Blockchain technologies and IP ecosystems: A WIPO white paper

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

Table of contents

Foreword

Blockchain technologies have both disruptive and transformative potential; they are among a number of frontier technologies that could offer new ways to do business and manage intellectual property (IP) assets. The IP community has only recently started to explore blockchain technologies, and there are some operative solutions in the public and private sectors. However, there is still a generalized lack of understanding and adoption of blockchain within the IP ecosystem.

This white paper explores potential applications and opportunities presented by blockchain technologies to IP ecosystems. It also identifies the challenges and issues that should be addressed to determine the feasibility and cost-effectiveness of utilizing such technologies for the benefit of all IP stakeholders. We hope that this white paper will help IP offices and other interested parties with their strategic policy and decision making on the adoption of blockchain technologies in their businesses, as well as providing information for further discussions and collaborations among interested parties. This white paper suggests that the primary considerations of using blockchain in IP ecosystems are technical standards, regulatory framework, blockchain-network governance, and capacity building.

The white paper consists of an executive summary, a main part and four annexes. Annex I provides an overview of IP ecosystems and IP value chains. Annex II captures the results of a survey conducted with the aim to gather industry information to support the writing of this white paper on the use of blockchain in IP ecosystems. Annex III includes a detailed repository of potential use cases for the IP ecosystem, such as time-stamping, anti-counterfeiting and IP licensing, among others. Lastly, Annex IV is prepared as a mock-up to explain how blockchain technology could be used to address the long-standing challenge of identifying an actor or a participant in IP ecosystems at the global level.

WIPO wishes to express its appreciation to the Korean Intellectual Property Office (KIPO) for its financial support towards the preparation of this White Paper under the WIPO-KIPO Funds-in Trust. We also deeply appreciate the kind collaborations and support of IP offices and other contributors who participated in preparing the paper through various activities.

Ken-Ichiro Natsume
Assistant Director General
Infrastructure and Platforms Sector

Executive summary

I. Background

Blockchain is one of the frontier technologies associated with the concept of the Fourth Industrial Revolution, which is significantly affecting the way businesses operate while revolutionizing numerous innovation ecosystems.

Given that blockchain technologies affect every industry and have been extensively used in the intellectual property (IP) community, the member states of the World Intellectual Property Organization (WIPO) established the Blockchain Task Force under the Committee on WIPO Standards (CWS). Its mandate is to develop reference models for using blockchain in the field of IP and to propose for a new WIPO Standard supporting potential applications of blockchain technology within IP ecosystems.

This white paper aims to explore potential applications and opportunities presented by blockchain to the existing IP ecosystems. It also identifies the challenges and issues that should be addressed to determine the feasibility and cost-efficiency of introducing such technologies in IP ecosystems.

II. Key features and applications of blockchain

Blockchain can be defined as a distributed database storing a permanent and tamper-proof ledger of data. The key features of said technology are: decentralization, distributed ledgers, consensus mechanisms, immutability of records and encryption. When applied in real-world applications, blockchain potentially 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 due to the immutability that blockchain provides.

Key applications of blockchain include digital identity, time-stamping, fraud prevention, tokenization, traceability and smart contracts. Depending on the strategic interests of the stakeholders involved, blockchain can gradually transition from a purely decentralized and open (permissionless) system – where ledgers are distributed among participating parties or nodes who validate the transactions that are added via a decentralized consensus model, such as Bitcoin or Ethereum – to a centralized (permissioned) system where the ledger is centrally managed by a specific entity; or distributed among a limited number of participants, and governed by a specific entity or a few concerned parties. In terms of access to the network, blockchain-based solutions can be public (i.e., anyone can make use of the blockchain applications) or private (i.e., only certain entities can make use of them).

During the next few years, the combination and convergence of frontier technologies such as blockchain, biotechnology, big data, Internet of Things (IoT) and artificial intelligence (AI) will likely have a direct impact on most industries as well as an extensive impact on the technical processes of the national and international governance systems that regulate those industries. Blockchain thus has transformative effects not only on the primary commercial and innovation processes of IP users and their business models in many industrial and creative sectors, but also, simultaneously, on the governance processes and systems themselves through which WIPO member states regulate and incentivize those primary innovative, creative and commercial processes in their jurisdictions. One directly affected category of these governance systems are the existing IP ecosystems. In the

former sense, enterprises are already beginning to deploy blockchain-inspired solutions and business models either by themselves or in association with others; and in the latter sense, governments and international organizations have been exploring the implications and use cases of blockchain in their public services. As a matter of fact, blockchain platforms such as Bitcoin, Ethereum and Hyperledger are being used by consortia and industry alliances in several business sectors. The initiatives of these consortia and alliances aim to overcome known technology-related problems, such as the lack of interoperability among the existing implementations in the market, legal uncertainty and its complexity, and to facilitate its widespread use. In the meantime, national governments and international organizations are leading projects to facilitate its adoption not only in the private sector but also in the public sector to increase the level of efficiency of public services for the benefit of societies in general.

III. Potential applications of blockchain in IP ecosystems

According to the activities that were conducted for this white paper, including surveys, there are numerous potential blockchain use cases within the existing IP ecosystems. However, before introducing any blockchain-based applications, a deeper analysis should be made on whether that technology is the most suitable among the various digital technologies and which blockchain solutions are the most appropriate, taking into account potential benefits and challenges of the respective solutions, and their cost-effectiveness. The potential applications provided in this document should be perceived without any prejudice regarding whether or not blockchain is the most appropriate solution in those cases.

IP broadly refers to the legal rights that result from intellectual activity in the industrial, scientific, literary and artistic fields. It is traditionally divided into two branches, “industrial property” and “copyright.”[1] This white paper explores potential applications of blockchain mainly in the two traditional branches and provides some potential use cases for protection and access to digital data and IP right enforcement.

To explain the blockchain potential use cases in IP ecosystems, this white paper defines IP ecosystems as a network of various actors (e.g., creators, inventors, enterprises, organizations, IP offices and enforcement authorities) that interact with each other in collaborative and competitive ways in the IP environment, using resources to generate, protect, manage and/or commercialize intellectual assets. These interactions can be modeled into an IP value chain with four phases: Generation, Protection, Management and Commercialization.

Industrial property rights

In relation to industrial property rights, blockchain technologies might be of great help from the generation of an intangible asset to the commercialization of IP rights.

In the Generation phase, blockchain applications can help with proof of generation and record keeping of IP assets, by proving the date and ownership of preparatory documentation that may lead to the filing of an application for a patent, utility model or any other industrial property right.

For registration in the Protection phase, permissioned-blockchain solutions would allow for a centrally managed ledger facilitating append-only transactions and the sharing of immutable IP data. Blockchain could also be used to provide tamper-proof and solid evidence during the life cycle of the application, including examination, opposition and cancellation stages.

In the Management and Commercialization phases, the introduction of blockchain solutions in the administration of IP registries might also allow right holders to streamline numerous management activities needed to raise the value of their IP rights portfolio. To start with, registered rights might be autonomously managed by their owners with a consequent efficiency increase. The IP right holder may also use smart contracts for the licensing and assignment of registered IP rights. Tokenization can also help the right holder to securitize their IP assets or to use them as collaterals.

It has been argued that the highest benefits from blockchain solutions would be obtained if interoperability were facilitated. The use of interoperable blockchain systems could facilitate the collaboration among IP offices and streamline the administration of international IP systems.

Copyright and related rights

Original creative works are protected without the need for registration or formal requirements. However, in some instances, right holders may voluntarily register the works in copyright registries as a proof of authorship and/or ownership, the date of generation to justify protection and to facilitate management and economic exploitation of their copyright.

Blockchain technologies may also facilitate the automation of processes and systems used by collective management organizations (CMOs), and information access by potential users. This latter example could be also implemented via the use of non-fungible tokens (NFTs). Further, smart contract solutions may facilitate additional patterns for negotiating licenses either individually or collectively by CMOs or other entities. Blockchain solutions facilitate user access to both digital content and identification of the actors involved in the process that goes from its generation to where it is accessible to the public. The use of blockchain may facilitate the calculation of royalties for collection from users and how these royalties have to be distributed among the different right holders.

Finally, similar to industrial property rights, copyright and related rights can be tokenized and used as bonds to finance artistic projects. In practice the application of smart contract and blockchain solutions in this context creates a technical continuum between licensing, other contractual practices and technological protection measures for original literary and artistic works on the one hand and for other non-original digital content on the other.

Protection and access to digital data

Blockchain technologies can provide efficient solutions to protect data. Having in mind the uncertainties that exist in relation to its protection under the current IP rights regimes, tokenization could provide solutions to ensure that data sets and their owners are clearly identified and kept confidential, and that only authorized users can make use of proprietary data. For instance, where reasonable measures to maintain secrecy of data have been taken and other requirements fulfilled, the adoption of these measures along with the use of smart contracts would allow holders of undisclosed information to claim protection of that data as trade secrets in case of unlawful appropriation.

IP right enforcement

An essential challenge for participants in IP ecosystems is the enforcement of their IP rights before judicial courts, administrative bodies, custom authorities or institutions providing alternative dispute resolution (ADR) services. The use of smart contracts may reduce litigation in so far as performance of the obligations takes place, while the contract can be automatically terminated once the software detects that a condition is either met or not met anymore.

In case of disputes, blockchain solutions can help to secure evidence in relation to ownership and time of content generation. In case of disputes concerning licenses on digital assets, it may also provide evidence on unauthorized use by third parties, thereby enabling blockchain solutions to be more easily introduced in ADR institutions. Lastly, blockchain applications may considerably impact the prevention of counterfeiting and piracy.

IV. Considerations

There are certain considerations that need to be weighed by participants in IP ecosystems in the decision-making process: (a) whether or not to transition to blockchain-based solutions with other frontier technologies in their digital transformation; (b) what applications provide added value to the existing solutions; and (c) what kind of blockchain is the most suitable. These considerations are mainly related to a lack of interoperability from three different perspectives in the fields where the interaction among solutions is expected: technical standards, blockchain governance and regulatory frameworks. Another relevant consideration refers to the collaboration and capacity building that IP offices and other IP stakeholders may need in their adoption of blockchain within IP ecosystems.

Technical standards

Interoperability may 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 trusted ledgers using blockchain solutions implemented by participants in the IP ecosystem needs to be ensured.

The first pillar of interoperability is the development of common technical standards at different layers such as infrastructure, data and transaction layers. Due to the complexity of the field and its diverse applications, the development and adoption of standards would be a complex process. At present, standardization initiatives for specific sectors rely on market-defined solutions, such as the Hyperledger toolset under the umbrella of the Linux Foundation or the Ethereum Foundation that introduces standards to the Ethereum community through the Ethereum Improvement Proposals. In the meantime, some technical specifications developed by international standardization bodies such as the International Standards Organization (ISO) and the International Telecommunications Union (ITU) are gaining traction for terminologies, security and other areas.

The CWS has a consolidated tradition in acting as a collaborative international forum for discussing and reaching an agreement on IP standards. In accordance with the decision of the member states, the work of the CWS Blockchain Task Force would merit developing a new WIPO Standard supporting the potential applications of blockchain technologies within IP ecosystems. In particular, it would be useful for the participation in such a forum to include, in addition to the primary representatives of the member states and IP offices, also observers from other international organizations, the private sector and other stakeholder groups, in particular entities that are currently working on blockchain projects. It is critical to synchronize and streamline all the efforts to facilitate the adoption of the said technology and to avoid fragmentation by working in a cohesive manner.

Governance

For a blockchain to be successful, the governance framework needs to balance the interests of all stakeholders. These include founders, network validators (nodes), users of the blockchain, application developers and regulatory authorities. Depending on the particular purpose of a blockchain network, its founders may choose a type of blockchain such as public or private but should consider the network governance ensuring that all stakeholders can express their views and defend their interests where possible. The blockchain governance should be established before launching the blockchain solutions and must be considered and agreed on at the designing stage, taking into account the existing relevant IP ecosystem governance processes. However, it needs to be flexible enough to admit changes to incorporate technical development in the system or to adapt to new stakeholder needs. Stakeholders in the blockchain-enabled IP ecosystems will likely come from different countries and regions and thus multi-jurisdictional regulations should be considered at the designing stage, to avoid any regulatory breach.

Finally, the analysis of the governance structure of existing blockchain consortia and ongoing projects in the field of IP may be very useful for identifying common practices as well as for developing reference models and guiding principles related to the establishment of governance frameworks.

Regulatory framework

Currently, there is a high degree of legal uncertainty about several blockchain aspects and whether legal systems are fully adapted to this technology. While the entity administering a blockchain network may be located in a single member state, stakeholders may come from different jurisdictions. This is particularly the case in IP ecosystems, where most of its actors tend to act at an international level. These concerns should be considered while deciding the feasibility of employing a blockchain solution and conducting its risk assessment from a legal standpoint.

Competent authorities face three main challenges when performing basic legal and regulatory functions, depending on the nature of the blockchain itself. Such challenges are ascertaining liability, determining the applicable law for blockchain activities and carrying out regulatory monitoring or enforcing rules. The first challenge is decentralization itself. The absence of a central authority in the blockchain environment is concerning, as this may entail that there is no responsible entity for legal compliance and ultimate accountability for the exchanged data. The second issue is the pseudonymity or anonymity provided by blockchain-based platforms to users and miners. This makes it difficult to know who uses the platform and to what end. The third essential characteristic of blockchain that poses a challenge is its

multi-jurisdictional dimension. This is usually the case when participants in a blockchain are established in different jurisdictions. When the blockchain is connected to legal orders with different approaches to regulatory issues, it might be difficult to design a governance framework that accommodates all those approaches. This is particularly true in relation to personal data protection issues.

The international communities have not neglected the challenge that legal uncertainty entails. It is generally agreed that blockchain-based innovation should rely upon an easily understandable, predictable and relevant legal framework. With this mindset, works have already commenced at national, regional and international levels so as to accommodate the legal framework to the special features of blockchain applications.

Collaboration and capacity building

IP offices and other institutions should evaluate their capabilities, capacities and organizational maturity to assess their readiness for blockchain. The introduction of blockchain technologies to IP ecosystems might require public IP authorities to develop new legal and accounting policies using smart contracts and autonomous agents to allow the management of their clients' IP assets. IP offices and other stakeholders would need to collaborate to explore and determine impact and implications of blockchain to IP ecosystems.

Capacity building and education pose a great challenge for blockchain implementation in IP ecosystems. Efforts to help individuals and entities explore and use blockchain-based systems will be futile if they are not accompanied by the rest of the participants in IP ecosystems.

In this regard, it is necessary that all participants within IP ecosystems share their experience, knowledge and blockchain solutions, or even cooperate in pilot projects, for all stakeholders, including those from developing countries, to learn and benefit from them. This will likely require the exploration of potential blockchain use cases within the IP space and collaboration on pilot projects. For example, a pilot project of a blockchain-based reference implementation on verifiable digital identifiers of individuals and entities could streamline data processing across various systems, thus benefiting all actors in IP ecosystems. Such collaborations may result in the development of a new WIPO standard to ensure interoperability among related blockchain-based applications.

Section 1

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 (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 revolutionizing the ecosystem of innovation and creativity by improving the automation of tasks with yet unseen capabilities.

In the context of this white 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 that bring trust to users are:

- the potential of decentralization, avoiding the role of traditional intermediaries (trusted third parties) and providing transparency to the participating blockchain nodes; the immutability of the records, for once a transaction is recorded it is almost impossible to alter; 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 a 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 only recently started 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 their 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:

(a) 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;
(b) 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;
(c) 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

(d) Prepare a proposal for a new WIPO Standard supporting the potential application of blockchain technologies within the IP ecosystems.[2]

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.

To produce this white paper, 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 was 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 expected 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 white paper 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 white paper for reference purposes as Annex I to this paper. This overview and reference model of the IP ecosystem and the IP value chain are generalizations for illustrative purposes and may require further development 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 startups and established industry players in the field of IP have started projects that are promising and these are 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 that 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.

Section 2

Blockchain and the Fourth Industrial Revolution

The Fourth Industrial Revolution (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 (AI), 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*.[3] 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,[4] it is in the biological domain where he sees the biggest hurdles for appropriate regulation and consequently biological and genetic resources (GRs) 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.[5] The average annual growth in patenting inventions related to 4IR at the European Patent Office, between 2010 and 2018, has been close to 20 percent.[6]

All scientific and technical revolutions bring advantages and disadvantages, challenges and opportunities. The scope and complexity of the impact that 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 the 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 flexibility and rapid adaptation required of the acceleration of the change processes.

The biggest challenge that the 4IR will likely cause is the impact on employment. In 2017, McKinsey reported that due to automation, between 400 million and 800 million jobs will disappear by 2030.[7] However, this may also be an opportunity, as new professional skills will be requested, thus creating millions of jobs in new sectors.

In the next few years, the combination of blockchain and other disruptive technologies will have a direct impact on various industries, acting as a facilitator of the Programmable Economy in which 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 points are:

- to identify and analyze the governance, legal and operational implications of blockchain applications for existing IP systems, both in terms of opportunities and challenges; and

- 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 that 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 that 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.

Disruptive technologies of the 4IR are playing a key role in supporting the COVID-19 response and recovery efforts in emerging markets, opening up new opportunities for an accelerated adoption of blockchain technologies. For example, the so-called maker community addressed the shortage of face masks by distributing 3D templates that 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, in both private and public circles. It created opportunities for new and emerging business models and potentially a new generation of IP assets, paving the way for the 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 ways to treat the victims of the pandemic. To quickly evaluate prototypes and effectively scale-up production, 3D printing was used. 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 the 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, 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, innovative 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:

- the date of disclosure;
- the scope of disclosure (i.e., the original disclosed sequence);
- the version of the sequence data (sequence data are continuously optimized and annotated); and
- 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 that are undergoing 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 the 4IR are far-reaching. Organizations, businesses and individuals that hope to take advantage of the 4IR in the post-pandemic scenario will need to rethink their strategic approach to leveraging technology and digitalization. In adapting to the 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. The retail industry has seen how stores need to coexist with digital channels to continue operating, impacting their logistics and their relationship with their customers or investors. The leisure industry, for instance, cinemas, theaters, events, trade fairs and concerts, has seen closures and cancellations. This has allowed for home entertainment businesses such as Netflix and Microsoft Xbox to become household names and forced an entire industry to revise its distribution strategies and explore new technologies such as virtual and augmented reality.[8]

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 became 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 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.

There was also a surge in cybercrime activity with the pandemic. Several large companies and hospitals around the world 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 toward remote working and homeworking technologies is increasing the necessity of protection against cyberattacks, and personal data is more accessible. Furthermore, as remote consultation in industries such as 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 to fight identity fraud.

Numerous contractual relationships between companies still require that contractual transactions are documented in writing and verified by the physical signature of documents in the presence of a notary. In fact, a physical signature and paper still takes precedence, otherwise doubts arise over the legal certainty and reliability of the generated electronic evidence. In the 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 time-stamping by acting as a digital ledger.

To summarize, the global digitalization of the supply chain has cut out many intermediaries from distribution. Both global and local players are required to reposition themselves, for example, 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 also 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 on the potential of blockchain,[9] specialist Mike Schwartz praised "blockchain for enabling an economy between machines," redefining our world as did the combustion engine, the telephone, the computer, the internet – each at their own time. Blockchain also has numerous applications: all kinds of assets can be stored such as 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, especially including those that 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 that is 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, which at the same

time are 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 (i.e., log in with a 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), which represent a certain value or the right to use a service/asset as agreed via the smart contract.

Blockchain's inherent main characteristics are:

- 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 preestablished rules that all must comply with;
- distributed ledgers: blockchain is a network of identical ledgers shared and synchronized across multiple sites, bodies or geographies, which can record the transactions performed in multiple places at the same time;
- 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 preestablished rules that are defined in the smart contracts. The integrity and deterministic execution flow of such smart contracts is also guaranteed;
- 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 be incorporated and, subsequently, said block is mined; and
- 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:

- Tokenization: to put it simply, tokenization is the process of converting physical, financial or intellectual assets into a digital token. Normally, one asset is broken down into smaller parts that 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 completely 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.
- Smart contracts: the term "smart contract" was originally coined by Nick Szabo and relates to software automating the terms of an agreement that 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 preprogrammed conditions are met.
- 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.
- Self-sovereign identity (SSI): blockchain enables SSI or the decentralized idea 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 decentralized identifiers (DIDs), which are a form of digital identifier 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, which 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. A 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:

- *Proof of work (PoW)*: this is notably used as the consensus model behind Bitcoin and a number of cryptocurrencies. The PoW model requires users who want to publish a new block be the first one to solve a computational puzzle to demonstrate that 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.[10] If accepted, the user submitting the correct solution to the puzzle is rewarded or incentivized for the 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.
- *Proof of stake (PoS)*: this consensus model is funded on the basis that the more stake or investment one has in a network the more likely the investor wants the system to succeed and the less likely one would sabotage their own investment.[11] In the design of a PoS 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.[12] This model is not as reliant on compute to prove the ability to add a new block on the chain. However, additional complexities are introduced in the design approach used to secure the intended proof by stake outcome. One of the ways to achieve this is through Byzantine fault tolerance (BFT). BFT relies on the assumption that a majority of the nodes in the chain is behaving as intended, a majority of the nodes could vote to agree an execution; this is seen as consensus. A risk with the BFT model is that an agreement may be prevented from reaching consensus when there are significant malicious attacks or faulty nodes.[13] A notable application of BFT is in Hyperledger. As opposed to PoW, which necessitates a large amount of energy and the eventual sale by miners of their coins to cover their costs, 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.
- *Proof by authority*: this consensus model is a commonly used and applicable consensus model in permissioned blockchain networks. For proof by authority to be implemented, 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.[14] As a result, a node can lose its ability to publish or access 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.

- *Round Robin*: this consensus model is more suitable for 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.[15] This ensures that no one node is able to create the majority of the blocks. 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 develop from a pure decentralized (permissionless) system – for example, Bitcoin – into a private (permissioned) system governed in accordance with the interests of a few concerned parties – namely, closed blockchains. Both types of blockchain present different characteristics. The first blockchain networks were public, mainly due to the philosophy behind blockchain, which seeks absolute transparency and ease of adoption by the maximum number of users.

- *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 they have computing power at their 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, which 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.
- 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, for instance, 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, thus more efficient consensus algorithms can be used that prioritize performance and scalability, over the total decentralization that characterizes public blockchains.
- 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 a 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.

Table 1. Permissionless vs. Permissioned

Permissionless	Permissioned
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 an authority, either through a single trusted party or decentralized 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 the public.
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 a 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 different 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 authorized entity or owner(s).

One of the first decisions to make when implementing a blockchain system is what 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 for a product or service, consumer use of that product or service 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 they received to the IP asset owner. 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 with 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 is 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 field. For example, the Global Blockchain Policy Forum of the Organisation for Economic Co-operation and Development (OECD),[16] where policy aspects, such as standardization and governance, are debated and information and opinions exchanged; the United Nations Conference on Trade and Development's (UNCTAD) paper on "Harnessing blockchain for sustainable development:

prospects and challenges";[17] the UN Joint Inspection Unit's (UNJIU) paper titled "Blockchain applications in the United Nations system: towards a state of readiness,"[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's (UN/CEFACT) Blockchain White Paper Project;[19] and the European Union (EU) Blockchain Observatory's aim to accelerate blockchain innovation and the development of the blockchain ecosystem within the EU.[20] Initiatives in the private sector are also multiple, such as the International Chamber of Commerce (ICC) projects on blockchain-backed Incoterms[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 fully interact digitally with public instances. Furthermore, a number of governments around the globe have established blockchain guideline and roadmap documents that lead the way and benchmark considerations required of government entities prior to engaging in blockchain implementations or provision of service aided by blockchain technology. For example, in 2018 the National Institute of Standards and Technology of the US Department of Commerce published a Blockchain Technology Overview,[22] which serves as a comprehensive survey of blockchain technology. This overview identifies that the use of blockchain technology is not a silver bullet and that close consideration must be given to how to deal with malicious users, to control and, particularly for government entities, to operational considerations and governance.

According to Gartner's 2020 reports on blockchain,[23] enterprises are beginning to deploy blockchain-inspired solutions that require the reconsideration of the implemented architectures and technologies for optimum exploitation of blockchain with the least possible business friction. However, blockchain is still at an early stage of development, lacks standardization and has a variety of divergent implementations. As the technology matures further, leaving the enterprise perimeter and being used to facilitate and automate business transactions – for instance, using 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 to 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 monetary 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 intermediaries. 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"[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, such as 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 at the early stage of development and adoption. We should also bear in mind that blockchain, compared to other emerging technologies, has a much higher

speed of implementation, given the revolution that it represents and the amount of diffusion it has had thanks to the use and support of Bitcoin and other cryptocurrencies 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 SSIs without intermediaries in transactions. Such new value chains will disrupt current value chains and require 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. An SSI can be implemented on a blockchain, removing the need for an intermediary to validate identities. Smart contracts, using DIDs 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 to 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 the early adoption of blockchain technologies remain inconclusive on its long-term sustainability and scalability.

Blockchain, in addition to encouraging the evolution of companies, institutions and communities toward 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 toward 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 toward 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, which could link any information stored in the blockchain to themselves. This identity model is already being defined in different environments such as SSI, a decentralized identification system that generates a digital identity for its users using blockchain technologies. According to the DID specification of W3C,[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 the 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.

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, it would be possible for an accounting book on a blockchain platform, which records identity transactions and manages the sharing of necessary information, 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.

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 initial public offerings (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, an independent security assessment, an 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 life cycle 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 kept 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 other external technologies or data sources such as the 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 are buying, 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, which 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 toward 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 secondhand goods, such as diamonds, since blockchain allows the use of physical elements, for instance cryptochips, which are connected in real time to a blockchain database, to verify their identity through links to information that allow the client to confirm their legitimacy via the front-end of an application in a simple way. In this way, for example, consumers 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 it makes it harder to commit and has the 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 permanent and time-stamped evidence for every stage of the transaction, and providing 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 fraud, risks also include human error, which can lead to an incorrect execution of certain processes, for example, in the case of payroll. Through blockchain, the clauses of a contract can be executed automatically without giving rise to error, consequently avoiding the cost derived from claims and legal processes that may arise due to this type of error. In relation to this, numerous potential business models have emerged, the best known 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.”[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 network of computers that are 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, such as 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 complete, all the involved parties 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 impose an immutable feature on it. This means that, once the data are 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 that the discipline of law has been brought in 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 go-betweens 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 for the 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 the 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 to conduct business using them. Blockchain characteristics such as immutability play a key role in tokenization because transparency allows for certification of ownership of the asset to all the participants in the blockchain and traces the entire history of the activities performed with the asset. Immutability provides the certainty that the stored data in the blockchain is accurate and has not been changed by any of the participants.

Non-fungible 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.[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 are associated to one digital or physical object they provide scarcity in the market. Last but not least, fungibility is an important aspect of NFTs – and part of the acronym. 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 token, 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[28] or Cryptokitties[29] or Bored Apes,[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 NFTs are gaining notoriety in the creative business and 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 physically and virtually as NFTs, reaching several thousands of dollars in sales on the OpenSea[31] platform.

Blockchain technology SWOT analysis

Blockchain has become a disruptive emerging technology since 2008, when Nakamoto introduced it with the conception of Bitcoin, and it is receiving increasing attention from researchers and industries

that aim to understand how blockchain can improve their efficiency. 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.

A SWOT (strengths, weaknesses, opportunities and threats) analysis can be used to 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 may 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 applied, causing some inherent blockchain features and benefits to be omitted from its 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 chain of transactions – there is traceability and transparency toward all participants in the transaction. The network-based feature of blockchain allows you to build distributed ledgers across multiple nodes. These strengths should permit several industries, especially the IP community, to develop digital trade solutions whereby the 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 intermediaries in many processes for fields such as payments and licensing. In comparison to traditional financial services, blockchain facilitates faster transactions by allowing peer-to-peer cross-border transfers with a digital currency.

The blockchain ledger allows each transaction performed in the network to be recorded on the blockchain. This can help not only improve security and prevent fraud in exchange-related businesses, but also 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. Further, to some extent, blockchains have dependency to validate on-chain data on the block, as they are isolated networks and likely need associated data and services, which are available on off-chain systems, for accuracy. One major challenge is how to ensure, manage and enforce the quality of off-chain data that is input into the blockchain. As the technology is still at an early stage of development, there are many divergent implementations that have a vertical focus and require further attention on interoperability and standardization to ensure a wider degree of adoption.

If blockchains are widely used in the future, they may be used more often as evidence in legal proceedings or other dispute mechanisms. It is therefore important to consider the issue of legal admissibility and the 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 in each jurisdiction, thus making it difficult to generalize about how such evidence might be treated by the courts, and therefore 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, for example, smart contracts, reducing or potentially eliminating intermediaries who are currently 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 that allow for the development of a digital trade ecosystem, within specific "vertical" industries, to avoid the development of stovepipes, which will hamper the wider adoption and interoperability of blockchain.

Threats

As the technology is still at an early stage of development 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.[32]

The early adopters need to be able to respond quickly to potential security flaws and emerging trends and to 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 intermediaries when validating and underwriting transactions. By cutting out these transaction underwriters, 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 the cost to compute and to 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:[33]

- *51 percent attacks*. A 51 percent attack refers to an attack on a blockchain by a group of attackers who gain control of 51 percent 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 had not taken place, since they control which transactions get confirmed.
- *Phishing*. Phishing is already 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 confidential data and/or financials for their personal gain.
- *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 is 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.
- *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

Strengths	Weaknesses	Opportunities	Threats
• confidentiality, integrity and availability of information; • the immutable nature of the technology creates an immutable chain of transactions; • traceability and transparency towards all participants in the transaction; and • increases information processing efficiencies, through enabling peer-to-peer "trustless" trade reconciliation and settlement.	• lack of centralized control and governance; • scalability and sustainability limitations; • it is still in an early stage and requires further focus on interoperability and standardization to ensure a wider degree of adoption; • cybercriminals look for blockchain network vulnerabilities and exploit them; • legal uncertainty deriving from the novelty of the technology and multijurisdictional character; and • laws and regulations governing the legal admissibility of information recorded and stored on the block chain differ according to jurisdiction.	• further technical standardization will be needed to harmonize the use of this technology; • implementation of proper data protection and authentication mechanism, policies and common governance practices; • possibilities in tracking and tracing both digital and physical assets; • blockchain can accelerate the digital transformation in many industries, defining new business models through innovative digital trade platforms; and • smart contracts can reduce or potentially eliminate middlemen.	• there is no common international regulatory framework for users of blockchain solutions; • blockchiain networks are not immune to cyberattacks and fraud such as 51 percent attacks, phishing, routing attacks, Sybil attacks, etc. • it could be perceived as unsecure/unreliable and quick response time to potential security flaws is needed to mitigate this perception; • blockchain networks are not immune to cyberattacks and fraud; and • lack of understanding of the technology among potential users as well as technological knowledge and experience requiring high investments for implementation.

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.[34]

Main blockchain implementations

Among others, there are currently four major blockchain platforms: 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 transaction in the bitcoin network: those of creation or issuance of Bitcoin and those of transfer of Bitcoin between users. 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, which allows them 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 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 account: 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 PoW consensus algorithm to a 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 JPMorgan 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, thus they 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 multisectoral 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 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 J.P. 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 to 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 euro (20,000 to 25,000 euro per participant).

Enerchain

Enerchain is a 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 within 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 multisector 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 startups. 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 to 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.

Section 3

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, intellectual property (IP) plays a pivotal role. The effective generation, protection, management and commercialization of IP assets, therefore, have been considered one of the top priorities for businesses in the private and public sectors, but at the same time, they have a great challenge. 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 section explains how the blockchain applications explained above may help public and private actors in IP ecosystems to address these challenges and make use of the opportunities that the digital environment offers. This section 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 the decision flow shown in Figure 2 below) 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 as well as 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 that result from intellectual activity in the industrial, scientific, literary and artistic fields, and it has traditionally been divided into two main branches: "industrial property"[35] and "copyright."[36] It is also to be noted that there are branches of IP law and practice that lie beyond the distinction between the two main branches, 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 Fourth Industrial Revolution (4IR), intangible assets that may fall beyond the classical branches of IP, namely, industrial property and copyright, such as big data sets, algorithms, TK and TCEs, are assuming increased significance and, because they are not directly and fully protected by

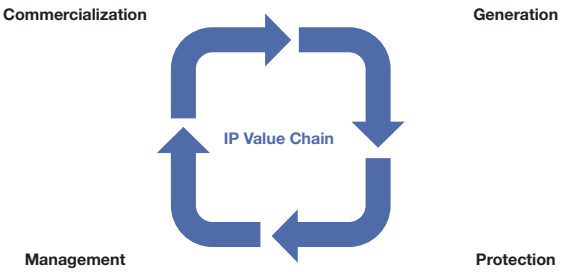
the classical main branches of the IP system, they have been discussed as subject matter of potential use cases for blockchain applications.

