP holders to look at multiple stakeholders at once and in relation to a single IPR.

All of the aforesaid suggests that blockchain could be a transversal solution, applying in the different stages of the IP value chain, and to different industrial property rights (patent, trademarks, industrial designs, geographical indications) and trade secrets (confidential information, know-how and, as explained later and digital data).

### Blockchain application from a public sector perspective

From the perspective of public authorities such as IP Offices, blockchain can be useful for a wide variety of activities, including digital identification of applicants and rights holders, or the creation of an interconnected and to some extent synchronized network of IP Offices’ registers for timely service.

An interconnected system of registers based on a blockchain network has the potential to bring prosecution of applications and maintenance of IPRs to the next level. Similarly, a blockchain-based system may improve IP licensing and IP assignments, indicating to potentially interested parties the current owner of IPRs. It should be recalled that national legislators usually require assignments or licenses of industrial property rights to be made in writing and registered with effect from the date the request was made, or from the date the supporting evidence or the fee was paid (whichever action is the last one). In this regard, blockchain solutions introduced by IP Offices have the potential to support these transactions by making it easier to create and manage the evidence of the agreement between the licensee/assignee and the licensor/assignor for the license or the transfer of the IPR. In the latter case, the transfer is effected by timestamping the change of ownership of the transferred IPRs and by supporting the data exchange among the parties.

Although IP registration processes are mature, they are complex, expensive and usually require professional services and expertise. This makes it a challenge for most SMEs to register the idea conceived in the Generation phase of the IP value chain. Blockchain could potentially make the registration process easier, faster and cost-effective, reducing hurdles and burdens of IP registrations. In this regard, some of the benefits of blockchain-based systems are:

* the improvement of the system’s security with less maintenance;
* the efficiency of an automated database update; and
* the costs associated with the identification of applicants and rights holders would be lowered, as well as the handling of opposition-related fees, and any other act related to the application and registration of an IPR, since processing time for this information can be shortened to a few minutes.

In relation to the security mentioned above, it is evident that the system, by using a blockchain, will drastically improve its security, since every change on any record will be easily and effortlessly recorded, localizable and associated to the user who has appended such a transaction. Additionally, since every node owns a full copy of the ledger of transactions, being simultaneously copied in all nodes, blockchain guarantees in this way a higher layer of security (i.e. decentralized security), in view of the fact that in order to corrupt or alter the data or a transaction, this will be reflected on the blockchain itself.[[52]](#footnote-53) Further security may be achieved and vary on the basis of the type of blockchain adopted. Regardless of the choice between a private or public blockchain, security is enhanced with the use of a blockchain infrastructure. A permissionless public blockchain like the Bitcoin network, for instance, may certainly be more secure, but it results in the loss of full control on the blockchain and may also affect sustainability, in view of the higher computational effort needed to create blocks through the Proof of Work system. On the other hand, while a private and permissioned blockchain may consume less resources that contribute to climate change , it offers slightly minor guarantees on the security and immutability of transactions on its degree of decentralization.[[53]](#footnote-54) Additionally, the system requires less maintenance, particularly in relation to the aforesaid. It is to be mentioned, however, that the use of blockchain entails the impossibility to modify a record, or better, any modification will be reflected on the system, which means that any entry, being it a deletion, addition or request, will appear on the blockchain record.

As per the efficiency mentioned above, while using a blockchain-based solution, efficiency may increase, since smart contracts can automatically execute transactions when certain conditions occur (i.e. at the completion of the payment for a renewal, the IP Office may process it and publish it). Similarly, in relation to identifying IP holders, every holder will own a digital identity, associated with all of his/her IP assets that the Office will be able to access much quicker. If the databases that are used or consulted by the IP Offices during the examination process are kept in a secure blockchain to which all such authorities have access, the assessment of whether an invention fulfils the novelty requirement might be accomplished through the cooperation of an AI-based software and blockchain technology. The implementation of blockchains thus could result in IPRs autonomously or efficiently managed by their owners in the IP process such as renewals, cancellations, licensing and assignments, while using an interoperable digital identifiers such as DIDs from any jurisdiction across the world, thereby leading to a significant increase in efficiency. The drastic impact in this phase of the IP value chain may be envisaged in the next 5-10 years.

In order to manage the transfer of rights by IP Offices, written evidence of the agreement signed by the parties must be delivered, then reviewed by an agent, and if no deficiency is found, the transfer will be registered as of the date the request was submitted, or the supporting evidence or the fee was paid – whichever action is last. Blockchain has the potential to support all parties involved in this process, making it easier to create and manage the evidence of the agreement between the assignee and the assignor for the transfer of the IPR by timestamping the change of ownership of the transferred IPRs and supporting the data exchange among the parties. No human intervention might be needed.

Lastly, in relation to the cost-effectiveness mentioned above, thanks to the administrative processes being more efficient and the operational flow being more streamlined, IP Offices will be able to lower administrative costs.

Different actors play a role in the transfer, namely the right holder and the party to which the right is transferred. Both parties may have legal representatives who actually handle the transfer and the IP Office may have one or more agents involved investigating any deficiencies. The actors’ identity and their roles in the process may need to be validated. Assuming that all these actors have a “digital identity” proven by a digital certificate registered in a recognized Certificate Authority, the transfer process can automatically validate these certificates and instantly confirm that the signatories for the IP transfer are authentic and authorized to make the transfer. One or more Certification Authorities may be involved in the process. As many Governments have encouraged their citizens, business and public services to adopt digital signatures, they can be considered as reliable sources to store, manage and validate identities during the IP transfer process.

The creation of digital identities for IP ecosystems actors will enable faster interactions where identification requiring legal certainty is required. However, given the proliferation of available digitized identity solutions, it is necessary to build a digital identity ecosystem allowing interoperability between different entities and systems, ensuring compliance with current regulations, and improving services and operations of companies involved. Considering the identity solutions adopted by governments for public citizen usage, the interactions between actors can be facilitated providing both legal certainty and a degree of interoperability.

Currently, most relevant records are kept separately by either IP Offices, private companies or right holder organizations even though Offices put efforts to share information among their databases, e.g. through web services. Blockchain technology could foster this collaboration by providing interconnected ledgers for IP assets and facilitate the processing of IP assets, protection, renewals, and changes to registered IPRs or oppositions.

At the IPOs Meeting on ICT Strategies and AI for IP Administration held in May 2018, the participants discussed 40 Recommendations, including “R12. In cooperation with interested Member States, the International Bureau of WIPO should develop a prototype for a distributed IP registry. The prototype could be used for IP applications to create an authentic registry of IP application numbers, for example, to be used for validation of priority claims. Study the possibility of using a distributed IP registry linking to WIPO CASE or the International Register. The potential of blockchain technologies for linking such distributed registries should also be explored.”[[54]](#footnote-55)

Furthermore, there is a proposal for an international patent application system based on a permissioned blockchain named Patent Application System Based on Blockchain (PABC). This aims to connect Patent Offices in the world and promote the exchange of patent data among them in a highly secured blockchain environment. The proponent explains that PABC could address some issues currently experienced by patent systems such as inefficiency, expensiveness, and uncertainty to obtain a patent in multiple countries.[[55]](#footnote-56) It seems, however, that there would be several technical and legal challenges to implement the proposal. Firstly, someone should create a global patent system network. Each IPO would act as a node in a blockchain network in order to verify relevant requests and approve all operational records on a patent application so that such records can be admitted by all relevant patent Offices at a decentralized level instead of only by a specific Office at once. Furthermore, even if a global blockchain-powered network is established and maintained, Offices might not be able to share information on the unpublished patent applications with other Offices in the network, as some Offices or applicants are not allowed to share it according to their national laws.

Some IP Offices and institutions have been exploring and fostering the use of blockchain in relation to a wide variety of applications. The European Parliament has mentioned that blockchain encryption and proof-of-existence may be used by patent holders to prove that registrations existed at any given time, without revealing its content.[[56]](#footnote-57) This latter application is relevant for IP Offices since the offering of such services may allow IP holders a more transparent bureaucracy and access to their data. This could be extended to any type of IP by registering a cryptographic summary of the description of their creation or invention in the blockchain. In the meantime, the European Union Intellectual Property Office (EUIPO) has launched the eRegister, a blockchain based append-only database, controlled by the EUIPO itself directly, that will allow everyone to access to the whole history of every entry in relation to a single trademark or design registered before the EUIPO. Similarly IP Australia is working on a platform that allows the tracing of products through APIs and unique identifiers such as NFCs, UiDs or any other tag applicable to the product itself.[[57]](#footnote-58) Other entities such as the IEEE have discussed how a permissioned blockchain system can be used to construct an international patent application system.[[58]](#footnote-59)

Blockchain technology could provide an opportunity to establish a distributed IP register benefitting both Offices and applicants: (i) A considerable reduction in the costs associated with identifying right holders since the time to process this information can be shortened to a few minutes as all records would be stored, while additional savings can be found in the more effective and efficient system security with far less maintenance; (ii) IPRs would be managed by their owners rather than by intermediaries; and (iii) In addition to the creation of the work and its IPRs, right holders would also be able to produce smart contracts for potential future transactions concerning the IPRs. By having such contracts running on a blockchain, transaction processing, such as licensing, would be greatly simplified. Through this system, transaction costs for right owners would be substantially reduced, considerably increasing their earnings.

Henceforth, blockchain technologies may benefit Offices by streamlining administrative or operational processes, providing IP holders with digital identity, the ability to renew and interact directly with IPO’s database, cybersecurity improvements, less maintenance, just to mention a few. In addition to all of the previously mentioned, which perfectly applies to all Offices individually, the advantages of a global system materialize in a more interconnected network of Offices which, for the purposes of international or regional systems, represent an ideal solution. In fact, automation and record tracking may allow IP holders to closely follow their IPR’s lifecycle in a fully transparent manner at a global scale. At the same time, efficiency in IP Offices may increase due to the possibility given to examiners to focus on more tangential and concrete aspects and less on mechanical procedures.

Blockchain offers a decentralized network where different IP Offices can exchange data or documents in a secure and traceable way. This will allow, automating, in one single operation, the process of sending priority patent documents from the Office of First Filing to the Office of Second Filing in which the applicant applies for the patent.

## COPYRIGHT AND RELATED RIGHTS

The advent of the Internet has posed a number of challenges in the management of copyright and related rights, including in relation to authenticity, authorship, ownership and enforcement. In recent years, the online world has proved to be commercially relevant, in some sectors even more than the traditional analogue market. There is a clear need for assuring an effective protection and management of these creative assets in the digital world, including through technology and infrastructure. Some of the challenges linked to the digital environment are related to the fact that reproduction and distribution of copies of creative works is easy and low cost; also data on authorship and ownership might be unavailable or hard to obtain.

Blockchain may constitute a helpful tool in assisting creators and copyright holders in the protection and management of their rights. Blockchain can, as a matter of fact, provide trustable information in the contexts of ownership, licensing and tracking the use of digital (but not limited to) content. In this sense, the European Commission states that blockchain has the potential to contribute towards achieving more transparency and better rights data management, specifically targeting copyright.[[59]](#footnote-60)

As it is generally known, while industrial property rights require registration in order to achieve protection (patents, trademarks and industrial designs, for instance), creative works are protected under copyright from their creation according to the provisions in international treaties that no formalities for copyright protection are required. Because of this, there exists a tendency of not taking any measures (or insufficient ones) in the process of creative works, which might result in long disputes over copyright matters that lack evidentiary proof concerning the date of creation and proof of ownership. Blockchain technology, through timestamping, is able to provide creators and authors with the proof of ownership and is able to establish the actual *dies a quo* of the corresponding protection attributed to a specific work. Additionally, blockchain can also record who is using a work, so that a fair remuneration can be calculated. Some above-mentioned companies in the industrial property rights section, such as Bernstein, MyTitle, Zertifier or Creativity Safe, also provide such a record service in the copyright field.

By using blockchain to register the creative works, creators can store their works in a hash which can be used as evidence of creatorship, based on the fact that the information registered in blockchain is immutable. Not only will the registration be stored, but all transactions performed in the blockchain will be saved. Furthermore, the author is able to make direct agreements with final consumers, thus reducing transaction costs.

Evidence of creation, ownership and existing binding contracts can be validated by reading the blockchain and extracting the required information by the IP Office or CMO who inspects and validates that the transfer can take place.

Recently, NFTs have led many to consider such an aspect of the blockchain as a great tool to attribute authorship, ownership and authenticity to digital works. It is said that NFTs bring scarcity to the digital space by associating a unique identifier to a digital asset (e.g. a work of art in digital format), allowing the author to sell it as the original work, or one of a limited number of copies of the original, if chosen by the author. NFTs are intangible and non-fungible tokens that represent unique digital items, meaning that such digital work is unique, original and no other item will bear such characteristics or attributes. Thanks to the use of NFTs, for now mainly powered by the Ethereum blockchain,[[60]](#footnote-61) creators can draft smart contracts through which a series of conditions can be laid out that determine the life of the NFT-associated digital item. Amongst these, the most relevant is the resale percentage to be paid to the author, the assigned rights which among the economic exploitation rights are to be considered assigned (in some jurisdictions, unless expressly established in writing, the economic rights are to be considered as not assigned). However, the issue revolving around the nature of NFTs themselves must be solved, whether these are to be considered as personal property or IP licenses and, lastly, what is determined by the content of smart contracts.[[61]](#footnote-62) In fact, the nature of the NFT’s smart contract will determine the faculties of the acquirer on such NFT, bearing in mand that territorial differences may apply on the basis of the applicable legislation.

NFTs can be anything physical or digital, “minted” (“uploaded”, encrypted and associated with a unique identifier) on the blockchain. For instance, the digital artist known as Beeple, sold through the world-renowned Auction House Christie’s an artwork called “EVERYDAYS: THE FIRST 5000 DAYS”[[62]](#footnote-63) for a record of 69 million US dollars.[[63]](#footnote-64) An NFT can also be a digital cat bred on the blockchain such as Dragon (sold for the equivalent of over 170 thousand dollars on the Cryptokitties[[64]](#footnote-65) platform), a tweet (the first tweet published by Twitter CEO Jack Dorsey was sold in 2.9 million dollars[[65]](#footnote-66)), or any other digital item.

Blockchain technologies may also facilitate the administration of repertoires by CMOs, as well as the interconnection between CMOs, and the access to the information of repertoires by potential users. In 2019, the Italian Collective Management Organization (SIAE) announced a partnership with Algorand[[66]](#footnote-67) for the development of a blockchain platform for royalty distribution. The project has seen the first tangible results in March 2021, with the creation of over four million NFTs that represent the over ninety-five thousand authors associated with SIAE. The partnership aims to share the project with other CMOs, since the ultimate target is to accelerate the digital conversion of works in order to facilitate their protection. Even though NFTs are powered by smart contracts, these latter have also different scopes and applications. As a matter of fact, smart contract solutions may facilitate the negotiation of licenses both individually or collectively by CMOs.

Additionally, blockchain may prove to be useful as it may be the ideal layer for a marketplace in relation to licenses, whereby CMOs’ platforms, powered by blockchain, offer the possibility to market operators to buy, sell and license IPRs, all under a perfectly tracked ledger. Surely, this may represent an interesting perspective. Also in this sense, CMOs may find potential benefits from using blockchains both nationally and regionally. In the first case, blockchain would allow traceability and record-keeping of any movement, transaction and value exchange between the author and potential assignees or licensees, allowing for full transparency of the license system and security in relation to ownership. Similarly, copyright licenses powered by regionally or even internationally managed and interoperable blockchains may provide a clear, transparent and efficient system for all players involved.

Another potential application of blockchain for the commercialization of works consists in the creation of digital blockchain-based music passports for singers and authors. Such a passport provides these individuals with a single identification of themselves and their music that is interoperable and freely transferable from one streaming service to another by choice of the author. An example of this is the platform MyCelia, developed by singer Imogen Heap.[[67]](#footnote-68)

Finally, blockchain or distributed ledgers may also provide solutions to creative expressions which do not fulfill the originality requirements of copyright protection. For example, in the context of TCEs, it would be conceivable through blockchain or DLTs to establish a register in which indigenous peoples and local communities (IPLCs) and countries may, if they so wish, record the TCEs that they claim as theirs. In the absence of international legal protection for TCEs, such notifications would be for declaratory purposes only. Such a blockchain based register could also serve as an invitation to third parties to collaborate with the IPLC or country in the development and commercialization of the TCE through licensing opportunities. This has been raised in the context of the TK related work of the International Bureau of WIPO.