An IP ecosystem can be understood as a network of various actors (e.g., creators, inventors, enterprises, collective management organizations [CMOs], IP offices, enforcement authorities) that interact with each other in collaborative and competitive ways in the IP environment[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, namely, 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 therefore there are demands for generalization. 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 life cycle model with four phases:

- 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.
- 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.
- Management. This phase refers to the activities that the IP right holder may undertake to develop and raise the value of the IP right portfolio. It may include sub-phases such as IP audit, IP portfolio analysis, IP life cycle analysis, competitive technology intelligence (CTI) and IP landscape.
- Commercialization. This phase includes all those activities directly involved in generating revenue from the IP rights portfolio. It may be subdivided into 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 they do 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 CMO.[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 that are equally important for a vibrant ecosystem, but that 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 of providing important inputs for innovation and protecting 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 and the public domain, which provide input for further innovation in the ecosystem. Further detailed descriptions of IP ecosystems and IP value chains referred to in this paper are explained in Annex I.

Potential blockchain use cases along IP value chains

While blockchain and distributed ledger technologies (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 that 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, for example, 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, use 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:

- Decentralized identifiers (DIDs): the creation of DIDs for IP ecosystem actors enables faster interactions along the different phases of the IP value chains.
- Time-stamping: a digital time-stamp is the proof that a document, file or any type of relevant digital content existed or was set in a digital place, for instance, attaching it to a blockchain, at a particular date and time.
- 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.
- 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.
- Version management: many IP assets are continuously and rapidly transforming (e.g., ongoing annotation, value-added data sets) and thus transparent and trusted version management is important to maximize legal certainty regarding IP rights in such assets.
- 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 that are the subject of IP protection, such as the vertical use cases of trade secrets or creative works, and intellectual assets that 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:

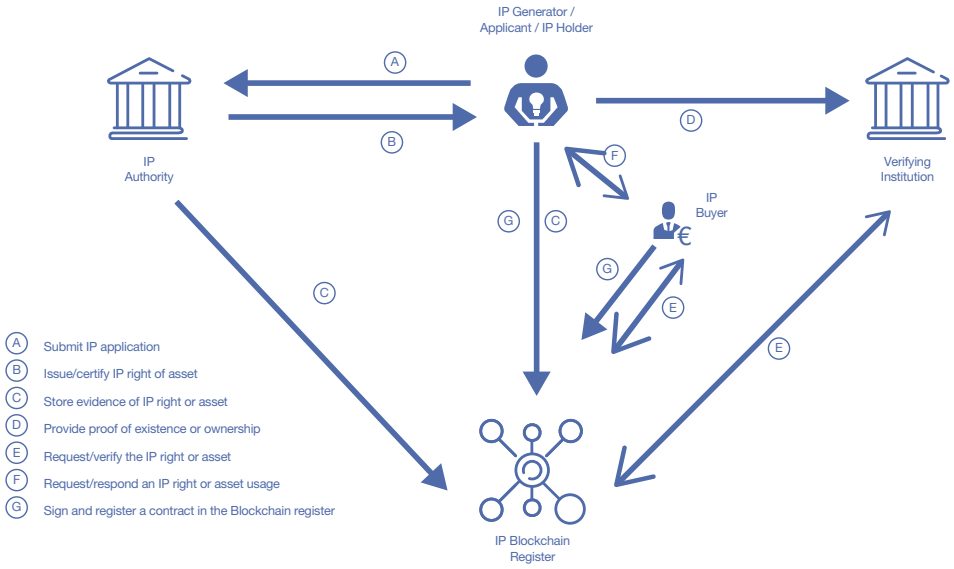
- IP register (Generation/Protection): entering creative or innovative assets and the details of its generation into a blockchain would create a time-stamped record and trustable proof of generation that owners could use to manage and commercialize their intangible

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, for instance copyright and unregistered design rights, as it can easily provide evidence of the time of generation, rights management information (if applicable) and jurisdictional requirements.

- Evidence of generation (Generation): uploading newly generated IP assets and the details of its generation to a blockchain would allow the registration of a time-stamped record and trustable proof of generation. The owners can use this to safeguard it from potential misappropriation and infringement, for example, complex data sets, such as sequence data generated by genomic sequencing.
- 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.
- 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.
- 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.
- 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.
- Evidence of trademark use (Protection): blockchain may provide reliable and time-stamped 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.
- 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 any PVP matters after it is granted (e.g., keeping the rights in force, nullity and cancellation).
- 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.
- IP licenses (Commercialization): blockchain could bring a secure, reliable and scalable distributed transaction process to licensing IPR. It could introduce traceable and verifiable ownership and an accurate distribution of royalties, allowing for the possibility of paying the right holders directly, reducing the use of intermediaries.

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.[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.

Figure 2. Overview of blockchain use in IP ecosystems



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.

Industrial property rights

In the context of industrial property rights,[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 time-stamped 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.[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 such as Bernstein, MyTitle, Creativity Safe, Origin Stamp or Zertifier, as well as services developed by law firms specifically for clients.[42]

The digital recordation service provided by these entities is usually divided into three steps:

- Upload: this phase consists in uploading a specific digital item of any kind – for example, research notebooks, confidential information, etc. – in an encrypted cloud service connected to a blockchain through an Application Programming Interface (API), the outcome of which 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. This document is usually encrypted adopting the so-called zero-knowledge

technology, meaning that the provider offering the API service that 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.

- Certification: once the document is uploaded to 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 as a personal record attesting to the possession of a specific document at a particular moment in time. The relevant information may consist of the name of the owner, the date and time of the encryption, the transaction ID (hash) and all of the accessory and additional information that may be customized and filled in (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).
- 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. 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, to verify the authenticity of the transaction, two factors need to be checked:
  - The existence of the transaction associated to the hash. As per the localization of the transaction, blockchains such as Ethereum and Bitcoin already offer free specific services that allow searches for a transaction in their whole blockchain,[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 access to the transaction ID to localize it.
  - The possession of the original document uploaded. On the other hand, to determine whether such a transaction contains a specific document and not a modified or subsequent version, providers have enabled a service normally called the "verification tool" (the commercial name of such a 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, the 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 life cycle of IP assets.

A time-stamp 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 time-stamping services for IP rights and related IP data covering multiple participants and multistep time-stamp 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, to be accepted, has to show use of the trademark for a period of time in relation to the goods and services for which protection is sought and must bear a relevant date within the requested time frame. 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 a sign. Many right holders faced inconveniences due to undated evidence, which may have also led the IP offices to decide unfavorably due to a lack of secure, immutable and solidly dated evidence. It has to be borne in mind that such a process will only work if IP holders carry out periodical blockchain time-stamping, 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 they have performed the corresponding generation of evidence during the five-year time frame 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 time-stamped 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 and vis-à-vis subsequent applications for registrations. Such evidence may prove to be useful in IP proceedings, potentially valid and acceptable before IP 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 time-stamped 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, discreet, 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.[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 as 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.[45] Blockchain solutions can also contribute to the publication of prior art where databases may be difficult to create, for example, for natural GRs 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, to successfully determine such defensive publication as prior art and to 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 InterPlanetary File System (IPFS).[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 time frames, 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 with the market speed. In fact, in light of the above, unregistered designs under EU regulation are protected for the period of three years (non-renewable). Such a figure, however, confers protection only against identical designs, which is different to Community registered designs, which furthermore confer protection over a period of five years, renewable for a total of 25 years. Even in unregistered design cases, however, the main issue revolves around the *dies a quo* from when protection starts to apply because, as registration is not 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, is 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 ability to handpick 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, time-stamped on the blockchain and accessed through a "zero-knowledge platform." This provides, on the one hand, compliance with legal requirements concerning trade secret protection – namely, 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[47] with their solution HASH4LIFE,[48] which may have relevant applications for protecting confidential information. In fact, this solution uses blockchain to send documentation in a safe manner. 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[49] application, only using blockchain for further security features). Furthermore, the blockchain-powered service allows ownership of the document to be authenticated through a verification tool. This application may be useful in the context of trade secret licenses or assignments, know-how, as well as potentially in relation to due diligence in 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 on 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 on third parties' rights.

Blockchain solutions can also help to monetize industrial property rights – for example, 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 have recourse to smart contracts that can be automatically concluded and performed. For example, IPwe[50] provides a blockchain-enabled patent registry and ratings database currently containing basic information on 80 percent of the world's patents.[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) potentially allows for the tokenization of an IP asset in the results of future research projects (e.g., the invention of a new medicine). In the short to medium term, this facilitates the funding of research and innovative activities. An example of this could be the tokenization of a patent, which, by being divided into several fragments, can increase monetization and have the possibility of multiple assignments, licenses and so forth.[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, if applied to the different stages of the IP value chain and to different industrial property rights (patents, trademarks, industrial designs, geographical indications) and trade secrets (confidential information, know-how and, as explained later, 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 right 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 of the supporting evidence or the fee was paid (whichever action is the most recent). 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 time-stamping 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 more cost-effective, reducing the hurdles and burdens of IP registration. 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 lowered costs associated with the identification of applicants and right holders, as well as the handling of opposition-related fees and any other act related to the application and registration of an IPR, since the 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 to corrupt or alter the data or a transaction, this will be reflected on the blockchain itself.[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 such as the Bitcoin network, for instance, may certainly be more secure, but it results in the loss of full control of 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.[54] Additionally, the system requires less maintenance, particularly in

relation to the aforesaid. It is to be noted, the use of blockchain entails the impossibility to modify a record or, better, that any modification is 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 their IP assets, which the office will be able to access faster. 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 fulfills 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 five to ten years.

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 or the supporting evidence was submitted, 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 time-stamping 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, the 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, for example, 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 Artificial Intelligence (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."[55]

Furthermore, there is a proposal for an international patent application system based on a permissioned blockchain named the Patent Application System Based on Blockchain (PABC). This aims to connect patent offices in the world and to 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.[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 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 one specific office at a time. 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 specific registrations existed at any given time, without revealing its content.[57] The 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's (EUIPO) IP Register in Blockchain project has implemented a blockchain based append-only database, distributed and managed across participating IP offices, with access to the history of every entry in relation to trademarks and industrial designs registered before the participating IP offices. Similarly IP Australia is working on a platform that allows the tracing of products through APIs and unique identifiers (UiDs) such as near-field communications (NFCs), UiDs or any other tag applicable to the product itself.[58] Other entities such as the Institute of Electrical and Electronic Engineers (IEEE) have discussed how a permissioned blockchain system can be used to construct an international patent application system.[59]

Blockchain technology could provide an opportunity to establish a distributed IP register benefiting both offices and applicants: (1) 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; (2) IPRs would be managed by their owners rather than by intermediaries; and (3) 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 and less maintenance, just to mention a few. In addition to all of the previously mentioned benefits, which perfectly apply to all offices individually, the advantages of a global system materialize in a more interconnected network of offices that, 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 life cycle 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 toward achieving more transparency and better rights data management, specifically targeting copyright.[60]

As it is generally known, while industrial property rights require registration 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 time-stamping, 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 companies mentioned above in the industrial property rights section – such as Bernstein, MyTitle, Zertifier and Creativity Safe – also provide 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 also 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, non-fungible tokens (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 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,[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. Among these, the most relevant is the resale percentage to be paid to the author, 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.[62] In fact, the nature of the NFT's smart contract will determine the faculties of the acquirer of such NFT, bearing in mind 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"[63] for a record of USD 69 million.[64] An NFT can also be a

digital cat bred on the blockchain such as Dragon (sold for the equivalent of over USD 170,000 on the CryptoKitties[65] platform), a tweet (the first tweet published by Twitter CEO Jack Dorsey was sold for USD 2.9 million[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 Society of Authors and Publishers (SIAE) announced a partnership with Algorand[67] for the development of a blockchain platform for royalty distribution. The project saw the first tangible results in March 2021, with the creation of over 4 million NFTs that represent the more than 95,000 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 to facilitate their protection. Even though NFTs are powered by smart contracts, the latter also have 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.[68]

Finally, blockchain or distributed ledgers may also provide solutions to creative expressions that 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: (1) the content identity; (2) the rules and protocols required for verified attribution; and (3) an open and transparent system that immutably connects the work, metadata about the work and the entity or person able to authorize the use of a work.[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[70] or Unison rights[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,[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.[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.[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.[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.[76] As explained asset tokenization involves the representation of preexisting 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.[77] This is particularly relevant in relation to industrial data – for example, 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,[78] Ocean Protocol,[79] Ecosteer,[80] IOTA[81] or Kneron.[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."[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.[84] Consequently, the blockchain infrastructure brings the data token both control and flexibility to securely trade with the data as an asset – namely, controlling the access to the data set.[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.

Depending on the chosen token (fungible or non-fungible) 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[86]), where exclusive access to the data set will be restrained to the stakeholder holding the NFT, or by means of a fungible token (ERC-20[87]), in case the data holder is interested in providing access to the data set 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[88]) are implemented.[89] These are used to collect together the existing offered types of data tokens on a given data set, 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 data set where new data is being constantly gathered (i.e., a dynamic data set vs. a static data set), and it can even be designed so as to provide not just access to the data set but also computing services (i.e., access to a server where the data set can be used for, for instance, AI purposes).[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., the right to access and use the data set for a specific purpose).

Datum's White Paper may give the reader a simple way of understanding how a data marketplace and the life cycle of the data-as-asset within a blockchain might work:[91]

- a user submits a data set 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 for DAT tokens (the data is stored in a distributed way and thus it is replicated in the other storage nodes[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 they can either agree or counteroffer; and
- the user accepts the proposal, they send 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,[93] data marketplace should be conceived as electronic infrastructures allowing economic actors to interact and perform data-based transactions.[94] Even though Datum's aforementioned example is a pertinent one, others such as IOTA may well also serve to illustrate a blockchain-based data marketplace.[95] The theoretical conception of data markets and their materialization have contributed to the institutionalization of data transactions and, broadly, data trade. As a result of this market structure and the 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 policymakers to design legal frameworks and policy strategies seeking to promote data-driven economies based on data-driven innovation and data sharing.[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 regard 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 data sets traded in the blockchain may include personal data. In addition, the users of a blockchain network generate data that might have a

personal character – namely, 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:

- articulating all activities stemming from data marketplaces; and
- providing legal certainty notwithstanding the current lack of specific regulations relating to data markets.

These concerns will be assessed in the following section.

IPR enforcement

Another group of potential uses of blockchain solutions for participants in the IP ecosystems is related to 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 to prevent further infringement of their IPRs and to recover the losses thereby incurred. They must also be able to involve state authorities to deal with counterfeits.[97] 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 (ADR) systems. 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."[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 – namely, risks of machine-based binary approaches. Moreover, the use of blockchain technologies may bring new and complex conflicts – for example, errors in the code of the smart contract, malfunctioning of an oracle and so on. 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 be useful in legal disputes (i.e., time-stamping 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,[99] there are several projects that aim to introduce this technology into different EU member states with one or some of the following purposes:

- To identify both of the parties in the proceedings and their representatives and to control access to the information about the proceedings or identification in cases where hearings are taking place virtually.
- To secure the records of the proceedings, to facilitate their internal administration and to 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.

- In those cases where part of the information analyzed in the framework of the proceeding is sensitive, the blockchain solution may help to keep the confidentiality of such information and to administer access to it. This is particularly relevant in cases where the dispute concerns trade secrets.
- To secure evidence related to the proceeding.
- To foster 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.[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.
- To promote international cooperation: the use of permissioned blockchain could potentially enable international collaboration among different judicial systems in other countries. This may facilitate judicial notifications, help in obtaining evidence abroad, expedite requests for information, assist 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.
- Other advantages are the agility to access the information and the 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 on the Use of Innovation Technologies*, most of these projects are public/private initiatives based on open-source platforms such as Ethereum, which aim to create 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), the connection with other authorities (notaries, public administration bodies, judicial government bodies) and the provision of evidence.

For the 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 time-stamped 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.[101] Potential guides or training to judges and courts' personnel might be needed to foster and achieve fluidity in this sense.

The Chinese Cyberspace Courts' blockchain allows the 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 in preparation for a future complaint. This is the case for instance of Alibaba's Ali IPP Platform.[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.[103]

The example of the Chinese Cyberspace Courts shows not only the potential that blockchain has for judicial IPR enforcement but also the legal obstacles that their implementation may encounter. Generally speaking, despite the integrity and immutability that blockchain offers, 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, the The Supreme People's Court of the People's Republic of China issued an opinion with special rules for the cyberspace courts to identify and authenticate electronic data. The opinion proposes the encouragement and guidance of the parties concerned to apply blockchain technology.[104] In addition, the cyberspace courts have adopted standards with technical specifications for electronic

data, which interface with the judicial application methods as well.[105] This example also shows that the use of blockchain solutions by the judiciary in other countries will likely require legal amendments.

Alternative dispute resolution systems

Alternative dispute resolution refers to a number of different procedures that parties may use to resolve their disputes. The three main ADR procedures are:

- 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.
- 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 an agreement, the mediator cannot impose a decision on the parties.
- 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 and flexibility of proceedings; technical expertise of arbitrators, mediators or experts; confidentiality of 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 – namely, 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.[106]

Blockchain technology has potential applications in the management of ADR proceedings:[107]

- 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.[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.
- Security: blockchain can increase security in relation to the evidence related to the dispute and communications between the parties. Some arbitral institutions still use "unencrypted email and commercially available cloud data repositories." The IT systems of the 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.
- Confidentiality:[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[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, JAMS, an ADR service provider, is working on a set of rules that would apply specifically to resolution of disputes arising from smart contracts – the JAMS Smart Contract Rules.[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.[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 predesignated participants have control over, and access to, the dispute resolution process.[113]

The most innovative ADR blockchain solutions envisage a decentralized dispute resolution system, which is 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:[114] jurors are asked to anonymously vote on the outcome to the case; those who voted with the majority 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; 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 commercial 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.[115] Furthermore, the lack of a reasoned opinion on the merit of the case and the written award might also be a problem when the decision needs to be enforced outside of 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 more expensive, 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 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.[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.[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 and EUIPO Report, in 2019, fake goods amount to 3.3 percent of world trade.[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."[119]

In the private sector, several companies in the pharma, sportswear and luxury industries as well as the spare parts industry are already using blockchain and AI-based technology together to fight the distribution of counterfeit products with great benefits in terms of fraud reduction and the streamlining of the control processes. This can be done by adding a QR code or NFC chip, as well as through laser marking systems[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 (e.g., the quality and source of the materials used, the time of production, the authorized manufacturers and importers, etc.).[121] This increases the difficulty of counterfeiting activities and facilitates the detection of suspicious products both by customs authorities and/or by online marketplaces.

An example of an online marketplace using blockchain technology is Alibaba. In 2020, the Chinese company announced a tool to track and verify food items being sold on its platforms.[122] Customers on Alibaba's marketplace would be able to verify whether the product they had bought was genuine by scanning the code on a product with their cell phone.

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 IPR 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.[123]

In Europe, in 2018, the EUIPO launched the Anti-Counterfeiting Blockathon, which aimed to create a network of people and organizations, from IP and blockchain industries, who could work together to design and implement a blockchain solution to fight against counterfeiting. According to a use case published by the EUIPO, a blockchain system can give its users (right holders)

"permissions to create tokens representing goods (tokenized goods) and proving the goods' authenticity through a Blockchain Access Portal. Right 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."[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.[125] To start with, customs authorities can take advantage of proven authenticity provided by blockchain, to allow the swift clearance of customs checks of tokenized goods. Eventually, customs could even automatically clear the goods within the blockchain itself.[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 right holders and custom authorities.[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: IP Enforcement Portal (Exchange Module) or IPEP is an essential tool that police and customs 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 trademark 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.

Section 4

Considerations

Blockchain has several potential applications in the IP ecosystems. However, the actors in the IP ecosystems should not let themselves be confused by the hype around blockchain and introduce the technology simply to emulate others. Blockchain implementation might entail considerable investment, 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 frameworks, governance, technical standards, sustainability and scalability, and training. It is up to each actor to analyze these considerations to assess whether the introduction of the technology is beneficial; and 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 necessary for governments and international organizations to adopt measures to reduce such risks and to facilitate the introduction of blockchain.

Before starting the journey of 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, consideration should be given as to which blockchain should be applied. When defining what criteria should be met, the use of the decision flow in Figure 3 is recommended.

This section presents the most important aspects and characteristics that should be considered when assessing blockchain technology: interoperability, standardization, governance and a 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 across the different layers of the system such as the 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.[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.[129]

In the meantime, formal technical specifications developed by international standardization bodies such as the International Standards Organization (ISO) and the International Telecommunications Union (ITU) are gaining traction[130] by agreeing on common terminologies, security and other general technical specifications. For instance, ISO has been actively working on distributed ledger technologies (DLTs) with a specific technical committee (ISO/TC 307), which aims to improve security, privacy, scalability and interoperability.

According to the European Commission's latest event report of blockchain standardization, the

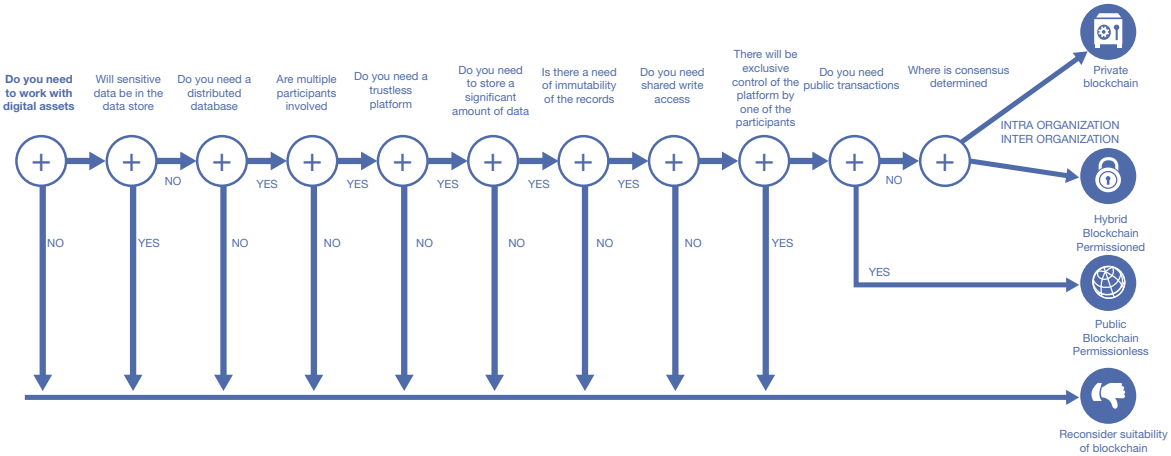
"Gap in blockchain standardisation: In particular, the lack of interoperability – whether tech to tech, tech to law, region to region, etc. – hinders DLT deployment. Standardization of many of these aspects is lacking. In terms of governance and processes, discussions and leadership are not sufficiently transparent and remain very far from being representative of society, or even of the global interests as a whole."[130]

The Global Blockchain Business Council has identified two key challenges with regard to blockchain standards: (1) aligning standards and codes of conduct across jurisdictions and industries; and (2) ensuring that stakeholders of all sizes have a voice.[131] Henceforth, for the development and adoption of common technical standards, all interested parties working on blockchain and/or other DLTs 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 toward the realization of a digital transformation of the IP offices and the services they provide to their customers and business partners. WIPO with its member states has been developing and providing standards to streamline and harmonize the filing, processing, dissemination and exchange of IP data and documentation within the IP ecosystems. For example, WIPO Standard ST.96[132] recommends the XML (eXtensible Markup Language) resources to be used for filing, publication, processing and exchange of information for all types of IP, namely, patents, trademarks, industrial designs, geographical indications and copyright. WIPO Standards ST.27,[133] ST.61[134] and ST.87[135] provide standardized codes to promote the efficient exchange of legal status data for patents, trademarks and industrial designs respectively in a harmonized manner between IPOs, 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 the IP community, the WIPO member states established an expert group under the Committee on WIPO Standards (CWS), the Blockchain Task Force, in 2018, to explore blockchain's impact on the IP space and to develop recommendations on its use in the IP ecosystems. As already mentioned above, interoperability concerns different layers. The following section aims to explain some considerations in regard to standards for integration, data exchange and security among the available blockchain platforms. It is recommended that these factors should be considered in the development process of the new WIPO standard on blockchain for the IP ecosystems. It also proposes that this new WIPO standard be developed in partnership with other international standardization bodies and blockchain platform providers.

Figure 3. Decision flow



Interoperability among existing blockchain platform networks and consortium projects

Interoperability among blockchain networks will be defined here 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 the 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 and Fabric opts for NoSQL storage (key value for very simple scenarios).

Some efforts are currently being made to solve these problems or to reduce the friction between the variants to create cross-platform applications following different strategies or seeking to tackle the issue from the point of view of concrete technology and a particular use case. Also, several working groups and organizations are approaching the problem from the standardization point of view such as the ISO/TC 307 working group focusing on the definition of standard terminology, taxonomy, ontology and governance; the Internet Research Task Force,[136] researching open issues in decentralized infrastructure services; and the ITU-T DLT group focusing on the creation of a reference ITU DLT architecture.

It is important to note that protocols allow for integration and interoperability with not only blockchain but also existing solutions (already deployed databases, message queues, Enterprise Service Bus (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 (EIPs) Ethereum Improvement Proposals, which aim to formalize common patterns and use cases in the form of standardized Interfaces.

As a real reference, "The Baseline Protocol"[137] is an open-source initiative that combines 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. To widen acceptability and adoption of the technologies across contexts and to foster trade via smart contract transactions, a degree of interoperability among various blockchain networks, and between blockchain (on-chain) and the outside world (off-chain), is needed. The interoperability among blockchains will need to be standardized to facilitate exchange and to harmonize the processes and types of transactions. This should be done to maintain a coherent blockchain ecosystem, to keep the value chain intact and to represent values reliably and consistently.

Furthermore, blockchain-based systems are connected to and interact with off-chain systems such as data providers, web APIs, enterprise backends, cloud providers, Internet of Things (IoT) devices, e-signatures and payment systems to get data from the real world and to 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 the 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.[138] 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 governance and/or a set of regulations to give legal and/or operational certainty to the participants in the value chain.

Corda, designed to coexist 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 time of writing, do not have 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 the IEEE Standards Association (IEEE SA),[139] exist in the form of working groups (IEEE 2418.2-2020 – IEEE Standard for Data Format for Blockchain Systems[140]) 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, such as Eventeum, which bridges blockchain events generated by transactions to backend decoupled microservices for further processing; Alethio,[141] which connects Ethereum data to IA services for advanced analytics; or Etherquery, which allows blockchain data to be uploaded to BigQuery.

Of special relevance is the integration of GraphQL, a new cross-technology standard for the complex query of graph-like related data, which simplifies data extraction from the blockchain. The Graph Protocol, a decentralized network protocol for indexing and querying data from blockchains, is an even more advanced technology that enables the exposure of 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 "secure by design," so to speak, 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:

- Public key infrastructure: PKI and X.509 UIT-T are well supported by blockchain platforms such as Hyperledger Fabric or R3 Corda. Both Fabric and Corda define services and users' identities around X.509 certificates, PKI and CAs, allowing for the reuse of existing infrastructure. Ethereum, on the contrary, will need an Ethereum-centric approach, with wallets as alternative to X.509 certificates.
- eIDAS regulatory framework for digital signatures: it is to be expected that all blockchain will be compliant with this framework, but probably with higher efforts based on cryptography constraints.
- 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. The newest standards have adopted JSON and OpenAPI and adapted to be eIDAS compliant.[142]
- Other approved security schemes: it is important to analyze any mismatch of the to-be-adopted blockchain platform with the existing security standards to guarantee compatibility between them. Ethereum, which was designed as a network-on-isolation, is expected to offer more friction, while DLT technologies that are able to integrate with existing SQL databases are "theoretically" more friendly to existing IT deployments.
- Standard Authentication, Authorization and Access (AAA) systems: 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 IP ecosystems need to take into account when deciding whether to introduce blockchain solutions is governance. As this factor is urgent and important for blockchain networks, there are several efforts underway by different institutions with different approaches based on established governances such as corporate 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 design a use case on a public or private permissioned network. 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:

- Participants. Accurately identifying participants and aligning 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 the like.
- 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.
- 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 actions. 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.
- Dispute resolution mechanisms. Establish dispute resolution mechanisms that can be applied to potential problems. As a basic governance requirement, a responsible party who can address any 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's internal governance framework.

As an example, transparency will become part of an organization's values, as providing guidance to the participants will be necessary so that they can 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 resolved in 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 the infrastructure and the chosen framework.

Legal structure

A legal structure is one of the governance elements that gives legal recognition and a framework of decision rights and accountability to the network in practical and enforceable ways. The decision-making power can be centralized to a single entity/person or small group, 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 a challenge for both governance and regulation. 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 is 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, 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, the mechanisms of dispute resolution and the responsibilities of the parties, among other considerations, established by the technical architecture. It is worth giving consideration to the choice of legal structure. 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 may arise concerning the anonymity/pseudonymity of some participants, 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 of 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 in it. Thus, it is mandatory to understand whether the network is a general- or special-purpose one. The former is built with the capacity to build on the top through smart contracts the way Ethereum, NEO or EOS works, and the latter, for instance, Bitcoin, Litecoin or Dash, serves as an efficient electronic payment system.

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–benefit analysis for the four primary consensus mechanisms is depicted in Table 3.

Permissionless blockchains do not require permission to join them 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 been 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 which currently uses PoW, but is now moving to Proof of Stake (PoS) for its version 2.0. PoS has been thought of for general-purpose networks with the demand of high level of transactions (considering the high demand of smart contract transactions). This algorithm has been

Table 3. Comparison of consensus methods

Consensus method	Benefits	Costs
PoW	Suits a trustless network Low governance overheads	Slow transaction time High resource consumption
PoS	Low governance overheads Incentivizes investment in the system Short transaction time	Prone to 51 percent attacks 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

demonstrated to be less inefficient than PoW, due to the transaction costs, volatility, and scalability for public permissionless networks, but it comes with better energy efficiency, reduces the hardware requirements and provides stronger immunity to centralization.

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 and 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 Table 4.

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 privacy practices, limitation of liability or disclaimers, IPR, advertisement or endorsements, payment terms, termination, notifications, contact information and dispute resolution methods.

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, the updating, removing and adding of nodes, testing procedures, encryption key administration, 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 network's ledger(s). In the blockchain field, like in any other type of network, a clear understanding of data ownership, its authorized use, 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 plays 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 to and accepted by all the network participants, granting the best coordination

Table 4. Advantages and disadvantages of permissionless and permissioned blockchain

	Permissionless	Permissioned
Advantages	Broader decentralization Highly transparent Security resilience Tamper-proof	Faster transaction speed and more scalable Stronger information privacy Offers lower energy consumption Can offer more customizability
Disadvantages	Slow transaction speed and harder to scale Not energy efficient Less information privacy	Not truly decentralized Less transparent to outside oversight Less anonymous

possible and complying with the current data regulations.

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 the 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, why is a blockchain required?

It may be appropriate to record on a blockchain that a transaction affecting a non-OPI asset has occurred without providing any of the non-OPI information. For example, the sale of an asset, such as land or a business, may need to be on a public register so that 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

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).

In 2018 the above-mentioned considerations 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 such as Quorum (JPMorgan Chase) and Pantheon (ConsenSys), a new concept of public-permissioned networks was created and defined by ISO/TC 307 typology.[143] 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.

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.

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.

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.

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

Regulatory framework

Currently, there is a unanimous position among institutions concerning the potential of blockchain. However, the strong benefits that have been identified are coupled with a high level of legal uncertainty with regard to the technology.[144] 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.[145]

It should be noted that legal uncertainty not only refers 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. These include, 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. Legal uncertainty is increased by the fact that participants in a blockchain can be established in multiple jurisdictions.[146]

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 because 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.[147] With that aim, works have already commenced at national, regional and international levels.[148]

Uncertainty in relation to the general aspects of blockchain

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[149] and ultimate accountability for the data exchanged.[150] The degree of difficulty increases 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 ascertaining liability, determining what law is applicable in a particular situation, carrying out regulatory monitoring or enforcing rules.[151]

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.[152] 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.

Cross-border issues. It is usually the case of participants in a blockchain (founder, nodes and users) located in different jurisdictions.[153] 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.[154] Legal uncertainty increases where the different jurisdictions the blockchain is connected to adopt different approaches to regulatory issues.[155] 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 regulations 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.[156]

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.[157]

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.[158] 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?[159]

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, as per the definition, the information on the blockchain is replicated in each of them.[160] States are adopting legislation[161] and specific rules in free trade agreements against these categories of measures to facilitate the free data flow.[162] However, many states still endorse data location requirements with different objectives.[163] This may constitute an obstacle for the deployment of multinational blockchain networks.

Uncertainty in relation to some applications of blockchain

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), time-stamps (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).[164] 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 when talking about blockchain applications for IPR enforcement, 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 the eIDAS Regulation to be legally binding.[165]

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 fide effects to the digital information stored in blockchains.[166] There are ongoing projects in relation to real estate registries[167] that can be taken as examples for IP registries.

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.[168]

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 the issue of which information should be taken, but this is not a new challenges compared to other digital technologies.[169] 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.[170] 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.[171]

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 codes 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.[172] 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 the case of a dispute or an error. It should further be noted that the use of a smart contract, or any blockchain code off open source may be bound by open-source requirements or certain terms and conditions.

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).[173] Nonetheless, many states have either proposed or enacted legislation applicable to smart contracts or contracts in electronic format.[174] 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 a requirement is met if the contract is stored in a durable medium.[175] 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 condition 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."[176]

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 that are difficult to answer. What happens if the legal document and the computer code differ? What if the applicable law changes or *force majeure* situations – for example, a pandemic such as COVID-19 – arise? What happens if a court orders that a smart contract is unenforceable? Such a decision may arise when the smart contract obligations have already been automatically performed, what happens then? Since no case law currently exists 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.[177]

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 that 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 tokens, utility tokens, currency tokens and hybrid tokens – 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.[178] This uncertainty augments due to the absence of uniform definitions.[179]

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.[180]

Ongoing works on the regulatory framework adoption

There is emerging consensus that the adoption of legislative instruments will reduce legal uncertainty and encourage innovation in relation to digital technologies in general.[181] In this sense, as shown by the documents cited in this section, international organizations such as UNCITRAL, UNIDROIT,[182] 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.

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.[183] In this regard, at the first stage such instruments may take the form of minimum standards or guidelines – namely, soft law.

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*[184] 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."

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."[185]

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.

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.

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

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 attacks and the 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.

Blockchain has the ability to transform current systems toward 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.

Blockchain has the ability not only to detect an error or attempted fraud within the network but also to prevent 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.

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 error. 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

When talking about blockchain technology, warnings 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.[186] 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 data centers in which they are hosted. This continuous upscaling may reach a sustainability

limit requiring different strategies other than simply adding central processing units (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.

Another important challenge of this technology is scalability, namely, 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 to warrant strong consistency. While some consensuses 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 upgrades and for which the consistency level can be relaxed.

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 also be noted that consensus balances throughput with other aspects, such as the level of "trust-less" and/or responsiveness, and 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 one patent per year on average, since value is "something scarce" by its very nature.

Technology gap and capacity building

Frontier technologies, in general, bring opportunities to improve business operational efficiency and to make working and thinking more effective. However the adoption of those technologies has different phases and various manners due to different interests 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, and it would be desirable to reduce the technological gap between actors through collaborations for capacity building.

As the blockchain is one of the frontier technologies, the common issue of 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 life cycle of IP assets will be decreased since IPR 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, to promote the IP market or the fight against counterfeiting and piracy.

The efforts to help public bodies in their transition to blockchain-based systems would have been totally futile if they were not accompanied by 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.

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 stovepiped: 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.

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 to hamper 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.

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 percent of the world's top universities offer blockchain courses,[187] 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, startups and so on. At the same time, governments, universities and technology companies should include this new technology in their academic offerings.

Notes

1. Intellectual property shall include rights relating to:
   - literary, artistic and scientific works,
   - performances of performing artists, phonograms and broadcasts,
   - inventions in all fields of human endeavor,
   - scientific discoveries,
   - industrial designs; trademarks, service marks and commercial names and designations,
   - protection against unfair competition,

   and all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields. See WIPO (2004). Intellectual Property Handbook. Geneva: World Intellectual Property Organization, p. 15. www.wipo.int/edocs/pubdocs/en/wipo_pub_489.pdf
2. Committee on WIPO Standards (CWS) (2018). Sixth Session Geneva, October 15–19, 2018. www.wipo.int/edocs/mdocs/classifications/en/cws_6/cws_6_4_rev.pdf
3. World Economic Forum (2016). The Fourth Industrial Revolution: what it means, how to respond. World Economic Forum, January 14.
4. Schwab, K. (2016). *The Fourth Industrial Revolution*, p. 23. New York: Crown Business.
5. World Economic Forum (2016). The Fourth Industrial Revolution: what it means, how to respond. World Economic Forum, January 14.
6. European Patent Office (2020). Fourth Industrial Revolution.
7. McKinsey & Company (2017). Jobs lost, jobs gained: What the future of work will mean for jobs, skills, and wages. McKinsey Institute, November 28.
8. EY (n.d.). How can blockchain transform a gaming platform into a game changer? https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2020_7_english.pdf
9. Schwartz, M. (2016). The potential of blockchain. TED, May.
10. Ibid.
11. Ibid.
12. Ibid.
13. Hyperledger (2017). Hyperledger Architecture, Volume 1: Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus. www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf
14. Yaga, D., P. Mell, N. Roby and K. Scarfone (2018). Blockchain Technology Overview. NISTIR 8202. National Institute of Standards and Technology and US Department of Commerce. https://doi.org/10.6028/NIST.IR.8202
15. Ibid.
16. OECD (n.d.). Blockchain and distributed ledger technology. www.oecd.org/daf/blockchain
17. UNCTAD (2021). Harnessing blockchain for sustainable development: prospects and challenges. June 25. https://unctad.org/webflyer/harnessing-blockchain-sustainable-development-prospects-and-challenges
18. UNJIU (2020). Blockchain applications in the United Nations system: towards a state of readiness. www.unjiu.org/content/blockchain-applications-united-nations-system-towards-state-readiness
19. UNECE (2020). White Paper on Blockchain in Trade Facilitation. ECE/TRADE/457. https://unece.org/trade/publications/white-paper-blockchain-trade-facilitation-ecetrade457
20. EU Blockchain Observatory and Forum (n.d.). www.eublockchainforum.eu
21. International Chamber of Commerce (2020). Intercoms® 2020. https://iccwbo.org/resources-for-business/incoterms-rules/incoterms-2020
22. Yaga, D., P. Mell, N. Roby and K. Scarfone (2018). Blockchain Technology Overview. NISTIR 8202. National Institute of Standards and Technology and US Department of Commerce. https://doi.org/10.6028/NIST.IR.8202
23. Litan, A. And A. Leow (2020). Hype Cycle for Blockchain Technologies, 2020. *Gartner*, July 13.
24. Ibid.
25. W3C (2021). Decentralized Identifiers (DIDs) v1.0. https://w3c.github.io/did-core
26. Szabo, N. (1994). Smart Contracts. www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html
27. EU Blockchain Observatory and Forum (2021). NFT – Legal Token Classification, p. 2.
28. CryptoPunks (n.d.).
29. CryptoKitties (n.d.).
30. Bored Ape Yacht Club (n.d.). https://boredapeyachtclub.com
31. OpenSea (n.d.). www.opensea.io
32. Vota, W. (2019). 10 Blockchain Implementation Risks in International Development. ICTWorks, February 27.
33. IBM (n.d.). What is blockchain security? www.ibm.com/topics/blockchain-security
34. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf
35. In the sphere of industrial property one can find rights of various sorts, 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. WIPO (2016). Understanding Industrial Property, p. 6.
36. Copyright and related rights protect literary, artistic and scientific works; performances of performing artists, phonograms and broadcasts. WIPO (2016). Understanding Copyright and related rights, p. 6.
37. IP environment includes laws, agreements, practices, economy, culture, traditions, moral and economic rights, the rights of the public to access those creations.
38. In fact, the value chain model for copyrights and related rights could be described in different ways, for example, 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 as coinciding with the management phase from the copyright perspective.
39. WIPO (2011). The Patent System and Genetic Resources. WIPO/GRTKF/IC/9/13. www.wipo.int/meetings/en/doc_details.jsp?doc_id=152237 and WIPO (2007). Additional Explanation from Japan Regarding the Document WIPO/GRTKF/IC/9/13 on the Patent System and Genetic Resources. WIPO/GRTKF/IC/11/11. www.wipo.int/meetings/en/doc_details.jsp?doc_id=81052
40. WIPO (2016). Understanding Industrial Property, p. 6.
41. Barulli, M. (2021). IP is a journey: blockchain and encrypted storage are your best friends. *WIPO Magazine*, February.
42. 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, Spanish-based law firm Pons IP developed a solution called Safe Evidence that uses electronic signature.
43. These services are called *EtherScan* or *BitScan*.
44. Boucher, P. (2017). How blockchain technology can change our lives. European Parliamentary Research Service. PE 581.948.
45. Henkel, J. and S.M. Lernbecher (née Pangerl) (2008). Defensive Publishing – An Empirical Study. https://ssrn.com/abstract=981444

46. Bernstein (n.d.). The decentralized future of defensive publishing and IPFS. https://ipfs.io
47. Zertifier (n.d.). https://www.zertifier.com/hash4life.html
48. HASH4LIFE (n.d.). https://hash4life.com
49. WeTransfer (n.d.). www.wetransfer.com
50. IPwe (n.d.). https://ipwe.com
51. Krajewski, T. and R. Lettiere (2019). Efforts Integrating Blockchain with Intellectual Property. *Les Nouvelles - Journal of the Licensing Executives Society*, 54(1). https://ssrn.com/abstract=3317053
52. Please see the IBM-IPwe project of patent tokenization. IBM (2021). IPwe and IBM Seek to Transform Corporate Patents with Next Generation NFTs Using IBM Blockchain. April 20. https://newsroom.ibm.com/2021-04-20-IPwe-and-IBM-Seek-to-Transform-Corporate-Patents-With-Next-Generation-NFTs-Using-IBM-Blockchain
53. 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.
54. In any case, permissioned blockchains do not offer low levels of security. An example of that is Hyperledger Fabric, an open-source project offered by the Linux Foundation, which is a permissioned blockchain, guaranteeing a high level of security.
55. WIPO (2018). Meeting of Intellectual Property Offices (IPOs) on ICT Strategies and Artificial Intelligence (AI) for IP Administration. May 23–25. Geneva: World Intellectual Property Organization.
56. Bian, S., G. Shen, Z. Huang, Y. Yang, J. Li and X. Zhang (2021). PABC: A Patent Application System Based on Blockchain. *IEEE Access*, 9, 4199–4210. https://doi.org10.1109/ACCESS.2020.3048004
57. European Parliament (2017). How blockchain technology can change our lives, pp. 10–11.
58. Further details will be given in the IPR enforcement section.
59. IEEE Xplore (n.d.). https://ieeexplore.ieee.org/Xplore/home.jsp
60. 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. November 25. Brussels: European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0760&from=EN
61. Some other blockchains are introducing NFTs, such as TRON.
62. Fairfield, J. (2021). Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property. *Indiana Law Journal*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3821102
63. Christie's (2021). Beeple (b. 1981). https://onlineonly.christies.com/s/first-open-beeple/beeple-b-1981-1/112924
64. 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 USD 6 million.
65. CryptoKitties (n.d.). www.cryptokitties.co
66. Harper, J. (2021). Jack Dorsey's first ever tweet sells for $2.9m. BBC News, March 23.
67. Algorand (n.d.).
68. The Creative Passport (n.d.). http://myceliaformusic.org/
69. Access©, Prescient and Attribution Ledger (2020). Future of content monetization and next era of digital interactions. February. Toronto: Prescient Innovations.
70. Peertracks (n.d.). www.peertracks.com
71. Unison (n.d.). www.unisonrights.es/en
72. Maecenas (n.d.).
73. See WIPO (2020). Wipo Conversation on Intellectual Property (IP) and Artificial Intelligence (AI). WIPO/IP/AI/2/GE/20/1 REV. Geneva: World Intellectual Property Organization, paras. 28 to 34.
74. OECD (2019). Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies. Paris: OECD Publishing. https://doi.org/10.1787/276aaca8-en
75. For more, see Drexl, J. (2017). Designing Competitive Markets for Industrial Data Between Propertisation and Access. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8, 257–292.; Stepanov, I. (2020). Introducing a property right over data in the EU: the data producer's right – an evaluation. *International Review of Law, Computers & Technology*, 34(1), 65–86. https://doi.org/10.1080/13600869.2019.1631621
76. For a technical approach to blockchain based data tokenization, see Zhou, T., X. Li and H. Zhao (2019). DLattice: A Permission-less Blockchain-based on DPoS-BA-DAG Consensus for Data Tokenization. *IEEE Access*, 7, 39273–39287. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8672629
77. OECD (2020). The Tokenisation of Assets and Potential Implications for Financial Markets. OECD Blockchain Policy Series, p. 11.
78. Datum (n.d.). https://datum.org
79. Ocean (2021). Tools for the Web3 Data Economy. https://oceanprotocol.com
80. Ecosteer (n.d.). https://ecosteer.com
81. IOTA (n.d.). Home. https://data.iota.org
82. Kneron (n.d.). Introducing KNEO.
83. OECD (2020). The Tokenisation of Assets and Potential Implications for Financial Markets. OECD Blockchain Policy Series, p. 16. www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.htm
84. See Haenni, R. (2017). Datum Network: The decentralized data marketplace. White Paper V15. 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.
85. Ibid., p. 11.
86. ERC-721 is an Ethereum open standard for non-fungible tokens, see ERC-721 (n.d.). What is ERC-721? http://erc721.org
87. ERC-20 is an Ethereum open standard for fungible tokens. See Ethereum (2021). ERC-20 Standard. https://ethereum.org/en/developers/docs/standards/tokens/erc-20
88. For a composable non-fungible token standard, see ERC-998 (n.d.). What is ERC-998? http://erc998.org
89. 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. https://blog.oceanprotocol.com/data-tokens-2-fungible-composable-54b6e0d28293
90. McConaghy, T. (2019). Datatokens 1: Data Custody. Ocean Protocol. https://blog.oceanprotocol.com/data-tokens-1-data-custody-1d0d5ae66d0c
91. See Haenni, R. (2017). Datum Network: The decentralized data marketplace. White Paper V15, pp. 14ff. https://datum.org/assets/Datum-WhitePaper.pdf
92. Ibid., pp. 16, 19.
93. Spiekermann, M. (2019). Data Marketplaces: Trends and Monetisation of Data Goods. *Intereconomics – Review of European Economic Policy*, 54(4), 210–211; for a definition and examples of data marketplaces, see also Carnelley, P., H. Schwenk, G. Cattaneo, G. Micheletti and D. Osimo (2016). Europe's Datamarketplaces – Current Status and Future Perspectives. Report for the European Commission, p. 10. https://datalandscape.eu/data-driven-stories/europe's-data-marketplaces-–-current-status-and-future-perspectives

94. 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., F. Stahl, F. Schomm and G. Vossen (2015). A classification framework for data marketplaces. Working Paper No. 23. European Research Center for Information Systems, p. 8.
95. IOTA (2019). Part 1: IOTA Data Marketplace – Update. https://blog.iota.org/part-1-iota-data-marketplace-update-5f6a8ce96d05
96. European Commission (2020). A European strategy for data. Doc. COM(2020) 66 final; US Federal Data Strategy (n.d.). https://strategy.data.gov; UK Department for Digital, Culture, Media & Sport (2019). National Data Strategy. July 8.
97. See WIPO (2004). *Intellectual Property Handbook*, p. 207. Geneva: World Intellectual Property Organization.
98. WEF (2020). Bridging the Governance Gap: Dispute resolution for blockchain-based transactions, p. 6.
99. European Commission (2020). Study on the use of innovative technologies in the justice field, pp. 43–44. https://op.europa.eu/en/publication-detail/-/publication/4fb8e194-f634-11ea-991b-01aa75ed71a1/language-en
100. Allessie, D., M. Sobolewski and L. Vaccari (2019). Blockchain for digital government, ed. F. Pignatelli. EUR 29677 EN. Luxembourg: Publications Office of the European Union. https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-digital-government
101. See Du, G. (2019). Why are Chinese Internet Courts Keen on Blockchain Technology? *China Justice Observer*, December 15.
102. See Tokenpost (2019). Alibaba to implement blockchain in intellectual property system. May 28. https://tokenpost.com/Alibaba-to-implement-blockchain-in-intellectual-property-system-2010
103. See Du, G. (2021). When Blockchain Meets Electronic Evidence in China's Internet Courts. *China Justice Observer*, March 29.
104. Article 11 of the SPC Provisions on Several Issues Concerning the Hearing of Cases by Internet Courts.
105. See Du, G. (2021). When Blockchain Meets Electronic Evidence in China's Internet Courts. *China Justice Observer*, March 29.
106. WEF (2020). Bridging the Governance Gap: Dispute resolution for blockchain-based transactions.
107. Shehata, I. (2018). Three Potential Imminent Benefits of Blockchain for International Arbitration: Cybersecurity, Confidentiality & Efficiency. *Young Arbitration Review*. https://ssrn.com/abstract=3290028
108. European Commission (2018). Study on Blockchains – Legal, governance and interoperability aspects. SMART 2018/0038, p. 78. https://digital-strategy.ec.europa.eu/en/library/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038
109. The WIPO Arbitration and Mediation Center provides a secure and confidential online case management tool for parties resolving their disputes under WIPO ADR Rules. For further information regarding this service, see WIPO (n.d.). WIPO eADR.
110. See LAWTECHUK (2021). Digital Dispute Resolution Rules: UK Jurisdiction Taskforce. https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2021/04/Lawtech_DDRR_Final.pdf
111. See JAMS (n.d.). JAMS Smart Contract Clause and Rules (DRAFT).
112. In this regard, see the section on Sustainability and Scalability in Chapter 4.
113. Shehata, I. (2018). Three Potential Imminent Benefits of Blockchain for International Arbitration: Cybersecurity, Confidentiality & Efficiency. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3290028
114. Rabinovich-Einy, O. and E. Katsch (2019). Blockchain and the Inevitability of Disputes: The Role for Online. *Journal of Dispute Resolution*, 2019(2). https://scholarship.law.missouri.edu/jdr/vol2019/iss2/6
115. WEF (2020). Bridging the Governance Gap: Dispute Resolution for Blockchain-based Transactions, p. 13.
116. 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.
117. In relation to Kleros, see IPCHAIN (2019). ODR and its applications in IP-related services in the EU, p. 11. https://ipchain.global/docs/legal_research/en/ODR_and_its_applications_in_IP-related_services_in_the_EU.pdf
118. OECD and EUIPO (2019). *Trends in Trade in Counterfeit and Pirated Goods*. Illicit Trade. Paris: OECD Publishing. https://doi.org/10.1787/g2g9f533-en
119. See EC and EUIPO (2019). Blockchain Report. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Blockathon/Blockathon_Report.pdf
120. www.iTracetech.com
121. 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.
122. Hin, P. (2020). Alibaba's Koala Introduces Blockchain to Help Buyers Track Origin of Goods. Coins Network, March 18.
123. See Australian Government (n.d.). Smart Trade Mark™. https://smarttrademark.search.ipaustralia.gov.au
124. See EC and EUIPO (2019). Anti-Counterfeiting Blockchain Use Case. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Blockathon/Blockathon-Forum_Blockchain-Use-Case.pdf
125. WCO (2019). Study report on Disruptive Technologies, p. 19.
126. Okazaki, Y. (2018). Unveiling the Potential of Blockchain for Customs. WCO issued Research Paper No. 45.
127. See EUIPO (2019). Anti-Counterfeiting Blockchain Use Case. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Blockathon/Blockathon-Forum_Blockchain-Use-Case.pdf
128. World Economic Forum (2020). Global Standards Mapping Initiative: An overview of blockchain technical standards. White Paper, p. 8.
129. Ethereum Improvement Proposals (n.d.). https://eips.ethereum.org
130. European Commission (2020). Joining Forces for blockchain Standardisation. European Commission, July 29, pp. 13–14. https://ec.europa.eu/digital-single-market/en/news/joining-forces-blockchain-standardisation
131. Global Blockchain Business Council (2020). Global Standard Mapping Initiative. Insight Report, p. 27.
132. WIPO (2021). STANDARD ST.96.
133. WIPO (2020). STANDARD ST.27.
134. WIPO (2020). STANDARD ST.61.
135. WIPO (2018). STANDARD ST.87.
136. Internet Research Task Force (n.d.). Overview. https://irtf.org
137. EEA Community Projects – Baseline (n.d.). The Baseline Protocol. www.baseline-protocol.org
138. Curran, B. (2018). What Are Oracles? Smart Contracts, Chainlink & "The Oracle Problem." Blockonomi,

September 19. https://blockonomi.com/oracles-guide

139. IEEE SA (n.d.). About Us. https://standards.ieee.org/about/index.html
140. IEEE SA (2020). IEEE 2418.2-2020 – IEEE Standard for Data Format for Blockchain Systems. https://standards.ieee.org/standard/2418_2-2020.html
141. Eventeum (n.d.). https://github.com/ConsenSys/eventeum
142. Hühnlein, D. (2020). New APIs for the eIDAS-Ecosystem. eIDAS, January 20. https://blog.eid.as/tag/oasis-dss-x-core-2-0-en
143. 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.
144. UN Joint Inspection Unit (2020). Blockchain applications in the United Nations system: towards a state of readiness.
145. Ibid., para. 240.
146. 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
147. EU Blockchain Observatory and Forum (2019). Legal and regulatory framework of blockchains and smart contracts, p. 10.
148. 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
149. Finck, M. (2019). *Blockchain Regulation and Governance in Europe*, ch. 2. Cambridge: Cambridge University Press.
150. See European Commission (2020). Study on the use of innovative technologies in the justice field.
151. EU Blockchain Observatory and Forum (2019). Legal and regulatory framework of blockchains and smart contracts, p. 6. www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf
152. European Commission (2018). Study on Blockchains - Legal, governance and interoperability aspects. SMART 2018/0038, p. 46. https://digital-strategy.ec.europa.eu/en/library/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038
153. Le Conseil Fédéral (2018). Bases juridiques pour la distributed ledger technology et la blockchain en Suisse, pp. 74ff.
154. OECD (2021). Regulatory Approaches to the Tokenisation of Assets. OECD Blockchain Policy Series, p. 31, JUI, para. 263. www.oecd.org/finance/Regulatory-Approaches-to-the-Tokenisation-of-Assets.htm
155. EU Blockchain Observatory and Forum (2019). Legal and regulatory framework of blockchains and smart contracts, p. 13. www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf
156. 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 HCCH [2020]. Conclusions and Decisions adopted by CGAP at its meeting of 3–6 March 2020, para.15. https://assets.hcch.net/docs/70458042-f771-4e94-9c56-df3257a1e5ff.pdf).
157. EU Blockchain Observatory and Forum (2019). Legal and regulatory framework of blockchains and smart contracts, p. 14. www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf
158. Ibid., p. 19.
159. European Parliament (2019). Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?
160. European Commission (2018). Study on Blockchains – Legal, governance and interoperability aspects. SMART 2018/0038, p. 49. https://digital-strategy.ec.europa.eu/en/library/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038
161. 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
162. See, for instance, Article 19.11 of the United States-Mexico-Canada Agreement or Article 14.11 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP).
163. Svantesson, D. (2020). *Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines*. OECD Digital Economy Papers, No. 301, Paris: OECD Publishing. http://dx.doi.org/10.1787/7fbaed62-en
164. EU Blockchain Observatory and Forum (2019). Legal and regulatory framework of blockchains and smart contracts, p. 12.
165. Ibid., p. 11.
166. European Commission (2018). Study on Blockchains – Legal, governance and interoperability aspects. SMART 2018/0038, p. 55. https://digital-strategy.ec.europa.eu/en/library/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038
167. UK Land Registry case, see Tombs, L. (2019). Could blockchain be the future of the property market? HM Land Registry, May 24. https://hmlandregistry.blog.gov.uk/2019/05/24/could-blockchain-be-the-future-of-the-property-market
168. "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 percent of all 100) replies from stakeholders have been received, where 6 (or 11 percent of the 56 replies) selected 'Yes', 38 (or 68 percent of the 56 replies) indicated 'No', and 12 (or 21 percent of the 56 replies) selected 'Other'." See European Commission (2018). Study on Blockchains – Legal, governance and interoperability aspects. SMART 2018/0038, p. 71. https://digital-strategy.ec.europa.eu/en/library/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038
169. European Commission (2018). Study on Blockchains – Legal, governance and interoperability aspects. SMART 2018/0038, p. 55. https://digital-strategy.ec.europa.eu/en/library/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038
170. Unofficial Translation of the Report and Application of the Government to the Parliament of the Principality of Liechtenstein concerning the Creation of a law on Tokens and TT Service Providers (Tokens and TT Service Provider Act; TVTG) (Blockchain Act) (2019). https://impuls-liechtenstein.li/wp-content/uploads/2021/02/Report-and-Application-TVTG-extract.pdf
171. EU Blockchain Observatory and Forum (2019). Legal and regulatory framework of blockchains and smart contracts, p. 12.
172. Ibid., p. 22.
173. UK Jurisdiction Task Force (2019). Legal statement on cryptoassets and smart contracts. https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf
174. European Commission (2018). Study on Blockchains – Legal, governance and interoperability aspects. SMART 2018/0038, p. 59. https://digital-strategy.ec.europa.eu/en/library/study-blockchains-legal-governance-

and-interoperability-aspects-smart-20180038

175. See, for instance, Article 5 of the United Nations Convention on the Use of Electronic Communications in International Contracts (2005). New York: UN. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/06-57452_ebook.pdf
176. European Commission (2018). Study on Blockchains – Legal, governance and interoperability aspects. SMART 2018/0038, p. 64. https://digital-strategy.ec.europa.eu/en/library/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038
177. "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 (2018). Study on Blockchains – Legal, governance and interoperability aspects. SMART 2018/0038, p. 55. https://digital-strategy.ec.europa.eu/en/library/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038
178. Hacker, P. and C. Thomale (2019). The Crypto-Security: Initial Coin Offerings and EU Securities Regulation, in P. Hacker, I. Lianos, G. Dimitropoulos and S. Eich, (eds.), *Regulating Blockchain: Techno-Social and Legal Challenges*, pp. 214–225. Oxford: Oxford University Press.
179. 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
180. European Commission (2018). Study on Blockchains – Legal, governance and interoperability aspects. SMART 2018/0038, p. 91. https://digital-strategy.ec.europa.eu/en/library/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038; Le Conseil Fédéral (2018). Bases juridiques pour la distributed ledger technology et la blockchain en Suisse, pp. 47ff. www.newsd.admin.ch/newsd/message/attachments/55151.pdf
181. See, for instance, UN Joint Inspection Unit (2020). Blockchain applications in the United Nations system: towards a state of readiness, p. v. www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2020_7_english.pdf
182. 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 UNIDROIT (n.d.). Digital Assets and Private Law: Study LXXXII – Digital Assets and Private Law Project.
183. UN Joint Inspection Unit (2020). Blockchain applications in the United Nations system: towards a state of readiness, p. v. www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2020_7_english.pdf
184. UNCITRAL (2020). Legal issues related to the digital economy - Note by the Secretariat. Doc. A/CN.9/1012. https://undocs.org/en/A/CN.9/1012
185. https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2020_7_english.pdf
186. 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.
187. Kaaru, S. (2019). Over half of the top 50 universities offer blockchain courses: Report. CoinGeek, August 29. https://coingeek.com/over-half-of-the-top-50-universities-offer-blockchain-courses-report

Annex I
Overview of IP ecosystems and IP value chains

IP ecosystem[1]

Intellectual property (IP), broadly, means the legal rights that result from intellectual activity in the industrial, scientific, literary and artistic fields.[2] IP law has been traditionally divided into two classical branches of law, namely, "industrial property" and "copyright and related rights" law,[3] and also encompasses legal systems that do not fall neatly within the distinction. Those systems, which lie beyond the classical distinction of "industrial property" and "copyright and related rights," are referred to as *sui generis* IP laws (i.e., laws granting rights "of their own kind") and cover subject matter such as new varieties of plants, non-original databases, software, traditional knowledge (TK) and traditional cultural expressions (TCEs). Besides these established legal systems, which are constituted by formalized, statutory IP law frameworks (at a national, regional or international level), there are additional closely related branches of law that have historically provided the origins and basic principles of currently established IP standards and which therefore are often also considered to be part of the field of IP law, for example, unfair competition law and certain branches of regulatory law relating to market approval of agricultural and pharmaceutical products.

Traditionally, international agreements as well as legal literature regarding the availability of such rights over IP refer to "systems for the protection of intellectual property."[4] This document refers to "IP ecosystems" rather than IP systems. For the purposes of this white paper, the use of the term "IP ecosystems" is useful to appropriately describe the full breath of the potential impact(s) of blockchain on "IP" and the existing IP systems.

In this document, the term "IP ecosystem" refers to a network of various actors that interact with each other in collaborative and competitive ways in an IP environment[5] using resources to generate, protect, manage, make available and/or commercialize intellectual assets.

Intellectual assets constitute a subclass of "intangible assets, which are [defined as] non-physical assets such as leases, brands, digital assets, use rights, licenses, intellectual property rights, reputation or agreements."[6] An "asset" in general, including an intangible asset, is defined as an "item, thing or entity that has potential or actual value to an organization."[7] In an IP context, the actual or potential value of an intellectual asset may refer to its economic (e.g., monetary), epistemic (e.g., scientific and technological) or affective (e.g., goodwill) value. Value can be tangible or intangible, financial or non-financial, and includes consideration of risks and liabilities.[8] It can be positive or negative at different stages of the asset's life.

The interactions by which actors interact within IP ecosystems can be modeled into value chains of IP, namely, IP value chains. IP value chains are sets of activities through which actors add to or appropriate the value of intellectual assets. Generally, the interactions of value chains are highly diverse, context- and case-specific and often discontinuous. However, when they form continuous interactions taking place over a continuously evolving (set of) intellectual asset(s), they have been described as value chains of IP, namely, 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 a simplified, general description. Therefore, when simplified for illustrative purposes into a single generic model, they could be described in the following generalized model of an IP value chain.

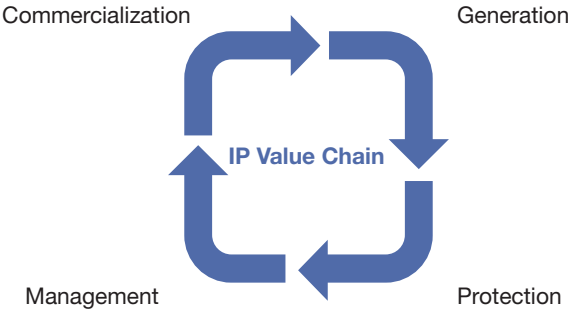
Value chains can generally be represented in a life cycle model. The life cycle of an intellectual asset is defined as the stages involved in the management of that asset, whereby the naming and number of the stages and the activities under each stage usually vary in different industry sectors and are determined by the relevant organization. While recognizing that the naming of phases and activities under each phase vary, in the IP context a very generalized model often refers to four phases, even though many IP assets do not go through every phase or proceed through phases in a sequential manner. Therefore, these phases and activities identified in each phase of the model are not necessarily sequential and they can overlap and not always take place, especially with regard to unregistered IP rights. For example, in the case of copyright, the generation phase usually coincides with the protection phase because a work is usually protected upon generation; and the management phase may be often mixed with the commercialization phase, especially when the copyright is managed and at the same time licensed by a copyright management organization (CMO).

IP value chain phases

The type of IP value chains[9] that are oriented toward commercialization of IP assets could be composed of four phases, mostly for registered IP rights such as patents, but not all activities in phases apply to all IP rights, in particular some activities may not apply for copyright and related rights and IP assets that are subject primarily or exclusively to unfair competition law:

- Generation;
- Protection;
- Management; and
- Commercialization.

Figure 4. IP value chain chases



In the following sections, generalized, exemplary sub-phases and activities within each phase are described in further detail. Each phase and the related activities of the illustrative IP value chain is described with three key components: activities, actors and resources. It is important to note that a natural or legal person, namely, an individual or organization, can play the different roles of many key actors. For example, creators of creative content are often "small businesses" and are directly involved in many more of the phases. This is increasingly the case with the democratization of content production and distribution enabled by technology. Blockchain as an enabling technology can play an important role in this trend.

IP generation phase

In general descriptions of asset life cycles, this phase is also referred to as the Generation phase. Since in the field of IP, "creation" and "creativity" are technical terms specifically associated with the field of copyright and related rights, to include the origination of all types of IP assets this paper uses the term "generation."[10] This phase includes all steps from the initial intellectual activity resulting in potential IP value to the existence of an initial intellectual asset eligible for IP protection. This phase includes not only the creation of creative works but also the activities needed to embody the idea of an innovator and, in many cases, it requires the involvement of third party actors.

For copyright and related rights, any original creative work is protected by copyright law from the moment it is created, and a formal registration process is not needed in most jurisdictions, but this could, in certain circumstances, make it difficult to prove ownership and for users of the work to identify the creator.

The initial terms used to describe the sub-phases of this phase are preliminarily modeled on the branches of IP law, which concern intellectual activity related to ideas (rather than expressions or distinctive signs) and include: ideation, exploration, conception, production of intellectual assets and development of IP protection strategy. Considerations regarding the field of distinctive signs are not so closely addressed in this representation of this phase and will be added in further elaborations of the phase.