Blockchain solutions could facilitate access by users to both the digital content and the identity of the actors involved in the process that goes from its creation to where it is accessible to the public such as authors, performers, producers, record labels, promoters and distributors. The use of blockchain to identify digital content may facilitate the calculation of royalties that need to be collected from users and how these royalties have to be distributed among the different right holders.

For instance, in Canada, the Access Copyright Foundation has created “Attribution Ledger” aiming to connect a creative work to its lawful creator and rights owner in a reliable and authoritative manner. The blockchain-powered initiative is based on three main considerations: (a) the content identity; (b) the rules and protocols required for verified attribution; and (c) an open and transparent system which immutably connects the work, metadata about the work and the entity or person able to authorize the use of a work.[[68]](#footnote-69) The initiative highlights, among others, the important role of Attestation Providers (i.e. verifiers) in the verified attribution. Certainty in activities such as the verification of the identity of the stakeholders involved in the ownership of the works or in the transaction performed by each of them would increase the trust system that blockchain can provide. Blockchain allows authors to transfer creative works with the assurance of immutability and the ability to audit all transactions made between authors and customers. This while also defining new pricing models based on real access to the copyright-protected content makes blockchain a powerful tool.

Services based on blockchain’s smart contracts and cryptocurrency micro-payments may provide efficient solutions for artists to manage their rights and consumers to access copyright-protected material against a fair fee. The transactions are regulated by a blockchain which validates them and facilitates the payment based on the accessed creative work. Available platforms such as PeerTracks[[69]](#footnote-70) or Unison rights[[70]](#footnote-71) are examples of services available to artists wanting to maintain ownership and directly manage access and monetization of their copyright-protected works. Smart contracts are used to define copyright ownership, contract the usage of copyrighted works and the related royalties to pay.

Finally, similar to industrial property rights, copyright and related rights can be tokenized and used as bonds to obtain financing for artistic projects (a film, a music record, a video game, etc.). An example of this is the Maecenas platform,[[71]](#footnote-72) a marketplace that allows the purchase of a fraction of an artwork, which is tokenized on the blockchain. In this context, such fractions are like shares, therefore if the value of the artwork increases, the value of each token increases too.

The management and licensing of the different forms of intellectual property is important to the success of the business that invents or creates a product. Each license includes contractual information related to the licensed content, who may use the IP and under what conditions, the duration and the termination of the agreement and the economic conditions.

As the licensing contract could be defined in a smart contract, licensing conditions, pricing and duration of the contract, could be stored as part of the blockchain related to the licensed IP. This allows the verification of the license right and it further allows for building market intelligence analyzing market prices and duration of licenses per sector.

## DATA PROTECTION AND ACCESS

Data is an essential component in the digital era and a key to many new technologies. There is increasing debate about frameworks for data across many regulatory fields including the IP framework for data protection. The latter is set out in the WIPO Revised Issues Paper and was discussed at the Second Session of the WIPO Conversation on AI and IP Policy in July 2020.[[72]](#footnote-73)

Data recorded in the blockchain is not just digitized information accomplishing the sole purpose of transparency and traceability. In other instances, data might be the traded asset, thus data itself is the object of transactions. In this regard, as it should be recalled from the developments in data processing tools and the constant horizontal sectoral expansion of AI techniques, data has become a highly valuable intangible asset for private and public organizations.[[73]](#footnote-74)

A recurrent concern for such organizations, institutions and communities of practice is therefore how to protect their data assets so as to avoid potential unlawful uses of it by third parties. However, for the time being there is no specific property right devoted to data and there is uncertainty as to its protection by existing categories of IPR – in particular as databases under copyright or the EU sui generis regime, or as trade secrets.[[74]](#footnote-75) An additional element of uncertainty refers to the application of privacy regulations such as the EU General Data Protection Regulation (GDPR) in those cases where data sets include personal data.

Blockchain and tokenization have the potential to provide private organizations with means to protect, manage and monetize their data.[[75]](#footnote-76) As explained in Section II, asset tokenization involves the representation of pre-existing real assets on the ledger by linking or embedding by convention the economic value and rights derived from these assets into digital tokens created on the blockchain.[[76]](#footnote-77) This is particularly relevant in relation to industrial data – e.g. machine-generated data, since data holders do not need to face the legal constraints imposed by privacy regulations. Examples of private entities providing blockchain-based data tokenization services are, among others, Datum,[[77]](#footnote-78) Ocean Protocol,[[78]](#footnote-79) Ecosteer,[[79]](#footnote-80) IOTA[[80]](#footnote-81) or Kneron.[[81]](#footnote-82)

Blockchain could provide the infrastructure on which the data token will rely. As pointed out by the OECD, “the distributed nature of the network with no single ‘point of failure’, the immutability of the ledger and the application of cryptography may add to the resilience and safety of the infrastructure”.[[82]](#footnote-83) A practical example in the data tokenization market is Datum. In this blockchain platform, ‘storage nodes’ are in charge of securely storing the recorded data in a decentralized manner.[[83]](#footnote-84) Consequently, the blockchain infrastructure brings the data token both control and flexibility to securely trade with the data as an asset – i.e. controlling the access to the data set.[[84]](#footnote-85) It is worth noting that, in case of misappropriation of data on behalf of a third party, the data holder would be able to claim trade secret protection before the competent authorities (see Section IV).

Depending on the chosen token (fungible or non-fungible token) and the contractual terms, the data holder will tailor the access to its data. For instance, in Ocean Protocol’s blockchain-enabled data marketplace, the data holder/provider might give access to data either by means of non-fungible tokens (ERC-721[[85]](#footnote-86)) where exclusive access to the dataset will be restrained to the stakeholder holding the NFT; or, by means of a fungible token (ERC-20[[86]](#footnote-87)), in case the data holder is interested in providing access to the dataset to anyone holding a given number of data tokens (thus, the access to the data is not restrained to a single stakeholder). Also, in some instances, composable tokens (ERC-998[[87]](#footnote-88)) are implemented.[[88]](#footnote-89) These are used to collect together the existing offered types of data tokens on a given dataset, as each type of data token might bring a different data service in Ocean Protocol’s blockchain.

Therefore, different types of tokens might be offered embedding different sets of rights to use the content. In short, the data token holder has a license to access the data digitally represented by the token, and the use is restricted to the terms stipulated in the smart contract connected to the data token. For instance, as Ocean Protocol specifies a data token can be designed to give access to a specific data set for 24 hours (one time access vs perpetual access); it can also be designed to give access to a dynamically evolving dataset where new data is being constantly gathered (i.e. dynamic dataset vs static dataset); and it can even be designed so as to provide not just access to the dataset but also computing services (i.e. access to a server where the dataset can be used for, for instance, AI purposes).[[89]](#footnote-90) Finally, unless specified otherwise, the token holder can transfer the token to other stakeholders, and by doing it, the rights embedded within it are also transferred (e.g., right to access and use the dataset for a specific purpose).

Datum’s White Paper may give the reader a simple way of understanding how a data marketplace and the lifecycle of the data-as-asset within a blockchain might work:[[90]](#footnote-91)

* A user submits a dataset to the Datum network and pays a fee (i.e. gas) for the data submission (the data is encrypted and the user is the one providing access to third parties with a decryption key);
* A storage node receives and stores the data, in exchange of DAT tokens (the data is stored in a distributed way and thus it is replicated in the other storage nodes[[91]](#footnote-92));
* A data consumer wants to purchase data;
* The User receives a purchase request with the details (e.g. identification of the data consumer and the offered price), and can either agree or counter-offer; and
* The User accepts the proposal, he/she sends the decryption key to the Data consumer who pays in DAT tokens.

Henceforth, data tokenization by means of a blockchain infrastructure provides economic actors with a marketplace where different interests are at stake depending on the side of the platform. Although multiple definitions can be found,[[92]](#footnote-93) data marketplace should be conceived as electronic infrastructures allowing economic actors to interact and perform data-based transactions.[[93]](#footnote-94) Even though Datum’s aforementioned example is a pertinent one, others such as IOTA marketplace may well also serve to illustrate a blockchain-based data marketplace.[[94]](#footnote-95) The theoretical conception of data markets and the materialization of these by data marketplaces have contributed to institutionalize data transactions, and broadly, data trade. As a result of this market structure and organization of economic actors, transparency, legal certainty, and ultimately data sharing practices are being progressively improved and fostered. The paramount relevance of so-called ‘data economies’ have pushed regulators and policy makers to design legal frameworks and policy strategies seeking to promote data-driven economies based on data-driven innovation and data sharing.[[95]](#footnote-96)

Notwithstanding the promising benefits, the risks of data tokenization (as many other blockchain niche implementations) should not be disregarded. There are two main sets of risks: blockchain-derived ones and data specific ones. With regards to blockchain inherent risks (and to avoid redundancy along the paper), while the technology increases security, cybersecurity threats might not be disregarded, in particular in private and permissioned networks. When it comes to data-specific risks, it should be recalled that datasets traded in the blockchain may include personal data. In addition, the users of a blockchain network generate data which might have a personal character – i.e. user-generated data. Moreover, non-personal data might also pose issues related to the quality and veracity of it. Hence, data protection and monetization by means of blockchain infrastructures needs to integrate a solid data governance policy capable of: (i) articulating all activities stemming from data marketplaces; (ii) providing legal certainty notwithstanding the current lack of data markets specific regulations. These concerns will be assessed in the following section of this paper.

## IPR ENFORCEMENT

Another group of potential uses of blockchain solutions for participants in the IP ecosystems is related with the enforcement of their rights. For the purposes of this paper, enforcement refers to the means provided to right holders to take action against infringers in order to prevent further infringement of their IPRs and recover the losses thereby incurred. They must also be able to involve state authorities to deal with counterfeits.[[96]](#footnote-97) As explained in the first section, enforcement is part of the “protection” phase of the IP value chain.

Right holders can enforce their rights before courts, administrative bodies, or alternative dispute resolution systems (ADR). In the case of counterfeiting and piracy activities, actions can be taken *ex parte* or *ex officio* by customs or police authorities. There are potential blockchain solutions in all these areas.

### IPR enforcement before courts and administrative bodies

Hypothetically, the use of smart contracts for the management and commercialization of IP assets may help the reduction of litigation. This is because in these contracts, the performance of the obligations takes place automatically once certain condition(s) agreed by the parties are met. At the same time, the contract can be automatically terminated once the software detects that a condition (e.g. the royalty payment, the digital content is made available) is either met or not met anymore. In this way, potentially, disputes about the interpretation of the contract disappear, thus parties are less willing to go to court (i.e. efficiency gains and reduction of transaction costs).

Nonetheless, smart contracts can also create unexpected results and actually cause disputes. It has been affirmed that “network providers should consider limiting the automation of complex functions that have significant probability of error or far-reaching consequences” [[97]](#footnote-98). For example, having a contract automatically terminated if one party breaches the contract may not be ideal as the other counterparty may wish to waive the breach or amend the contract– i.e. risks of machine-based binary approaches. Moreover, the use of blockchain technologies may bring new and complex conflicts – e.g. errors in the code of the smart contract, malfunctioning of an oracle, etc. Furthermore, in many cases, the performance of contractual obligations (even if expressed in digital terms) takes place in the physical world. Consequently, disputes will continue to occur even in a blockchain-enabled world.

Blockchain solutions can help to secure evidence that may result in being useful in legal disputes (i.e. timestamping features as explained previously in relation to industrial property rights and copyright). In the case of disputes concerning licenses of digital assets stored in a blockchain network (on-chain transactions), it also provides evidence on whether the content was used by an authorized person or in a way that was or was not authorized in it. Applications explained in the previous sections can be consulted as examples.

Blockchain solutions may have potential benefits for the management of judicial or administrative proceedings. According to a recent *Study on the use of innovation technologies* in the justice field commissioned by the European Commission[[98]](#footnote-99), there are several projects for the introduction of this technology in different EU Member States with one or some of the following purposes:

1. Identification of both the parties in the proceedings and their representatives to control access to the information about the proceedings or identification in cases where hearings are taking place virtually.
2. Secure the records of the proceedings, facilitate their internal administration and ensure their traceability (who has accessed or modified them). Documents can be safely stored and only be made visual/readable to a third ‘party’ based on a private key.
3. In those cases where part of the information analyzed in the framework of the proceeding is sensitive, the blockchain solution may help to keep confidentiality and administer access to such information. This is particularly relevant in cases where the dispute concerns trade secrets.
4. Secure evidence related to the proceeding.
5. Inter-agency cooperation: blockchain is a unique enabler of a trusted evidence layer. It will help to exchange information (securely) between different organizations of the public administration.[[99]](#footnote-100) So, for instance, courts may automatically retrieve information from the blockchain system of a national IP registry about the status of a registered IPR or an IP license under dispute.
6. International cooperation: the use of permissioned blockchain could potentially enable international collaboration among different judicial systems in other countries. This may facilitate judicial notifications, obtaining evidence abroad, expediting the requests of information, the recognition of the authenticity of foreign judgments, and reduce the risks of parallel litigation or, the case being, facilitate the coordination between the proceedings.
7. Other advantages are the agility to access the information and almost immediate time of response. The information availability could be potentially used for the generation of statistical information to help improve the judicial system, justice actions and internal processes.

According to the information provided in the Study, most of these projects are public/private initiatives based on open-source platforms such as Ethereum, aiming at creating a permissioned blockchain. While not exclusively focused on IP disputes, the Chinese Cyberspace Courts may be the best-known example of judicial authorities making use of blockchain both for the administration of the procedure (real-time authentication, electronic signatures, time stamps, keeping a record of the electronic data by users and access to it), connection with other authorities (notaries, public administration bodies, judicial government bodies), and the provision of.evidence.

For this latter purpose, the Chinese Cyberspace Courts in Hangzhou, Beijing and Guangzhou have created their own blockchain platforms which parties to the dispute can use to secure evidence. For instance, if the dispute is referred to the commercialization in a webpage of an infringing product or content, the plaintiff can save a timestamped copy of the webpage on to the blockchain. When the lawsuit is filed, the court verifies that the electronic evidence submitted is consistent with the electronic data stored on the platform. The court reviews the entire process of generating, storing, disseminating and using electronic data on the platform. If deemed credible, then such evidence would be admitted. The system is cost-effective because the parties do not need to provide a notarized copy of the electronic record, or to hire an expert appraiser to verify its authenticity or explain the technology before the judge.[[100]](#footnote-101) Potential guides or training to judges and Courts’ personnel might be needed in order to foster and achieve fluidity in this sense.

The Courts’ blockchain allows online marketplaces to connect their IPR complaint systems to the platform. Thanks to this, right holders can directly store the evidence obtained in the online market on the Court’s platform as a preparation for a future complaint. This is the case for instance of Alibaba’s Ali IPP Platform.[[101]](#footnote-102) The Hangzhou Internet Court is promoting the launch of a judicial blockchain alliance nationwide, which can unite administrative organs, courts, notary offices, and judicial appraisal centers at all levels as nodes of the entire judicial blockchain[[102]](#footnote-103)

The example of the Chinese Cyberspace Courts shows the potential that blockchain has for judicial IPR enforcement but also the legal obstacles that their implementation may find. Generally speaking, despite the integrity and immutability that blockchain ensures, it is usually the case that records protected with this technology are considered private documents, thus the parties need to notarize them to prove their authenticity. Cumulatively, or alternatively, they may provide the appraisal of an (computer) expert to explain to the judge how blockchain ensures the integrity and immutability of the document.