Ideation

In the ideation sub-phase, key activities are all those taken by actors such as innovators, R&D departments or, by analogy, creators. The objectives of such activities that are relevant to blockchain and distributed ledger technologies (DLTs) during this sub-phase may include, if applicable, depending on the nature of the IP rights concerned, proving the existence and development of the future IP asset and, in some instances, keeping it secret (mostly applicable for industrial property and trade secrets). Since the present account of activities during this sub-phase is a provisional generalization that focuses on blockchain applications and will be differentiated during further elaboration of the sub-phase, it is important to note at this stage that not all activities apply to all IP rights (copyright, industrial property, *sui generis* systems, unfair competition law, etc.) and some activities apply to some IP rights only.

Examples of actions in the ideation sub-phase that may help in a potential future request for IP protection are proof of generation and record keeping, which can help prove the generation date

and existence of the invention. Since innovation is often incremental, version management of both the intellectual assets being generated as well as the resources being developed and utilized for their generation is important to maintain legal certainty for IP at this sub-phase of IP generation.

Examples of actions in the ideation sub-phase that may help in a potential future request for IP protection are proof of generation and record keeping, which can help prove the date and ownership of the invention.

Also, it is common business practice that organizations try to keep IP secrecy during this phase through several actions, for example:

- using confidentiality agreements among the partners involved in the development of the potential intangible asset;
- ensuring employees, researchers and collaborators have in place confidentiality obligations; and
- reviewing public disclosures to ensure confidential information is not revealed.

Table 5. Key activities, actors, and data and resources for ideation in industrial property

Key activities	Key actors	Key data and resources
• Proof of existence of relevant assets • Confidentiality agreements • Record keeping • Version management	• IP generators • R&D department • IP advisors • Strategy department	• Strategic goals • IP strategic goals • R&D policy • Records, lab notes • Related physical assets

[Note: It should be noted that the key activities, actors and resources are quite different between, on the one hand, the industrial property innovation trajectory, upon which this representation of the present sub-phase is modeled and, on the other hand, creative works such as movies, books and songs. These differences are important to note since each individual iteration of a creative work can be protected by copyright in and of its own right. In principle and from a technical point of view, blockchain marketplaces would be conceivable that track the authenticity, for example, of the hundreds of sketches that eventually resulted in a famous painting or sculpture. The same could apply to many script rewrites and storyboards that are part of the ideation process for a movie.]

Exploration

During the Exploration sub-phase, depending on the nature of the IP rights concerned, actors such as IP right holders, innovators and their legal representatives may explore the possibility of IP acquisition and take strategic, tactical and operational decisions based on public and private data sources (such as IP data, non-IP literature, litigation data, corporate data, market reports) that help them better understand a number of elements such as:

- the technology landscape surrounding their innovation;
- the situation of their area of specialization in the market;
- the key players;
- the technology trends;
- the IP scoring, through the analysis of strengths and weaknesses of IP rights and research projects;
- the level of maturity of their idea in the market;
- the preliminary opportunities for IP commercialization;
- the preliminary estimation of IP value and IP risks; and
- the potential acquisition targets.

The understanding created from these data sources about the context, features and potential value of the initial intangible asset(s) will allow the actors to explore and decide whether the further development, research and investment into those assets is merited based on a range of considerations, including their potential future eligibility for IP protection, the potential value of that IP, the possibilities for its effective commercialization or other forms of the exercise of the acquired IP rights. The specific applicable elements among the new intangible assets that will enable the granting of IP rights concerned are also identified in this stage.

Table 6. Key activities, actors, and data and resources for exploration

Key activities	Key actors	Key data and resources
• Identification of elements eligible for IP protection • Understand technology landscape • IP scoring • Preliminary valuation analysis	• IP generators (if applicable) • R&D department • IP advisors • IP investment fund • IP information service & analytics provider	• Intangible asset information from public and private data sources (such as IP data, non-IP literature, new litigation data, corporate data, market reports) • Geographical scope

Conception

If applicable, depending on the nature of IP rights concerned, key activities in the Conception sub-phase are an ongoing watch on technology to quickly identify and analyze new market trends, and freedom-to-operate (FTO), which is a common practice in technology-intensive sectors (mostly for industrial property) to determine if there would be any potential infringement if the IP asset being conceived were commercialized. FTO involves an exhaustive review of sources of information with specialized tools.

Table 7. Key activities, actors, and data and resources for Conception

Key activities	Key actors	Key data and resources
• Technology watch • Freedom-to-operate (FTO)	• IP generators (if applicable) • R&D department • IP advisors • IP information service and analytics provider	• Intangible asset information • Geographical scope • Market reports

If applicable, depending on the type of creative works, research activities or rights clearance activities to ensure the feasibility to use some content that could be copyright protected will be performed. This is common in the audiovisual industry or in the elaboration of some scientific or other articles, books where pictures or data will be needed or in media content, which can include copyright-protected content and it is needed to determine if there would be any potential infringement in the use of IP these assets.

Table 8. Key activities, actors, and data and resources for rights clearance

Key activities	Key actors	Key data and resources
• Diligence searches	• Creative content creators • Producers	• Collections of publicly accessible creative works • Relevant creative works databases

Production of intellectual assets

Creative works production plays an important role in the development of copyright-protected content, including book production, music, visual arts and performing arts (e.g., theatre, dance, etc.). It encompasses the entire production process from the preparation of the written script to the release of copies ready for management.

The Production sub-phase includes all the activities to make the initial idea realized such as performing all the necessary preparatory work by, for instance, looking for funding, contracting actors and other personnel, and obtaining the necessary materials and technical facilities. Where necessary materials may have contractual obligations or other legal encumbrances attached from their transfer, such as may be the case in genetic material for making certain inventions, which needs to be taken into account. After completion of the preliminary work, a company may sign a contract with a film studio, for example, to rent studio space, and the studio constructs the sets and provides all the necessary technical facilities. Due to the focus on blockchain applications, in the present description of this sub-phase, the making of inventions, the production of distinctive signs through investment in the development of goodwill and the production of trade secrets as intellectual assets through the implementation of reasonable steps and measures for the maintenance of their secrecy are not reflected in this generalized account and will be reflected during further elaboration of the sub-phase.

Table 9. Key activities, actors, and data and resources for Production of creative works

Key activities	Key actors	Key data and resources
• Investment and marketing decisions • Fundraising • Hire the services of production studios • Hire performers and other personnel • Acquire materials and technical facilities • Determine potential legal encumbrances pertaining to acquired materials and facilities	• IP generators • IP investment fund • Material providers such as costumes and scenery • Production department	• Collections of publicly accessible creative works or other production inputs • Relevant databases of creative works or other data • Contractual agreements

IP Protection phase

The Protection phase includes all the legal, administrative and technical activities involved in obtaining legal protection for a work in the form of

IP rights, including voluntary ownership registration. These activities are here, preliminarily and in generalized form, grouped into four sub-phases:

- IP rights prosecution;
- ownership registration;
- IP maintenance; and
- IP enforcement.

This is a simplified description of the IP protection phase for the purposes of highlighting potential blockchain and DLT applications, which will be differentiated during further elaboration, especially in two regards. First, the IP protection phase is highly diverse for different IP titles and different branches of IP law diverge widely regarding the structure of this phase (and do not all conform with the sub-phases below). Second, it is important to note that, even if the Protection phase of a particular IP asset does reflect the below phases (e.g., in the case of utility patents and utility models), the activities, which are grouped here into a seemingly singular and unified "sub-phase," do not occur in a single temporal continuity, in direct sequence or consequence of each other and, for many IP assets, some may not occur at all even if others do.

Table 10. Key activities, actors, and data and resources for IP protection strategy

Key activities	Key actors	Key data and resources
• Develop IP protection strategy for potential industrial property rights • Develop protection strategy for potential copyright/related rights • Develop protection strategy for potential *sui generis* rights (e.g., new varieties of plants, databases, TK, etc.)	• IP generators • R&D department • IP department • Applicant • Legal representatives • IP advisors	• Intangible asset information • Legal information • Business information • Classification

IP rights prosecution

Mostly for industrial property, the IP prosecution sub-phase includes all the steps of the IP prosecution process, from the preparation of the application form by the applicant to request the granting of an IP right, until an official final decision is reached on the submitted application.

For other IP rights such as copyright and related rights or trade secrets, these activities do not apply. In the majority of countries, copyright protection is obtained automatically without the need for registration or other formalities. Most countries nonetheless have a system in place to allow for the voluntary registration of works. Such voluntary registration systems can help solve disputes over ownership, creation or authorship, as well as facilitate financial transactions, sales and the assignment and/or transfer of rights. Trademarks in some cases can also receive limited protection automatically without the need for registration based upon their consumer recognition and use in the marketplace.

[Note: It may be relevant to discuss the formation of unregistered trademark rights and the relevant resources, such as evidence of trademark use or consumer recognition. These activities can include additional actors/key actors, such as marketing or sales departments, licensees, distributors or retailers.]

Table 11. Key activities, actors, and data and resources for IP rights prosecution

Key activities	Key actors	Key data and resources
• Drafting IP rights applications • Filing with the IP office • Granting the IP right • Registration of IP rights • Oppositions	• IP generators • Applicants • Legal representatives • IP advisors • IP offices • IP information service and analytics provider	• IP right application data, IP data, non-IP literature, geographical scope, classification and goods and services • IP offices filing and maintenance systems

Ownership registration

Creative work is normally protected by copyright law from the moment of its creation without any formal requirement of registration. However, for the purpose of efficient rights administration, the authorship of any creative work could be voluntarily registered and certified alongside the presence of related rights over the same piece of work. This can help third parties identify the original author and avoid infringements while

at same time will make it easier for the creator to know who is using their works and claim for fair compensation.

In contrast to creative works under copyright, ownership registration in the field of industrial property is entirely different, where multiple and diverging systems of formal registration of ownership titles exist. Blockchain and DLT solutions may be equally relevant for such systems and their description will be supplemented in the further elaboration of the present life cycle description and in the elaboration of the blockchain use cases.

Table 12. Key activities, actors, and data and resources for ownership registration

Key activities	Key actors	Key data and resources
• Create evidence of ownership recording the fundamental elements of the works	• IP generators (creators, phonogram producers, audiovisual producers) • CMOs • Legal representatives • Certifying entities of ownership (banking, solicitors, posts, etc.)	• IP rights registries • All relevant information on the creative work that allows identifying the work, the rights that lay upon it and the legitimate right holders • Creative works, sketches, scores, copies of the original of the works

IP maintenance

Depending on the nature of the IP rights concerned and their applicability, IP maintenance refers to the activities to be performed when the duration of the IP right is limited, including renewal and changes in IP rights as well as fees payment. While certain IP maintenance activities might be simplified by blockchain or DLT solutions, they are legally determined by the procedures and formalities for the maintenance of protection, which must conform with certain minimum standards for the various IP asset classes in the various branches of IP law.

Table 13. Key activities, actors, and data and resources for IP maintenance

Key activities	Key actors	Key data and resources
• Renewal of IP rights • Changes on the IP rights • Fees payment	• IP offices • Legal representatives • IP right holders • IP advisors	• IP offices • Legal representatives • IP right holders • IP advisors

IP enforcement

IP enforcement refers to procedures and remedies aimed at addressing any infringement of an IP right. Key actors are right holders, law enforcement authorities, courts and tribunals, as well as institutions providing alternative dispute resolution services, such as the WIPO Arbitration and Mediation Center.

Table 14. Key activities, actors, and data and resources for IP enforcement

Key activities	Key actors	Key data and resources
• To prevent and/or to stop acts constituting infringements of IP rights • IP monitoring or copyright-protected content monitoring • Report suspected piracy or unauthorized use or distribution of copyright-protected content • Disposal or destruction of infringing items	• IP right holders • Legal representatives • IP enforcement authorities • Anti-counterfeiting and anti-piracy bodies • Judges and courts • IP alternative dispute resolution bodies • IP advisors • IP right holders	• Granted IP rights, relevant technical information on the IP rights and the company • Communication channels between law enforcement authorities and the IP right holders • Information as to the location, nature, origin and quantity of infringing items • Evidence of losses incurred by right holders

IP management phase

The IP Management phase for industrial property includes all those management activities that the IP right holder may take to develop and raise the value of their IP rights portfolio: IP audit, IP portfolio analysis, IP life cycle analysis, competitive technology intelligence and IP landscape analysis. This does not apply to copyright and related rights, where the rights are managed either individually, by the right holder(s) concerned or collectively, via a CMO.

The activities in the first three sub-phases (IP audit, IP portfolio analysis, IP life cycle analysis) are mostly performed internally within the organization. The other two (competitive technology intelligence and IP landscape) are mostly external. It should be noted that the IP Management phase also includes other forms of IP management exercises.

Copyright and related rights are managed either individually, by the right holder(s) concerned, or collectively, via a CMO.

IP audit

An IP audit is a review of the IP portfolio together with the relevant procedures used by the business to obtain and protect their IP. An IP portfolio can be understood as the scope of IP assets that are within an IP asset management system of an enterprise or organization. The purpose of an IP audit is to contribute to better identifying and monitoring the whole intangible asset portfolio, better secure and effectively monetize the IP and set up an effective IP administration structure.

The audit might be carried out by using a combination of different auditing techniques such as:

- online questionnaires;
- follow-up face-to-face interviews with management staff, key employees and users of IP processes;
- analysis of contracts, sales invoices, marketing material, material transfer agreements (MTA), access agreements and other documents with the legal counsel;
- reviews of laboratory notebooks and related research records;
- reviews of computer files;
- reviews of data collections; and
- analysis of relevant documents collected during the preparation phase and identified during the interviews.

The resulting audit report will be a key input for IP portfolio analysis and IP life cycle analysis.

Table 15. Key activities, actors, and data and resources for IP audit

Key activities	Key actors	Key data and resources
• Online questionnaires • Follow-up face-to-face interviews • Documentation analysis • SWOT analysis of IP assets	• IP auditors (usually external) • IP right holders • R&D department • IP advisors • Production department • Market research department	• Intangible asset information from internal corporate documentation • Asset commercialization agreements • Asset access and transfer agreements

IP portfolio analysis

The objective of the portfolio analysis is to gain the level of intelligence on the asset portfolio that enables a targeted execution of the strategy. Where multiple asset portfolios and asset management systems are employed, asset management activities should be coordinated between the portfolios and systems. The information gathered during the audit report helps align specific activities for the development of current or potential IP assets throughout the IP value chain.

The following steps are part of this sub-phase:

- business strategy: understand the markets, customers and technology areas that are important to the future needs of the business;
- inventory of assets: understand what is owned within the existing portfolio;
- categorize assets by stage of life cycle, product line, business unit, technology area and remaining useful life;
- gap analysis: assess whether the portfolio profile supports the business strategy of the company, that is, whether it has enough IP in key technology areas; and
- develop a plan to close gaps through, for example, licensing, innovation or acquisition.

Table 16. Key activities, actors, and data and resources for IP portfolio analysis

Key activities	Key actors	Key data and resources
• Business strategy analysis • Inventory of assets • Asset categorization • Strategic gap analysis • Development of a plan to close gaps	• R&D department • Legal representatives • Production department • IP advisors	Based on audit report, business strategy and IP strategy: • Intangible asset information • Business strategic goals • IP strategic goals

IP life cycle analysis

This life cycle analysis sub-phase focuses on the complete analysis of the status of IP assets within the IP value chain to determine actions that need to take place with the highest priority to increase the overall IP portfolio value. This is performed in alignment with the IP strategy, strengths, weaknesses, opportunities and threats (SWOT) analysis and conclusions of the IP audit. The asset life can be understood as the

period from asset generation or acquisition to asset end-of-life.

Table 17. Key activities, actors, and data and resources for IP life cycle analysis

Key activities	Key actors	Key data and resources
• Analysis of status of each IP asset within the IP value chain resulting in initial asset valuation and identification of risks, dependencies and key actions	• R&D department • Legal representatives • Production department • IP advisors • IP commercialization service	• Intangible asset information from IP audit report

Competitive technology intelligence

The activities in this competitive technology intelligence sub-phase refer to the collection, analysis and application of publicly available information on external activities in technology that could affect a company's business.

A key advantage is the improved quality of strategic and operational decisions by adding the perspective of external conditions and events.

Table 18. Key activities, actors, and data and resources for competitive technology intelligence

Key activities	Key actors	Key data and resources
• Collection, analysis and application of publicly available information on external activities in technology that could affect a company's business	• Market research department • Legal representatives • IP advisors • IP information service and analytics provider	• Intangible asset information • Market trends

IP landscape

The goal of the IP landscape is to identify broader trends to determine pockets of IP for acquisition. Activities include an FTO analysis and patent invalidity searches. Patent landscape reports provide a snapshot of the IP situation of a specific technology, either within a given jurisdiction or region, or globally. They can inform strategic research planning and technology transfer. They can also be used to analyze the validity of IP titles based on data about their legal status.

Table 19. Key activities, actors, and data and resources for IP landscape

Key activities	Key actors	Key data and resources
• FTO analysis • Patent invalidity searches	• Market research department • Legal representatives • IP advisors • IP information service & analytics provider	• Intangible asset information • Market trends

IP commercialization phase

Where applicable, depending on the nature of the IP rights concerned, the Commercialization phase may include all those activities directly involved in generating revenue from the IP rights portfolio: finance and monetization.

The commercialization strategy can be designed and updated as a result of all the activities and documentation generated in the Management phase, such as IP audit reports, market research reports, contracts with third parties, etc. It includes activities performed to raise funds to support the execution of the IP strategy.

In the case of collective management for copyright, the income source stems from the agreements that the relevant collecting society agreed upon with the users. The CMO is then responsible for redistributing royalties to right holders according to the reported usage of the works.

IP finance

IP finance includes various activities such as the valuation of IP, collateralization, securitization and fundraising.

An IP valuation gives the value of an IP portfolio of an organization at a specific point in time. The value of IP assets largely depends on the technology life cycle and monetization potential of the IP. Based on these value estimations, investment and marketing decisions can be taken. The valuation of the IP portfolios of an enterprise or other entity may

also play an important role in the constitution of a comprehensive and adequate information base for decisions on acquisitions and mergers of enterprises. Through IP collateralization and securitization, organizations are able to gain access to financing based on their IP asset portfolio.

Table 20. Key activities, actors, and data and resources for IP finance

Key activities	Key actors	Key data and resources
• IP valuation • Investment and marketing decisions • IP collateralization/ securitization • Fundraising	• Executive management • Finance department • Legal representatives • IP right holders • IP advisors • IP investment fund • IP information service & analytics provider • IP finance	• Market conditions and trends • Intangible asset information • Business strategy objectives • IP strategy objectives • Contract information • Data IP audit report

Collection and distribution of creative works

Specifically in the field of copyright and related rights, once a creative work is completed, it can be made available for consumers and audiences through the collection and distribution of the content. This is the process that makes the creative work go from private to public and then people can access it from any distribution platform (cinemas, TV, video streaming or broadcasting platforms).

There are many actors involved in getting a creative work from creation to accessibility by the public. Producers, authors, record labels, promoters, publicists and distributors all play a role. CMOs acting as legal representatives of the rights owners or the authors or owners themselves, in alignment with the distribution strategy, will agree in relationship with the distributors to make the created content public.

Table 21. Key activities, actors, and data and resources for distribution of creative works

Key activities	Key actors	Key data and resources
• Identify distributors • Create licenses for the commercialization of the rights	• Producers • CMOs • Creators, authors • Creative content distributors	• Distribution strategy • Contractual agreements with distributors • Licenses between CMOs and owners of the rights

IP monetization

Monetization includes all those activities that directly generate revenue for organizations based on their IP portfolio.

Key sources of information on which monetization decisions are based are the documents mentioned in other sub-phases, such as the IP strategy, the IP audit report, market reports, the IP valuation, contracts, etc.

Possible options for the monetization of IP assets are:

- licensing: a license is a contract under which the holder of an IP title (licensor) grants permission for the use of its IP asset to another person (licensee);
- franchising: franchising is a special type of licensing, enabling the replication of the owner's (franchisor) business concept in another location by providing continuous support and training to the recipient (franchisee). Since business concepts include the use of IP allowing the business to be run, franchising has an intrinsic connection with IP based on licensing of IPRs and know-how;
- joint ventures: IP has an important role in the creation of joint ventures, since ventures bring their own intellectual assets. Joint venture agreements set out contributions, responsibilities and obligations;
- spin-offs: these are separate legal entities created by a parent organization to bring its IP assets into the market. It is generally an efficient solution for the parent organizations, for which the further direct development, management and commercialization of their own IP assets may not be the most effective business and IP strategy, or not possible, such as universities and research institutions;
- technology transfer: situations in which universities (or their staff) and industries formalize agreements on research and development. Such relations may imply the transfer of technology developed within universities, consultancies and transfer of know-how or collaborative research projects. It may also include co-development of technology and know-how;
- assignment: assignment is the transfer of ownership of an IP right between two parties. In this case, the assignee becomes the new owner and right holder of the IP right; and

- collection and distribution of Royalties: in the field of copyright and related rights, collection includes all those activities that directly generate revenue to organizations based on the use of creative works. The royalties collected will be distributed among all the owners of the work in alignment with the shares of the rights.

Table 22. Key activities, actors, and data and resources for collection and distribution of royalties

Key activities	Key actors	Key data and resources
• Payment of the royalties	• IP right holders • CMOs • IP utilizers • IP aggregators • IP brokers • Universities	• Contract conditions • NDAs • Type of license • Granted rights • Payment conditions • Warranties • Termination conditions • Material transfer agreements (MTAs)

Appendix: List of KEY ACTORS

Key actors	Phases key actors are mainly involved in	Description
IP generators (such as creator, innovator, inventor, author, producer, performer, publisher, phonogram producers, audiovisual producers, IP right holder, individual/organization, enterprise, R&D department, laboratory, university)	Generation *[Note: an individual or organization can play the role of many key actors in different phases. For example, creators of creative content are often "small businesses" and are directly involved in many more of the phases.]*	Individual or organization that contributes to the conception or generation of a creative content.
IP department	Generation, Protection, Management, Commercialization	Area in organizations in charge of legal and/or IP matters.
Executive management/Strategy department	Generation, Management	Area in organizations in charge of advising on organizational strategy.
IP commercialization service	Management, Commercialization	Area in organizations in charge of definition and execution of commercialization strategies. A firm or individual who provides IP commercialization services.
IP advisor	Generation, Protection, Management, Commercialization	External entity providing advisory services to companies on intellectual property matters.
Legal representative	Generation, Protection, Management, Commercialization	Individual or organization appointed by the innovator or IP right holder that has legal personality and that may, acting in its own name, exercise rights and be subject to obligations.

Applicant	Generation, Protection	Individual or the company who files a (voluntary) application for registration of an IP right with the relevant IP office. Depending on the nature of the IP rights concerned and with the exception of copyright and related rights (because in the case of copyright, the Generation phase usually coincides with the Protection phase, as a creative work is usually protected upon generation), the applicant may become the owner of the IP right once it is registered upon the conclusion of the application process.
IP alternative dispute resolution bodies	Protection	Authorized bodies that provide an alternative, effective and less time-consuming way to enforce IPRs and resolve IP-related litigation.
IP offices	Protection	Official national or intergovernmental bodies responsible for advising and assisting on the management of intellectual property rights.
IP right holders	Management, Commercialization	Owner of private legal rights that protect the creation of the human mind: inventions, literary and artistic works, and symbols, names, images and designs used in commerce. They are commonly divided into two categories: industrial property rights (e.g., patents, trademarks, industrial designs, geographical indications) and copyright and related rights (e.g., depending on the copyright or related rights concerned, authors [such as writers, composers, painters and photographers], performers [such as musicians, actors and dancers], publishers, phonogram producers, film producers and other right holders).
IP enforcement authorities	Protection	Police, customs, market inspectors and other administrative and/or judicial authorities that ensure the effective enforcement of intellectual property rights (IPRs).
Judges and courts	Protection	
Anti-counterfeiting and anti-piracy bodies	Protection	
IP auditor	Management	Individual or organization responsible for performing a systematic, thorough and solution-focused review of the intellectual assets owned, used or acquired by the businesses to ascertain their legal status, value, potential IP-related risks and the means for protection and to capitalize on them.
IP utilizer (such as the government, a company, SMEs, ventures, partner companies, franchisor/franchisee)	Commercialization	Individuals or entities, who do not own the IP right, but seek a right to use it or have a right to use it.
IP aggregator	Commercialization	Individuals or entities that negotiate with IP holders on behalf of groups of IP utilizer.
Patent collective	Commercialization	A patent collective can be used by entrepreneurs to pool patents, so that small and medium-sized firms will have better access to critical IP they need to grow in early stages without fear of infringing on a patent. The main aim of this collective is to give businesses the freedom to operate.
IP investment fund	Generation, Commercialization	Help create, build and support IP-based companies with services such as financial capital, strategic and commercial expertise, executive search and development, and corporate finance and capital raising.

IP information service & analytics provider	Generation, Protection, Management, Commercialization	IP expert services using metrics, models and algorithms to deliver analytical approaches using techniques such as natural language processing, network analytics, artificial intelligence and machine learning, and geo-mapping and visualization.
IP conference & training provider	Generation, Protection, Management, Commercialization	Organizations and institutions with areas dedicated to IP knowledge sharing and training for multiple internal and external audiences such as national IP offices and related institutions, IP advisors, judges and legal professionals, universities and research centers, and businesses and SMEs.
IP broker	Commercialization	An IP broker mediates between the buyer and seller of IP and may manage the many steps in the process of creating a deal with regard to the purchase, sale, license or marketing of IP assets.
IP finance	Commercialization	IP finance plays various roles where IP meets money, including securitization and collateral, IP valuation for acquisition and balance sheet purposes, tax and R&D breaks, and product financing.
Production department	Generation, Management, Commercialization	The production department plays various roles in different phases, which include overlooking the part of the business that is responsible for the manufacture of goods, including conversion of raw materials into finished products, assembly of components and packaging, among other activities.
Market research department	Management	The market research department collects information regarding consumers' requirements and preferences.
Collective management organization (CMO)	Protection, Management, Commercialization	CMOs provide appropriate mechanisms for the exercise of copyright and related rights, in cases where the individual exercise by the right holder would be impossible or impractical. Collective management is an important part of a functioning copyright and related rights system, complementing individual licensing of rights, resting on robust substantive rights, exceptions and limitations, and corresponding enforcement measures. In this vein, CMOs can provide a bridge between right holders and users, facilitating both access and remuneration. Function: CMOs provide a mechanism for obtaining permission to use copyright materials, as well as for paying the corresponding fees or remuneration for certain uses of such materials, through an efficient system of collection and distribution of license fees and/or remunerations. Some CMOs provide social, cultural and promotional services. A performing rights organization (PRO) is a subset of a CMO.
Material providers	Generation	An individual or entity who provides materials for creative works such as costumes and scenery.
Certifying entities of asset ownership	Protection, Management, Commercialization	An entity that certifies the asset ownership such as an IP office, bank or solicitor.

Notes

1. Prepared in the context of the WIPO Blockchain White Paper Project, this white paper does not seek to define exhaustively IP ecosystems and their IP value chains. It provides an initial, high-level, generalized approximation of IP ecosystems and value chains through illustrative, generalized descriptions, to serve as a starting point for further elaboration in future work. These descriptions focus on aspects of the ecosystems and value chains relevant to blockchain and distributed ledger technologies (DLTs). Further work is needed to develop exhaustive and adequately differentiated descriptions of IP ecosystems and their IP value chains.
2. Convention Establishing the World Intellectual Property Organization, Article 2(viii).
3. "Intellectual property shall include rights relating to:
   - literary, artistic and scientific works,
   - performances of performing artists, phonograms and broadcasts,
   - inventions in all fields of human endeavor,
   - scientific discoveries,
   - industrial designs; trademarks, service marks and commercial names and designations,
   - protection against unfair competition,

   and all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields." See WIPO (2004). *Intellectual Property Handbook*, p. 15. Geneva: World Intellectual Property Organization.
4. See preambular paragraph 5, Article 23.4, 27.3(b) and 65.3, TRIPS Agreement; Article 18(1), Paris Convention for the Protection of Industrial Property (1979); Article 27(1), Berne Convention for the Protection of Literary and Artistic Works; and other relevant international IP agreements as well as numerous national and regional IP legislative frameworks.
5. The IP environment includes laws, agreements, practices, economy, culture, traditions, moral and economic rights, and the rights of the public in access to those creations.
6. ISO 55000 *Asset Management*, Note 2 to Article 3.2.1.
7. ISO 55000 *Asset Management*, Article 3.2.1. The opposite of "intangible assets" are physical assets. Physical assets usually refer to equipment, inventory and properties owned by the organization. In some cases intangible and tangible assets may be very closely related, for example, in characterization data of properties in natural resources.
8. ISO 55000 *Asset Management*, Note 1 to Article 3.2.1.
9. The value chain described in this document is intended to embrace all intellectual property types at a high level, noting that definitions and categorizations could be various, for example, a value chain model for copyright and related rights could be described in different ways, for example, 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 as coinciding with the Management phase from the copyright perspective. In the proposed definition, the production is defined in the Generation phase and distribution and consumption are under the Commercialization phase.
10. See, for example, Article 2(5), Berne Convention (1979).

Annex II
Survey report

Introduction

The aim of this survey was to gather industry information to support the writing of a white paper on the use of blockchain in IP ecosystems. This white paper will identify how blockchain technology can contribute to establishing robust, streamlined, cost-effective, inclusive and transparent IP processes in the era of digital transformation.

The present survey was conducted from July 2020 to August 2020. Regarding participation, the number of survey answers totalled 546. After a data cleansing process[1] a total of 434 entries were discarded following the criteria listed below:

- Disqualified: 9
- Test: 4
- Empty, non-contact detail entries: 340
- Duplicated entries from the same user: 28
- Non-relevant partial answers (only those entries where more than 20 out of 63 questions were answered): 53

After this process, the final number of responses was 112, with 82 completed and 30 partially relevant entries.[2]

The survey questions were divided into six blocks: (1) general information; (2) blockchain knowledge within the organization; (3) implementation of blockchain technology; (4) benefits and challenges; (5) specific questions for IP offices and other governmental organisations; and (6) specific questions for the IP industry in relation to their business in the IP value chain. The summary of each question block is explained below. The general statistical explanation and analysis of the survey responses throughout the document are followed by selected, illustrative quotations from respondents, which exemplify the spirit of the responses received.

General information

This section centers on profiling participants and the role they play within the IP ecosystem. As questions 3 and 4 show, the vast majority provide IP legal services (44 percent) and management services (39 percent) focusing on the protection and management aspects of the IP ecosystem.

Blockchain knowledge within the organization

About the level of awareness and knowledge of blockchain technology, out of 112 participants: 50 (45 percent) know little about its main concepts and advantages, 38 (34 percent) have substantial knowledge about the technology and 15 (13 percent) consider themselves blockchain experts.

Among technical experts, when asked about the most valuable blockchain characteristics, the top three answers were:

- the immutability of blockchain data, which remains unchanged, unaltered and indelible;
- blockchain traceability to identify, track and trace transactions and data from the moment they are entered and their use over time; and
- blockchain transparency where users can view recorded transactions depending on the system's openness.

When it comes to technical knowledge, half of the participants were aware that use cases such as identity, notarization, tokenization and time-stamping can be implemented on blockchain, as well as of how smart contracts are built, or they were familiar with the definition or implementation of smart contracts. The other half, however, were aware of the main aspects of the technology and how it works from a technical perspective, but had never used it before.

"We understand the importance of Standards for data interoperability, security and scalability" – Civic Ledger.

Regarding business expertise within the organization, most participants highlighted that they either already have a dedicated team for blockchain initiatives or are considering forming one. However, 30 participants mentioned not having any plans in the foreseeable future to establish a dedicated blockchain group.

"We have a cross-functional working group that evaluates opportunities that impact our organization, stakeholders, and partners within our ecosystem. It promotes interoperability standards and relevant opportunities to stakeholders and partners within our ecosystem" – NBA Professional Sports League.

"The entire company is based on the assumption that public blockchains are an effective way to protect and manage IP assets" – Bernstein Technologies GmbH.

Implementation of blockchain technology

Participants currently implementing blockchain technology or those with the intention of doing so within the next 12 months chose to use blockchain for the reasons given in Figure 5.

"In the context of intellectual property, blockchain and related distributed ledger technology offer obvious possibilities for IP protection and registration as evidence, either at the registry stage or in court. This also promises a cost-effective way to speed up such processes" – Clarke Modet.

While 27 percent of the companies implementing blockchain solutions are currently experimenting and validating the potential of blockchain, 18 companies are implementing wide end-user solutions in cooperation with partners.

The areas where companies plan to use blockchain are shown in Figure 6.