To overcome this problem, China’s Supreme People's Court issued an opinion with special rules for the Cyberspace Courts for identifying the authenticity of electronic data. The opinion proposes to encourage and guide the parties concerned to apply the blockchain technology.[[103]](#footnote-104) In addition, the Cyberspace Courts adopted standards with technical specifications of electronic data, specifications of electronic data standard interfaces and judicial application methods as well.[[104]](#footnote-105) The example also shows that the use of blockchain solutions in the judiciary in other countries will likely require legal amendments

### Alternative Dispute Resolution systems

Alternative Dispute Resolution (ADR) refers to a number of different procedures that parties may use to resolve their disputes. The three main ADR procedures are arbitration, mediation, and expert determination:

1. Arbitration: a dispute is submitted, by agreement of the parties, to one or more arbitrators who make an award which is binding on the parties. Parties may select the arbitrator(s), applicable law, language and venue of the arbitration. An arbitration award is enforceable by national courts under the New York Convention 1958, to which over 165 states are party. There are limited rights to appeal an award.
2. Mediation: a procedure in which a neutral intermediary, the mediator, helps the parties reach a mutually satisfactory settlement of their dispute which may be recorded in an enforceable contract. If the parties do not reach agreement, the mediator cannot impose a decision on the parties.
3. Expert Determination: a dispute or difference between the parties is submitted, by agreement of the parties, to one or more experts who make a determination. The parties may agree whether or not the determination will be binding.

ADR procedures have a number of potential advantages over national court litigation: neutrality, flexibility of proceedings; technical expertise of arbitrators, mediators, or experts; confidentiality of the proceedings (unless the parties agree otherwise); and, with respect to arbitration, relative ease of cross-border enforcement of arbitration awards under the New York Convention 1958. The complexity of disputes concerning digital technologies may require arbitrators, mediators, or experts to have specific technical expertise; such expertise may be particularly necessary in disputes deriving from so-called on-chain transactions – i.e. transactions between the members of a blockchain in relation to assets recorded in it. For wide-scale adoption, in particular by large-scale commercial users, a blockchain solution will likely require some mechanism for resolving potential disputes that arise during the use of the blockchain solution.[[105]](#footnote-106)

Blockchain technology has potential applications in the management of ADR proceedings.[[106]](#footnote-107)

1. Automation. Smart contracts may be able to streamline the administrative tasks related to ADR in a timely, effective and secure manner. For example, a “smart arbitration clause” may be conditionally programmed and its activation made dependent on a particular event constituting a breach of the parties’ agreement.[[107]](#footnote-108) This may trigger the automatic submission of a notice of arbitration to an institution, the commencement of proceedings and the notification to the other party. When the dispute relates to a digital asset in the blockchain, the award may also be automatically enforced.
2. Security. Blockchain can increase security in relation to the evidence related to the dispute and communications between the parties. Somearbitral institutions still use “unencrypted email and commercially available cloud data repositories”. IT systems of parties involved in dispute resolution processes are also vulnerable to cyber-intrusions. Blockchain could potentially help to improve cybersecurity as it can impede fraudulent activities and detect data tampering based on its underlying characteristics of immutability, data encryption and operational resilience.
3. Confidentiality[[108]](#footnote-109). Users of ADR strongly value confidentiality. Blockchain may be an optimal solution to provide a higher level of confidentiality for the participants in the ADR process.

Aware of these potential applications of blockchain to ADR, the UK Jurisdiction Taskforce (part of the LawTech Panel of the Law Society) recently adopted the Digital Dispute Resolution Rules[[109]](#footnote-110) for resolving disputes arising from new technologies such as cryptoassets, cryptocurrency, smart contracts and distributed ledger technology. The Rules allow for automatic dispute resolution processes where a decision may be implemented directly within the digital asset system. In the United States, ADR service provider, JAMS, is working on a set of rules that would apply specifically to resolution of disputes arising from smart contracts – the JAMS Smart Contract Rules.[[110]](#footnote-111)

While other ADR institutions are considering the introduction of blockchain solutions, it has been suggested that public permissionless blockchains may not always provide added value in the context of ADR systems due to their lack of efficiency in terms of processing time and energy consumption.[[111]](#footnote-112) A private-permissioned blockchain would likely be the optimal type of blockchain to be used in ADR systems as it would be most suited to ensure confidentiality and to ensure that only pre-designated participants have control over, and access to, the dispute resolution process.[[112]](#footnote-113)

The most innovative ADR blockchain solutions envisage a decentralized dispute resolution system, which are unlike current established dispute resolution systems. Companies such as Kleros, Aragon, Juris, Jur or Mattereum provide blockchain-based dispute resolution mechanisms in which the nodes of the network act as jurors[[113]](#footnote-114); jurors are asked to anonymously vote on the outcome to the case; the voters who voted for the outcome for which the majority voted are rewarded with a token. Such dispute resolution mechanisms may be particularly useful for on-chain conflicts since a decision can be automatically enforced on the asset tokenized in the blockchain network. While based on similar ideas, these services show differences:

* In certain services, any node can act as a juror, in others, only a few are selected; and in others such as Juris, there are lists of experienced jurors (High Jurists) for complex disputes.
* Some of these services encourage jurors to vote on the outcome on which they think their fellow jurors are more likely to vote. In others, the group of jurors are asked to give a brief opinion.

The fact that jurors are anonymous, and that decisions may not be based necessarily on the merits of each party’s position but on a prediction of how other jurors will vote may be problematic in certain types of disputes. It has been suggested that while this may be acceptable for anonymized disputes in low-risk situations, it is unlikely to be adopted by commericial users because of the inherent uncertainties in a dispute resolution process where an outcome may be based on matters other than the merits of the case.[[114]](#footnote-115)

Furthermore, the lack of a reasoned opinion on the merit and a written award might also be a problem when the decision needs to be enforced outside the blockchain. To solve this, Juris has established the Preemptory Agreement for Neutral Expert Litigation (PANEL) judgment stage which is meant for those disputes in which parties would like to reach a legally binding award under the New York Convention. While this option is costlier, it can provide parties with an award that is legally binding and enforceable worldwide.

Besides the above-mentioned problems, it should be borne in mind that the introduction of any blockchain-based solutions would need to comply with existing legal frameworks in order to be effective. In respect of arbitration, it should be recalled that several national legislations and the New York Convention require the arbitration clause to be in writing, therefore arbitration clauses in smart contracts run the risk of not being enforceable, unless they have an equivalent traditional written contract signed by both parties.[[115]](#footnote-116) If awards cannot be automatically enforced in the blockchain, then awards would also need to comply with the New York Convention requirements, such as the requirement for a final award to be in writing and with authenticated signatures. Furthermore, national arbitration systems may require arbitrators to have certain qualifications and for final awards to be adequately reasoned. Finally, any automation of certain stages of arbitral proceedings would need to respect parties’ rights to due process. It is obvious that decentralized blockchain dispute resolution systems do not fit within the established notions of arbitration. Given the greater flexibility in mediation and expert determination, it may be worth exploring whether such options would be more suitable for certain disputes in the blockchain environment.[[116]](#footnote-117) In any case, there is a pattern among state regulators to encourage the introduction of alternative and online dispute resolution (ODR) in commercial disputes so effective ADR dispute resolution mechanisms may be developed in the future.

### Counterfeiting and Piracy

Counterfeiting and piracy are still one of the main problems of participants in the IP ecosystems. According to an OECD/EUIPO Report, in 2019, fake goods amounts to 3.3% of world trade.[[117]](#footnote-118) Blockchain applications may considerably impact the prevention and prosecution of counterfeiting and piracy activities.

As the EUIPO has expressed, “there are many tools and solutions currently used by businesses and public authorities to identify counterfeits but they work separately, are decentralized, have little synchronization and there is no way to connect all the relevant players: the EU, IP Offices, governments, customs and other enforcement authorities, manufacturers, retailers, shipping companies, ports and airports and citizens. A potential solution to this challenge is the kind of decentralization and synchronization blockchain technology can deliver to create a secure and collectively shared record of authenticity. This should allow the track and trace of an authentic product through the entire supply chain and empower all players involved to tackle counterfeiting more effectively”.[[118]](#footnote-119)

In the private sector, several companies in the pharma, sportswear or luxury industries as well as the spare parts industry are already using blockchain and AI-based technology together in fighting the distribution of counterfeit products with great benefits in terms of fraud reduction and the streamline of the control processes. This can be done by adding a QR code or near-field communication chip (NFC), as well as laser incision marking systems[[119]](#footnote-120) applied directly to the products. Anyone in the chain of distribution up to the final consumer can verify the authenticity of the product by scanning the QR or marking system used and accessing the information gathered in the blockchain (quality and source of the materials used, time of production, authorized manufacturers and importers, etc.).[[120]](#footnote-121) This increases the difficulty of counterfeiting activities and facilitates the detection of suspicious products both by custom authorities and/or by online marketplaces.

An example of an online marketplace using blockchain technology is Alibaba. The Chinese company announced in 2020 a tool to track and verify food items being sold on its platforms.[[121]](#footnote-122) Customers on Alibaba’s marketplace would be able to verify whether the product they had bought is genuine by scanning the code on a product on their mobile.

Counterfeiting is not new and many companies are trying to fight against this activity. Different strategies and technologies are being used, from changing periodically their transport routes and production factories location, to include holograms, smart tags and biometric markers in the products.

Building an anti-counterfeiting platform to trace the routes and the stakeholders involved in the delivery of the goods will make it easier for the enforcement authorities to identify possible counterfeiting products and where the detection and seizing occurred.

This decentralized system will use the information stored in the IP registries of IP organizations, data stored in enforcement authorities’ systems and additional data that will be shared between IPRs holders and enforcement authorities.

In the public sector, IP Australia is using blockchain to provide a solution to supply chain weaknesses: Smart Trade Mark is a digital fingerprint for registered trademark owners based on blockchain technology that establishes product provenance and provides protection against counterfeiting in global marketplaces.[[122]](#footnote-123)

In Europe, in 2018, the EUIPO launched the Anti-Counterfeiting Blockathon, aiming to create a network of people and organizations, from IP and blockchain industries, working together to design and implement a blockchain solution to fight against counterfeiting. According to a use case published by EUIPO, a blockchain system can give their users (right holders) “permissions to create tokens representing goods (tokenized goods) and proving the goods’ authenticity through a Blockchain Access Portal. Rights holders may authorize other parties in the network, such as manufacturing and packaging suppliers, to create and handle tokens on their behalf and record events and information for their goods. The record in the blockchain is a unique and immutable token. As goods pass from one party to another they exchange the token between digital wallets. The combination of a unique product identity and the continuous transferal of the digital identity between wallets create a mathematical proof that the goods are genuine”.[[123]](#footnote-124)

The use of blockchain solutions can also help to streamline the work of customs authorities. The World Customs Organization (WCO) considers that blockchain-based solutions can significantly improve their capacity for risk analysis and targeting, thus contributing to greater trade facilitation.[[124]](#footnote-125) To start with, custom authorities can take advantage of proven authenticity provided by blockchain, to allow the swift clearance of custom’s checks of tokenized goods. Eventually, customs could even automatically clear the goods within the blockchain itself.[[125]](#footnote-126) In addition, the blockchain can automatically generate event warnings that the goods’ integrity is at risk or detect an anomaly as goods pass between parties in the supply chain. Permissioned applications can monitor such events and send notifications to rights holders and custom authorities.[[126]](#footnote-127)

In any case, the efficiency of these systems is dependent on the interoperability among blockchain networks. The EUIPO provides an example of such necessity: The Enforcement Database (EDB) is an essential tool that police and custom authorities in Europe use to identify counterfeits. It contains information provided by right holders themselves on products that have been granted an IP right, such as a registered trade mark or design. EDB features, such as secure authorization and product line definition, are relevant for the development of a solution like the Blockchain Access Portal. It would therefore be a great advantage if both were interoperable, since blockchain would allow immutability and traceability and the EDB would be the link with the right holder and the EUIPO portal. Similarly, the solution should be compatible with other existing systems. It should not seek to replace or duplicate already well served functionality.

Blockchain technology allows the creation of a decentralized platform where all parties involved in the protection of IPRs (enforcement authorities, right holders, IP Offices, and other parties) have access to relevant product-related information. This platform would allow the enforcement authorities and IPR holders to share (confidential) data securely, thereby contributing to support the fight against counterfeiting.

# IV. CONSIDERATIONS

Blockchain has several potential applications in the IP ecosystems. However, the IP ecosystems actors should not let themselves be confused by the hype around blockchain and introduce the technology simply to emulate others. Blockchain implementation might entail considerable investments, the benefits of which the actors need to carefully assess in advance, and if they do eventually introduce it, it is necessary to evaluate what solutions and conditions are the most suitable.

For this assessment, several considerations need to be taken into account: regulatory framework, governance, technical standards, sustainability and scalability, and training. It is up to each actor to analyze these considerations in order to assess whether the introduction of the technology is beneficial; if so, which risks they will face and which measures can be taken to mitigate such risks; and whether it is worth using this technology considering the investment that needs to be made to mitigate those risks. It may be needed that governments and international organizations adopt measures in order to reduce such risks and facilitate the introduction of blockchain.

Before starting the journey for the adoption of blockchain technology, it is critical to determine whether or not blockchain is an appropriate technology to improve or resolve business issues or problems. Like any other technology, blockchain can solve some but not all problems. If blockchain technology is chosen, it should be considered which blockchain should be applied. When defining what criteria should be met, the use of the following decision flow is recommended:

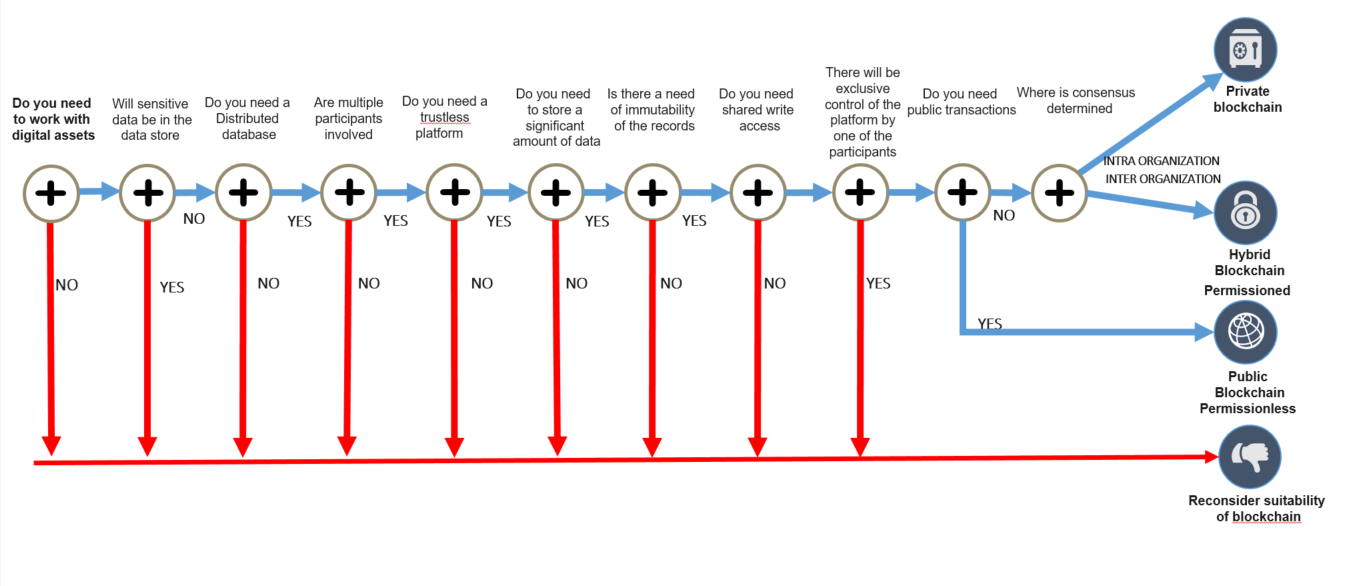


Figure 3: Decision flow

This chapter presents most important aspects and characteristics that should be considered when assessing blockchain technology.  Those are interoperability, standardization, governance, regulatory framework.

## INTEROPERABILITY AND TECHNICAL STANDARDS

Briefly speaking, interoperability can be defined as the ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged. For the technology to deploy its full potential, interoperability between any blockchain solutions implemented by participants in the IP ecosystems needs to be ensured. For instance, interoperability among IP offices’ blockchain would surely allow the achievement of more efficient data exchange in a timely manner where a number of actors participate.

The first pillar of interoperability is the development of common technical standards at different layers such as application, platform, data and security/network layers. Due to the complexity of the field and its diverse applications, the adoption of standards is not an easy process. At present, several standardization initiatives related to specific blockchain features are being developed.[[127]](#footnote-128) However, for the time being, the blockchain industry relies on market-defined solutions, such as the Hyperledger toolset under the umbrella of the Linux Foundation or the Ethereum Foundation, through the Ethereum Improvement Proposals.[[128]](#footnote-129)

In the meantime, formal technical specifications developed by international standardization bodies like the International Standards Organization (ISO) and the International Telecommunications Union (ITU) are gaining traction109 by agreeing on common terminologies, security and other general technical specifications. For instance, ISO has been actively working on DLTs with a specific Technical Committee (ISO/TC 307), aiming to improve security, privacy, scalability and interoperability.

According to the European Commission's latest event report of blockchain standardization, the "Gap in blockchain standardisation: In particular, the lack of interoperability – whether tech to tech, tech to law, region to region, etc. – hinders DLT deployment. Standardization of many of these aspects is lacking. In terms of governance and processes, discussions and leadership are not sufficiently transparent and remain very far from being representative of society, or even of the global interests as a whole."[[129]](#footnote-130)

The Global Blockchain Business Council has identified two key challenges with regard to blockchain standards: (a) aligning standards and codes of conduct across jurisdictions and industries; (b) ensuring that stakeholders of all sizes have a voice.[[130]](#footnote-131) Henceforth, for the development and adoption of common technical standards, all interested parties working on blockchain and/or other distributed ledger technologies should be brought together. It is critical to synchronize and streamline all the efforts so as to promote technology adoption and avoid fragmentation by working cohesively.

In the case of IP space, current technical standards reflect the efforts made towards the realization of a digital transformation of the IP Offices and their services provided to their customers and business partners. WIPO with its Member States has been developing and providing Standards to streamline and harmonize filing, processing, dissemination and exchange of IP data and documentation within the IP ecosystems. For example, WIPO Standard ST.96[[131]](#footnote-132) recommends the XML (eXtensible Markup Language) resources to be used for filing, publication, processing, and exchange of information for all types of IP, i.e. patents, trademarks, industrial designs, geographical indications and copyright. WIPO Standards ST.27[[132]](#footnote-133), ST.61[[133]](#footnote-134), and ST.87[[134]](#footnote-135) provide standardized codes to promote efficient exchange of legal status data of patents, trademarks and industrial designs respectively in a harmonized manner between IPOs in order to facilitate access to that data by actors in the IP ecosystems as well as improving worldwide availability, reliability and comparability of IP legal status data.

As other WIPO Standards were developed and as soon as blockchain technology was tested and used in IP community, WIPO Member States established an expert group under the CWS in 2018, the Blockchain Task Force, to explore its impact on the IP space and to develop recommendations on blockchain for the IP ecosystems. As already mentioned above, interoperability concerns different layers. The following section aims to explain some considerations in regards to standards for the integration among available blockchain platforms, data exchange and security. It is recommended that those should be considered in the development process of the new WIPO Standard on blockchain for the IP ecosystems. It is also recommended to establish partnership with other international standardization bodies and blockchain platform providers to develop the new WIPO Standard.

### Interoperability among existing blockchain platform networks and consortium projects

Interoperability among blockchain networks will be defined as the set of network protocols and best-pattern architectures when orchestrating distributed transactions among two or more blockchains. By network protocol we understand a formal set of messages that can be interchanged between remote peers, following well defined rules and/or protocols, including integrity validation and handling of errors.

There is no common or short-term planned standard in terms of protocol or integration tools among the different blockchain variants (Fabric, R3 Corda, Ethereum, etc.). The possibility to converge to a common solution is impeded due to different internal data structures and runtime environments. For instance, Ethereum-based blockchain technologies choose a simple key-value store on top of which more advanced storage structures can be implemented manually, Corda relies on the assumption of a pre deployed relational database for each peer, Fabric opts for NoSQL storage (key-value for very simple scenarios).

Some efforts are currently in place trying to solve these problems or reducing the friction between the variants in order to create cross-platform applications following different strategies or seeking to tackle the issue from the point of view of concrete technology and particular use case. Also, several working groups and organizations are approaching the problem from the standardization point of view such as the ISO 307 WG focusing on the definition of standard terminology, taxonomy, ontology and governance; [Internet Research Task force](https://irtf.org/), researching open issues in decentralized infrastructure services, or the ITU-T DLT group focusing on the creation of a reference ITU DLT architecture.

It is important to note that interoperability through protocols also allows to integrate and interoperate not only with blockchain, but also with existing solutions (already deployed databases, message queues, ESBs) and can serve as a reference to strengthen current WIPO Standards and IT systems.

In terms of consortium projects, Ethereum standards are being developed in the form of EIP (Ethereum Improvement Proposals), trying to formalize common patterns and use cases in the form of standardized Interfaces.

As a real reference, "[The Baseline Protocol](https://www.baseline-protocol.org/)"[[135]](#footnote-136), is an open-source initiative to combine advances in cryptography, messaging, and blockchain to deliver secure and private business processes at low cost via the public Ethereum MainNet. This initiative is led by the Ethereum-OASIS and funded by the Ethereum Foundation and the Enterprise Ethereum Alliance with the participation of relevant IT companies.

### Interoperability with external and internal blockchain data

Currently, a multitude of isolated blockchain silos are being implemented. Although all are based on the same common technology standards and inspired by the original paper of Satoshi Nakamoto, they vary widely in features and industry adoption. Each of them follows an agreed governance model within their silo. In order to widen acceptability and adoption of the technologies in a wider context and foster trade via smart contract transactions, a degree of interoperability among various blockchain networks, and between blockchain (on-chain) and outside world (off-chain). The interoperability among blockchains will need to be standardized in order to facilitate the exchange between them and harmonize the processes and types of transactions. This should be done to maintain a coherent blockchain ecosystem, keep the value chain intact and represent values reliably and consistently.

Furthermore, the blockchain-based systems are connected to and interacted with off-chain systems such as data providers, web APIs, enterprise backends, cloud providers, IoT devices, e-signatures and payment systems in order to get data from the real world and execute their transactions. Therefore the interoperability between blockchains and the connected off-chain systems are also crucial. Bridging the two worlds requires additional and separate systems known as oracles which gather and store data from the real world and provide the data for blockchain. There are various discussions and initiatives concerning blockchain oracles, which include oracle problems with the trustworthiness and reliability of oracles, and interoperable data format because oracles act as a bridge that can digest external and non-deterministic information into a format that a blockchain can understand[[136]](#footnote-137). The external data refers to any type of information stored digitally in any structured and unstructured format, created by any off-chain systems or procedure external to the blockchain. The interoperability standards themselves will likely require a set of governance and/or regulations in order to give a legal and/or operational certainty to the participants in the value chains.

Corda, designed to co-exists with systems already in place, is currently the most suitable platform to operate with existing external data. Corda, by design, supports data in XML format and integration with SQL, allowing users to synchronize DLT peer-status to their own internal SQL databases for further reporting or analysis. While Corda is a supportive platform for external data interoperability, other blockchain platforms such as Hyperledger Fabric and Ethereum, at the moment of this paper is prepared, do not support any standard support for interoperability with external data. In the case of Hyperledger Fabric, the code can be implemented "ad-hoc" using any runtime supported by the Linux container technology but code must be maintained internally. With Ethereum, the payload could be codified in the transaction. Both Hyperledger Fabric and Ethereum can add blockchain client support, in the form of middleware of libraries, to translate the external data to/from SQL sources, always in an ad-hoc way.

Internal data refers to any information stored digitally that can be consumed by software applications inside the blockchain. Some efforts, led by IEEE Standards Association (IEEE SA),[[137]](#footnote-138) exist in the form of working groups (IEEE 2418.2-2020 - IEEE Standard for Data Format for Blockchain Systems[[138]](#footnote-139)) to push standardization of data format for blockchain systems.

Talking about existing platforms, similar to the interoperability with external data, Corda offers excellent support to manage internal data, since this is a must-have feature by design. The Persistence API allows automatic export to SQL databases, while the internal historical status ("provenance of current data") is easily accessible through the Vault Queries API.

The Ethereum community has developed versatile tools to integrate transaction execution output with external systems. By design, Ethereum is a stream-of-event architecture, and external clients can subscribe to receive historical and real-time events upon successful transaction execution. Some examples can be cited, like [Eventeum](https://github.com/ConsenSys/eventeum), bridging blockchain events generated by transactions to backend decoupled microservices for further processing; [Alethio](https://aleth.io/), connecting Ethereum data to IA services for advanced analytics; or [EtherQuery](https://github.com/Arachnid/etherquery) allowing to uploads blockchain data to BigQuery.

Of special relevance is the integration of GraphQL, a new cross-technology standard for complex query of graph-like related data, allowing to simplify the way to extract data from the blockchain. An even more advanced technology is reached by the Graph Protocol, a decentralized network protocol for indexing and querying data from blockchains, enabling to expose internal blockchain entities and indexes to external clients. While the project aims to be blockchain technology agnostic, the first working version is just Ethereum compliant.

While all blockchain platforms can be considered, so to speak, "secure by design", compatibility with existing security technologies is taken for granted in modern IT infrastructure systems and different blockchain solutions can offer different support for them. Among others, the following security technologies should be considered when a blockchain platform is selected and a blockchain application designed:

1. Public Key Infrastructure: PKI and X.509 UIT-T are well supported by blockchain platforms like Hyperledger Fabric or R3 Corda. Both Fabric and Corda define services and users' identities around X.509 certificates, PKI, CAs allowing reuse of existing infrastructure. Ethereum, on the contrary, will need an Ethereum-centric approach, with wallets as alternative to X.509 certificates.
2. eIDAS regulatory framework for Digital Signature: it is to be expected that all blockchain will be compliant with this framework, but probably with higher efforts based on cryptography constraints.
3. OASIS Digital Signature Services: Oasis DSS defines the basic functionality for the creation (SignRequest /-Response) and validation (VerifyRequest /-Response) of CMS- and XMLDSig-compliant signatures. This standard is widely adopted in some industries. Newest standards have adopted JSON and OpenAPI ("swagger Remote HTTP API definition) and adapted to be eIDAS compliant.[[139]](#footnote-140)
4. Other approved security schemes: It is important to analyze any mismatch of the to-be-adopted blockchain platform with the existing security standards in order to guarantee compatibility between them. Ethereum, being designed as a network-on-isolation, is expected to offer more friction, while DLT technologies able to integrate with existing SQL DDBBs are "theoretically" more friendly to existing IT deployments.
5. Standard Authentication, Authorization and Access systems (AAA): the requirement to be compliant with existing AAA systems (OAuth2, Kerberos, LDAP/AD) can influence the final decision or modify the design of the proposed architecture.

## GOVERNANCE

The second consideration that actors in the IP ecosystems need to take into account is governance when considering the introduction of blockchain solutions. As the governance for blockchain networks is urgent and important, there are several efforts underway by different institutions with different approaches based on established governances such as corporate governances or IT governances. The concept of blockchain governance is still under discussion and it can be understood differently depending on the domain of the application area. In this paper , governance refers to the means to adopt decisions in a distributed network in accordance with the goals and interests of the stakeholders. Blockchain governance can be categorized into two types: *on-chain* (decisions related to the underlying software) or *off-chain* (decisions related to the management and structure of the network).

The governance framework - or governance of the network- should be discussed at an early stage and agreed upon before implementation. The framework will be radically different depending on the blockchain solution, whether we consider a solution based on a public permissionless network or designing a use case on a permissioned network, either public or private. The consensus mechanism of the protocol will be different in each case.

### Four foundational elements of governance

When designing the governance framework, promoters of the network should take into account the following four foundational elements:

1. Participants. Accurately identifying participants and align the implementation scope with their expectations. This would cover the *stakeholders.* 'Who are the network's participants?' is the proper question to ask at this point. Stakeholders can be IPR holders, creators, regulators, IP Offices and alike.
2. Values and Goals. Identifying the *Values and Goals* of the blockchain networks. Answering the question "What are the values that we all agree on and what is the ultimate goal that we want to achieve?" will later define the technical guidelines and the internal policy strategy. Values are part of the internal system guiding the behavior of all the participants. A clear and overt definition of the values and goals can divert, for instance, the governance model from a centralized one, to a more open model offering collective and transparent participation.
3. Incentives. Identify aligned incentives for the participants. Enterprise blockchain initiatives should take the power of incentives in the governance model seriously. The incentives should be designed to align the actions of different participants in the value chain. While the organization values address the participants' expected behavior as a collective, the incentives aim to drive their action. Therefore, after profiling the blockchain ecosystem participants, any incentive model should be created with special consideration of the regulatory compliance, policies and best practices, and decision-making mechanisms.
4. Dispute Resolution Mechanisms. Establish Dispute Resolution mechanisms that can be applied to potential problems. As a basic governance requirement, a responsible party to address problems is needed. For DLT/Blockchain initiatives, either unintended or unwanted behaviors from participants or unforeseen events can occur at any time. Even external events outside the network could trigger problems and disputes. The organization should consider its own rules to solve arising problems among participants and alternative dispute resolution processes.

Each of these four elements represents the foundation and the starting point for the design of any governance model and should be aligned with each organization internal governance framework.

As an example, transparency will become part of the existing organization values because it would be necessary to guide the participants to work in this new environment. The policies will include guidelines for the stakeholders, and new measures will be set to penalize unwanted practices. A similar case could be a new "segment of stakeholders" due to the nature of a distributed network. The same considerations apply to the set of incentives of the participants and to the way conflicts should be solved on a new network.

### Governance framework: aspects to address

After concluding the foundational elements mentioned above and depending on the scope of the blockchain implementation, some other considerations should be made regarding theinfrastructure and the chosen framework.

#### Legal structure

A legal structure is one of the governance element that gives legal recognition, and a framework of decision rights and accountability to the network in practical and enforceable ways. Decision-making power can be centralized to a single entity/ person or small group (centralized), or decentralized to participants. The decision to register the legal structure in charge of the blockchain in a given jurisdiction in which its legislation guarantees favorable conditions is both a governance and a regulatory challenge. This legal structure will become the governance entity, with the aim of documenting and setting the rules by which participants of the network are expected to comply. This set of rules are based on the blockchain infrastructure and framework chosen for the network. This is the main reason why the legal entity should be considered within the governance of the network and not only in terms of regulatory benefits. Through its statutes, the governance entity may monitor the nodes’ behavior and their relationship with each other, the authorization levels, mechanisms of dispute resolution, and responsibilities of the parties, among other considerations established by the technical architecture. The right choice for this legal structure is a challenge worth considering. Certainly, blockchain networks can be informally developed by groups of participants in the IP ecosystem with the aim of facilitating cooperation or even as trading platforms. While in the beginning, it might be difficult to identify an entity responsible for the network and problems concerning the anonymity/pseudonymity of some participant may arise, however, in the long run these blockchain technologies should develop some kind of governance structure and adopt legal status to avoid legal problems.

#### Type of blockchain network

In the process of designing and implementing a blockchain network, the topology of the network should be defined by the different types of nodes, the different tasks nodes can perform, and the way they will be connected to each other. Based on that, the topology's final decision will have an impact on the governance, security, scalability, and latency of the network.

Most of the public-permissioned network topologies are oriented by the use of two main groups of nodes. On one side, validator nodes participate in the consensus mechanism creating new blocks and maintaining the network's functionality. On the other side, writer nodes are enabled to generate the transactions to be recorded in the network and read and access information from the network.

#### The consensus mechanism

The consensus mechanism constitutes the primary representation of governance on a blockchain network. The decentralized and anonymous (or pseudonymous) transaction validation process between nodes has a direct dependency on the consensus mechanism. However, not all the networks have the same design, topology, and consensus mechanism. The consensus mechanism establishes the incentives between nodes based on the network's design and the role each type of node will play on it. Thus, it is mandatory to understand whether the network is a general-purpose one or if it is a special-purpose network. The first is built with the capacity to build on the top through smart contacts the way Ethereum, NEO, or EOS works, or if it is a special-purpose network, for instance, Bitcoin; Litecoin or Dash where the goal is to serve as efficient electronic payment systems.