Figure 5. Participants implementing blockchain technology

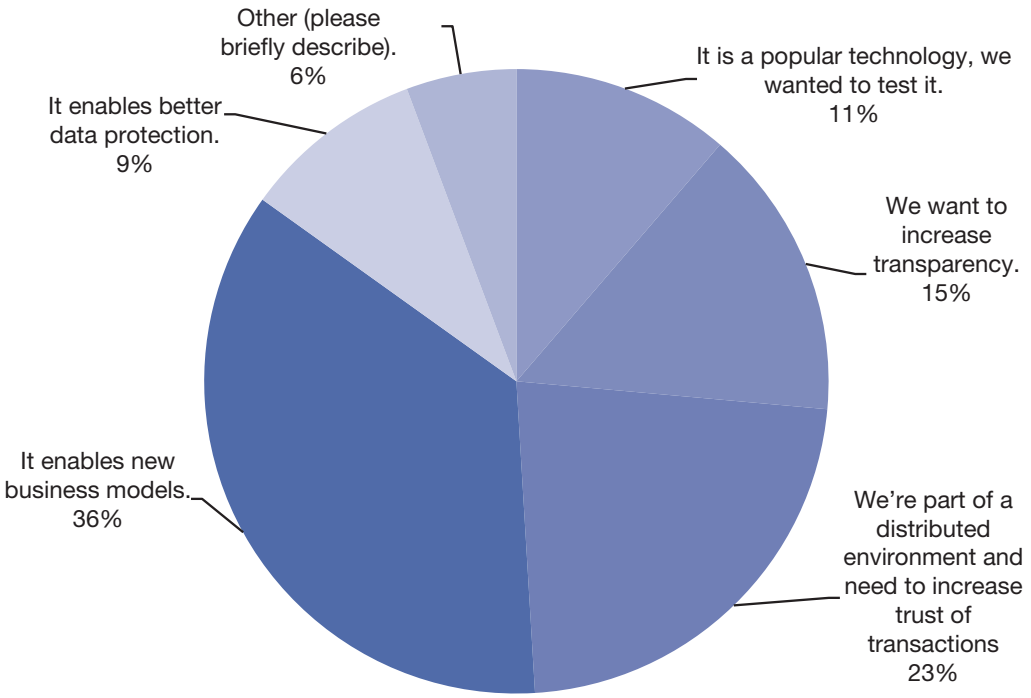


Figure 6. Areas where companies plan to use blockchain technology

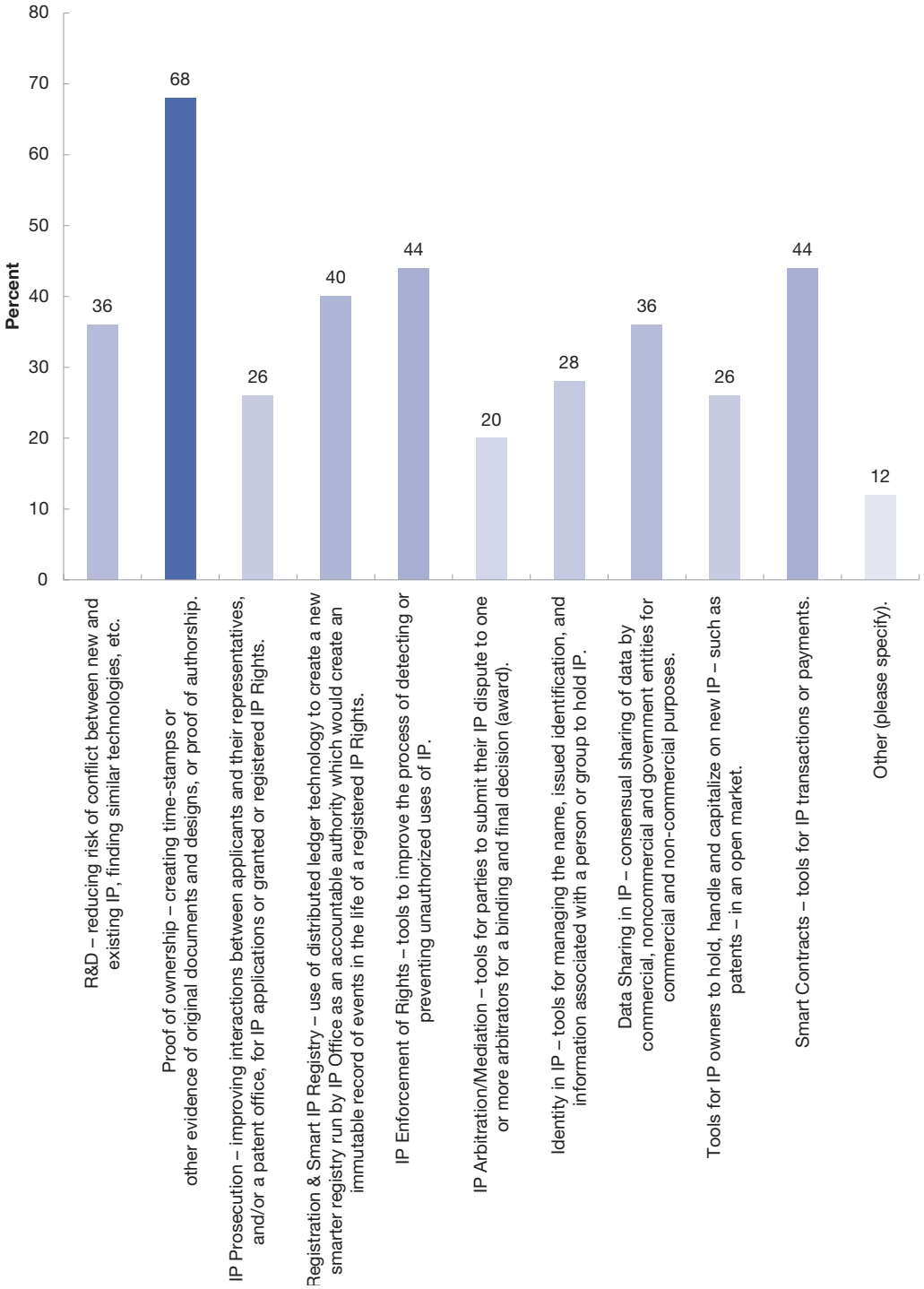
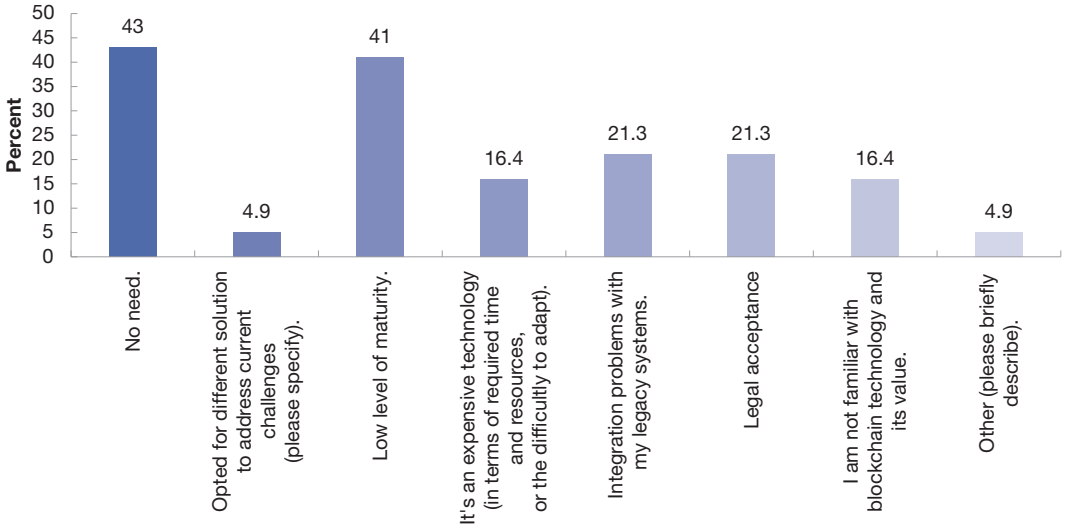


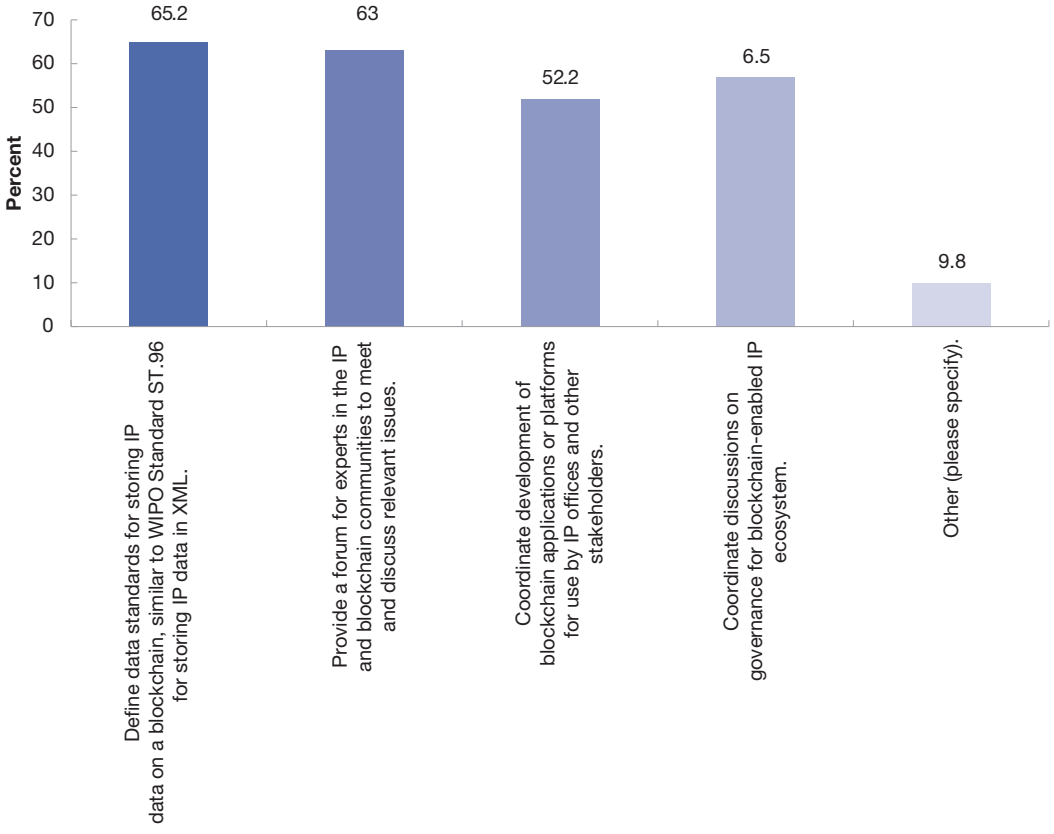
Figure 7. Main reasons for not implementing blockchain technology



Regarding the data governance of the solutions, only 15 percent have a clear model while the majority have not defined any specific governance and are also not considering any scalability criteria to cover other IP rights.

On the other hand, the main reasons for not implementing blockchain solutions are shown in Figure 7.

Figure 8. Suggested actions for a WIPO facilitated blockchain-enabled IP ecosystem



Benefits and challenges

The next set of questions targets the benefits and challenges of adopting blockchain within the IP community. In this line, the most relevant statement about the benefits of using this technology is the ability to increase transparency and traceability by enabling all participants to record their transactions and share this information within the network.

Among the expected challenges for blockchain adoption, the most common is governance and regulatory interoperability (e.g., different legal frameworks, lack of standards, data protection, digital identity and so on), followed by a lack of awareness of blockchain's potential and the immaturity of blockchain products. For these reasons, cloud storage and centralized databases are preferred to blockchain solutions.

"The biggest challenge is that in an increasingly global world where IP rights of parties routinely transcend borders, the lack of a unifying framework or platform (both at tech and policy / treaty level) will make it difficult, if not impossible, to implement solutions effectively and to their full potential" – Ajay Sahni Associates.

An effective solution would be for WIPO to take the following actions to facilitate a blockchain-enabled IP ecosystem:

"Advocate for change at the different IP offices to allow blockchain-based transactions" – Koch Industries, Inc.

"Develop reference models for using blockchain technology in the IP field, including guiding principles, common practice, and use of terminology" – Clarke, Modet & Cia.

Figure 8 shows suggestions for a WIPO facilitated blockchain-enabled IP ecosystem.

IP offices and other governmental authorities' specific questions

In response to the questions targeting the perception of IP offices, 40 percent of respondents replied that blockchain implementation would be useful to provide secured services to the IP industry as well as to create a worldwide trust platform.

Further, they responded that it would also provide an opportunity to create a shared registry and redefine the relationship between IP offices. Moreover, the use of blockchain for anti-counterfeiting and IP Rights enforcement is seen as the most relevant use case for the IP ecosystem.

IP industry specific questions

With regard to the participants working in the IP industry, 54 percent believe that with the adoption of blockchain they will implement a new way of managing and monetizing IP under new governance forms, and new ways of protecting intellectual property.

Creation phase

The biggest challenge in the creation phase is represented by non-registered IP rights, such as copyright and design rights, which should be more formally regulated to allow for greater protection against unauthorized copying.

The most effective use cases for this technology are (1) the implementation of legal smart contracts for confidentiality agreements with partners and testers, and (2) keeping an immutable record of inventions to help prove the date and ownership of the invention.

Protection phase

In the protection phase, the idea of IP offices taking steps toward a unique and global blockchain-based IP registry is perceived as follows:

- 36 percent of respondents think it would be a great improvement for all IP stakeholders, as it would save time, money and reduce complexity.
- 24 percent would be in favor, but do not think it is possible since it is a governance issue, not a technical one.
- 19 percent think that it is maybe not possible for the time being, but the first step could be to create a network to enable information exchange in a more efficient, transparent and secure way across the IP ecosystem.
- 17 percent think that we would first need a unique digital identity model for the IP ecosystem and a trust framework, then we could build global applications.
- 4 percent responded other.

Management phase

The main benefits of using blockchain during this phase are expected to be, firstly, a single IP registry blockchain that can simplify IP audits and due diligence, and, secondly, the creation of trust network hubs that can improve outcomes by facilitating interactions between firms and institutions (30 percent).

Commercialization phase

In the final phase, 22 out of 39 participants from the IP ecosystem believe that blockchain could change the way IP rights are transferred by creating an automatic process from the launch of the offer to the execution of a smart contract, once payment is completed. Moreover, 27 participants think that the adoption of blockchain technologies in the supply chain could increase the efficiency, speed and volume of global trade by limiting the costs associated with international transactions. Finally, 23 participants believe that the adoption of blockchain technologies could lead to increased consumer protection and confidence in digital trade. In line with the above, an automatic system for IP rights transfers, payments and rights of use is the use case participants are most interested in.

Notes

1. Data cleansing: the process to identify incomplete, incorrect, inaccurate or irrelevant parts of the data and then replace, modify or delete dirty or coarse data.
2. Partial answers: the participant did not go through the complete survey.

Annex III
Potential blockchain use cases for IP ecosystems

1. Time-stamping

Topic	Time-stamping
Summary	A digital time-stamp is a proof that a digital file or any type of digital content existed at a particular date and time. The legal validity of a time-stamp is provided by the validity of the digital signature's date. A digital signature is issued and provided by the service provider upon customer request. By creating the time-stamp according to a given activity, the service provider will ensure trust (by means of a blockchain). The client will benefit from the trusted time-stamp once created to prove that a given transaction/activity took place at a given date and time. The digital signature also serves as legal proof in case of a dispute. For instance, this might prove relevant for scenarios involving the transfer or license of an IP right to a third party. The legal validity is proportional to the legal certainty provided by the service signing the time-stamp. Under the eIDAS (Electronic Identification, Authentication and Trust Services) regulation, a qualified time-stamp is the technological instrument that the European Union has adopted to validate that a digital file was created before a certain date and has not been modified since then, thus providing legal certainty within the EU members' jurisdictions and possibly foreign ones integrating similar standards.[1]
Relevant IP value chain phases	Time-stamping might be implemented in every phase of the IP value chain. For instance, it might be relevant for: • digital identity; • proof of evidence for trade secrets; • IP transfers; or • exchange of priority documents.
Business rationale	A digital time-stamp can be used as proof of existence at a certain point in time to protect trade secrets, creative works or know-how, minimizing transaction costs when proving the existence of an IP right (IPR) at a given moment in time. A digital time-stamp provides electronic evidence of the existence of a document that is quick and easy to operate and authenticate, prevents misuse and misappropriation, and in some courts can be used as evidence in case of legal dispute. A time-stamp can provide complementary features to the existing IP system to reduce complexity, costs and time spent during the application process, at the same time strengthening the protection of: • designs, creative works, such as art, music, lyrics, software and textile designs; • trade secrets and know-how, including software algorithms, formulas, recipes, manufacturing processes, client lists, business plans, etc.; and • research, development and related data of pre-patent investigations.

	A blockchain-based digital time-stamping service encrypts the code generated including the IPR data linked to the date and time. Thus, it establishes legal evidence of an IP-related event at a given time. When a digital file is electronically sent to a time-stamp authority, the system instantly generates a unique time-stamp, and the combination of the digital file and its unique time-stamp is then translated into an evidence of existence. The provided data is hashed locally (off-chain) using cryptographic hashing algorithms (one-way mathematical functions), in a similar way to non-blockchain PKI solutions, ensuring that manipulated digital files are easily identifiable and real documents can be verified. The hash proof is then added to a transaction, signed and sent to the blockchain network for validation by consensus. The digital signature is either locally signed by the digital file holder (using, for example, a web browser extension) or signed by a TSA (Timestamp Authority). Once accepted by network consensus, the digital signature will be registered in the immutable blockchain. The exact time at which this is done can vary, depending on the consensus and network selected, between a few seconds and a few minutes (for public networks).
Potential solution	Pure blockchain solutions usually refer to the block number when dealing with time and time ordering since it is guaranteed that all node participants in the network will see the same block number regardless of local time, clock offset or temporal hardware failures. The block number can then be translated to physical local time in an approximate way. For example, in Ethereum, transactions coming from nodes whose internal clocks have an offset greater than 15 minutes will automatically be ignored by the rest of the network. Independence (trust-less) of local node clocks is gained at the cost of losing time precision. The user will receive a transaction receipt confirming the correct time-stamping of their document file (equivalent to the tokens used in PKI-based solutions). Even in cases where the user loses the transaction receipt, it is still possible to check the validity of the time-stamp by examining the blockchain, especially if metadata is added to the transaction along with the time-stamp. All participants granted access to the network will be able to certify and verify digital files using a standard blockchain software (no need to trust non-auditable software controlled by third parties). Further nodes can be deployed in the network for cross-area validation and certification. **Components:** • Wallet: a software/hardware device protecting secrets and signing transactions to be sent to a blockchain. A wallet in practice can be a hardware device in the user's local PC, a web-browser plugin like Metamask, a mobile application, etc. It can also be a hardware security module (HSM) placed in WIPO (for delegated digital signatures).

	• Client app: a client application (web, Android, console, etc.) that is connected to a blockchain network. • Blockchain network: a network of nodes building the blockchain (potentially thousands in public networks).
Blockchain rationale	Current blockchain technologies compare and compete with existing PKI time-stamping solutions. Both use similar hashing and digital signature cryptographic algorithms. From an IP point of view, there are no sensible advantages among the different technologies, considering that the cryptographic approaches behind them will be similar. Some potential differences, advantages and disadvantages of blockchain-based time-stamping from a low-level technical point of view, and how similar features can be achieved with the current PKI, include: • The elimination of trust in hardware clocks by replacing physical time ordering with block time ordering (the high precision of the hardware clock can still be recorded as transaction metadata). If different nodes, potentially distributed across the planet, were used for time-stamping, and they were to be governed by different participants, a Byzantine node trying to falsify the real signature time would be detected promptly, since such a node could manage to falsify its local clock, but not to rearrange the block order. At the same time, time-stamping data synchronization among such nodes would be provided for free. The current PKI can similarly add an absolute time-stamp ordering by cryptographically linking time-stamps to the previous ones forming time-stamp chains. • If a blockchain network is already in place, and users are already in control of their own wallets (signature private keys), support for self-signed user time-stamps would provide extra legal value because parties could present the time-stamp self-signed by its counter-party as legal proof to accept an obligation at a given time. Self-signed time-stamps are technically possible with PKI-based solutions, but they would probably require a much more complex setup on the user side (versus a simple wallet for the blockchain alternative). • The distribution of transactions among nodes automatically adds resilience to the architecture, providing cluster-like protection for free. Also, the Merkle-tree data-at-rest structure used by blockchain platforms will promptly detect any hardware failure that could otherwise destroy the time-stamp probe (a single wrong bit in a multi-terabyte blockchain would be detected). Similar mechanisms can be applied to protect PKI-generated data-at-rest time-stamps, for example, using a ZFS file system. • Using token artifacts could allow in some contexts automated or simplified billing and monetization of the time-stamping service, for example, through the use of APIs, allowing users of the service to pay for tokens in advance, receive token discounts, exchange tokens for other services, etc., reducing costs. This could be useful for big corporations making intensive use of the service.

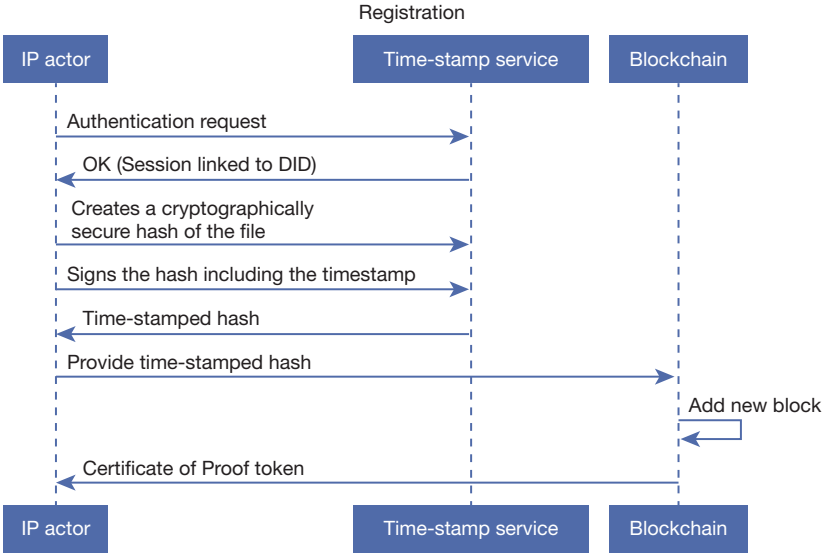
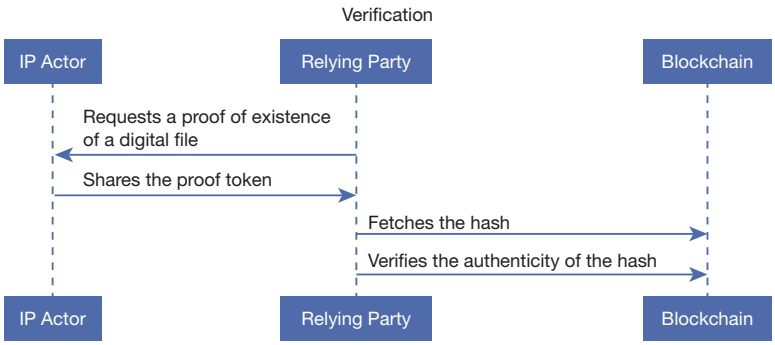
Potential outcome	Building new time-stamping services covering end-to-end business processes and making a profit from the use of smart contracts and the immutability of blockchain technology can provide higher evidence and legal value to all participants involved. To have a proof of possession of a digital file at a specific date, the users can request a time-stamp of the digital file and obtain a proof of existence (token or transaction receipt) and a conflict resolution authority can verify that a provided digital file contains exactly the same data as a registered document at a specific moment in time.
User stories	**Figure 9. Registration**  1. the IP actor authenticates into the time-stamping service; 2. the IP actor creates a cryptographically secure hash of the file in their local laptop or device; 3. the IP actor signs the hash using a local wallet or delegates the digital signature to the time-stamping service, creating a new signed transaction ready to be sent to the blockchain. This signed transaction can also contain any suitable metadata, for example, the time-stamp from a trusted hardware clock at the time of signing; 4. the IP actor forwards the signed transaction to the underlying blockchain (either directly or indirectly through the time-stamp exposed remote API); 5. the blockchain receives the transaction and through the established consensus adds it to a new block. The blockchain block number will serve as non-physical “time” with some extra guarantees over the registered clock time; 6. the transaction receipt is returned, indicating where to locate the time-stamped proof (the “proof token”) on the blockchain; and 7. the IP actor writes down/saves the proof token in a secure place.

Figure 10. Verification



1. a relying party requests proof of the previous existence of a digital file to the IP actor;
2. the IP actor shares the proof token (transaction receipt), the original file and their DID to the requesting relying party;
3. the relying party uses the receipt to fetch the hash in the blockchain; and
4. the relying party (their local application to be more precise) compares the hash calculated locally together with the DID with the one registered in the blockchain. It also verifies the (approximate) time-stamp of the block containing the time-stamp and, optionally, the metadata from a trusted clock source with a more precise local time-stamp.

Actors (or stakeholders) interacting in the use case and their role in the use case:

IP actor	The user that requests a new time-stamp proof for a digital file to the time-stamping service. It also refers to the software that has been installed locally to interact with the software components.
Relying party	User that requests for proof of the digital file and its creation to the IP actor. It also refers to the software that has been installed locally to interact with the software components.

Interactions

Pre-set up	The IP actor must set up a wallet (if a digital signature is not delegated to the time-stamping service) containing their private key. This wallet can be a hardware wallet, a password-protected file or a remote service providing a digital signature.
Connects application	The user authenticates to the time-stamping service establishing a new session.
Hash creation	A unique hash of the file is generated.
Transaction creation	The transaction will consist of the hash, plus any metadata requested by the blockchain protocol, as well as any user metadata considered appropriate (local clock time-stamp).
Registration in the blockchain	A blockchain client registers the signed transaction on the blockchain.
Time-stamping	The blockchain creates a new block with the transaction. The time-stamp of the blockchain block will be the official time-stamp, any local clock metadata will also be considered valid according to the signer's origin of trust.
Proof token	The application generates a proof token with the transaction data.
Upload proof token and file to verify	The relying party uses the proof token (transaction receipt) to fetch the transaction data from the blockchain.

Verification	The relying party's local application compares the locally computed hash with the hash registered on the blockchain. It also checks the time-stamp returned by the block containing the transaction and (optionally) the time-stamp in the transaction metadata. It also checks that the signer was valid at the time of sending the transaction (this requires a parallel registry not described in this document). If all checks pass, the verification is valid.

Key data (general information applicable to other use cases):

Document	The original data to be time-stamped.
Metadata	The metadata related to the documents, to a time-stamp or to the time-stamp process.
Hash	The result of the hash algorithm processing the document.
Transaction	The order to be submitted to the blockchain containing the hash plus the metadata.
Signed transaction	The transaction once it is signed by the IP actor or the delegated service.
Cryptographic parameters	The set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing.
Register's information	The register's information.

Blockchain technical maturity

Optimizing: already exists in the production environment in the market.

Blockchain technical complexity

Low: due to the solutions on the market being highly tested.

Type of blockchain implementation

Blockchain Type	Main Consensus scheme	Pros	Cons
Public permission-less	PoW PoS	Maximum decentralization. 100 percent of trust in mathematical consensus. Anybody can access the solution to create and verify certificates.	Variable and potentially high transaction costs and no real time registration. No control of the infrastructure, dependency on public ecosystems. Undefined legal framework. Eventual transaction finality.
Consortium permissioned	Istanbul Byzantine Fault Tolerance[2] (IBFT)	Lower transaction costs. (Much) better performance with transaction finality.	Higher centralization. Less resilient to Byzantine attacks. Governance and maintenance agreements must be signed.

Legal assessment

The time-stamping solution should ensure alignment with best practices, standards and regulations at all times.

In terms of regulation, it should be compliant with, at least, the regulatory framework for the particular jurisdiction composed of:
- digital identity regulation;
- any certified authority/trust agent regulation; and
- data protection/privacy regulation.

No specific regulation exists at the national or regional level to regulate a blockchain-provided time-stamp, aside from eIDAS. eIDAS is an EU regulation on electronic identification and trust services for electronic transactions in the European Single Market.

	In India, the Information Technology Act 2000 mandates that certifying authorities (CAs) shall provide a time-stamping service for their subscribers. These time-stamps can be verified to establish the time attestation required for references. Like CAs, time-stamping services are also managed by trusted personnel, operated in a secure environment and subjected to audit and compliance. Thereafter, a regulatory assessment should be performed for compliance on a case-by-case basis according to the following levels in a given jurisdiction: • national/country/federal level; and • state/local level (if applicable). Some regulations applicable in other jurisdictions include: • the Pan-Canadian Trust Framework™ (PCTF); • the UK Data Protection Act (DPA 2018); and • the California Consumer Privacy Act (CCPA). In terms of standards and best practices, some examples are: • ETSI Electronic Signature Format standards TS 101 733, along with other ETSI standards; and • ISO/IEC 27002 is an international standard used as a reference for controls when implementing an information security management system, cryptographic control of sensitive data and key management.
Challenges and risks of using blockchain	The main challenges are: (1) the legal consideration of these types of proofs; and (2) the creation of an ecosystem of entities that will use the solution and manage the blockchain in a distributed manner (i.e., scalability and network effects). Another possible challenge is acquiring specific and exact time-stamping, especially if the goal is to compare it with another time-stamping service. The registered date and time are those for the transaction block commit. For this reason, two dates are needed for setting the highest precision on a blockchain time-stamping system: • date and time of the transaction block commit; and • date and time of the signing of the transaction.
References and contact information	Korean Government Time Stamp Authority (GTSA), www.gtsa.go.kr/requestIssueInit.action Kangxin Partners (2020). China: Time Stamp – An Effective Solution For Copyright Protection. *Mondaq*, May 4. www.mondaq.com/china/copyright/926768/time-stamp--an-effective-solution-for-copyright-protection Khipus (n.d.). Khipus, register anything from your mobile. https://khipus.io/en/?lang=true WIPO IP Portal (n.d.). Home. https://wipoproof.wipo.int/wdts/about-wipo-proof.xhtml

2. Digital identity

Topic	Digital identity
Summary	A digital identity is created online using personal identity documents, thus avoiding any physical appointment with a national public office. It can be used to securely access a range of official services. Digital identities can be created for any natural or legal person. Creating digital identities for the actors in the IP ecosystem will enable faster interactions where identification requiring legal certainty is needed. Moreover, in this era of digital transformation, the capacity to comprehend and utilize the power of digital identity is critical for effective business optimization and scalability. However, given the proliferation of solutions, it is necessary to enable a digital identity ecosystem that allows interoperability between different entities and systems, ensuring compliance with current regulations and improving the services and operations of companies. Digital identity using blockchain technology have been implemented in different industries and in various countries. This can be also used in IP ecosystems.
Relevant IP value chain phase	The identification of all the actors is a core component in most operations across IP ecosystems. Therefore, digital identity is a horizontal use case covering multiple applications. Because of this, it can be incorporated in all four phases of the IP ecosystem – Generation, Protection, Management and Commercialization – and is applicable to all IP rights. More than a use case per se, digital identity would be an enabler for IP ecosystem members using blockchain for IP-related business.
Business rationale	One of the long-standing issues in the IP community is whether it is possible to use an identity that is verifiable by participants across systems at national, regional and international levels. Digital identities with legal validity provide multiple benefits: • trust between entities: more secure management and storage of digital identities by providing a unified, interoperable and tamper-proof infrastructure with key benefits to enterprises, users and management systems; • improvement of the efficiency of operations: public and private services benefit from reduced operating costs by reducing the effort and time needed to identify and classify counterparts in each operation, transaction or deal; • reduction of complexity by providing a more seamless and streamlined service experience, removing duplication and making online transactions easier; • standardized procedure of identification, agreed by network consensus (versus central authorities); • private entities control their identity and the information they share in each operation/transaction; and • all the network entities are able to see the claims made against other legal entities (non-GDPR [General Data Protection Regulation] protected).
Potential solution	A digital identity ecosystem consists of different agents with different roles. When forming the ecosystem, a series of needs and concepts must be considered. Every ecosystem requires a trust framework involving all solutions, and setting the standards, regulations and infrastructure for action in each case. • Agents: identity providers, service providers, credentials providers, certifying authorities, users. • Functional elements: identity issuing, authentication, identity custody, sharing credentials, authorization, verification of credentials.

Digital identities have been already used for businesses and individuals in various ways, including in sectors such as banking, e-commerce, healthcare, travel and hospitality, among others in developed countries.

In this trend, developing countries like Nigeria and India have initiated projects to build a digital ID for their citizens. The ongoing digital identity enrollment in Nigeria is expected to issue digital ID numbers to about 150 million Nigerians by 2023 as the NIN (National Identity Number) will soon be made mandatory for accessing government services and interventions. India has one of the world's largest biometric ID systems called Aadhar, which is a 12-digit unique identity number. The Aadhar system provides a single source of online identity verification for over 1.2 billion residents across the country. The unique ID ascribed to Indian citizens through Aadhar is used to provide multiple services including access to mobile SIM cards, bank accounts, old age pension and a large number of public welfare schemes.

The above examples indicate a paradigm shift in countries across various developmental stages, towards recognizing digital identity as a vital route to inclusive growth, providing demonstrable economic value to individuals and entities, in addition to significant non-economic benefits.

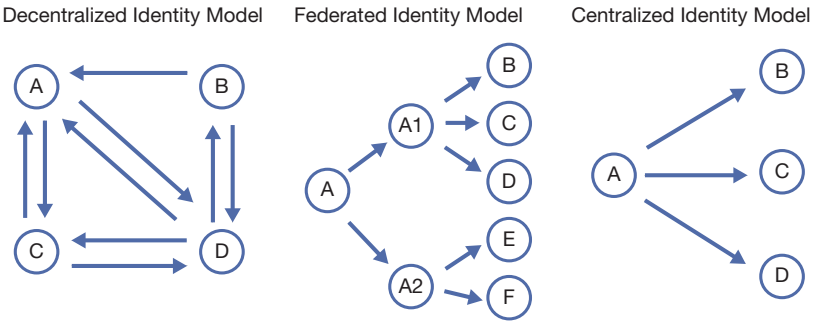
Below are the examples of different models through which digital identity can be managed. This diagram shows a simplified representation of the decentralized vs federated vs centralized identity models.

In the conventional centralized identity model, an entity represented by Node A manages the identity of all participants in its private database. Arrows represent a row in the internal database of Node A. There is an information asymmetry between the central authority and the rest of the network, which can be used to provide unfair competitive advantage.

A step forward in decentralization is the federated model, where centralized governance is split into a tree of delegated governance subsets and the central authority allows authorized actors to manage the identity of a subset of participants. This is the most common scenario in today's enterprise identity system. It is still far from a decentralized system and very close to the centralized model in terms of information control. Central and delegated nodes continue to be the only source of trust. No other actor is allowed to provide identity information about "peers."

In the decentralized version all nodes share the same information. Arrows represent claims that one node makes over another. To protect privacy, for nodes representing private entities, the arrows will not contain the claimed information itself, but only a pointer linked to a verifiable credential. Nodes will emit verifiable credentials against other nodes, share such credentials privately with the node and register a "pointer" in the blockchain. For public non-GDPR protected entities, the claims can be stored in the public blockchain. For example, Node B could be a hospital rating the quality of medical material (face masks) provided by Node A, a provider in China. All hospitals can see the information before deciding to place an order with Node A. Node A cannot remove the claim made by Node B.

Figure 11. Potential solutions



It is also important to highlight that in centralized and federated models, an identity is described by a set of key-value attributes describing it (roles, data and metadata), plus a coordinate (email, login, public key, etc.) to uniquely identify the key-value set. The arrows in the centralized and federated models in Figure 11 represent just a path or coordinate to identify or reach the identity, while the nodes contain the real identity data.

In the decentralized model, an identity is also uniquely identified by a coordinate (a public key in practice), but the real identity data is described by the claims toward such a coordinate. The pointing arrows represent the claims, while the nodes represent the coordinates. A node can also contain a set of key-value attributes describing it, but in this case it is just considered extra metadata about the identity. Claims, done by peer identity nodes, represent the real identity.

Blockchain rationale

Self Sovereign Identity
A blockchain protection mechanism provides a tamper-proof and (Byzantine) fault tolerant system of distributed identity based on public/private cryptography. Such mechanisms can be reused to protect current identity issues (identity data provenance, fraudulent identities and centralized control).

Furthermore, blockchain technologies can be key enablers for secure cross-border electronic transactions of value (IP and others); allow actors to manage their identity autonomously, securely, reliably; and offer a further possibility for actors and citizens to manage data flows and usage based on individual free choice and self-determination with no asymmetric player.

Decentralized Identity
Implementing a generic decentralized identity capability allows entities to create and control their own DIDs across borders without relying on central authorities and without information asymmetries. DIDs could be a potential model for addressing the long-standing issue of applicant name standardization in IP ecosystems.

Verifiable Credentials
Generating verifiable credentials consists of a documented statement containing claims about a legal entity. In the case of IP ecosystem, verifiable credentials can contain claims about identity, patents, trademarks or creative content, among others.

	Blockchain-based DIDs have been already implemented in different industries and countries, or are under consideration. Some examples are explained below. With the eIDAS regulation, Europe has recently brought into existence a powerful framework for digital identity and trust services setting the standards and criteria for simple electronic signature, advanced electronic signature, qualified electronic signature, qualified certificates and online trust services. The regulation also applies to electronic transactions and their management, ensuring functional cross-border trust.[3] In the same vein, the European Blockchain Services Infrastructure (EBSI) is a joint initiative from the European Commission and the European Blockchain Partnership (EBP) created to deliver EU-wide cross-border public services using blockchain technology. The EBSI will be materialized as a network of distributed nodes across Europe (the blockchain), leveraging an increasing number of applications focused on specific use cases. In 2020, a prototype application on the EBSI blockchain has been delivered and EBSI has become a Connecting Europe Facility (CEF) Building Block, providing reusable software, specifications and services to support adoption by EU institutions and European public administrations. Technical work has been developed to integrate EBSI with eIDAS-compatible signature services. Estonia has been a leader in transforming government services into adaptable e-solutions for its citizens and residents, using digital identity, which are also compliant to eIDAS regulations. Every Estonian citizen, regardless of their location, has a state-issued digital identity, which can been used for services such as e-banking, digital signatures, traveling (within the European Union), national health insurance card and i-voting. Exemplifying the role of digital identity in the ownership registration sub-phase of the Protection stage of the IP value chain, the Electronic ID card can also be used for e-services provided by the Estonian Patent Office to file new applications for registration of a patent or a utility model. The documents related to the application, its processing and registrations can be filed via email provided that the document has been digitally signed by the applicant as a proof of their unique digital identity.[4] In order to fortify their DID solutions from cyberattacks, the Estonian Government developed scalable blockchain technology solutions to promote data compliance for government repositories and to prevent insider threats. The Keyless Signatures Infrastructure (KSI), a globally distributed system with server-supported digital signature and time-stamping, is a Blockchain technology developed in Estonia that has been deployed in the Estonian Government networks and is also utilized around the world to ensure that networks, systems and data are secure while maintaining complete data privacy.[5] This KSI technology has also been used to create VaccineGuard – a distributed data exchange platform for vaccination campaign management during COVID-19 that provides early counterfeit and diversion warnings for manufacturers; authentic vaccine and supply guarantee for governments; and transparent access to authentic vaccines along with smart vaccination certificates for citizens. This Blockchain use case demonstrates the IP Enforcement sub-phase in the Protection phase of the IP value chain and is currently being piloted by the Government of Estonia in collaboration with the World Health Organization.[6]
Potential outcome	Quality improvement of the identity data with new models of identity based on claims. Full transparency for audit and supervision of non-tampered identity data by all involved actors.
User stories	Detailed user stories are available as a mock-up document (Annex IV to the Blockchain white paper).

Blockchain technical maturity

Optimizing: already exists in the production environment. Examples include Hyperleder Indy, Sovrin and Ontology. Up to 75 different solutions are registered in the W3C DID Registry at the time of writing.

Blockchain technical complexity

Low: due to the solutions on the market being highly tested.

Type of blockchain implementation

Blockchain Type	Pros	Cons
Private Permissioned	Lower transaction costs (probably free). (Much) better performance with transaction finality. Higher privacy.	Higher centralization. Not adapted to Byzantine attacks. Decentralized identity will work only if there is mutual confidence and common interests among node members.
Public Permissionless	Byzantine tolerant. Potentially millions of identities. Potentially much higher business value (it is possible to evaluate an unknown identity in another continent by looking at the network graph). Digital identity systems require first a well-defined, controlled and monitored platform not available in public networks, as well as strict governance rules that need to be defined by a central institution. Fully trustless/decentralized architecture.	Not suitable for handling internal clients. Lower privacy. Higher transaction costs (depending on selected technology).
Public Permissioned	All the advantage of public-permissionless. Controlled membership access.	All the disadvantages of public-permissionless.

Legal assessment

The digital identity should be compliant with – at least – one of the following regulatory frameworks for the particular jurisdiction:

- digital identity regulation
- data protection/privacy regulation.

For instance, the following regulation is applicable in the European Union (EU):

- eIDAS (Electronic Identification, Authentication and Trust Services) is an EU regulation on electronic identification and trust services for electronic transactions in the European Single Market. eIDAS is a trust framework created before the blockchain upswing. The European Commission developed a study called *eIDAS Bridge* to reduce the regulatory gap between eIDAS and the Self-Sovereign Identity (SSI) models.
- The General Data Protection Regulation (GDPR) is the regulation on data protection and privacy in the EU and the European Economic Area (EEA). It also addresses the transfer of personal data outside of the EU and EEA areas. Both the network architecture and the SSI data must comply with the GDPR.

Thereafter, a regulatory assessment should be performed for compliance on a case-by-case basis according to the following levels in a given jurisdiction:

- national/country/federal level; and
- state/local level (if applicable).

Some regulations applicable in other jurisdictions include:

- the Pan-Canadian Trust Framework™ (PCTF);
- the UK Data Protection Act (DPA 2018); and
- the California Consumer Privacy Act (CCPA).

Challenges and risks of using blockchain	The main challenges are: (1) the legal validity and characterization of these types of proofs; and (2) the creation of an ecosystem of entities that will use the solution and manage the blockchain in a distributed manner (i.e., scalability and network effects).
References and contact information	Framework and regulation: • EBSI (n.d.). CEF Digital. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI • eIDAS, see EUR-Lex (2014). Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG Examples of existing solutions: • SOVRIN: an open-source project creating a global public utility for self-sovereign identity. https://sovrin.org • Serto: identity management services. https://serto.medium.com

3. IP register

Topic	IP register
Summary	This use case proposes the creation of a distributed and common IP register focusing on the simplification of the registration process for the convenience of applicants or legal representatives and the interconnected systems of IP offices for synchronized and secure data exchange between offices. IP registries are currently separated across countries. Therefore, building a distributed ledger rather than traditional centralized databases could effectively turn the IP business into a ledger that incorporates rights without geographic barriers, interconnecting the offices and their data. This solution would create an immutable record of "events" in the life of a registered IP right, globally. It could include the moment when an IP application was filed, registered, first used in trade; when an IP right such as industrial design, trademark or patent was licensed, assigned and so on, covering the entire life cycle of the IP asset. It would also resolve the practicalities of collating, storing and providing such evidence.
Relevant IP value chain phases	The most relevant phase of the IP value chain for this use case is the Protection phase and it is applicable for all of the IP rights. It is also relevant for the IP Management and the IP Commercialization phases.
Business rationale	Given the regulations, IP rights are registered either at the national or regional level (e.g., EU) or have worldwide coverage (WIPO). Nevertheless, they are in many cases represented in a national database and aggregated (using a limited set of attributes) in supranational and international databases such as TMview or DesignView. Current practices require that applicants register the same information in several instances, which are not always interconnected. At the same time, IP offices can exchange documents using FTP tools and services such as WIPO DAS, but there is no commonplace register where they can share information provided by the applicant, and there is no simplification of common processes established. This service is a complement to services already working as WIPO DAS. This use case focuses on the simplification of the registration processes for the applicants and the connection between different offices, by interconnecting the offices with a common tool and improving the information exchange. This use case represents one of the steps for the achievement of the "Once Only" Principle applied to the IP value chain: in a generic way it entails that citizens and businesses provide diverse data only once in contact with public administrations, while public administration bodies take actions to internally share and reuse the data – even across borders – always in respect of data protection regulations, which must be addressed through data governance as explained in the white paper and other constraints. Translated to the IP value chain, it will allow the applicants and legal representatives to provide the data only once, which can be implemented in the form of a blockchain. When the IP right holder decides to ask for protection in several countries, there is limited synchronization between the systems and the data provided in

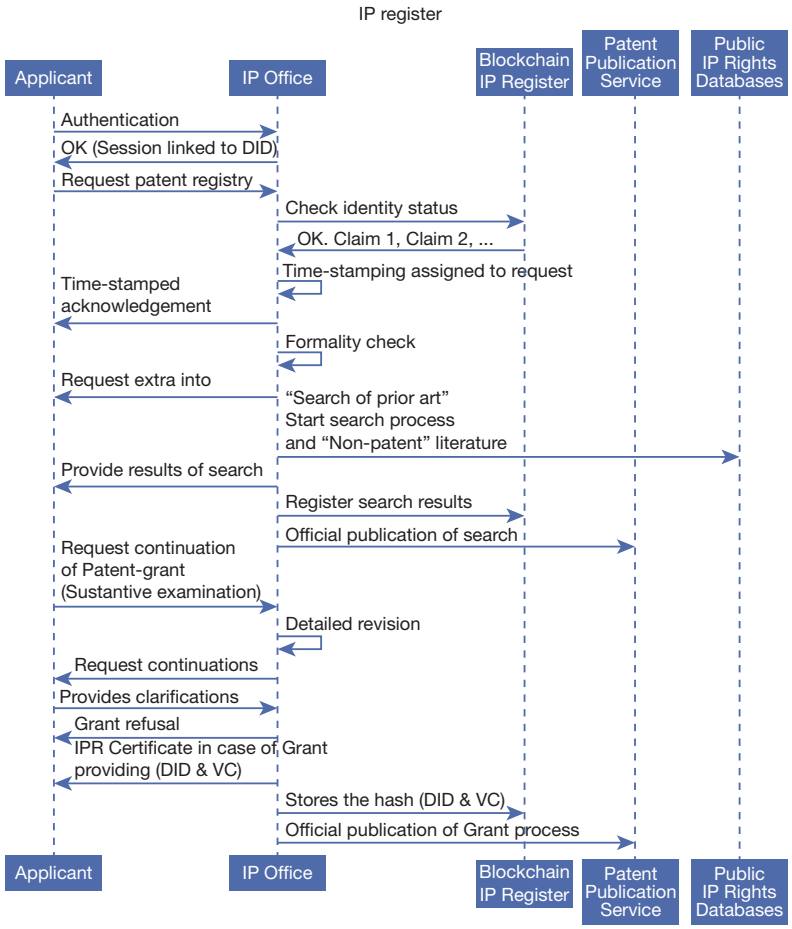
	each register may be different. In addition, the cost for the applicants is high, not only during the application of the IP right but also during its maintenance. This is due to the fact that each process requires that all the documentation is provided as many times as countries are selected, and each of them has its own fee to be paid. A common decentralized IP register should mitigate the reiterative process and enhance the efficiency of the process.
Potential solution	The solution is to create a common register using distributed ledger technology managed by the IP offices – using an agreed consensus model – and to allow the applicants and legal representatives to provide the data only once. This common IP register is the first step to connect offices and to interconnect their data. Such an approach reduces the duplication of data and creates further opportunities for the harmonization of registration practices. Additionally, different services could be created around this solution and the first ones are obvious: exchange data in real time and have an immutable track of data history. It will create an immutable record of IP rights applications on the chain, tracking all the activities performed with each of them during the IP right grant process, stamping each of the transactions performed and using trust data sharing among all the actors involved. A smart contract provides a self-executed agreement between the parties and can be used during the whole IP value chain, from filing an application for an IP right to the commercialization of the right. By replacing centralized registration systems with decentralized ones, it is easier to record the information for registering a new IP right only once and records the complete application grant process including the filing application date, plus the different activities performed during the search and examination processes and their results. This common register contains shared information of IP right attributes between IP offices, so the applicant will provide the information once, and then the different IP offices can share this information in a secure way. This is applicable to the provided documentation as well.
Blockchain rationale	The decentralized nature of blockchain disintermediates central authorities and reduces the amount of trust required among the participants in the registration. The participants' motives are fully aligned with the goals of the register mechanism because the participants are both users and operators of the system. So blockchain, by definition, is a decentralized register. Depending on the on-chain governance model, IP offices could define different smart contracts with their own business rules or, in case of Hyperledger Fabric, for every transaction, smart contracts will be executed by all endorsing peers taking part in the consensus. The advantages of using blockchain-based registries are plentiful. First, records are immutable: once a record is published, no one can remove it. They are publicly available to anyone to search for and consult. You have complete traceability of records. Second, it is totally digital: papers and signature checks are not needed anymore. Transferring ownership of records is as easy as sending an email. There is no central point of failure since all of the infrastructures are decentralized. Third, security: blockchain technology uses cryptographic algorithms, giving a high degree of security to all operations.

	This technology brings the opportunity to make IP registration more efficient, more accurate and faster. This improved registration process is available not only for industrial designs but also for copyright, which could as well be registered recoding a unique block of hash that identifies one creative work as evidence of the creation and link it to its authorship.
Potential outcome	Blockchain-based decentralized IP register among IP offices allowing applicants and legal representatives to record the information only once. It eliminates duplicates and enables the sharing of information between offices. The applicant will receive the following benefits: • record the information only once; • save time thanks to the information shared between offices; and • a simplified registration process among offices; Decentralized information time-stamped valid in case of legal disputes. The office will receive the following benefits: • digital framework for standardized data sharing among offices; • better service to the applicants, a simpler process could increase the number of registrations; • eliminate mistakes and typos in the registration process; and • the first step toward full tracking of the IPR life cycle.
User stories	**IP right application for industrial property** When a user (an applicant or IP legal representative) wants to apply for an IP right, they should be a user, with the role of applicant or representative, in the IP office in which they are going to apply for the IP right. The user will access the e-filing tool, which will provide the details of the requested right. To ensure the confidentiality of the data provided by the user once the data is submitted, it will be automatically encrypted, creating a hash that will be recorded with a time-stamp and used as evidence of the filing date and stored in the blockchain ledger with a unique identifier. At this moment the IP right grant process will start and all the transactions will be stored and linked to this unique identifier on the blockchain. 1. the applicant or IP legal representative authenticates into the receiving e-filing application through any secure mechanism; 2. the applicant or IP legal representative fills in all pertinent data and submits it to the receiving office; 3. the encrypted string containing specific details about the IP right application is recorded in the receiving IP office; 4. the transaction ID is created on the chain; 5. the IP office acknowledges receipt of the application providing time-stamp proof with the application date; 6. the IP office reviews the application and proceeds with any established procedures to check the provided data; 7. data exchange is established between the IP office and the applicant or IP legal representative in case any clarification is needed during the formality check phase; 8. the IP office confirms the correctness of the application by signing it with a corresponding private key and updating the IP register (before recording the transaction and creating the new entry on the register, the consensus mechanism is activated to validate the mentioned transaction);

User stories

9. the IP office proceeds with the search (for patents) and examination process of the application, if needed;
10. the IP office provides the applicant or IP legal representative with the result of the examination process;
11. the IP office registers the result of the examination process in the blockchain;
12. the IP office publishes the result of the examination process;
13. where the IP right is granted, the IP office provides the IP right certificate to the IP right owner as well as the verifiable credential (VC) linked to the DID;
14. the IP office stores the hash in the blockchain including the DID and VC and it is made available for IP offices in the IP register network;
15. where the applicant wants to apply for the same IP right in another IP office, the second filing office can access the priority documents stored in the blockchain; and
16. where the applicant wants to apply for the same IP right in another office, the system will allow the applicant to recover the already shared information in previous registrations.

Figure 12. IP register



Actors (or stakeholders) interacting in the use case and their role in the use case:

IP right holders	Owner of private legal rights that protect the creation of the human mind: inventions, literary and artistic works, symbols, names, images and designs used in commerce. They are commonly divided into two categories: industrial property rights (e.g., patents, trademarks, industrial designs, geographical indications) and copyright and related rights (e.g., rights of the authors/ creators and those of performing artists in their performances, producers of phonograms in their recordings and those of broadcasters in their radio and television programs).
IP offices	Official national or international bodies responsible for the management of intellectual property rights.
Applicant	The individual or company who files an application for registration of an IP right with the relevant IP office. The applicant will become the owner of the IP right once it is registered upon the conclusion of the application process.
IP legal representative	The individual or organization appointed by the innovator that has legal personality and that may, acting in its own name, exercise rights and be subject to obligations.
Receiving IP office	The official national IP office in which the IP right application is filed.
Designated IP office	The official IP office in which the IP right owner is asking for protection.

Activities or interaction or transaction

Pre-set up	The distributed administration of wallets could be supported by IP offices according to an agreed governance model. The participants (IP right holders and IP offices) must set up a wallet (if signature is not delegated to the time-stamping service) containing its private key. This wallet can be a hardware wallet, a file protected by password or a remote service providing a signature.
Connects application	The users authenticate to the IP rights management systems.
Upload information	The IP right holder uploads the information related to the IP right and the IP office uploads the information related to the grant process.
Hash creation	A unique hash of the files is generated.
Fulfill information	The IP right holder fills out the requested information with the data that will be used for the registration of the IP right.
Transaction creation	The transaction will consist of the hash, the required information, plus any metadata requested by the blockchain protocol and any user metadata considered appropriate (local clock time-stamp).
Registration in the blockchain	A blockchain client registers the signed transaction on the blockchain.
Time-stamping	The blockchain creates a new block with the transaction. The time-stamp of the blockchain block will be the official time-stamp, any local clock metadata will also be considered valid according to the origin of trust of the signer.
Proof token	The application generates a proof token with the transaction data for the participant.
Receive the data	The purpose of the wallet will be to support the data related to IP rights. All data exchange notifications will be implemented through traditional means. The other participants receive the notification in their wallets that the new data has been exchanged and they can access it.
Update the information	Both parties can exchange as much information as they need with a new transaction.
Upload proof token and file to verify	The viewers can use the proof token (transaction receipt) to fetch the transaction data from the blockchain.
Verification	The relying party's local application compares the locally computed hash with the hash registered on the blockchain. It also checks the time-stamp returned by the block containing the transaction and (optionally) the time-stamp in the transaction metadata. It also checks that the signer was valid at the time of sending the transaction (this requires a parallel register not described in this document). If all checks pass, the verification is valid.

Key data (general information applicable to other use cases):

Documents	The information provided by the applicant that will be used in the IP right registration process including different formats such as documents, images, XML files, videos, among others. All the information should be managed according to the data governance framework defined. The information part of this IP registration process will include data related to the IP right, which must be treated as confidential, and personal data, which must be handled according to the GDPR.
Metadata	The metadata related to shared information (application number, applicant data, abstract, filing date, etc.).
Hash	The result of the hash algorithm processing the document.
Transaction	The order to be submitted to the blockchain containing the hash plus the metadata.
Signed transaction	The transaction once signed by the participant or the delegated service.
Cryptographic parameters	The set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing.
Participant's information	The data shared between the IP office and the applicant or the IP representative related to the application.

Blockchain technical maturity

Basic: at the time of writing, EUIPO has a system in production – the "IP Register in Blockchain" – powering TM DS View, where a blockchain solution based on Hyperledger Fabric already stores more than 3.5 million IP rights. The solution incorporates nodes for two IPOs, with three more to join by the end of 2021, and 27 by the end of 2025.

Collective management organizations (CMOs) such as Access Copyright or the partnership composed by the American Society for Composers, Authors and Publishers (ASCAP), the Society of Authors, Composers and Publishers of Music (SACEM) and PRS for Music have performed analysis and conceptual definition of potential IP registers based on blockchain.

Regis is a platform for creating distributed registers developed by ConsenSys on the Ethereum platform.

Blockchain technical complexity

High: complex technical development due to the fact that there is no reference of real use cases in the market.

Type of blockchain implementation

Blockchain Type	Pros	Cons
Private Permissioned	Lower transaction costs (probably free). (Much) better performance with transaction finality. Higher privacy.	Higher centralization. Not adapted to Byzantine attacks. Decentralized identity will work only if there is mutual confidence and common interests among node members.
Public Permissionless	Byzantine tolerant. Potentially millions of identities. Potentially much higher business value (it is possible to evaluate an unknown identity in another continent by looking at the network graph). Digital identity systems require first a well-defined, controlled and monitored platform not available in public networks, as well as strict governance rules that need to be defined by a central institution. Fully trustless/decentralized architecture.	Not suitable for handling internal clients. Lower privacy. Higher transaction costs (depending on selected technology).
Public Permissioned	All the advantage of public-permissionless. Controlled membership access.	All the disadvantages of public-permissionless.

Legal assessment	One of the main obstacles for blockchain technology is the lack of adequate regulations and the absence of a proper legal framework with regard to blockchain. This still novel technology has emerged and developed much faster than anticipated and using it for IP registration could create new gray areas in light of existing and inadequate regulations. There are issues regarding the applicable laws and questions of jurisdiction, the interoperability of blockchain solutions and lack of standardization and also the creation of digital identities and parties validating additions to the chain.
Challenges and considerations	Although some jurisdictional courts allow blockchain as evidence such as Estonia, China, Azerbaijan or Italy, among others, its full adoption into law is still far off, and the presence of IP experts is still necessary for legal matters and examinations. With regard to a method to connect registries across the world through a single distributed ledger, this reality is far from simple. Successful management of IP rights using blockchain requires a mutually agreed, internationally supported platform. The problem with this is (and always will be) the issue of aligning multiple national and regional judicial frameworks and traditions. Another challenge is the fact that the creator may have to comply with the formalities of the appropriate authority to hold their full bundle of rights despite the registration of the creation on the blockchain. For example, a patent can only be delivered by the competent authority and the inventor can only claim patent rights if they have a patent. Nonetheless, the registration of the invention on the blockchain will allow the inventor to protect their invention if another person claims to have invented the same work. The inventor will be able to prove that the other's invention is not new (a requirement for patentability). An existing challenge for IP registries, especially when talking about creative works, is how the authenticity of the works' ownership can be verified at the point of entry to the blockchain register, which is already a problem in the traditional registries. Identity of the IP objects and the people involved with an IP register is another clear challenge that has to be addressed. It is crucial for the IP system to ensure that the identity of the different actors involved in a potential IP register is trustable to ensure the authenticity of the ownership of the IP rights. Interoperability between blockchain-based applications is another challenge to be addressed and WIPO standards should contribute to the interoperability. It is suggested to establish an international forum among stakeholders to discuss the regulatory framework, governance and the technical standard for a blockchain-enabled IP register.

References and contact information	COALA (n.d.). How blockchains can support, complement, or supplement intellectual property. www.intgovforum.org/multilingual/index.php?q=filedepot_download/4307/529 European Union Intellectual Property Office (2016). IP in the Digital World Working Group (WG). December. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/meetings/IP_in_the_Digital_World_Working_Group_01-12-2016/IP_in_the_Digital_World_Working_Group_01-12-2016_en.pdf European IPR Helpdesk (n.d.). Your Guide to IP Commercialisation. http://www.iprhelpdesk.eu/landing-page/ip-guides European IPR Helpdesk (n.d.). In a Nutshell: Blockchain and IP. http://iprhelpdesk.eu/ip-highlights/ip-special-blockchain/blockchain-in-a-nutshell Gürkaynakİlay, G., I. Yılmaz, B. Yeşilaltay and B. Bengi (2018). Intellectual Property Law and Practice in the Blockchain Realm. *Computer Law & Security Review*, 34(4) (August), 847–862, doi.org/10.1016/j.clsr.2018.05.027 ISO (2020). ISO/DIS 56005 Innovation management — Tools and methods for intellectual property management — Guidance. www.iso.org/obp/ui#iso:std:iso:56005:dis:ed-1:v1:en Taylor Wessing (2017). Blockchain technology and IP. March. www.taylorwessing.com/download/article-blockchain-technology-and-ip.html *WIPO Magazine* (2018). Blockchain and IP Law: A Match made in Crypto Heaven? February. www.wipo.int/wipo_magazine/en/2018/01/article_0005.html *WIPO Magazine* (2020). Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights. June. www.wipo.int/wipo_magazine_digital/en/2020/article_0002.html
Remarks	This use case has been frequently mentioned in answers received in the surveys performed during the preparation of the Blockchain White Paper. From these answers the following could be highlighted: • Question, “Categories for which you are using, or plan to use blockchain”: 40 percent of respondents selected: “Registration & Smart IP register – use of distributed ledger technology to create a new smarter register run by an IP Office as an accountable authority which would create an immutable record of events in the life of a registered IP right.” • Question, “As an IP Office, how do you see the usage of blockchain in the future of your business area?”: 40 percent of IP offices selected: “It would be useful to provide secured services to the IP Industry and create a worldwide trust platform.” • Question, “As an IP Office, what is your general perception of the technology and the impact it can have on the IP sector?”: 21 percent of respondents selected: “We see that it is an opportunity to create a shared register and to redefine the relationship between IP offices.”

	• Question, “How do you see the impact of this and other technologies in your internal Office?”: 23 percent of respondents selected: “We don’t see any internal impact, but rather in the relationship with other Offices and with other ecosystems.” • Question, “Some IP offices are making moves towards having a unique and global IP register based on blockchain. What are your thoughts on this idea?”: 24 percent of respondents selected: “It should be their top priority. It would save time, money, and reduce complexity; it would be a great improvement for all IP stakeholders.” • Question, “Which of the following blockchain-related use cases do you think are most relevant for IP Rights protection?”: 56.9 percent of respondents selected: “Unique and global IP register based on blockchain.”

4. Proof of existence

Topic	Proof of existence
Summary	This use case provides proof of existence of intellectual assets at a given time and stores the resulting evidence of that existence on a chain in an immutable, transparent and, if required, confidential manner, while enabling the intellectual assets themselves to be stored and controlled exclusively off-chain by the asset holders on their local system(s). The use case can have at least five vertical applications to fulfill diverse legal functions for various undisclosed and disclosed intellectual asset classes: trade secret protection, prior user rights recognition, technical public disclosure, prior art recognition and public prior use recognition.
Relevant IP value chain phases	This horizontal use case has multiple vertical applications during (a) the Generation, Protection and Management phases of the illustrative, commercialization-oriented IP asset life cycle of Annex I; and (b) during other non-commercialization-oriented intellectual asset life cycles in IP ecosystems.
Business rationale	While proof of existence is a standard technical operation in blockchain, this function takes on specific significance in the context of IP ecosystems because IP assets are immaterial objects of property for which the exact timing and contours of existence are often legally more difficult to establish than the temporal and physical contours of material tangible property. This is especially true for intellectual assets, which are not the object of IP protection with formal registration procedures. Whereas for IP systems with formal registration procedures, such as patents, trademarks, industrial designs and geographical indications, the exact temporal and substantive boundaries of the existence of the intangible object of protection are established with legal certainty by a registration system, the vast majority of intangible objects within innovation ecosystems are intellectual objects that occur without legally established, formal existence by registration systems. They consist of two basic categories: subject matter for which exclusive rights *are* available under certain conditions, but not registered through registration systems, for example, trade secrets, undisclosed information, copyright works, non-original databases, TK, etc.; and intangible assets within innovation ecosystems for which *no* exclusive rights are to be available, such as prior art, generic signs, literary, artistic and scientific works in the public domain. For both of these intellectual asset classes, legally certain evidence of their existence – in particular the temporal and substantive boundaries of its existence – is critical for legal certainty and economic efficiency in the overall IP ecosystems. Proof of existence is equally important for their legally certain transition from the former to the latter category of assets with legal certainty, for example, in the case of trade secrets.

For these reasons, the horizontal proof-of-existence use case of blockchain assumes particular significance for maintaining legal certainty and economic efficiency within modern IP ecosystems. This significance spans a wide spectrum of:

- IP asset life cycles (including, *but not limited to*, the illustrative commercialization-oriented IP asset life cycle described in Annex I to this white paper);
- multiple phases within those life cycles (e.g., the Generation, Protection and Management phases of the illustrative commercialization-oriented life cycle);
- multiple vertical applications within some life cycle phases (e.g., trade secret protection and prior user rights recognition during the Management phase); and
- within those vertical applications adding particular significance and value to some areas of the subject matter because of the preexisting distinctive properties of that subject matter (e.g., data characterizing natural material that has "natural" functions, such as genetic resources [GRs]; or innovation and creativity within "oral traditions" because proof of existence may be used to create immutable, distributed evidence of the existence of unwritten traditional cultural expressions [TCEs] or uncodified traditional knowledge [TK], even if such expressions or prior art are not protected through exclusive rights).

For these reasons, the description of such possible distributed ledger technology (DLT) or blockchain applications are illustrated by examples from WIPO's technical work on such subject matter areas. While the examples are subject matter specific and purely illustrative, the possible vertical applications apply to equivalent subject matter in all fields of technology, including trade secrets in all forms of trade. The vertical applications can be described along the spectrum from strictly undisclosed assets (e.g., trade secrets) to fully disclosed intellectual assets (e.g., non-patent literature prior art). Depending on the *legal effect* that the proof-of-existence function of blockchain fulfills for a given particular intellectual asset in relation to a particular IP system, the vertical applications of the proof-of-existence use case could be described as including at least: trade secret protection, prior user rights recognition, technical public disclosure, prior art recognition and prior public use recognition. Implementation of horizontal proof-of-existence functions of blockchain could increase legal certainty in all these vertical applications.