When designing the consensus mechanism, it is not a matter of deciding which one is better, but which one is more aligned with the business requirements. The design of the network and the consensus mechanism could vary drastically in each case, as well as the consideration of having intermediaries in the network. A cost and benefits analysis for the four primary consensus mechanisms is depicted in the following table:

|  |  |  |
| --- | --- | --- |
| **Consensus method** | **Benefits** | **Costs** |
| **PoW** | Suits trustless network  Low governance overhead | Slow transaction time  High resources consumption |
| **PoS** | Low governance overhead  Incentivises investment in the system  Short transaction time | Prone to ‘fifty-one percent’ attack for smaller systems Requires some level of trust |
| **PoA** | Short transaction time  Low resource cost | Needs administration of participants  Owners need to manage nodes and miners  Requires a high level of trust |
| **Round Robin** | Low resource cost  Can be added to other methods | Needs administration of participants  Owners need to manage nodes and miners  Requires permissioned network |

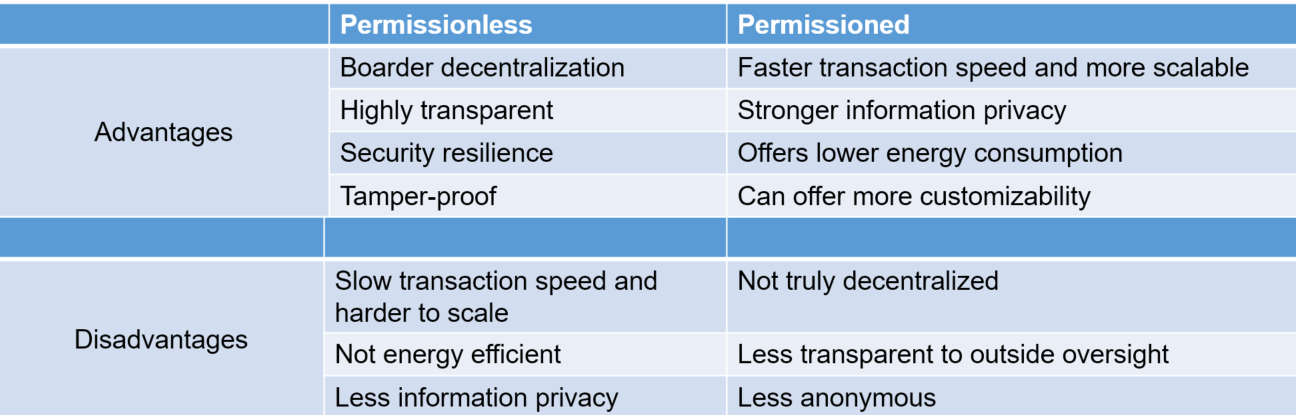
[Table 3: comparison of consensus model]

Permissionless blockchains do not require permission to join it from any authority. All participants are unknown and the transactions stored in the blockchain are validated by the participants. The first reference of permissionless blockchain is Bitcoin which uses the Proof of Work (PoW) consensus algorithm and has shown to be the most efficient mechanism for the so-called miners in the transaction validation process.

On the other hand, Ethereum is another permissionless blockchain with a different consensus algorithm. Proof of Stake (PoS), althought for general-purpose networks with high-level transaction demands, it has demonstrated to be less inefficient than PoW, due to the transaction costs, volatility, and scalability for public permissionless networks.

Permissioned blockchains are closed networks that require permission to join from an appointed authority that has the ability to decide who can or cannot be part of the network. Permissioned blockchains are built to establish rules for transactions aligned with the participants' needs and the information is validated only by approved members of that blockchain. Hyperledger Fabric, Corda, Quorum are a few examples of permissioned blockchains.

In summary, permissioned blockchains are more centralized and tend to be faster, more scalable and sustainable. Permissionless blockchains are more decentralized but slower and less scalable. Due to the fact that network-wide transaction verification is used, they require a high level of energy consumption. There are benefits and drawbacks for each of them, and the most relevant are summarized in the following table:



[Table 4: Advantages and disadvantages of permissionless and permissioned blockchain]

#### Terms and Conditions

The Terms and Conditions are the set of rules governing the external relationships between the service provider and the end-user. This acceptance of use agreement covers the following issues; privacy practices, limitation of liability or disclaimers, IPR, advertisement or endorsements, payment terms, termination, notifications, contact information, and dispute resolution method.

#### Operational Guidelines

Operational Guidelines are the internal operating rules the participants have to follow according to the topology and functionality of the network. These rules are related to network administration and management as well as security operations. Some of the issues that the operational guidelines must cover are the period of operation, network routing models, updating, removing and adding nodes, testing procedures, encryption key administration, security operations, security operations, etc.

#### Data Governance

Data is the core of a blockchain network. The main challenge associated with data is where multiple participants have the role of sharing, validating, and recording data on the ledger of the network’s ledger(s). In the blockchain field, like in any other type of network, a clear understanding of data ownership, its authorized uses, its IP implications, data collecting and hosting mechanisms and regulatory restrictions are essential parts of the data governance model.

Furthermore, in the case of public-permissioned blockchain networks, a transparent data governance model is mandatory, not only to determine by whom, when and how data can be generated or accessed to the network, but also to define what role each node has to play in the operational and functional model of the network.

An efficient data governance model demands the adoption of a set of policies and standards that should be committed and accepted for all the network participants, granting the best coordination possible and complying with the current data regulation.

The terms and conditions for users, as well as the disclaimers and disclosures of the network, should be aligned with the data governance model at any time. Furthermore, it should be noted that self interest driven and trustless nature of blockchain foundational concepts and design requirements on entities ensure that incentives and proof are in place. It is worth a special mention of the IP Offices and their potential role as stewards in the network as part of their duties and responsibilities.

Placing data that is not ‘Open for Public Inspection’ (OPI), known as ‘non-OPI data’, onto a blockchain needs to be carefully considered and will depend on the principle of ‘*who has access to see the blockchain will have access to the data*’. Those who can see the blockchain, should also be properly authorized to view all data on the blockchain. When considering the design of a blockchain for non-OPI data, you should consider why you are using blockchain for this data at all. If you can trust all of the users enough to share non-OPI data and your security is robust enough to ensure only trusted users have access then why is a blockchain required?

It may be appropriate to record a transaction on a blockchain that documents that a transaction effecting a non-OPI asset has occurred without providing any of the non-OPI information. e.g. the sale of an asset, such as land or a business, may need to be on a public register so ownership of the asset is public knowledge but the sale price or some other conditions of sale may be considered commercially sensitive and there is no legal requirement to place such detail on a public register.

#### Blockchain framework and infrastructure

269. One of the most important technical decisions to be made is choosing the most suitable blockchain framework. This choice will be paramount for the design of the governance model. There are at least six major frameworks that can be used for an Enterprise DLT/Blockchain implementation (R3 Corda, Ethereum, Hyperledger, Multichain, Hedera Hashgraph, Roostock).

270. Back in 2018 the considerations mentioned before were not very clear. The offer of a general-purpose blockchain protocol was limited to Ethereum. Some significant advances came from permissioned models. Between 2018 and 2020, after initiatives based on protocols like Quorum (JP Morgan Chase) and Pantheon (ConsenSys), a new concept of public-permissioned networks was created and defined by ISO 307 typology[[140]](#footnote-141). This public-permissioned approach was adopted by initiatives like the European blockchain Services Infrastructure (EBSI) and LACChain, a global alliance led by the Inter-American Development Bank (IDB) for Latin America and the Caribbean.

271. The public-permissioned model aims to solve the need to legally identify the network participants in terms of compliance, considering the liabilities and accountabilities they have off-chain. At the same time, the public component allows the general public to access information by definition.

272. On the other hand, the possibility of implementing different node profiles, competencies, authorizations, and capabilities allows the network promoters and developers to customize and align the network functionality according to off-chain regulations.

273. One of the significant challenges for public-permissioned infrastructures is the design of an economic model with precise and efficient incentive mechanisms for all of the participants to economically contribute to developing, deploying, maintaining, and finalizing the network operation.

274. Based on the evolution and development of public-permissioned initiatives like EBSI and LACChain, their main benefits are the network effect, the decentralization (with compliance) and the cooperation for the construction of a public and shared infrastructure.

## REGULATORY FRAMEWORK

275. Nowadays, there is a unanimous position among institutions concerning the potential of blockchain. However identified strong benefits are coupled with a high level of legal uncertainty, with regard to the technology.[[141]](#footnote-142) This uncertainty concerns central aspects of the technology as such and some of its applications, in particular smart contracts and tokens. Participants in the IP ecosystems must take these considerations into account when deciding whether the introduction of a blockchain solution adds value to the existing technology or not; if so, which solution would be less risky from a legal point of view; and which measures could be adopted (i.e. when designing the governance structure) to mitigate such risks.[[142]](#footnote-143)

276. It should be noted that legal uncertainty does not only refer to the IP-related legal framework, but also to other regulations that the actors in the IP ecosystems need to take into account when implementing these solutions. This includes, among others, contract law, procedural law, law enforcement issues or personal data protection. In this section, the paper will briefly address uncertainties surrounding the potential applications of blockchain in the IP ecosystems identified in Section III. Legal uncertainty is increased by the fact that participants in a blockchain can be established in multiple jurisdictions.[[143]](#footnote-144)

277. The international organizations have not neglected this problem. It is generally agreed that blockchain-based innovation should rely upon an easily understandable, predictable and relevant legal framework. Without it, startups with new ideas may not pursue them in fear of future legal liability, large-scale platforms may struggle to find users as many of them may be wary of blurred legal areas, and new types of digital assets could struggle to find buyers and sellers over concerns about running afoul of regulators.[[144]](#footnote-145) With such aim, works have already commenced at national, regional and international levels.[[145]](#footnote-146)

### Uncertainty in relation to the general aspects of blockchain

*278. Lack of a central authority*. The first regulatory challenge of blockchain derives from one of its core characteristics: decentralization. The absence of a central authority in certain blockchains has been raised as a concern, as this may entail that there is no entity responsible for legal compliance[[146]](#footnote-147) and ultimate accountability for the data exchanged.[[147]](#footnote-148) The degree of difficulty gets higher because a blockchain network does not need to be rooted in any specific location: nodes and users can be established in multiple jurisdictions. Hence, identifying the entity responsible for the network or for an action taking place in the network, and identifying the law applicable to determine compliance might be highly complicated. The latter can make it difficult for competent authorities to perform basic legal and regulatory functions, such as ascertain liability, determine what law is applicable in a particular situation, carry out regulatory monitoring, or enforce rules.[[148]](#footnote-149)

279. While these problems exist, they should however not be overestimated. As explained in the first section of this white paper, there are different levels of decentralization in the blockchain space. On the one hand, permissionless blockchain networks are open to anyone with the necessary hardware and know-how to participate in them by operating a node. Thus, if the necessary measures are not adopted (e.g. in the governance framework) these problems might appear. However, on the other hand, private-permissioned blockchains will generally have a legal entity at their core and established mechanisms to identify nodes and users in their governance frameworks.[[149]](#footnote-150) This would be the case of blockchains administered by an online intermediary platform (e.g. Kleros or Jur), by a private consortium of actors in the IP ecosystems, or those that can be deployed by IP Offices, whether individually or in groups. In such cases, identification of the accountable entity for legal compliance of the blockchain should not be a problem.

280. *Cross-border issues*. It is usually the case of participants in a blockchain (founder, nodes, and users) located in different jurisdictions.[[150]](#footnote-151) This creates a higher degree of uncertainty due to the difficulties associated with establishing what law should be taken as a reference for legal compliance, which one should be applicable in case of on-chain or off-chain disputes, and which state authorities have jurisdiction to monitor the blockchain or to hear such disputes.[[151]](#footnote-152) Legal uncertainty increases where the different jurisdictions the blockchain is connected to adopt different approaches to regulatory issues.[[152]](#footnote-153) This can make it difficult to design a governance framework meeting the legal requirements of all jurisdictions the blockchain is potentially connected with. This is further sustained, as the solutions provided to these challenges by private international law rules are not adapted to digital technologies and decentralized platforms, such as blockchain. This might not be rightly so: existing instruments in the field (such as Brussels I, Rome I and Rome II Regulation in Europe) are flexible enough to be applied in the digital environment. In any case, the main international organization in this field, The Hague Conference, has initiated works with respect to the private international law implications of DLT.[[153]](#footnote-154)

281. *Pseudonymity*. Another problem refers to the various degrees of pseudonymity and in some cases anonymity that blockchain-based platforms can provide to users and miners. This makes it difficult to know who is using the platform and to what end. . This might be a considerable obstacle when enforcing the law and imposing penalties and sanctions. However, this can be solved by employing digital identifiers that can be used within a blockchain context to identify and validate an identity. Again, this problem depends on the category of blockchain. In private-permissioned blockchain, all actors (nodes and users) are identifiable and accountability is easily determined. In public permissionless blockchains, the entries in the ledgers are immutable, providing an audit trail and evidence of wrongdoing. With some effort, parties behind an illegal transaction can be unmasked. It should be also borne in mind that open source ecosystems, such as Ethereum, which are widely used for blockchain projects, do not support anonymity.[[154]](#footnote-155)

282. *Personal data protection*. Plenty of personal data is stored and flows through blockchains. For instance, the data-as-asset analyzed in the former section might be traded in the blockchain and may include personal data. In addition, when participants in the platform are physical persons, the contact details they provide, and the trace they generate about the trading with their digital assets would be considered as personal. Most of the legislation in this area (including the GDPR) was written before the rise of blockchain and was therefore conceived with more traditional, centralized data-processing paradigms in mind.[[155]](#footnote-156) This has led to tensions between blockchains and the personal data protection regulations. The more decentralized blockchains are the more difficult it can be to identify data controllers and processors in charge of complying with the legislation. This is not only a problem for law enforcers but also for data rights subjects who may not know whom they should contact to exercise their rights. Such exercise of rights can also be difficult for other reasons. As previously explained, data that is recorded on a blockchain can generally not be altered or deleted (or better, not without leaving a trace on the blockchain). Thus, how can data subjects exercise their rights to be forgotten, to the rectification of personal data, to know if one’s data is being processed or the right to be protected from decisions made only on the basis of automated data processing?[[156]](#footnote-157)

283. *Data location requirements and data retention rules*. Certain Member States have adopted legal measures requiring digital platforms in general or in specific sectors to store data in infrastructures located in their territory taking into account data sovereignty. In other cases, these measures forbid or impose strict conditions for the transfer of such data abroad. These measures can constitute an obstacle to set up blockchain with nodes located in different jurisdictions since, per definition, the information on the blockchain is replicated in each of them.[[157]](#footnote-158) States are adopting legislation[[158]](#footnote-159) and specific rules in free trade agreements against these categories of measures to facilitate the free data flow.[[159]](#footnote-160) However, many States still endorse data location requirements with different objectives.[[160]](#footnote-161) This may constitute an obstacle for the deploying of multinational blockchain networks

### Uncertainty in relation to some applications of blockchain

284. *Legal value of digital registries*. Another issue related to blockchain has to do with the legal value before public authorities, such as judicial courts, of blockchain-based signatures (e.g. who performed the transaction), timestamps (e.g. when it was carried out), validations (e.g. who validated the transactions) and “documents” (i.e. the data associated with a transaction or contract).[[161]](#footnote-162) It is generally accepted that the validity of digital documents cannot be denied just on the sole fact that they are in electronic form. However, they may not be considered public documents. Therefore, as explained above talking about blockchain applications for IPR enforcement, in order to be able to submit blockchain-based records as evidence before public authorities or judicial courts, these may require accompanying explanatory documentation. Furthermore, in relation to digital signatures, at least in Europe, they need to be recognized by a Trust Service Provider (TSP) in accordance with eIDAS Regulation to be legally binding.[[162]](#footnote-163)

285. The introduction of blockchain solutions by IP registries should be accompanied by legislation ensuring that electronic records in the registry are considered public documents before other authorities without a notarization being required. If, over time, blockchains are implemented as replacements or alternatives to current registries, states should consider the feasibility/pertinence of recognizing constitutive effects of registration and bona fides effects to the digital information stored in blockchains.[[163]](#footnote-164) There are on-going projects in relation to real estate registries[[164]](#footnote-165) that can be taken as an example for IP registries.

286. In the judiciary field, following the example of China and its Cyberspace Courts, legislation to facilitate blockchain-based records as evidence would be needed as well. As the cited Study of the European Commission shows, there is a lack of legislation on the use of blockchain in the judiciary field in Europe.[[165]](#footnote-166)

287. *Tension between the information stamped in the blockchain and legal reality*. Situations may arise where on-chain information conflicts with or differs from that in the real-world or external data system (off-chain information), for example, when a transfer or a cancellation of an IPR is recorded in an off-chain registry, but it is not reflected on-chain. If the information on the same object is different, there is an issue on which information should be taken, but this is not a new challenges compared to other digital technologies.[[166]](#footnote-167) This issue is also related to the blockchain oracle problem. For information coherence and assurance in blockchain, countries such as Liechtenstein have introduced the role of “physical validators'', the main function of which is to ensure the connection between the physical object and the token that represents rights to it.[[167]](#footnote-168) Nonetheless, this approach could reduce the efficiency of decentralization of blockchains even though it may facilitate the reflection of changes in legal reality. Appropriate governance structures will likely make it possible to reflect these changes[[168]](#footnote-169).

288. *Smart contracts*. Legal uncertainty in relation to smart contracts starts in the definition of the term itself. As explained above, smart contracts are just computer codes, often self-executing, that make use of blockchain properties in many contexts. In certain cases, such code can be used to execute an existing legal contract (i.e. the smart contract is the means of executing a classical contract in a natural language) or can constitute a legal contract itself (i.e. the computer code itself would include the legal agreement in its entirety). In the first case, we talk about smart legal contracts while the second is about smart contracts with legal implications.[[169]](#footnote-170) In case of the latter, dispute resolution mechanisms should be in-built in the smart contract and provide a legal basis that is clearly articulated in case of a dispute or error. It should further be noted that use of Smart contract or any blockchain code off opensource, may be bound by open source requirements or certain terms and conditions.

289. It is widely accepted that smart contracts are enforceable under general principles of contractual law (freedom of contract, including on the form in which the contract is concluded).[[170]](#footnote-171) Nonetheless, many States have either proposed or enacted legislation applicable to smart contracts or contracts in electronic format.[[171]](#footnote-172) As previously mentioned, it is widely admitted that contracts cannot be denied validity due to their electronic format. Furthermore, it is generally accepted that in those cases where the law requires the contract to be concluded in writing, such requirement is met if the contract is stored in a durable medium.[[172]](#footnote-173) This is relevant from the point of view of IP, since it is usually the case that IP licenses must meet this requirement. It is, however, doubtful whether a smart contract would comply with this requirement if the contract is not expressed in a semantic language that the parties can understand. In this regard, it has been affirmed that “where national law requires a written contract, a smart contract consisting only of the computer code would not be enforceable whereas a combination of semantic and smart contract likely would be”.[[173]](#footnote-174)

290. Once recorded in the blockchain, smart contracts cannot be changed. Once these are integrated they are executed. While this type of contractual automation can be seen as an advantage, it may raise legal questions difficult to answer. What happens if the legal document and the computer code differ? What if the applicable law changes or *force majeure* situations – e.g. a pandemic such as COVID19 - arise? What happens if a court orders that a smart contract is unenforceable? Such decision may arise when the smart contract obligations have already been automatically performed, what happens then? Since no case laws currently exist on these matters, governance frameworks need to provide solutions to these questions. From a technical point of view, amendments to a smart contract can be introduced by ‘overriding’ it with a new smart contract.[[174]](#footnote-175)

291. *Tokens*. As explained above, tokens are data on a blockchain that represent a certain value, right or obligation. Smart contracts are used by users of a blockchain network to transfer tokens from the wallet of one of those users to others. Tokens represent certain rights and obligations which in the past would rather have been represented by paper copies and traded as such. Tokens can have different functionalities depending on the specific use case. These are primarily divided into four categories: investment token, utility token, currency token and hybrid token, however, the differences between them seem minor. Furthermore, tokens can combine multiple functionalities. From a legal point of view, this is problematic: depending on how a token is classified, regulatory obligations differ. There is uncertainty as to what classes of tokens fall within the scope of existing regulations.[[175]](#footnote-176) This uncertainty augments due to the absence of uniform definitions.[[176]](#footnote-177)

292. While most jurisdictions have not yet adopted specific legislation, others have or are in the process. This may drive entrepreneurs in the blockchain sector to specific jurisdictions that provide a more favorable regulatory framework with a lower degree of regulatory uncertainty.[[177]](#footnote-178)

### Ongoing works on the regulatory framework adaptation

293. There is emerging consensus that the adoption of legislative instruments will reduce legal uncertainty and encourage innovation in relation to digital technologies in general.[[178]](#footnote-179) In this sense, as shown by the documents cited in this section, international organizations such as UNCITRAL, UNIDROIT,[[179]](#footnote-180) The Hague Conference on Private international law, or the European Union are already exploring the best legislative options. At the same time, there are works in process in several jurisdictions.

294. Any instrument adopted in this field should foster the use and development of emerging technologies from a digital economy and should not be used as an obstacle to such use and development. In that sense, it seems too early to impose a rigid regulation on a technology subject to dynamic evolution.[[180]](#footnote-181) In this regard, at the first stage such instruments may take the form of minimum standards or guidelines – i.e. soft law.

295. It is advisable that texts with the broadest international scope possible are adopted. In this regard, the works UNCITRAL has initiated with its *Report on Legal issues related to the digital economy[[181]](#footnote-182)* seem to be a good starting point. The work plan proposed by the UN Secretariat to UNCITRAL includes, among other issues, preparatory work on legislative text dealing with automated contracting (including smart contracts), asset tokenization and digital assets in the form of cryptocurrencies. As established in its mandate, “international efforts to develop a harmonized response to legal issues could preempt fragmented national legal responses and contribute to bridging the digital divide”.

296. Having been assigned by the UN General Assembly as the core legal body in the UN system to coordinate legal activities in the field, the recommendation of the UN Joint Inspection Unit seems pertinent: “encourage Member States to engage with the UNCITRAL in its exploratory and preparatory work to avoid duplication of efforts, including among organizations and to promote efficiency, consistency and coherence in the modernization and harmonization of international trade law”.

297. These legislative initiatives do not excuse WIPO and public actors in the IP ecosystems from assessing whether the existing legal framework is adapted to the possible introduction of blockchain solutions.

298. For instance, it seems necessary to assess if certain amendments to the regulatory framework are needed for the implementation of blockchain solutions by IP registries. This is an assessment that needs to be made by each national or regional authority in relation to their corresponding regulatory systems. For instance, IP Offices would need to assess whether the introduction of blockchain solutions to streamline the registration process would be supported by current regulations governing the registration procedures or whether amendments would need to be introduced.

299. The same goes for those cases where blockchain is introduced for the purpose of facilitating cooperation among different IPOs. As previously explained, the potential benefits of the technology increase if blockchains are created among several IP Offices that interconnect their registries. International legal instruments that govern the relationship between the states and these IP Offices need to support the use of this technology.

## SECURITY

300. The cryptographic and decentralized character of blockchain increases the robustness of public and private ledgers and ensures the immutability of the embedded information in them. However, cybersecurity threats cannot be underestimated. Recent Bitcoin-related hacks have demonstrated security flaws despite total encryption and usage of state-of-the-art cryptographic protection measures. Some security issues that should be considered include forking, consensus rigging, Distributed Denial of Service (DDoS) node attack, long term threat from quantum computing among others. In many cases these flaws were due to deficient management by the keys users (e.g. they are stolen or lost) who needed to participate in the blockchain. Adequate measures to manage these risks need to be implemented by the blockchain administrators of blockchains.

301. Blockchain has the ability to transform current systems towards a more transparent model in which information can be constantly verified throughout the life cycle or value chain of a product or service. Through the use of blockchain we can verify in real time, who is the owner of a good or asset and to read the information linked to it and transfer its ownership to another participant of the network without giving rise to fraud. In other words, the level of traceability of the information, which blockchain provides in combination with the consensus between the nodes of the network for a transaction to be carried out, could eliminate the cost derived from the possible fraud.

302. Blockchain has not only the ability to detect an error or attempted fraud within the network, but it also prevents this from occurring thanks to the power of the network nodes over the transactional information of the same. The fact that a database is based on blockchain technology implies that it has the ability to analyze and detect the veracity of the information in real time so that patterns of fraudulent behavior can be detected and stopped instantly. But when talking about risks, it is not just about fraud. Sometimes a human error can lead to mistakes in the execution of processes, such as payroll, and so on.

303. Through blockchain, the execution of contractual clauses can be automatically ensured without giving rise to execution errors, consequently avoiding the costs derived from claims and legal processes that may arise due to this type of errors. In relation to this, numerous business models have emerged, the best known of which consists of automatically refunding the amount of an airline ticket in the event of a flight delay.

## SUSTAINABILITY AND SCALABILITY

304. When talking about blockchain technology, warning voices have been raised about the high energy consumption of this technology. Blockchain, especially in a public permissionless implementation, is computation-intense and requires a lot of computing power. The degree of required computing power depends on the chosen type of consensus mechanism and blockchain, either permissioned or permissionless. Most of the energy used for blockchain operations comes from coal and carbon-based fuels, thus impacting the environment.[[182]](#footnote-183) The latter phenomenon is partly due to the scalability of the technology. For instance, energy-intensive technical consensus processes, such as ‘proof-of-work’, require a large number of operations per second and therefore large amounts of computational and energy resources across the datacenters in which they are hosted. This continuous upscaling may reach a sustainability limit requiring different strategies other than simply adding CPUs, and it should be avoided as much as possible. There are other existing energy-efficient alternatives, such as the ‘proof-of-stake’ that implies a lower energy-intensive effort.

305. Another important challenge of this technology is scalability, i.e., its ability to multiply the number of transactions per second, without creating bottlenecks or losing reliability. By design, the blockchain consensus limits the number of transactions per second to warrant a global vision of the blockchain state among (potentially thousands of) nodes in order to warrant strong consistency. While some consensus have been tuned for optimized throughput, they still lag far behind what would be expected in a standard warehouse database in which scalability can be achieved through hardware upgrade and for which the consistency level can be relaxed.

306. Better results could be achieved by reducing the number of validator nodes, always at the cost of increasing the trust in a reduced set of centralized nodes or also increasing block size which is the number of transactions accepted per block at the expense of a higher response time. It must be also noticed that the consensus shall balance throughput with other aspects, such as the level of "trust-less" and/or responsiveness, and that most of the time extreme throughput is not an issue. By comparison, it is expected that a user interacting with an online application will execute hundreds of commands in a single session, but that the same user will not file more than a patent per year on average, since value is "something scarce" by its very nature.

## TECHNOLOGY GAP AND CAPACITY BUILDING

307. Frontier technologies, in general, bring opportunities to improve business operational efficiency and to transform a way of working and thinking to more effective manner. However the adoption of those technologies has different phases and various manners due to different interest and situations that different actors have. If businesses among the actors are not so interconnected, the differences are not so critical. However, IP ecosystems are closely interconnected, it would be desirable to reduce the technological gap between actors through collaborations for capacity buildings.

As the blockchain is one of the frontier technologies, the common issue on the technology gap has been observed. Actors in IP ecosystems, therefore, should evaluate their capabilities, capacities and organizational maturity to assess their readiness for blockchain taking into account the cost-effectiveness. They should also evaluate what type of blockchain provides the most benefits to their organization and customers. The blockchain-enabled IP ecosystems will require public IP authorities to develop new legal and accounting policies taking smart contracts and autonomous agents into account to allow for the management of their clients’ IP assets. The need for human intervention in the lifecycle of IP assets will be decreased since IPRs holders will be able to autonomously manage their registered rights, either to renew them or to register their licenses or assignments through automated and smart processing. It is foreseeable that the actors will likely need to determine how such new services will be monetized and how that will increase or replace current revenue streams. This will require long-term strategic planning and risk management taking into account operating in decentralized business models. A reflection is needed on whether IP Offices should divert resources to other areas related to blockchain such as increasing IP awareness, in order to promote the IP market or the fight against counterfeiting and piracy.

308. The efforts to help public bodies in their transition to blockchain-based systems would be totally futile, weren’t they accompanied with measures to convince the rest of the participants in the IP ecosystems about the benefits of the new technology, and to help them implement its different applications while educating their members on their use.

309. Blockchain could create the most value for organizations when used to work together on common challenges and shared opportunities, especially with problems that are specific to each industry sector, such as those encountered in IP. Despite this positive feature, the challenge with many current approaches is that they remain stove-piped: organizations develop their own blockchains and applications on top of the already existing systems. Additionally, in every single industry sector, many blockchains are being developed by organizations based on different standards and platforms.

310. Even though blockchain-based solutions have been gradually explored and used in IP ecosystems, many enterprises, especially SMEs, still lack awareness of the technology and understanding of its operation and utility. There is an unbalanced ratio of business and technical actors with too much weight on the technology side. This seems hampering investment and the exploration of new ideas. A more business-oriented approach is needed. This calls for an improvement in the experience of non-technical users.

311. In the same way, there is a lack of technical knowledge and experience in this technology when compared to other IT fields (enterprise app development, artificial intelligence or cloud technologies, among others). Educating employees to work with blockchain takes time and it is not yet taught at the majority of educational institutions. Only 50% of the world’s top universities offer blockchain courses[[183]](#footnote-184) and currently there is more self-learning in blockchain than formal learning. There are already hundreds of blockchain start-ups, all trying to attract the same limited talent, yet organizations are faced with a talent pool that is expanding much slower than demand is growing. Enterprises interested in developing blockchain solutions should start creating knowledge by actively cooperating with universities, start-ups, and so on. At the same time, governments, universities and technology companies should include this new technology in their academic offerings.