For simplicity and clarity, these multiple vertical applications of the proof-of-existence use case are listed in the following table along the undisclosed-disclosed spectrum with a description of the availability of the asset; the act of the intellectual asset holder for which proof-of-existence creates higher legal certainty, illustrative examples from technical discussions in past WIPO activities; and the legal function of proof-of-existence.

Application of proof-of-existence use case	Availability of the intellectual asset	Act by the asset holder for which proof-of-existence creates higher legal certainty	Illustrative examples from WIPO's technical work	Legal function of proof-of-existence
Trade secret protection measures	Undisclosed	"reasonable steps" or measures to maintain the secrecy of a trade secret	e.g., know-how, information or data maintained as trade secrets; TK, GR data as trade secret	1. Evidence of "reasonable steps" taken to maintain secrecy; 2. Evidence of material scope of trade secret; 3. Version management of trade secret protected know-how, information or data
Prior user rights recognition		Undisclosed use without full trade secret protection measures	e.g., undisclosed TK or GRs	(1) evidence of prior use; (2) version management of prior use
Technical public disclosure	Disclosure	Act of public disclosure	e.g., GR databases	Time, scope, nature and version of technical disclosure
Prior art recognition	Disclosed	Disclosure of information to the public and making available to patent examiners	e.g., documented/ codified TK	Evidence that information has been available to the public before a given date and might be relevant to a patent claims
Prior public use recognition		Undocumented public use	e.g., undocumented/ uncodified TK	Evidence that knowledge or information has been used in public before a given date

These different applications are briefly described through merely illustrative and non-exhaustive examples:

Trade secret protection: the objective of this use case is to make the protection of trade secrets more efficient and effective. The traditional means of demonstrating and proving the existence of a trade secret by notarizing documents and keeping them secret through "reasonable steps" or measures for long periods of time is a costly process. Moreover, notaries do not accept new formats such as 3D models, combinations of data and software, or large data sets of annotated sequence data. At times, confidentiality may not be fully assured.

Generally, traditional mechanisms are not designed to properly manage new developments of trade secret protection in the digital age. The current systems require that documentation of the trade secret is physically secured over a longer period of time. This makes the process expensive and time-consuming for the right holder.

These issues can have a direct impact on the way trade secret holders are protecting their information and know-how. In many cases, right holders might realize the importance of evidence of their trade secrets only shortly before or in the course of a litigation process.

Prior user rights recognition: where an innovator is interested in a defensive/offensive disclosure strategy, and therefore may decide not to file a patent application or establish trade secret protection, but is concerned that future patent filings by third parties could limit their existing use of an innovation, they may need evidence of their use of an innovation. In such cases, blockchain technology may give them evidence for recognition of their prior user rights.

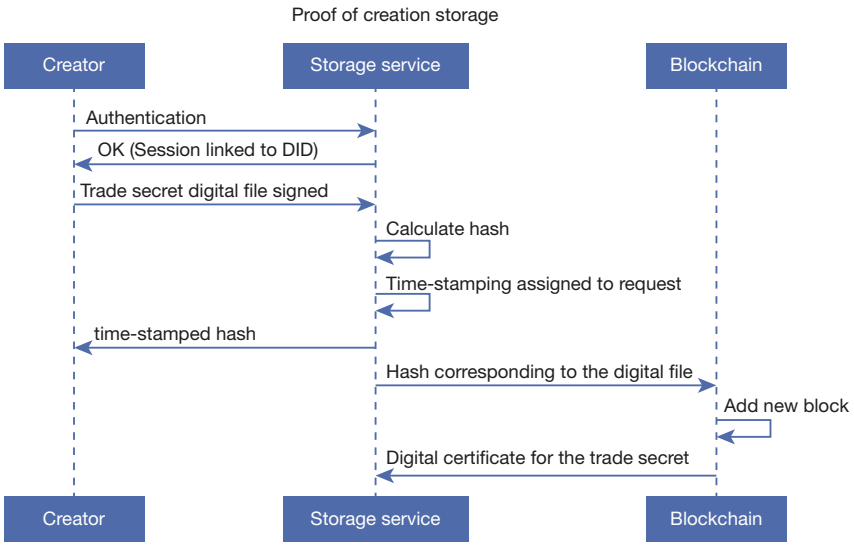
Technical public disclosure: one reason why there are currently disincentives for innovators to disclose certain data sets is that established processes for legally certain technical public disclosure of those data are lacking. For example, when sequence data of GRs at nucleotide or amino acid level are disclosed in public databases, currently, four critical elements of IP information are most often lost:

1. the date of disclosure;
2. the scope of disclosure (i.e., the originally disclosed sequence);
3. the version of the sequence data (sequence data are continuously optimized and annotated); and
4. the nature of disclosure (i.e., data on nucleotide/amino acid sequence vs. natural biological function vs. technical use).

The absence of such information in stable and immutable form creates high legal uncertainty, litigation and disincentives for innovators to disclose such data. A solid process for technical public disclosure based on simple proof of existence for a particular data disclosure at a given moment in time might incentivize innovators to disclose such data, enable cooperation, licensing and technology transfer and dissemination. A simple proof-of-existence function could improve legal certainty and incentives for disclosure of such data by actors in the various innovation ecosystems by providing innovators with the four IP-critical information elements above.

Prior art recognition: patent examiners need to be able to discover non-patent literature as prior art even when the originators of certain non-patent prior art literature wish to maintain that literature on their local systems in a distributed manner. This could be enabled through distributed ledger solutions. Additional benefits in the functioning of IP ecosystems with increased legal certainty concerning recognition of prior art could, for example, be achieved concerning disclosed GRs or TK as prior art. Extensive work on this subject has been done by the International Bureau at the request of the WIPO member states. Increased legal certainty in the recognition of GRs or TK as prior art has been proposed and accomplished through establishing conventional off-chain databases. 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. For example, permissioned DLT solutions could allow patent examiners to access GRs and TK placed on-chain by its holders as prior art, while those holders still control and store those data themselves on their local systems.

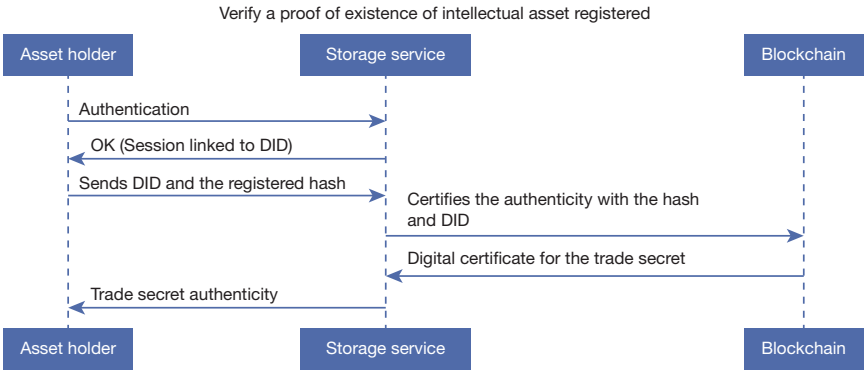
	Prior public use recognition: some types of TK that are transmitted in oral traditions may be disclosed through prior public use, but have never been documented in written form or "fixed" in other recorded forms, due to cultural concerns that their fixation and documentation should be managed by the TK holders themselves. In such case, DLTs might provide additional benefits by making this possible.
Potential solution	The aim of the proof-of-existence use case is to create secure, legally certain, immutable, transparent and, if required, confidential evidence of the existence of a particular intellectual asset at a given time, while retaining sole control and storage of that asset on distributed local systems. The means to an end relies on building a platform that generates a record of a digital fingerprint or hash of the origin of an intellectual asset with the time-stamp being the proof of the existence of the asset at a particular point in time, thus providing evidence of existence and possession of the asset before a court if needed. The legal validity of blockchain technology is already endorsed by different courts in countries such as the United States, the United Kingdom, Japan, Republic of Korea or China. The platform would aim to support all generation processes for evidence of an intellectual asset, generating cost-effective evidence that provides clear and undisputed traceability to support any legal action.
Blockchain rationale	Using blockchain technology to provide proof of existence of intellectual assets has: • lowered costs for trade secret holders when collecting evidence of their secrets, for which other companies usually resort to traditional methods, such as registering before a notary; • strengthened information security for undisclosed information. It allows registration of the evidence without the information leaving the company, institution or community at any time since the only element that travels through blockchain networks is a hash that guarantees its registration on chain. Thus, it is not necessary to make the information available to third parties at any time; • allowed right holders to obtain legally certain evidence of the existence at a particular time of information that has been made available to the public as prior art through published documentation or public prior use; • allowed for legally certain technical public disclosure of information, including the time, scope, nature and information version of the disclosure; • provided fast and immediate registration. Uploading a document to the platform and proceeding to register the evidence takes no more than a few minutes and is done in real time; • offered all legal guarantees. Blockchain technology, in addition to proving the existence of the information on a certain date, ensures that it has not been subsequently modified, and evidences its traceability and authenticity. Compared to the traditional notarization measures, the blockchain technology could drastically reduce time consumption and costs for companies or any other body owning a trade secret, by providing a simple and inexpensive registry of proof of existence, though it may not enjoy the same status as a traditional notarized record depending on the jurisdiction. The idea is that when the holder of an intellectual asset wishes, they can register it into the blockchain, creating a transparent and immutable hash with a time-stamp as evidence of existence. The information recorded will be verified by consensus between the members of the network and registered

	in the ledger. This process will be repeated with any new artifact that could be created in relation to the same asset, ensuring that the data will remain unaltered, and in the case of alteration of the stored data, it will be considered that it is not trustworthy. With regard to data protection, confidential data will be mathematically translated into the hash, avoiding making it publicly available to the network. In practice, this means that the holding company, institution or community will be the only one in possession of an encryption key that can connect the hash code to the information that is stored behind it.
Potential outcome	To build a blockchain registry platform to store proof-of-existence information of certain intellectual assets, which would consist of a chain of – if required, confidential – information, whereby only the hash and time-stamp would be public in the registry in which the holders of the assets can register the existence of an asset into a ledger. Every single step of the process is registered in a specific block in the blockchain, providing an individual hash and time-stamp for each block in the ledger. With a step-by-step registration process stored on a ledger, it is possible for the unregistered asset to establish an immutable, transnational-oriented evidence of existence for the whole life cycle of that asset. The proof-of-existence use case is here illustrated in a generalized manner.
User stories	An asset holder can register the existence of an intellectual asset at a particular time: 1. the asset holder authenticates into the evidence storage service; 2. the asset holder (optionally) signs the digital file; 3. the storage service automatically calculates the hash corresponding to the file stored locally or in a trusted system, for example, Cloud, by the asset holder; 4. the hash is transmitted and stored to the blockchain nodes; 5. once the transaction is correctly endorsed, a digital certificate is generated; and 6. the asset holder has at their disposal a document manager and a hash control for their internal organization. **Figure 13. Proof of existence of intellectual asset registration** 

A user can verify the existence of an intellectual asset registered in the blockchain:

1. the user authenticates into the evidence storage service;
2. the user sends the document registered previously and the DID for verifying the authenticity;
3. the verification storage service provides an answer to authenticity;
4. the user can verify the trade secret already registered; and
5. the user can verify the existence of the intellectual asset if it has already been registered.

Figure 14. Verify a proof of existence of intellectual asset registered



Actors (or stakeholders) interacting in the use case and their role in the use case:

User	Role
Intellectual asset holder	Can hash as many files as they consider appropriate, if they have enough blocks of files contracted. Will only have access to the hashes and certificates they have generated directly.
Storage Service	Service responsible of the storage of the management of proof of existence of intellectual assets.

Interactions (general information applicable to other use cases):

Pre-set up	The registrar must set up a wallet (if the signature is not delegated to the time-stamping service) containing its private key. This wallet can be a hardware wallet, a file protected by password or a remote service providing signature.
Connects application	The user authenticates in the time-stamping service establishing a new session.
Hash creation	A unique hash of the file is generated.
Transaction creation	The transaction will consist on the hash and also any metadata requested by the blockchain protocol, and user metadata considered appropriate (local clock time-stamp).
Registration in the blockchain	A blockchain client registers the signed transaction on the blockchain.
Time-stamping	The blockchain creates a new block with the transaction. The time-stamp of the blockchain block will be the official time-stamp, any local clock metadata will also be considered valid according to the origin of trust of the signer.
Upload proof token and file to verify	The relying party uses the proof token (transaction receipt) to fetch the transaction data from the blockchain.

Verification	The relying party's local application compares the locally computed hash with the hash registered in the blockchain. It also checks the time-stamp returned by the block containing the transaction and (optionally) the time-stamp in the transaction metadata. It also checks that the signer was valid at the time of sending the transaction (this requires a parallel registry not described in this document). If all checks pass, the verification is valid.

Key data (general information applicable to other use cases):

Document	The original data including the description of the intellectual asset for which proof of existence is to be provided.
Metadata	The metadata related to the document(s), to a time-stamp or to the time-stamp process.
Hash	The result of the hash algorithm processing of the document.
Transaction	The order to be submitted to the blockchain containing the hash plus the metadata.
Signed transaction	The transaction once signed by the registrar or the delegated service.
Cryptographic parameters	The set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing.
Register's information	The register's information.

Blockchain technical maturity	Optimizing: already exists in the production environment.
Blockchain technical complexity	Low: due to the solutions on the market being highly tested.

Type of blockchain implementation

Blockchain type	Pros	Cons
Public permissionless (PoW, PoS)	Fully trustless/ decentralized architecture.	Only proof-of-existence use cases
Consortium permissioned (IBFT)	Improved privacy. Allows to manage documentation in parallel to proofs.	Requires the deployment and maintenance of a custom infrastructure. To avoid governance issues, governance rules should be clearly agreed upon between all network participants.

Legal assessment	A main issue that is of essential interest for further analysis is related to how traditional courts will accommodate blockchain evidence.
Challenges and risks of using blockchain	An online platform can never be guaranteed as 100 percent secure, and the more complex the software, the more vulnerable. The network provider bears a great deal of responsibility to establish trust with the users and maintain and update security measures.
References and contact information	Trade Secret Protection Center, www.tradesecret.or.kr/kipi/web/serviceIntro.do?gb=411 ClarkeModet (n.d.). https://sred.clarkemodet.com Dyrhovden, S. (2019). *Blockchain and Trade Secrets: A Match Made in Heaven?* King's College London. https://static1.squarespace.com/static/5bb3ced9b9144976a1d4cb49/t/5de67fbecd1f1d1da57d7829/1575387075162/Blockchain+and+Trade+Secrets+A+Match+Made+in+Heaven.pdf

5. Evidence of generation

Topic	Evidence of generation
Summary	Due to the fact that blockchain enables trustable and time-stamped transactions verified by consensus among participants in the network, the authors could make use of this technology to evidence the generation of its unregistered IP rights. Uploading the creative content and the details of its authorship to a blockchain would allow the registration of a time-stamped record and trustable proof of generation. The owners can use this to commercialize, monetize and safeguard it from potential misappropriation and infringement. Blockchain makes it possible to store each creative work with a unique cryptographic identity, ensuring its immutability and the ability to audit all transactions made between authors and customers.
Relevant IP value chain phase	This use case is a vertical use case also related to time-stamping, focused on the generation phase.
Business rationale	As defined in the Berne Convention, copyright exists from the moment a creative work is created without the necessity of registration, coming automatically into existence upon generation of an original work. It is highly recommended that authors acquire certificates of ownership for their creative works as these might prove beneficial. Proof of ownership might become a challenge in infringement proceedings if the copyright-protected work is not duly registered or if there is no copyright notice on the work. Currently, in some countries, for the creative work to be copyright protected, it has to be created and fixed in a tangible form. The holders may use the services of collective management organizations or any other intermediaries to manage their rights and licensing, and the commercialization and monetization of the rights. In some cases, evidence of ownership of the work is authenticated by notaries. In all of these cases, there are intermediaries taking profit from these "notarization" services, which has a direct impact on the final revenues of the author. By using blockchain to register the creative works, creators can store their works in a hash that 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 in the blockchain, all of the transactions will also be performed in the blockchain. Furthermore, the author is able to make direct agreements with the final consumers, thus reducing transaction costs. Once the work is recorded on the blockchain, the author is able to prove the existence of the work at a particular point in time through a time-stamped hash and supported by the immutability of the record, in case they are involved in any litigation process.
Potential solution	The proposed solution is to create a system that can allow the following steps: • Digital evidence of generation is hashed locally (off-chain) using cryptographic algorithms (one-way mathematical functions) in a similar method to how it is done for non-blockchain solutions, ensuring that manipulated files are easily identifiable and real documents can be verified.

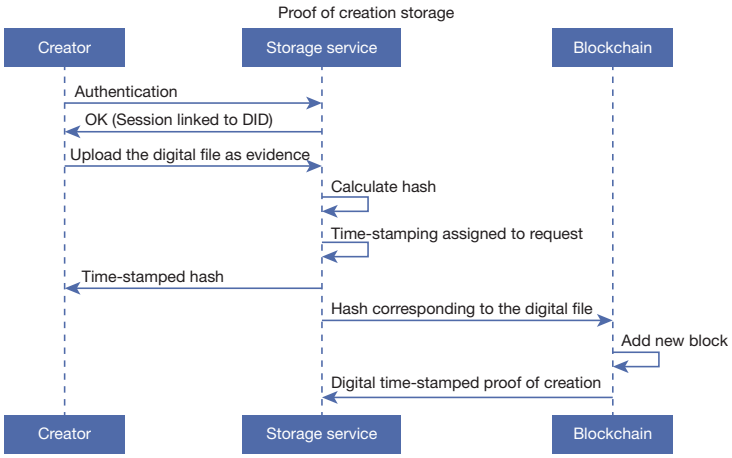
	• The hash proof is then added to a transaction, signed and sent to the blockchain network for validation by consensus. The signature is then locally signed by the digital file owner. • Once accepted by network consensus, the signed digital file is registered on the immutable blockchain. • The user then receives a transaction receipt confirming the correct time-stamping of their document. In the case that the user loses the transaction receipt, it is possible to check the validity of the time-stamp and the digital file authenticity by examining the blockchain. • When needed or required, anyone granted access to the network will be able to certify and verify the digital files using standard blockchain software. • The digital files can be used in legal disputes as evidence of generation (if supported by law).
Blockchain rationale	Blockchain is an excellent solution for sharing basic data on IPR ownership in a decentralized and secure manner. It improves the common issues of: (1) rights not being paid to the rightful owner because of not knowing who they are (publishers, CMOs, digital distributors, etc.); and (2) proof of ownership in a copyright infringement case. Registering a work on blockchain provides a digital certificate of authenticity. This can help third parties identify the author of a work, and IP owners to tackle infringements. Currently, IP owners have difficulties protecting their IP works online (i.e., once an IP work is uploaded to the internet, it becomes difficult to maintain control of the work and to monitor who is using it and for what purpose). Once the author uploads a file on the blockchain, a new record is created in which a time-stamp proof of the existence of the work is permanently linked to the record, and can be easily verified by third parties. The main features that blockchain provides for this use case are: • the immutable nature of blockchain technology allowing for the production of immutable proof of date of generation; and • the time-stamping feature of blockchain, which guarantees that the assertion of generation belongs to a particular date and time. However, it should be noted that blockchain solutions can prove who uploaded what in a distributed ledger, but cannot tell who owns what. The proof of ownership of a creative work should take a verification process via a traditional mechanism, for example, by CMOs or other trusted authorities.
Potential outcome	Blockchain-based platforms allow authors to make a record of their copyright ownership, which can then be used to see where and how the work is being used on the internet and to seek licenses from third parties. Registering a creative work provides a digital certificate of authenticity. This can help third parties identify the author of a work and IP owners to tackle infringements. The application of blockchain technology in the procedural context of the burden of proof might lead to the generation of new types of evidence procedures that combine decentralized technology with a centralized trust structure.

User stories

A creator of a creative work can register the evidence of the generation on the blockchain:

1. the creator authenticates into the evidence storage service;
2. the creator signs the digital evidence;
3. the creator uploads the digital file as evidence of generation;
4. the blockchain receives the transaction and through the established consensus adds it to a new block; and
5. the transaction receipt is returned indicating where to locate the time-stamped proof of generation (the "proof token") on the blockchain.

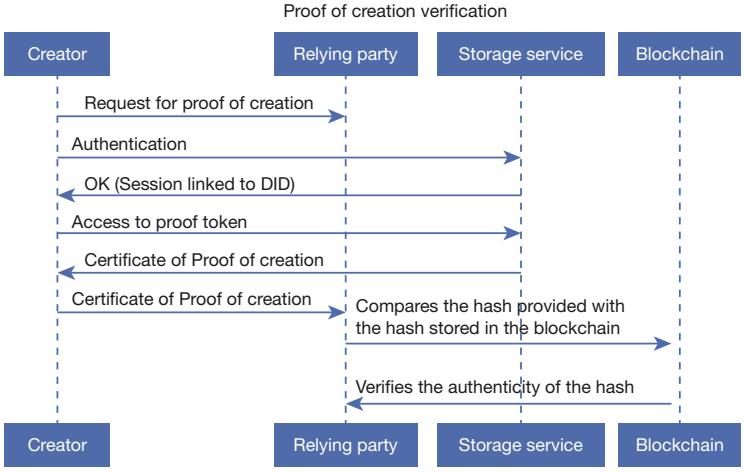
Figure 15. Proof of creation storage



An IP User can verify the evidence registered on the blockchain:

1. a relying party (law court) requests the existence of the proof of generation;
2. the creator shares the proof token (transaction receipt) and the original file requested by relying party/parties;
3. the relying party uses the receipt to fetch the hash in the blockchain; and
4. the relying party (its local application to be more precise) compares the hash calculated locally with the one registered in the blockchain. It also verifies the time-stamp of the block containing the time-stamp and, optionally, the metadata from a trusted clock source with a more precise local time-stamp.

Figure 16. Proof of creation verification



Actors (or stakeholders) interacting in the use case and their role in the use case:

Creator	A user that requests a new time-stamp proof for a document to the time-stamping service.
Relying party	A user that requests from the registrant a proof of the file document and its generation.

Interactions (general information applicable to other use cases):

Pre-set up	The registrant must set up a wallet (if a signature is not delegated to the time-stamping service) containing its private key. This wallet can be a hardware wallet, a file protected by password or a remote service providing a signature.
Connects application	The user authenticates to the time-stamping service establishing a new session.
Hash creation	A unique hash of the file is generated.
Transaction creation	The transaction will consist of the hash, plus any metadata requested by the blockchain protocol, plus any user metadata considered appropriate (local clock time-stamp).
Registration in the blockchain	A blockchain client registers the signed transaction on the blockchain.
Time-stamping	The blockchain creates a new block with the transaction. The time-stamp of the blockchain block will be the official time-stamp, any local clock metadata will also be considered valid according to the origin of trust of the signer.
Proof token	The application generates a proof token with the transaction data.
Upload proof token and file to verify	The relying party uses the proof token (transaction receipt) to fetch the transaction data from the blockchain.
Verification	The relying party's local application compares the locally computed hash with the hash registered on the blockchain. It also checks the time-stamp returned by the block containing the transaction and (optionally) the time-stamp in the transaction metadata. It also checks that the signer was valid at the time of sending the transaction (this requires a parallel registry not described in this document). If all checks pass, the verification is valid.

Key data (general information applicable to other use cases):

Document	The original data describing the creation time-stamped as a proof of generation.
Metadata	The metadata related to the documents proving the generation of the creative work, time-stamped or ready to be sent to the time-stamp process.
Hash	The result of the hash algorithm processing of the digital file as evidence of generation.
Transaction	The order to be submitted to the blockchain containing the hash with the digital file and the additional metadata generated.
Signed transaction	The transaction once it is signed by the creator.
Cryptographic parameters	The set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing.
Register's information	The register's information.

Blockchain technical maturity	Advanced: several proofs of concept are, or a real project is, being developed.
Blockchain technical complexity	Low: due to the solutions on the market being highly tested.

Type of blockchain implementation

Blockchain Type	Pros	Cons
Public Permissionless (PoW, PoS)	Fully trustless/ decentralized architecture	Only proof-of-existence use cases
Consortium Permissioned (IBFT)	Improved privacy Allows to manage documentation in parallel to proofs.	Requires deploying and maintaining custom infrastructure. In order to avoid governance issues, governance rules should be clearly agreed upon between all network participants.

Legal assessment

The main challenge nowadays is based on the reluctance of the judicial system to integrate and accept blockchain applications in specific parts of the judicial process. Moreover, doubts with regard to the technical reliability of blockchain applications might also be present. For instance:

- Chinese courts already set up a judicial blockchain system in 2017. However, the first time that it was confirmed that an electronic data stored on a blockchain could be considered as an electronic evidence was the Internet Court in Hangzhou in 2018.

Challenges and considerations

–

References and contact information

De Beer, J. (2016). Evidence-Based Intellectual Property Policymaking: An Integrated Review of Methods and Conclusions. *Journal of World Intellectual Property*, 19(5–6), 150–177. https://doi.org/10.1111/jwip.12069

Wu, H. and G. Zheng (2020). Electronic evidence in the blockchain era: New rules on authenticity and integrity. *Computer Law & Security Review*, 36, 105401. https://doi.org/10.1016/j.clsr.2020.105401

6. Anti-counterfeiting

Topic	Anti-counterfeiting
Summary	This use case aims to use blockchain 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. It involves producers, transporters and anti-counterfeiting and anti-fraud entities providing a traceable method to prove the source of origin, producer and other characteristics to prevent counterfeiting in a more transparent and automatic way throughout the value chain. The system allows, first, certification that the route followed by the products and the actors involved in the delivery is the same that the right holder declared – to those with an interest – of the goods, before the delivery process started. From the other side, in case enforcement authorities identify any change on the information provided by the right holder, a verification process may be initiated with the right holder before the goods arrive at the final destination. Last but not least, the final consumer will be able to check if the acquired product follows the process defined by the right holder and if it is certified/ undersigned by all the stakeholders involved.
Relevant IP value chain phases	This is a horizontal use case, and it is relevant for both industrial property and copyright. It focuses on the Protection and Commercialization phases.
Business rationale	Industry is impacted by counterfeited goods on a worldwide scale. The impact is not only economic, but it affects the consumer directly by receiving poor-quality goods at an excessive price and sometimes by exposing them to health and safety dangers. Counterfeiting is not new, many companies are trying to fight against it. Different strategies and technologies are being used, from periodically changing their transport routes and the location of their factories, to including holograms, smart tags and biometric markers in the products. Not only IP right holders but also enforcement authorities in borders and internal market areas are increasingly focusing on fighting against counterfeiting. Dedicated units for anti-counterfeiting matters have been created. Also, technical platforms are used by customs and the police to provide as much information as possible to the enforcers to make it easier for them to seize fake products. Besides the traditional business models, online marketplaces are facilitating easy access to counterfeited products. Through these marketplaces counterfeiters can sell their products without direct contact with the final customer, who often is unaware that they are acquiring counterfeited goods. If we look at the report published by the European Union Intellectual Property Office on the EU enforcement of intellectual property rights, between 2013 and 2017 the EU detained approximately 438 million items with an estimated market value of EUR 12 billion; 40 percent of seizures were made on borders and 60 percent in the internal market.

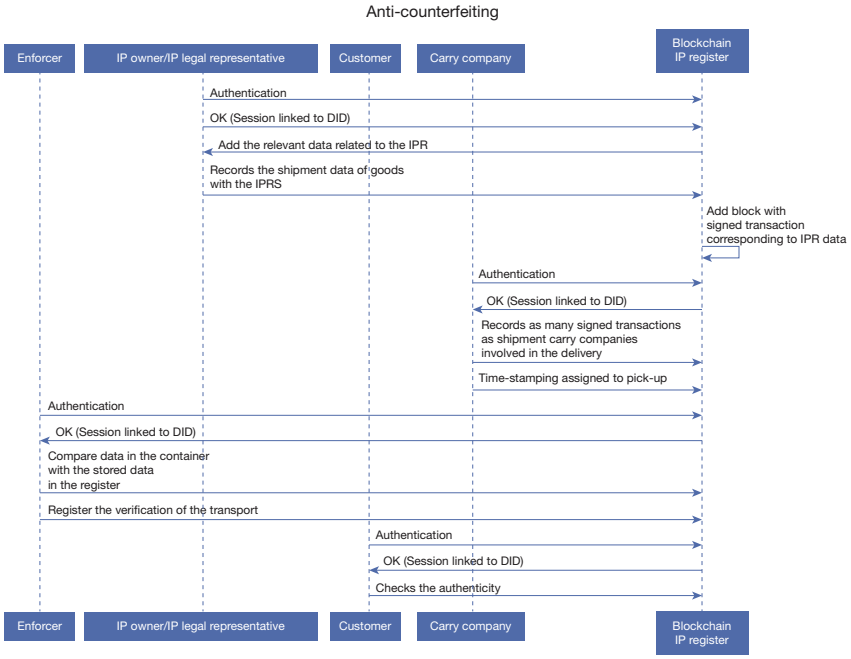
	Based on these figures, the anti-counterfeiting system needs to move forward, and one of the main areas for improvement is to stimulate and increase information sharing between enforcement authorities and IP right holders. Blockchain technology can help to improve the way the information is shared between the actors involved and across borders, allowing them to make decisions based on the available data in the blockchain, ensuring the confidentiality of the shared data.[7]
Potential solution	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 IP registries of the IP organizations. Further, data stored in enforcement authorities' systems and the additional data that will be shared between IP right holders and enforcement authorities will also be used. This information will be related to the registered IP rights (trademarks, industrial designs, plant varieties, copyright or patents).
Blockchain rationale	Blockchain technology has positioned itself as one of the emerging technologies with the greatest potential to respond to current anti-counterfeiting challenges in the coming years, such as: • end-to-end traceability of the IP assets creating immutable records of all the transactions made, creating digital twins of the assets with a unique identifier; • single source of truth, avoiding conflicts with evidence in case of litigations by ensuring that all the parties have access to the same data; • increasing security and protection, creating surveillance measures to take proactive action in case illegal acts are identified; • improving operational efficiency, reducing administrative costs, efforts, time and management performance related to paperwork procedures; • ensuring the sharing and trust of documents and information between all stakeholders using international standards; and • governance of the interpretability between the bodies involved in the process. For this use case, blockchain will serve as the decentralized ledger to protect and share IP related information needed to fight against counterfeiting. The different IPRs can be registered on the blockchain, along with authorizations of use. Enforcement authorities and other designated actors can check the recorded data to identify possible fraudulent use or fake products. Additionally, blockchain enables a method to anchor actors' digital identities (DIDs) with a high level of assurance (LoA) identification tool, which also respects data privacy and personal data regulations.
Potential outcome	Improvement of the data-sharing process and the information available for the enforcement authorities across borders, the right holder and other stakeholders involved in the delivery of the product. Warranty of authenticity of the acquired product and validation throughout the supply chain.

User stories

Tracing throughout the delivery chain

1. the IP owner authenticates as a user with his digital ID into the IP register and provides relevant information about the IP rights in the blockchain;
2. the IP owner records the shipment of goods with the IPRs included in the blockchain;
3. the first transport picks up the shipment and records it in the blockchain;
4. in case of change in the status of the transport (location, carry company, etc.), the new data is stored in the blockchain;
5. by scanning the container, customs officers at each border can check if there is any discrepancy between the information provided by the right holder and the stored data;
6. the product is delivered to the customer and the delivery is recorded; and
7. the final customer checks the authenticity of the product, verifying the delivery chain.

Figure 17. Anti-counterfeiting



Actors (or stakeholders) interacting in the use case and their role in the use case:

IP owner	The owner of the private legal rights that protect the generation of the human mind and seeks to protect it against counterfeiting.
Shipment carry companies	The companies involved in the transport and delivery of the product.
IP enforcement authorities	The authorities that fight against counterfeiting with the information provided by the IP right holders.
Customer	The person acquiring the product or the legal entity selling the product(s).

Interactions (general information applicable to other use cases):

Pre-set up	The participants (enforcement authority, shipment carry companies, IP right holders and customer) must set up a wallet (if a signature is not delegated to the time-stamping service) containing its private key. This wallet can be a hardware wallet, a file protected by password or a remote service providing a signature.
Connects application	The users authenticate the enforcement or marketplace services to the IP rights registries, establishing a new session.
Upload information	The enforcement authorities and IP right holder upload the information they want to exchange.
Hash creation	A unique hash of the files is generated and stored with all the data related to the supply chain.
Fulfill information	The sender participants fulfill the request information about the data that is going to be exchanged and select the receivers they want to exchange the data with.
Transaction creation	The transaction will consist of the hash, the required information, plus any metadata requested by the blockchain protocol, as well as any user metadata considered appropriate (local clock time-stamp). The hash will track all the actions that occur in the product distribution process, time-stamped by each of the actors.
Registration in the blockchain	A blockchain stores the signed and time-stamped transaction on the blockchain.
Time-stamping	The blockchain creates a new block with the transaction. The time-stamp of the blockchain block will be the official time-stamp, any local clock metadata will also be considered valid according to the origin of trust of the signer.
Proof token	The application generates a proof token with the transaction data for the participant.
Receive the data	All the participants involved in the delivery process receive in their wallets the notification of the new data that has been exchanged and they can access it.
Update the information	All the parties can exchange as much information as they need for new transactions.
Upload proof token and file to verify	The viewers can use the proof token (transaction receipt) to fetch the transaction data from the blockchain.
Verification	The relying party's local application compares the locally computed hash with the hash registered on the blockchain. It also checks the time-stamp returned by the block containing the transaction, and (optionally) the time-stamp in the transaction metadata. It also checks that the signer was valid at the time of sending the transaction (this requires a parallel registry not described in this document). If all checks pass, the verification is valid.