[Annex I follows]

1. World Economic Forum (2016), “The Fourth Industrial Revolution: what it means, how to respond”, available at <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/> [↑](#footnote-ref-2)
2. Schwab, Klaus (2016), “The Fourth Industrial Revolution.” New York: Crown Business, p.23. [↑](#footnote-ref-3)
3. World Economic Forum (2016), “The Fourth Industrial Revolution: what it means, how to respond”, available at <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/> [↑](#footnote-ref-4)
4. European Patent Office (2020), “Fourth Industrial Revolution”, available at <https://www.epo.org/news-events/in-focus/ict/fourth-industrial-revolution.html> [↑](#footnote-ref-5)
5. McKinsey & Company (2017), “Jobs lost, jobs gained: What the future of work will mean for jobs, skills, and wages”, available at [https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages#](https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages%23) [↑](#footnote-ref-6)
6. EY, “How can blockchain transform a gaming platform into a game changer?” available at <https://www.ey.com/en_gl/consulting/how-blockchain-helped-a-gaming-platform-become-a-game-changer> [↑](#footnote-ref-7)
7. TED (2016), “The potential of blockchain”, available at <https://www.ted.com/talks/mike_schwartz_the_potential_of_blockchain> [↑](#footnote-ref-8)
8. Ibid. [↑](#footnote-ref-9)
9. Ibid. [↑](#footnote-ref-10)
10. Ibid. [↑](#footnote-ref-11)
11. Hyperledger, Hyperledger Architecture, Volume 1, Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus, < https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger\_Arch\_WG\_Paper\_1\_Consensus.pdf> . [↑](#footnote-ref-12)
12. Dylan Yaga, Peter Mell, Nik Roby and Karen Scarfone, NISTIR 8202 Blockchain Technology Overview, <https://doi.org/10.6028/NIST.IR.8202>. [↑](#footnote-ref-13)
13. Ibid. [↑](#footnote-ref-14)
14. Ibid. [↑](#footnote-ref-15)
15. https://www.oecd.org/daf/blockchain/ [↑](#footnote-ref-16)
16. https://unctad.org/webflyer/harnessing-blockchain-sustainable-development-prospects-and-challenges [↑](#footnote-ref-17)
17. https://www.unjiu.org/content/blockchain-applications-united-nations-system-towards-state-readiness [↑](#footnote-ref-18)
18. https://unece.org/trade/publications/white-paper-blockchain-trade-facilitation-ecetrade457 [↑](#footnote-ref-19)
19. https://www.eublockchainforum.eu/ [↑](#footnote-ref-20)
20. https://iccwbo.org/resources-for-business/incoterms-rules/incoterms-2020/ [↑](#footnote-ref-21)
21. https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8202.pdf [↑](#footnote-ref-22)
22. LITAN, A., LEOW, A., “Hype Cycle for Blockchain Technologies, 2020”, 13 July 2020, available at <https://www.gartner.com/en/documents/3987450/hype-cycle-for-blockchain-technologies-2020> [↑](#footnote-ref-23)
23. *Ibid.* [↑](#footnote-ref-24)
24. https://w3c.github.io/did-core/ [↑](#footnote-ref-25)
25. N. SZABO, ‘Smart Contracts’, (1994), [www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html](file:///\\wipogvafs01\redirected$\chavas\Documents\www.fon.hum.uva.nl\rob\Courses\InformationInSpeech\CDROM\Literature\LOTwinterschool2006\szabo.best.vwh.net\smart.contracts.html) [↑](#footnote-ref-26)
26. EU Blockchain Observatory and Forum, ‘NFT – Legal Token Classification’ (2021) pg 2: <https://www.eublockchainforum.eu/sites/default/files/research-paper/NFT%20%E2%80%93%20Legal%20Token%20Classification.pdf> [↑](#footnote-ref-27)
27. <https://www.larvalabs.com/cryptopunks> [↑](#footnote-ref-28)
28. <https://www.cryptokitties.co/> [↑](#footnote-ref-29)
29. https://boredapeyachtclub.com/#/ [↑](#footnote-ref-30)
30. [www.opensea.io](http://www.opensea.io) [↑](#footnote-ref-31)
31. VOTA, W, ICTWorks. “10 Blockchain Implementation Risks in International Development”. Available at <https://www.ictworks.org/blockchain-implementation-risks/> [↑](#footnote-ref-32)
32. IBM. “What is blockchain security?”. Available at https://www.ibm.com/topics/blockchain-security [↑](#footnote-ref-33)
33. Nakamoto, S, “Bitcoin: A Peer-to-Peer Electronic Cash System” available at https://bitcoin.org/bitcoin.pdf [↑](#footnote-ref-34)
34. In the sphere of Industrial Property, one can find rights of various sort, such as patents for inventions, industrial designs (aesthetic creations related to the appearance of industrial products), trademarks, service marks, layout-designs of integrated circuits, commercial names and designations, geographical indications and protection against unfair competition. (Understanding Industrial Property – WIPO (2016), page 6, <https://www.wipo.int/edocs/pubdocs/en/wipo_pub_895_2016.pdf>) [↑](#footnote-ref-35)
35. Copyright and related rights protect literary, artistic and scientific works; performances of performing artists, phonograms and broadcasts. (Understanding Copyright and related rights – WIPO (2016), page 6 <https://www.wipo.int/edocs/pubdocs/en/wipo_pub_909_2016.pdf> [↑](#footnote-ref-36)
36. IP environment includes laws, agreements, practices, economy, culture, traditions, moral and economic rights, the rights of the public to access those creations. [↑](#footnote-ref-37)
37. In fact, the value chain model for copyrights and related rights could be described in different ways, e.g., phases of generation, production, distribution and consumption as any creative work is normally protected by copyright law when it is created and the commercialization phase may be regarded coinciding with the management phase from the copyright perspective. [↑](#footnote-ref-38)
38. WIPO/GRTKF/IC/9/13, WIPO/GRTKF/IC/11/11 [↑](#footnote-ref-39)
39. WIPO (2016), “Understanding Industrial Property –, page 6”, <https://www.wipo.int/edocs/pubdocs/en/wipo_pub_895_2016.pdf> [↑](#footnote-ref-40)
40. M. BARULLI (2021), “IP is a journey: blockchain and encrypted storage are your best friends”, WIPO Magazine, February 2021, available at <https://www.wipo.int/wipo_magazine_digital/en/2021/article_0002.html> [↑](#footnote-ref-41)
41. Clarke, Modet & Co. together with Minsait, developed a blockchain-based application for registration processes. Currently, the solution uses a private-permissioned network, whose integrity is audited in Alastria and in the Public Ethereum network. Similarly, also Spanish-based law firm Pons IP developed a solution called Safe Evidence that uses electronic signature. [↑](#footnote-ref-42)
42. These services are called *EtherScan* or *BitScan*. [↑](#footnote-ref-43)
43. European Parliament (2017) “How blockchain technology can change our lives”: <http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf> [↑](#footnote-ref-44)
44. HENKEL, J / AND LERNBECHER (NEÉ PANGERL), S.M. (2008), “Defensive Publishing - An Empirical Study”, available at SSRN: <https://ssrn.com/abstract=981444>. [↑](#footnote-ref-45)
45. <https://www.bernstein.io/defensive-publishing-blockchain-ipfs> and <https://ipfs.io/> [↑](#footnote-ref-46)
46. <https://www.zertifier.com/> [↑](#footnote-ref-47)
47. <https://hash4life.com/> [↑](#footnote-ref-48)
48. [www.wetransfer.com](http://www.wetransfer.com) [↑](#footnote-ref-49)
49. <https://ipwe.com/> [↑](#footnote-ref-50)
50. Krajewski, Trevor and Lettiere, Rich, “Efforts Integrating Blockchain with Intellectual Property” (January 16, 2019). Les Nouvelles - Journal of the Licensing Executives Society, Volume LIV No. 1, March 2019, Available at SSRN: <https://ssrn.com/abstract=3317053> [↑](#footnote-ref-51)
51. Please see the IBM-IPwe project of patent tokenization. Information available at https://newsroom.ibm.com/2021-04-20-IPwe-and-IBM-Seek-to-Transform-Corporate-Patents-With-Next-Generation-NFTs-Using-IBM-Blockchain [↑](#footnote-ref-52)
52. Every change in the ledger of transactions or in a single transaction will result in the blockchain registering such alteration and identifying it as a new transaction. [↑](#footnote-ref-53)
53. In any case, permissioned blockchains do not offer low levels of security. An example of that is Hyperledger Fabric, open source project offered by the Linux Foundation, which is a permissioned blockchain, guaranteeing a high level of security. [↑](#footnote-ref-54)
54. <https://www.wipo.int/edocs/mdocs/globalinfra/en/wipo_ip_itai_ge_18/wipo_ip_itai_ge_18_3.pdf> [↑](#footnote-ref-55)
55. S. BIAN, G. SHEN, Z. HUANG, Y. YANG, J. LI and X. ZHANG, "PABC: A Patent Application System Based on Blockchain," IEEE Access, vol. 9, pp. 4199-4210, 2021, doi: 10.1109/ACCESS.2020.3048004. [↑](#footnote-ref-56)
56. EUROPEAN PARLIAMENT (2017), “How blockchain technology can change our lives”, p. 10-11. <https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf> [↑](#footnote-ref-57)
57. Further details will be given in the IPR enforcement section. [↑](#footnote-ref-58)
58. <https://ieeexplore.ieee.org/Xplore/home.jsp> [↑](#footnote-ref-59)
59. See EUROPEAN COMMISSION (2020), “Making the most of the EU’s innovative potential, An intellectual property action plan to support the EU’s recovery and resilience”. [↑](#footnote-ref-60)
60. Some other blockchains are introducing NFTs, such as TRON. [↑](#footnote-ref-61)
61. FAIRFIELD, J. (2021), “Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property”. Indiana Law Journal, Forthcoming, Available at SSRN: <https://ssrn.com/abstract=3821102> [↑](#footnote-ref-62)
62. <https://onlineonly.christies.com/s/first-open-beeple/beeple-b-1981-1/112924> [↑](#footnote-ref-63)
63. The same artist sold also, over the same week, another artwork, an animation depicting former president of the United States of America Donald Trump and sold it on the marketplace Nifty Gateway for over 6 million dollars. [↑](#footnote-ref-64)
64. [www.cryptokitties.co](http://www.cryptokitties.co) [↑](#footnote-ref-65)
65. Jack Dorsey's first ever tweet sells for $2.9m”, 23 March 2021, BBC News, [https://www.bbc.com/news/business-56492358](https://www.bbc.com/news/business-56492358%20) [↑](#footnote-ref-66)
66. [www.algorand.io](http://www.algorand.io) [↑](#footnote-ref-67)
67. <https://www.creativepassport.net/> [↑](#footnote-ref-68)
68. Future of content monetization and next era of digital interactions, February 2020. Retrieved from <https://www.accesscopyright.ca/media/1417/attributionledger_summary_feb2020.pdf> [↑](#footnote-ref-69)
69. www.peertracks.com [↑](#footnote-ref-70)
70. [www.unisonrights.es/en](http://www.unisonrights.es/en) [↑](#footnote-ref-71)
71. <https://www.maecenas.co> [↑](#footnote-ref-72)
72. See paragraphs 28 to 34 of document WIPO/IP/AI/2/GE/20/1 REV., <https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_ai_2_ge_20/wipo_ip_ai_2_ge_20_1_rev.pdf>. [↑](#footnote-ref-73)
73. OECD (2019), “Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies”, OECD Publishing, Paris, <https://doi.org/10.1787/276aaca8-en>. [↑](#footnote-ref-74)
74. See more on Josef Drexl,  ‘Designing Competitive Markets for Industrial Data Between Propertisation and Access’ (2017) 8 Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 257–292, <https://www.jipitec.eu/issues/jipitec-8-4-2017/4636/JIPITEC_8_4_2017_257_Drexl>; Ivan Stepanov, ‘Introducing a property right over data in the EU: the data producer’s right – an evaluation’ (2020) 34 (1) International Review of Law, Computers & Technology, <https://www.tandfonline.com/doi/full/10.1080/13600869.2019.1631621> [↑](#footnote-ref-75)
75. For a technical approach to blockchain-based data tokenization see TONG ZHOU, XIAOFENG LI, HE ZHAO (2019), “DLattice: A Permission-less Blockchain-based on DPoS-BA-DAG Consensus for Data Tokenization”, *IEEE Access*, vol. 7, available at <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8672629>. [↑](#footnote-ref-76)
76. OECD, *The Tokenisation of Assets and Potential Implications for Financial Markets* (2021) 11 < <https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.htm>> [↑](#footnote-ref-77)
77. <https://datum.org> [↑](#footnote-ref-78)
78. <https://oceanprotocol.com> [↑](#footnote-ref-79)
79. <https://ecosteer.com> [↑](#footnote-ref-80)
80. [https://data.iota.org/#/](https://data.iota.org/%23/) [↑](#footnote-ref-81)
81. <https://www.kneron.com/technology/KNEO/> [↑](#footnote-ref-82)
82. OECD (2020), “The Tokenisation of Assets and Potential Implications for Financial Markets”, p. 16. [↑](#footnote-ref-83)
83. See “Datum’s White Paper”, available at <https://datum.org/assets/Datum-WhitePaper.pdf>. For other examples of companies focusing on blockchain-enabled data ownership and/or data tokenization see also Ocean Protocol, Ecosteer, IOTA or Kneron. [↑](#footnote-ref-84)
84. See “Datum’s White Paper”, p. 11. [↑](#footnote-ref-85)
85. ERC721 is an Ethereum open standard for non-fungible tokens, see <http://erc721.org>. [↑](#footnote-ref-86)
86. ERC20 is an Ethereum open standard for fungible tokens. See <https://ethereum.org/en/developers/docs/standards/tokens/erc-20/>. [↑](#footnote-ref-87)
87. Composable Non-Fungible Token standard is available at <http://erc998.org>. [↑](#footnote-ref-88)
88. Composable tokens bundle several complementary data tokens embedding different data services (i.e. a package of different data tokens). MCCONAGHY, T (2019), “Datatokens 2: Non-Fungible, Fungible, and Composable Datatokens’ *Ocean Protocol,* available at <https://blog.oceanprotocol.com/data-tokens-2-fungible-composable-54b6e0d28293>. [↑](#footnote-ref-89)
89. Trent McConaghy, ‘Datatokens 1: Data Custody’ (2019) Ocean Protocol, <https://blog.oceanprotocol.com/data-tokens-1-data-custody-1d0d5ae66d0c> [↑](#footnote-ref-90)
90. See Datum’s White Paper 14ff. [↑](#footnote-ref-91)
91. See Datum’s White Paper 16, 19. [↑](#footnote-ref-92)
92. SPIEKERMANN, M (2019), “Data Marketplaces: Trends and Monetisation of Data Goods”, *Intereconomics – Review of European Economic Policy*, vol. 54(4), pp. 210-11; for a definition and examples of data marketplaces see also CARNELLEY, P, SCHWENK, H., CATTANEO, G., MICHELETTI, G., OSIMO, D (2016), “Europe’s Datamarketplaces – Current Status and Future Perspectives” Report for the European Commission, p. 10, available at <https://datalandscape.eu/data-driven-stories/europe’s-data-marketplaces-–-current-status-and-future-perspectives> [↑](#footnote-ref-93)
93. EUROPEAN COMMISSION, (2017), “Commission Staff Working Document on the free flow of data and emerging issues of the European data economy”, Doc. SWD (2017) 02 final; VOMFELL, L, STAHL, F., SCHOMM, F., VOSSEN, G. (2015), “A classification framework for data marketplaces” *Working Paper No. 23*, European Research Center for Information Systems, p. 8. [↑](#footnote-ref-94)
94. IOTA (2019), “Part 1: IOTA Data Marketplace – Update”, available at <https://blog.iota.org/part-1-iota-data-marketplace-update-5f6a8ce96d05/> [↑](#footnote-ref-95)
95. EUROPEAN COMMISSION (2020), “A European strategy for data”, Doc. COM(2020) 66 final; “US Federal Data Strategy”, available at <https://strategy.data.gov>; “UK National Data Strategy”, available at <https://www.gov.uk/guidance/national-data-strategy>. [↑](#footnote-ref-96)
96. See WIPO (2004) Intellectual Property Handbook, p. 207, available at <https://www.wipo.int/edocs/pubdocs/en/wipo_pub_489.pdf> [↑](#footnote-ref-97)
97. WEF (2020), Bridging the Governance Gap: Dispute resolution for blockchain-based transactions, p. 6, available at <http://www3.weforum.org/docs/WEF_WP_Dispute_Resolution_for_Blockchain_2020.pdf> [↑](#footnote-ref-98)
98. EUROPEAN COMMISSION (2020), Study on the use of innovative technologies in the justice field, <https://op.europa.eu/en/publication-detail/-/publication/4fb8e194-f634-11ea-991b-01aa75ed71a1/language-en>, pp. 43-44. [↑](#footnote-ref-99)
99. ALLESSIE, D., SOBOLEWSKI, M. and VACCARI, L., Blockchain for digital government, Pignatelli, F. editor(s), EUR 29677 EN, Publications Office of the European Union, Luxembourg, 2019, <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-digital-government> [↑](#footnote-ref-100)
100. See, “Why are Chinese Internet Courts Keen on Blockchain Technology?”, China Justice Observer, 15 december 2019, available at <https://www.chinajusticeobserver.com/a/why-are-chinese-internet-courts-keen-on-blockchain-technology> [↑](#footnote-ref-101)
101. See “Alibaba to implement blockchain in intellectual property system”, Tokenpost, 28 May 2019, available at <https://tokenpost.com/Alibaba-to-implement-blockchain-in-intellectual-property-system-2010> [↑](#footnote-ref-102)
102. See “When Blockchain Meets Electronic Evidence in China's Internet Courts”, China Justice Observer, <https://www.chinajusticeobserver.com/a/when-blockchain-meets-electronic-evidence-in-china-s-internet-courts> [↑](#footnote-ref-103)
103. Article 11 of the SPC Provisions on Several Issues Concerning the Hearing of Cases by Internet Courts. [↑](#footnote-ref-104)
104. See “When Blockchain Meets Electronic Evidence in China's Internet Courts”, China Justice Observer, <https://www.chinajusticeobserver.com/a/when-blockchain-meets-electronic-evidence-in-china-s-internet-courts> [↑](#footnote-ref-105)
105. WEF (2020), Bridging the Governance Gap: Dispute resolution for blockchain-based transactions, available at <http://www3.weforum.org/docs/WEF_WP_Dispute_Resolution_for_Blockchain_2020.pdf> [↑](#footnote-ref-106)
106. SHEHATA, I (2018), “Three Potential Imminent Benefits of Blockchain for International Arbitration: Cybersecurity, Confidentiality & Efficiency. Young Arbitration Review, 2018, Available at SSRN: <https://ssrn.com/abstract=3290028> [↑](#footnote-ref-107)
107. EUROPEAN COMMISSION (2018), “Study on Blockchains - Legal, governance and interoperability aspects” (SMART 2018/0038), <https://digital-strategy.ec.europa.eu/en/library/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038> , p. 78. [↑](#footnote-ref-108)
108. The WIPO Arbitration and Mediation Center provides a secure and confidential online case management tool for parties resolving their disputes under WIPO ADR Rules. Further information regarding this service may be accessed here: <https://www.wipo.int/amc/en/eadr/wipoeadr/> [↑](#footnote-ref-109)
109. Available at <https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2021/04/Lawtech_DDRR_Final.pdf> [↑](#footnote-ref-110)
110. See <https://www.jamsadr.com/rules-smart-contracts#2> [↑](#footnote-ref-111)
111. See in this regard the section on Sustainability and Scalability in this paper. [↑](#footnote-ref-112)
112. SHEHATA, I (2018), “Three Potential Imminent Benefits of Blockchain for International Arbitration: Cybersecurity, Confidentiality & Efficiency” published at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3290028>. [↑](#footnote-ref-113)
113. RABINOVICH-EINY, O / KATSCH, E. (2019)“Blockchain and the Inevitability of Disputes: The Role for Online”, J. Disp. Resol, available at: <https://scholarship.law.missouri.edu/jdr/vol2019/iss2/6> [↑](#footnote-ref-114)
114. WEF (2020), Bridging the Governance Gap: Dispute resolution for blockchain-based transactions, p. 13. Available at <http://www3.weforum.org/docs/WEF_WP_Dispute_Resolution_for_Blockchain_2020.pdf> [↑](#footnote-ref-115)
115. The 2006 UNCITRAL Recommendations addressed the outdated idea of telegrams. UNCITRAL recommends that this requirement must be read to ‘include’ the electronic means of communication, and this would open the door to using blockchain as a means to conclude arbitration agreements. [↑](#footnote-ref-116)
116. In relation to Kleros, see IPCHAIN, ODR and its applications in IP-related services in the EU, p. 11, available at <https://ipchain.global/docs/legal_research/en/ODR_and_its_applications_in_IP-related_services_in_the_EU.pdf> [↑](#footnote-ref-117)
117. OECD/EUIPO (2019), *Trends in Trade in Counterfeit and Pirated Goods*, Illicit Trade, OECD Publishing, Paris, <https://doi.org/10.1787/g2g9f533-en>. [↑](#footnote-ref-118)
118. See “Blockchain Report”, available at <https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Blockathon/Blockathon_Report.pdf> [↑](#footnote-ref-119)
119. [www.iTracetech.com](http://www.iTracetech.com) [↑](#footnote-ref-120)
120. To this regard, potential infringers who may attempt to copy or reproduce the QR/barcode will need to face the whole uniqueness of the blockchain infrastructure, able to attribute unique identification to each and every product. [↑](#footnote-ref-121)
121. <https://www.coinsnetwork.com/2020/03/18/alibabas-koala-introduces-blockchain-to-help-buyers-track-origin-of-goods/> [↑](#footnote-ref-122)
122. Information available at <https://smarttrademark.search.ipaustralia.gov.au> [↑](#footnote-ref-123)
123. Information available at <https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Blockathon/Blockathon-Forum_Blockchain-Use-Case.pdf> [↑](#footnote-ref-124)
124. WCO (2019), Study report on Disruptive Technologies, P. 19. Information available at <http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/disruptive-technologies.aspx> [↑](#footnote-ref-125)
125. OKAZAKI, Y (2018), “Unveiling the Potential of Blockchain for Customs” WCO issued Research Paper N°. 45, available at <http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/research/research-paper-series/45_yotaro_okazaki_unveiling_the_potential_of_blockchain_for_customs.pdf?la=en> [↑](#footnote-ref-126)
126. Information available at <https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Blockathon/Blockathon-Forum_Blockchain-Use-Case.pdf> [↑](#footnote-ref-127)
127. World Economic Forum, ‘Global Standards Mapping Initiative: An overview of blockchain technical standards’ (White Paper 2020) 8. [↑](#footnote-ref-128)
128. https://eips.ethereum.org/ [↑](#footnote-ref-129)
129. European Commission. "Joining Forces for blockchain Standardisation." European Commission.Pp. 13-14. N.p., 29 July 2020. Web. Consulted 31 July 2020. Available at <https://ec.europa.eu/digital-single-market/en/news/joining-forces-blockchain-standardisation> [↑](#footnote-ref-130)
130. Global Blockchain Business Council, *Global Standard Mapping Initiative* (Insight Report 2020) 27. [↑](#footnote-ref-131)
131. <https://www.wipo.int/export/sites/www/standards/en/pdf/03-96-01.pdf> [↑](#footnote-ref-132)
132. <https://www.wipo.int/export/sites/www/standards/en/pdf/03-27-01.pdf> [↑](#footnote-ref-133)
133. <https://www.wipo.int/export/sites/www/standards/en/pdf/03-61-01.pdf> [↑](#footnote-ref-134)
134. <https://www.wipo.int/export/sites/www/standards/en/pdf/03-87-01.pdf> [↑](#footnote-ref-135)
135. https://www.baseline-protocol.org/ [↑](#footnote-ref-136)
136. What Are Oracles? Smart Contracts, Chainlink & “The Oracle Problem. Available online: https://blockonomi.com/oracles-guide. [↑](#footnote-ref-137)
137. https://standards.ieee.org/about/index.html [↑](#footnote-ref-138)
138. https://standards.ieee.org/standard/2418\_2-2020.html [↑](#footnote-ref-139)
139. https://blog.eid.as/tag/oasis-dss-x-core-2-0-en/ [↑](#footnote-ref-140)
140. Despite the protocol still being an Ethereum-based protocol, by the end of 2019, Pantheon was rebranded as a Hyperledger BESU because of the interoperability focus that the developers' team (PegaSys) took for the project. [↑](#footnote-ref-141)
141. UN JOINT INSPECTION UNIT (2020), “Blockchain applications in the United Nations system: towards a state of readiness”, available at <https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2020_7_english.pdf> [↑](#footnote-ref-142)
142. UN JOINT INSPECTION UNIT (2020), “Blockchain applications in the United Nations system: towards a state of readiness”, par. 240. [↑](#footnote-ref-143)
143. See EUROPEAN COMMISSION (2020), “Study on the use of innovative technologies in the justice field”, <https://op.europa.eu/en/publication-detail/-/publication/4fb8e194-f634-11ea-991b-01aa75ed71a1/language-en>, [↑](#footnote-ref-144)
144. EU BLOCKCHAIN OBSERVATORY AND FORUM (2019), “Legal and regulatory framework of blockchains and smart contracts”, p. 10, <https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf> [↑](#footnote-ref-145)
145. See, for instance, *The Stanford RegTrax Initiative*, working on the creation of an open blockchain regulation database (for the moment being, on the major world jurisdictions), <https://regtrax.law.stanford.edu> [↑](#footnote-ref-146)
146. M. FINCK (2019), *Blockchain Regulation and Governance in Europe*, CUP, Chapter 2. [↑](#footnote-ref-147)
147. See EUROPEAN COMMISSION (2020), “Study on the use of innovative technologies in the justice field”. [↑](#footnote-ref-148)
148. EU BLOCKCHAIN OBSERVATORY AND FORUM, “Legal and regulatory framework of blockchains and smart contracts”, p. 6. [↑](#footnote-ref-149)
149. EUROPEAN COMMISSION, “Study on Blockchains - Legal, governance and interoperability aspects” (SMART 2018/0038), <https://digital-strategy.ec.europa.eu/en/library/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038> , p. 46. [↑](#footnote-ref-150)
150. LE CONSEIL FÉDÉRAL (2018), “Bases juridiques pour la distributed ledger technology et la blockchain en Suisse”, p. 74 ff, available at <https://www.newsd.admin.ch/newsd/message/attachments/55151.pdf> [↑](#footnote-ref-151)
151. OECD (2021), *Regulatory Approaches to the Tokenisation of Assets,* OECD Blockchain Policy Series, p. 31, available at [www.oecd.org/finance/Regulatory-Approaches-to-the-Tokenisation-of-Assets.htm](file:///\\wipogvafs01\redirected$\chavas\Documents\www.oecd.org\finance\Regulatory-Approaches-to-the-Tokenisation-of-Assets.htm) (JUI, par. 263) [↑](#footnote-ref-152)
152. EU BLOCKCHAIN OBSERVATORY AND FORUM, “Legal and regulatory framework of blockchains and smart contracts”, p. 13. [↑](#footnote-ref-153)
153. The Council on General Affairs and Policy of the Hague Conference on Private International Law (CGAP) has invited the Permanent Bureau to monitor developments with respect to the private international law implications of DLT (see “Conclusions and Decisions adopted by CGAP at its meeting of 3–6 March 2020”, para.15, available at [https://assets.hcch.net/docs/70458042-f771-4e94-9c56- df3257a1e5ff.pdf](https://assets.hcch.net/docs/70458042-f771-4e94-9c56-%20df3257a1e5ff.pdf)). [↑](#footnote-ref-154)
154. EU BLOCKCHAIN OBSERVATORY AND FORUM, “Legal and regulatory framework of blockchains and smart contracts”, p. 14. [↑](#footnote-ref-155)
155. EU BLOCKCHAIN OBSERVATORY AND FORUM, “Legal and regulatory framework of blockchains and smart contracts”, p. 19. [↑](#footnote-ref-156)
156. EUROPEAN PARLIAMENT, “Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?”, <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf> [↑](#footnote-ref-157)
157. EUROPEAN COMMISSION, “Study on Blockchains - Legal, governance and interoperability aspects”, p. 49. [↑](#footnote-ref-158)
158. See, for instance, Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.), <http://data.europa.eu/eli/reg/2018/1807/oj> [↑](#footnote-ref-159)
159. See, for instance, art. 19.11 United States-Mexico-Canada Agreement or art. 14.11 Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) [↑](#footnote-ref-160)
160. SVANTESSON, D. (2020-12-22), “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, OECD Digital Economy Papers, No. 301, OECD Publishing, Paris. <http://dx.doi.org/10.1787/7fbaed62-en>. [↑](#footnote-ref-161)
161. EU Blockchain Observatory and Forum, Legal and regulatory framework of blockchains and smart contracts, p. 12, <https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf> [↑](#footnote-ref-162)
162. EU Blockchain Observatory and Forum, Legal and regulatory framework of blockchains and smart contracts, p. 11, <https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf> [↑](#footnote-ref-163)
163. EUROPEAN COMMISSION, “Study on Blockchains - Legal, governance and interoperability aspects”, p. 55. [↑](#footnote-ref-164)
164. REFERENCE NEEDED. UK land registry case ([link](https://hmlandregistry.blog.gov.uk/2019/05/24/could-blockchain-be-the-future-of-the-property-market/)) [↑](#footnote-ref-165)
165. “Does your country currently have legislation in force governing or applicable to the use of blockchain/DLT in the justice field? A total of 56 (or 56% of all 100) replies from stakeholders have been received, where 6 (or 11% of the 56 replies) selected 'Yes', 38 (or 68% of the 56 replies) indicated ‘No', and 12 (or 21% of the 56 replies) selected ‘Other’”. (EUROPEAN COMMISSION, “Study on Blockchains - Legal, governance and interoperability aspects” p. 71). [↑](#footnote-ref-166)
166. EUROPEAN COMMISSION, “Study on Blockchains - Legal, governance and interoperability aspects”, p. 55. [↑](#footnote-ref-167)
167. <https://impuls-liechtenstein.li/wp-content/uploads/2021/02/Report-and-Application-TVTG-extract.pdf> [↑](#footnote-ref-168)
168. EU Blockchain Observatory and Forum, Legal and regulatory framework of blockchains and smart contracts, p. 12, <https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf> [↑](#footnote-ref-169)
169. EU Blockchain Observatory and Forum, Legal and regulatory framework of blockchains and smart contracts, p. 22, <https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf> [↑](#footnote-ref-170)
170. UK JURISDICTION TASK FORCE, “Legal statement on cryptoassets and smart contracts”, available at <https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf> [↑](#footnote-ref-171)
171. EUROPEAN COMMISSION, “Study on Blockchains - Legal, governance and interoperability aspects”, p. 59. [↑](#footnote-ref-172)
172. See for instance, art. 5 United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005), <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/06-57452_ebook.pdf> [↑](#footnote-ref-173)
173. EUROPEAN COMMISSION, “Study on Blockchains - Legal, governance and interoperability aspects”, p. 64. [↑](#footnote-ref-174)
174. “The first smart contract executes (due to the irrevocability of blockchain transactions) but a second smart contract is used to reverse or change its effects (such as to reimburse the payment that was wrongfully executed)”. See EUROPEAN COMMISSION, “Study on Blockchains - Legal, governance and interoperability aspects”, p.55 [↑](#footnote-ref-175)
175. PHILIPP HACKER, CHRIS THOMALE, (2019), “The Crypto-Security: Initial Coin Offerings and EU Securities Regulation”, in Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos (eds.), Stefan Eich, *Regulating Blockchain: Techno-Social and Legal* *Challenges*, Oxford University Press, pp. 214-225. [↑](#footnote-ref-176)
176. OECD (2021), “Regulatory Approaches to the Tokenisation of Assets”, OECD Blockchain Policy Series, [www.oecd.org/finance/Regulatory-Approaches-to-the-Tokenisation-of-Assets.html](file:///\\wipogvafs01\redirected$\chavas\Documents\www.oecd.org\finance\Regulatory-Approaches-to-the-Tokenisation-of-Assets.html) [↑](#footnote-ref-177)
177. EUROPEAN COMMISSION, “Study on Blockchains - Legal, governance and interoperability aspects”, p.91; LE CONSEIL FÉDÉRAL (2018), “Bases juridiques pour la distributed ledger technology et la blockchain en Suisse”, p.47ff. [↑](#footnote-ref-178)
178. See, for instance, UN JOINT INSPECTION UNIT (2020), “Blockchain applications in the United Nations system: towards a state of readiness”, p. v. [↑](#footnote-ref-179)
179. As part of 2020-2022 Triennial Work Programme, a UNIDROIT Working Group has been established with the objective to develop a future legal instrument containing principles and legislative guidance in the area of private law and digital assets, see <https://www.unidroit.org/work-in-progress/digital-assets-and-private-law> [↑](#footnote-ref-180)
180. UN JOINT INSPECTION UNIT (2020), “Blockchain applications in the United Nations system: towards a state of readiness”, p. v. [↑](#footnote-ref-181)
181. UNCITRAL, “Legal issues related to the digital economy - Note by the Secretariat”, Doc. A/CN.9/1012 [↑](#footnote-ref-182)
182. According to a recent OECD Report, it cites an estimate stating that Bitcoin transactions may consume as much electricity as Denmark by 2020. OECD (2021), “The Tokenization of Assets and Potential Implications for Financial Markets”, p. 19, available at <http://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.htm> [↑](#footnote-ref-183)
183. KAARU, S. “Over half of the top 50 universities offer blockchain courses: Report”. Available at <https://coingeek.com/over-half-of-the-top-50-universities-offer-blockchain-courses-report/> [↑](#footnote-ref-184)