Key data (general information applicable to other use cases):

Documents	The encrypted information to be shared between the IP right holders and the enforcement authorities (carry companies, routes, packaging, etc.).
Metadata	The metadata related to the IP rights, data related to logistics of their rights as well as the data related to the logistics used for the delivery of this product.
Hash	The result of the hash algorithm processing the data related to the IP right and each of the changes in the delivery.
Transaction	The order to be submitted to the blockchain containing the hash plus the metadata.
Signed transaction	The transaction once signed by the participants or the delegated service.
Cryptographic parameters	The set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing.
Participant's information	The participant's information.

<table>
<tr><td>Blockchain technical maturity</td><td>Optimizing: already exists in the production environment.
At that moment IP Organizations such as EUIPO and Directorate-General for Taxation and Customs Union (DG TAXUD) are involved in implementing solutions that aim to create a communication platform between IP right holders and the enforcement authorities.
Besides that, many industries such as sportswear, fashion and other IP-intensive sectors are using blockchain to protect their IP rights, the provenance of origin and to help with anti-counterfeiting procedures.</td></tr>
<tr><td>Blockchain technical complexity</td><td>Medium: implementation can be inspired by solutions such as iTrace, Compello, Circulor, Zertifier, etc.</td></tr>
<tr><td>Type of blockchain implementation</td><td><table>
<tr><th>Blockchain type</th><th>Pros</th><th>Cons</th></tr>
<tr><td>Consortium permissioned (IBFT)</td><td>Traceability use cases require a platform that supports high numbers of transactions per second, as well as controlled access by different actors (enforcement authority, shipment carry companies, IP right holders and customer).
Allows fast synchronization of nodes and a high number of transactions per second.</td><td>Requires the deployment and maintenance of a custom infrastructure.
To avoid governance issues, governance rules should be clearly agreed upon between all network participants.</td></tr>
</table></td></tr>
<tr><td>Legal assessment</td><td>Anti-counterfeiting blockchain solutions must comply with national regulations about customs enforcement and, for WTO members that are not Least Developed Countries (LDCs), the Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS Agreement). In the European Union there is Regulation (EU) No 608/2013 of the European Parliament and of the Council of June 12, 2013, concerning customs enforcement of intellectual property rights. The harmonization of copyright regulation around the world allows for better legal interoperability than trademark and patent regulations. In both cases the main legal challenge is to comply with the minimum legal requirement to use the digital certification of the right as a proof in court. Most countries admit digital proof but with different levels of effectiveness and enforceability.</td></tr>
<tr><td>Challenges and risks of using blockchain</td><td>The legal regulation between countries.
High data volumes need to be stored.
GDPR and confidentiality requirements must be respected.
Upgrading of devices by the involved stakeholders will be needed.</td></tr>
<tr><td>References and contact information</td><td>European Union Intellectual Property Office (2020). 2020 Status Report on IPR Infringement: Why IP Rights are important, IPR infringement, and the fight against counterfeiting and piracy. June. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2020_Status_Report_on_IPR_infringement/2020_Status_Report_on_IPR_infringement_en.pdf
European Union Intellectual Property Office (2019). Report on the EU Enforcement of Intellectual Property Rights: Results at the EU borders and in Member States 2013–2017. September. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Report_on_Enforcement_of_IPR_at_EU_borders_and_in_MS_2013_2017/2019_Report_on_enforcement_of_IPR_at_EU_borders_and_in_MS_2013_2017_Full_en.pdf</td></tr>
</table>

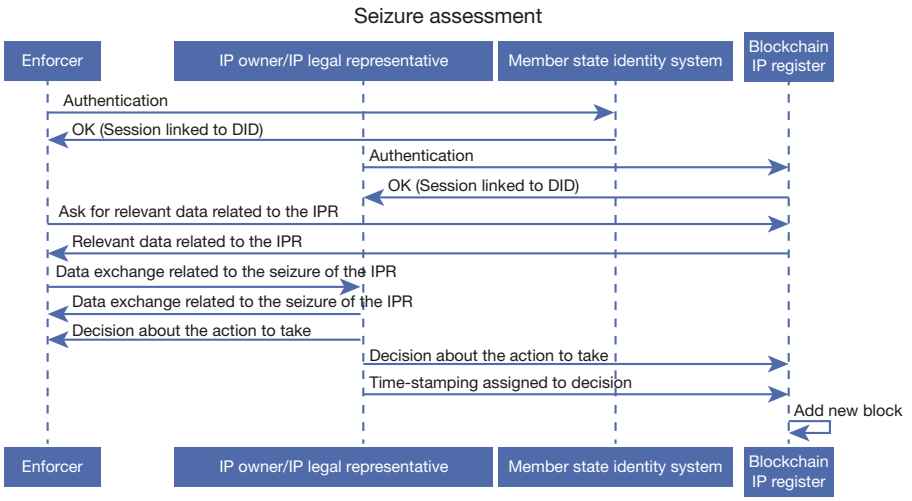
7. IP rights enforcement – seizure assessment

Topic	IPR enforcement – Seizure assessment
Summary	Blockchain can play a key role in the protection of IP rights and the support of enforcement authorities, right holders and other parties involved in the life cycle of associated products. Blockchain technology allows for the creation of a decentralized platform where all parties involved in the protection of IP rights (enforcement authorities, right holders, IP offices and other parties) have access to relevant product-related information. This platform would allow the enforcement authorities and IP right holders to share (confidential) data securely, thereby contributing to support the fight against counterfeiting. Greater effectiveness and efficiency can be established with IP right holders, enforcement authorities such as Interpol, the World Customs Organization (WCO), Europol or the DG TAXUD, and processes such as the EU Application for Actions for IPRs or the management of border seizures.
Relevant IP value chain phase	This is a vertical use case that can be mainly used in the Protection and Commercialization phases.
Business rationale	As OECD and EUIPO published in the *Trends in Trade in Counterfeit and Pirated Goods* report: "Organised criminal groups are seen as playing an increasingly important role in these activities, using profits from counterfeiting and piracy operations to fund other illegal activities." Losses due to counterfeit in the IP active industries are considerable. As the use of the IP system is increasing, potentially so will counterfeiting. To counter this, new initiatives to fight counterfeiting and piracy have been taken in which IP organizations and enforcement authorities are working closely together to implement systems to reduce the negative impacts on IP-protected products. For enforcement authorities, relevant information about protected rights, agile communication and coordination mechanisms with IP right holders and other enforcement authorities is critical to facilitate their activities. For IP right holders, it is necessary to ensure the confidentiality of the exchanged data. Blockchain technology can ease and improve the exchange of trustable data verified between all network participants, ensuring confidentiality and immutability through a digital identity.
Potential solution	To support the business need, a platform should be provided where the IP right holders and enforcement authorities can exchange relevant information related to their IP rights that can in turn support the fight against counterfeiting. This platform – which should be connected with the official registries of IP rights – should allow right holders to provide enough data to the enforcement authorities to ease the identification of potentially fake products during their supply chain management. In many cases, the information to be shared is confidential and additional to the stored data in the IP registries. This is where common consensus, integration, interoperability and security make blockchain a key technology for protecting IP rights. It is mandatory that enforcement authorities can validate the authenticity of shared information and registered evidence.

Blockchain rationale	Blockchain technology holds the potential to respond to the business need mentioned above and the current anti-counterfeiting challenges through: Traceability and trust. The possibility to have end-to-end traceability of assets with an immutable record of all transactions made and ownership control: • digital twins of assets with a unique identifier; and • a single source of truth for all parties, avoiding conflicts and having evidence in case of litigations. Security, protection and control. Improvements in time use and services by maintaining systematic and effective risk management control: • increasing surveillance measures to inhibit and identify illegal acts, and taking proactive action in a timely manner against those who make attempts to breach security; and • enforcing regulatory and safety compliance while maintaining efficiency in the distribution chain. Operational efficiency and the need to improve competitiveness. Improving processes, focusing on the end-user and favoring international competitiveness. Especially for the following topics: • reducing administrative costs, efforts and management performance related to administrative procedures; • reducing all associated time; and • assuring income collection according to regulation. Integration and interoperability. Ensuring the sharing and trust of documents and information between all stakeholders, guaranteeing trade facilitation and economic competitiveness: • harmonization and standardization (documents and processes) based on international standards; • coordination and interoperability between agencies involved in the management of customs offices and trade; • formation of trust environments between ecosystem actors (the public and private sectors); and • generation of distributed, open and mobile environments to avoid information duplication and siloed data storage. For this use case, blockchain will serve as the decentralized ledger to protect and share IP related information. The different IP rights can be registered on the blockchain, along with authorizations of use. Enforcement authorities and other designated actors can check the registry to identify possible fraudulent use or fake products. This system will also serve as the platform to carry out investigation processes. Blockchain additionally enables a method to anchor actors' DIDs with a high level of assurance (LoA) identification tool, which also respects data privacy and personal data regulations.
Potential outcome	A platform that enables: • the secure exchange of information between enforcement authorities; • the possibility to check IP rights authorizations of use; • easy identification of fraudulent uses of IP licenses; • easily trackable and synchronized information; and • a common registry of evidence of infringements ready to be reused.

	Blockchain has the potential to improve different flows in different ways: • greater agility and automation of processes; • improved transparency of, for example, production facilities, points of entry/exit for import/export and licensees. Increased trustworthiness of data entered in different IT platforms with all participants having access to real-time information; • increased traceability of key process events. End-to-end visibility of shipments and supply chains. It is possible to assert origin and quality; • interoperability among stakeholders even when they do not know or trust each other or operate different systems; • automation of workflows for stakeholders' duties and fee payments. A reduction of manual tasks related to the management and collation of documentation; • authentication of identities and portability of identities and data across service providers, including for protection; • immutability of transactions when registered on the blockchain, of which the associated information cannot be altered; and • blockchain holds the capacity to exchange real value through the network and so enables a new way of understanding digital commerce and trading.
User stories	**Detection and seizure evaluation** Upon detection of suspected infringing goods, enforcement authorities can exchange information with the IP right holder to determine if the goods are fake or genuine and to decide whether to seize and destroy the goods. In general there are two separate processes. The first is the making of the application by the right holder to the competent authorities and its acceptance or rejection by the competent authorities. The second stage is the handling by the competent authorities of suspect imports, which may occur as a result of an application or an ex officio action. In this stage the authorities will consider the information about genuine and counterfeit products provided by the right holder and evaluate the status of the suspect products before deciding whether to detain, release or, with the importer/consignee's consent, destroy them. Even though the user story below covers both processes, it is more related to the second. The data that will be shared will not only contain details of the IP rights but also information to allow both parties to confirm the authenticity of the products. 1. the enforcer identifies suspected fake products; 2. the enforcer authenticates into the member state system managing the digital ID; 3. the enforcer looks for the information related to the IP right stored in the IP register; 4. the enforcer provides relevant information to the IP right holder through the platform. Encrypted data is shared and signed by the enforcer; 5. the IP right holder authenticates into the platform using their digital identity; 6. the IP right holder checks the provided information and adds additional data if needed; and 7. when the evaluation is finished, the enforcer decides whether to detain or release the goods, or with the consent (actual or deemed) of the importer/consignee to destroy them.

Figure 18. Seizure assessment



Actors (or stakeholders) interacting in the use case and their roles in the use case:

IP right holder	The owner of the IP right seeking to protect their property.
IP office	The office providing services for the management of digital IPRs.
Importer or consignee	The persons or entities who are buying or responsible for the receipt of a shipment.
Enforcement authority	The person in the relevant enforcement authority/institution fighting against counterfeiting.

Interactions (general information applicable to other use cases):

IP right holder	The owner of the IP right seeking to protect their property.
IP office	The office providing services for the management of digital IPRs.
Importer or consignee	The persons or entities who are buying or responsible for the receipt of a shipment.
Enforcement authority	The person in the relevant enforcement authority/institution fighting against counterfeiting.
Pre-set up	The participants (the enforcement authority and the IP right holder) must set up a wallet (if signature is not delegated to the time-stamping service) containing its own private key. This wallet can be a hardware wallet, a file protected by password or a remote service providing signature.
Connects application	The users authenticates to the trust data sharing service establishing a new session.
Upload information	The enforcement authorities and the IP right holder upload the information they want to exchange.
Hash creation	A unique hash of the files is generated.
Fulfill information request	The sender participants fulfill the request for information about the data to be exchanged and selects the receivers they want to exchange the data with.
Transaction creation	The transaction will consist of the hash, the required information, plus any metadata requested by the blockchain protocol, as well as any user metadata considered appropriate (local clock time-stamp).
Registration on the blockchain	A blockchain client registers the signed transaction on the blockchain.

Time-stamping	The blockchain creates a new block containing the transaction. The time-stamp of the blockchain block will be the official time-stamp, any local clock metadata will also be considered valid according to the origin of trust of the signer.
Proof token	The application generates a proof token with the transaction data related to the IP right.
Receive the data	The other participants (IP right holders, IP offices, importer/ consignee and enforcement authorities) receive the notification in their wallets with the new data exchanged and can access it.
Update the information	Both parties will exchange all the information they need to confirm the authenticity or not of the product, and all the transactions will be stored in the blockchain.
Upload proof token and file to verify	The viewers can use their proof token (received from the transaction) to fetch the transaction data from the blockchain.
Verification	The relying party's local application compares the locally computed hash with the hash registered on the blockchain. It also checks the time-stamp returned by the block containing the transaction and (optionally) the time-stamp in the transaction metadata. It also checks that the signer was valid at the time of sending the transaction (this requires a parallel registry not described in this document). If all checks pass, the verification is valid.

Key data (general information applicable to other use cases):

Documents	The encrypted information to be shared in different formats (documents, images, videos, etc.).
Metadata	The metadata related to the shared information.
Hash	The result of the hash algorithm processing of the document.
Transaction	The order to be submitted to the blockchain containing the hash plus the metadata.
Signed transaction	The transaction once signed by the participant or the delegated service.
Cryptographic parameters	The set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing.
Participant's information	The participant's information.

Blockchain technical maturity	Optimizing: already exists in the production environment. At the moment IP organizations such as EUIPO and DG TAXUD are involved in implementing solutions aimed at creating a communication platform between IP right holders and enforcement authorities. Besides, many industries such as sportswear, fashion and other IP-intensive sectors are using blockchain to protect their IP rights, the provenance of origin and to assist with anti-counterfeiting procedures.
Blockchain technical complexity	Medium: some uncertainty with the implementation needed as well as some of the components, which need to be designed from scratch.

<table>
<tr><td>Type of blockchain implementation</td><td>Type of blockchain implementation recommended: consortium (private) network formed by nodes from IP offices, member states and customs offices.

IPR enforcement: seizure assessment requires an initially well-defined, controlled and monitored identity system – not available in public networks – as well as strict governance rules that need to be defined by a consortium of public institutions.

<table>
<tr><th>Blockchain Type</th><th>Pros</th><th>Cons</th></tr>
<tr><td>Consortium Permissioned (IBFT)</td><td>Traceability use cases require a platform that supports high numbers of transactions per second, as well as controlled access by different actors (enforcement authority, shipment carry companies, IP right holders and customer). Allows fast synchronization of nodes and a high number of transactions per seconds.</td><td>Requires deploying and maintaining custom infrastructure.
In order to avoid governance issues, governance rules should be clearly agreed upon between all network participants.</td></tr>
</table>
</td></tr>
<tr><td>Legal assessment</td><td>At the EU level, an anti-counterfeiting blockchain solution must comply with Regulation (EU) No 608/2013 of the European Parliament and of the Council of June 12, 2013, concerning customs enforcement of intellectual property rights.</td></tr>
<tr><td>Challenges and risks of using blockchain</td><td>National regulations.
High data volumes need to be stored.
Required upgrading of involved stakeholders devices.</td></tr>
<tr><td>References and contact information</td><td>Anti-Counterfeiting Blockathon Forum (n.d.). About. https://euipo.europa.eu/ohimportal/en/web/observatory/blockathon
European Union Intellectual Property Office (2019). Using blockchain in the fight against counterfeiting – EUIPO launches a Forum to support concrete solutions in that field. February 7. https://euipo.europa.eu/ohimportal/es/news/-/action/view/4963920
Saadaoui, Z. (n.d.). Blockchain@TAXUD experience.
European Commission. www.wto.org/english/res_e/reser_e/session_2c_4_zahouani_saadaoui_dg_taxud_blockchain_v1.0.pdf</td></tr>
</table>

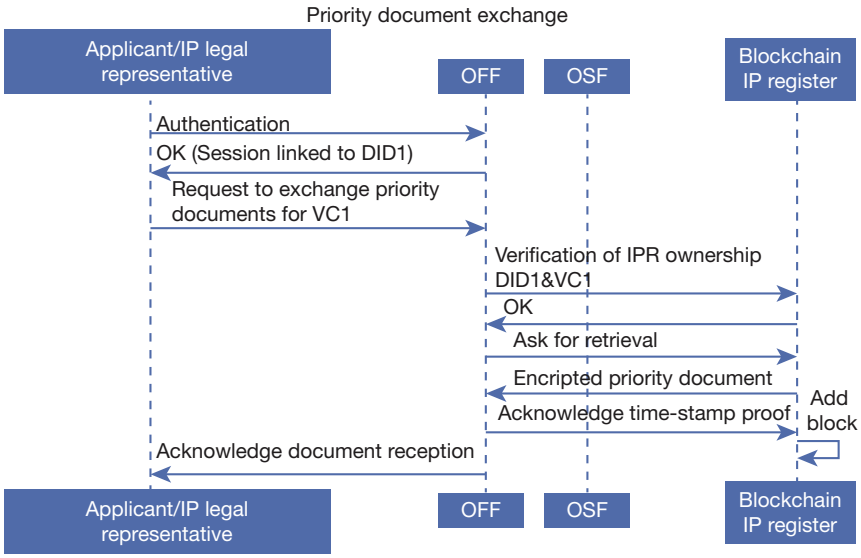
8. Priority document exchange among IP offices

Topic	Priority document exchange among IP offices
Summary	Priority document exchange among IP offices is a specific application of trusted data sharing where different IP offices create a common infrastructure for exchanging priority patent documentation within participating IPOs, for example, by relieving applicants of the need to submit documents to the Office of First Filing (OFF) in the process of patent approval request in IP offices of different countries. Nowadays, the most common way to do this is by mailing the physical documentation, or using WIPO DAS (Digital Access Service), which allows the exchange of certain documentation in a digital way. Note that there are already existing blockchain solutions offered by Zertifier, which use blockchain to store and encrypt documents via a hashing technique. Using a blockchain solution 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. The trust is built between the patent offices, which agree on the governance, the encrypted communication channels and the strict confidential rules about what information or documents to share, each sharing is made only by the required members and not the whole the network. Additionally, access to documents may be controlled and restricted.
Relevant IP value chain phases	This is a vertical use case with a wide usage, for example, used when an applicant asks to use the priority patent documents generated in the OFF and applies for the generation of an IP right in different countries.
Business rationale	The objective is to create an easy, secure and fast method of sharing priority documentation between IP offices. The desired result is an improvement of IP offices' procedures with a reduction in the manual procedures needed to share documents, the establishment of a common approval process, an improvement in the time spent on different flows and a good complement to the WIPO DAS system. This way, applicants save the time and effort of submitting the documents to the OFF, and IP offices can automate the procedure of sending updates and resolution of its own processed IP rights to the other IP offices, reducing the manual labor used in these tasks and a lot of time, as the documentation is shared digitally in real time.
Potential solution	The potential solution for priority document exchange among patent offices could be an extension of the current IP registry use case with a decentralized "smart IP Registry" in which the OFF stores the original patent application and correspondent priority documentation. This platform could allow the applicant to request the same patent in other countries and the priority patent documents to be exchanged between patent offices in a secure way with the consent of the applicant yet without the need for human intervention.

	The sensitive/confidential documentation is stored off-chain and hashed locally (on the user's PC) using agreed cryptographic algorithms (one-way mathematical functions) in a similar way to the process of non-blockchain solutions, ensuring that manipulated documents are easily identifiable and real documents can be verified. • The defined data model for the information to be shared can be stored on the blockchain, indicating all relevant information that needs to be shared publicly, and ensuring interoperability between different offices. • The hash proof of the information is also added to a transaction, signed and then sent to the blockchain network for validation by consensus. • The signature is either locally signed by the document owner (using a web browser extension for example) or signed by the sender entity (signature delegation), counterbalancing the legal value, security and usability of the solution. • The IP office will send the patent priority documents to the IP office(s) selected by the applicant at the location where the applicant wants the patent grant to be. • Once accepted by network consensus, the signature will be registered in the immutable blockchain. The exact time at which this is done can vary depending on the consensus and network selected, between a few seconds and a few minutes (for public networks). • The sender IP office will receive a transaction receipt confirming the correct time-stamping of its shared data and that it has been received by the different agents. Even in the case where the user loses the transaction receipt, it is still possible to check the validity of the time-stamp by examining the blockchain, especially if metadata is added to the transaction along with the time-stamp. • The applicant selected by the IP office(s) will receive the patent priority documents, and will be able to certify and verify the data using a standard blockchain software (no need to trust non-auditable software controlled by third parties). This documentation can then be stored in the IP offices' systems together with the "proof of ownership" information retrieved from the blockchain. • Each IP office can publish their status of the patent in their country and update it when needed. The rest of the IP offices and indicated viewers will be updated in real time and will be able to verify the information anytime.
Blockchain rationale	Blockchain offers a decentralized network where different IP offices can exchange data or documents in a secure and traceable way, and this will allow automation of the sending of priority patent documents from the OFF to the Office of Second Filing (OSF) in which the applicant applies for the patent. On a decentralized network governed by different participants, a Byzantine node trying to falsify the real signature time would be detected promptly, since the node could falsify its local clock, but not rearrange the block order. Agreed token artifacts could allow, in some contexts, for automation or simplification of the process of the time-stamping service for sending or receiving the priority patent documents.

Potential outcome	A new tool for IP offices to send the priority documents and communicate between themselves in a safe, quick and easy way. This new tool could be part of the smart IP Registry from which the applicant could use the hash of their stored and encrypted patent data by, firstly, using the time-stamp as evidence of the patent grant and, secondly, sending OFF-certified patent documents to the offices for which the applicant is requesting a patent to be granted, and this could be connected to WIPO DAS. This new solution would result in significant savings of time and resources for the different IP offices and also for the applicants.
User stories	**Priority patent documents exchange between patent offices** Prerequisites: one patent has been granted in the patent office considered the OFF; this patent was identified with the verifiable credential VC1. 1. the IP right holder or IP legal representative authenticates with DID1 into the patent office through any secure mechanism; 2. the IP right holder or IP legal representative requests the OFF to exchange the priority patent documents with the OSF to get the patent grant in a new patent office. The request includes DID1 and VC1; 3. the OFF verifies the IP right ownership in the IP Register (DID1 and VC1); 4. a code (hash code) is created for the OSF and automatically sent from the OFF to the OSF, through which the OSF will be able to retrieve the priority documents from the OFF; 5. the OSF asks for retrieval of the priority patent documents using the hash code received; 6. the encrypted string containing priority patent documents is sent to the OSF; and 7. the OSF acknowledges the previous step with the receipt of the priority patent documents proving time-stamp proof.

Figure 19. Priority document exchange



Actors (or stakeholders) interacting in the use case and their role in the use case:

Actors	Description
IP right holder	The owner of private legal rights that protect the generation of the human mind: inventions, literary and artistic works, symbols, names, images and designs used in commerce. These are commonly divided into two categories: industrial property rights (e.g., patents, trademarks, industrial designs, geographical indications) and related rights (e.g., rights of the authors/creators and those of performing artists in their performances, producers of phonograms in their recordings and those of broadcasters in their radio and television programs).
IP offices	The official national or international bodies that are responsible for granting, issuing or recording intellectual property rights.
IP legal representative	The individual or organization appointed by the innovator that has legal personality and that may, acting in its own name, exercise rights and be subject to obligations.
Office of First Filing (OFF)	The official IP office receiving the first application for a patent from. The applicant may ask the OFF to grant the same patent in other countries.
Office of Second Filing (OSF)	The official IP office receiving the application for a patent that is already registered in an OFF.

Interactions (general information applicable to other use cases):

Pre-set up	The IP offices must set up a wallet (if the signature is not delegated to the time-stamping service) containing its own private key. This wallet can be a hardware wallet, a password protected file or a remote service providing a signature.
Connects application	The IP offices authenticate to the trust data sharing service, establishing a new session.
Upload information	The applicant updates the patent documents required during the patent grant process in the OFF, which will be exchanged as priority patent document with the OSF.
	Hash creation A unique hash of the files is generated.
Fulfill information	The IP offices fulfill the request information about the data to be shared and select the IP offices with which the IP right holder wants to share the documents.
Transaction creation	The transaction will consist of the hash, the required information, plus any metadata requested by the blockchain protocol, as well as any user metadata considered appropriate (local clock time-stamp).
Registration in the blockchain	A blockchain client registers the signed transaction on the blockchain.
Time-stamping	The blockchain creates a new block containing the transaction. The time-stamp of the blockchain block will be the official time-stamp, any local clock metadata will also be considered valid according to the origin of trust of the signer.
Proof token	The application generates a proof token with the transaction data between the IP offices involved in the priority document exchange.
Receive the data	The selected OSFs receive notification in their wallets with the update that the shared documentation has been placed in the blockchain and that they now have access to these documents.
Update the information	The IP offices can update the patent status with a new transaction.

Key data (general information applicable to other use cases):

Documents	The information to be shared between the OFF and the OSF.
Metadata	The metadata related to the shared information.
Hash	The result of the hash algorithm processing of the document
Transaction	The order to be submitted to the blockchain containing the hash plus the metadata.
Signed transaction	The transaction once it has been signed by the participant or the delegated service.
Cryptographic parameters	The set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing.
Participant's information	The IP office's information.

Blockchain technical maturity

Basic: some conceptual definition or analysis has been done.

Blockchain technical complexity

Low: market available solutions are highly tested.

Type of blockchain implementation

Type of blockchain implementation recommended: Private Permissioned. The exchange of documents requires strict confidentiality among IP offices and a private node on the public blockchain would allow an even higher level of security.

Blockchain type	Pros	Cons
Private permissioned (IBFT)	Allows fast synchronization of nodes. In this case "Git" plus PGP signature would also better suit the use case requirements due to the nature of the managed information (binary documents registered as individual files) and the possibility of documentation versioning/ branching – an undesired feature for asset-like information, but a good-to-have for document-like data.	Requires the deployment and maintenance of a custom infrastructure. To avoid governance issues, governance rules should be clearly agreed upon between all network participants.

Legal assessment

The European Patent Office (EPO) has decided that as of November 1, 2018, the EPO will participate in the WIPO DAS for the exchange of certified copies of patent applications (priority documents). Currently, there are 21 participating offices, including the other IP5 Offices United States Patent and Trademark Office [USPTO], Japan Patent Office (JPO), The Korean Intellectual Property Office (KIPO), and China National Intellectual Property Administration (CNIPA) and the patent offices of Denmark, Estonia, Finland, the Netherlands, Spain, Sweden and the United Kingdom. An up-to-date list of participating offices can be found on the WIPO website at: www.wipo.int/das/en/participating_offices.html.

The USPTO transmits certain US priority applications as filed to any foreign IP offices that participate in the priority document exchange program (participating offices) and retrieves/accesses certain foreign priority applications as filed from the participating offices. The priority document exchange program includes two modes of exchange: direct bilateral exchange and WIPO DAS exchange.

Challenges and risks of using blockchain

There are technical, regulatory and business challenges of adopting the technology for the use case.

References and contact information	European Patent Office (2018). Notice from the European Patent Office dated October 18, 2018 concerning priority document exchange via the WIPO DAS. Official Journal, October 18, 2018. www.epo.org/law-practice/legal-texts/official-journal/2018/10/a79.html United States Patent and Trademark Office (2018). Electronic Priority Document Exchange (PDX) Program. www.uspto.gov/patents-getting-started/international-protection/electronic-priority-document-exchange-pdx#:~:text=The percent20European percent20Patent percent20Office percent20(EPO,of percent20exchange percent20are percent20mutually percent20exclusive World Intellectual Property Organization (n.d.). WIPO Digital Access Service. www.wipo.int/das/en/#

9. Certification mark

Topic	Certification mark
Summary	A certification mark is a mark indicating that the goods or services protected by such a mark comply with a given standard set out in the regulations of use and controlled under the responsibility of the certification mark owner, irrespective of the identity of the undertaking that actually produces or provides the goods and services at issue and actually uses the certification mark. Generally, the proprietor of a certification mark is not the end-user of the mark, but is the certifier, one who exercises legitimate control over the use of the certification mark regardless of the type of certification. Therefore, the typical feature of a certification mark is that it is used not by the holder of the mark but instead by the authorized users. The function of the certification mark is to guarantee to the relevant public that goods or services possess a particular characteristic. This use case proposes the creation of a distributed register of trademark certifications in which the certification 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 use of the trademark certification are stored.
Relevant IP value chain phases	This use case is applicable during the Protection phase for trademarks.
Business rationale	Trademark certification is a quality seal indication that a product/service is produced/delivered according to the standards defined by the mark owner whom is certifying that the good or service meets the established characteristics, in compliance with the performance of the services, the expected quality or any other defined requirement. Certification does not qualify as an approval, organizations are responsible for certifying and regularly reviewing if the products or services are created or delivered according to the standards defined by the trademark owner. In case the (re)examination of the request is successful, the use of the mark is (re)granted as a recognition of compliance with such specific standards. Certification marks are regulated by some trademark offices such as the USPTO and EUIPO, they have a similar registration process to trademark registration. After a certification mark is registered, owners must follow these rules to maintain their registrations: • non-discrimination: an owner must grant the right to use the certification mark to any company that meets the standards of certification; • exclusivity of use: an owner cannot use the mark for any purpose other than certification; • standards: an owner must establish clear standards for the mark; and • objectivity: an owner cannot sell their own products or services using the mark. This does not prevent the owner from manufacturing or selling products, only from using the certification mark on its own products. Once a trademark certification has been granted, its users may use the certification marks according to the standards defined in the trademark certification.

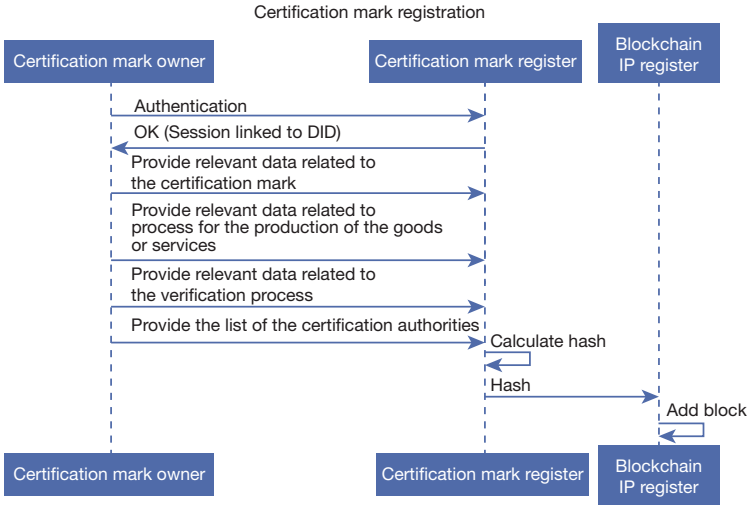
	The main challenges of the current processes are that potential users have difficulty obtaining the trademark, as it is not always clear where to request the trademark certification. On the other hand, the trademark certification owners must be sure that the users comply with all preestablished requirements before and after the authorization of use of the trademark.
Potential solution	Create a system able to issue trusted certificates in a decentralized shared network for different types of trademarks. This system will contain the certification marks' information in relation to the process for the production/ delivery of the goods/services and for the verification, authorized to proceed with the examination of the request, people authorized to use the mark, characteristics that the marks accomplish, thus achieving that it can be verified in real time. The aforesaid may be done via QR codes, laser incisions or similar systems. The digital recordation makes the data and files contained in the issued certificate transparent, secure and irrevocable over time.
Blockchain rationale	Blockchain technology can record data related to the regulations of generation or use of a certification mark, the conditions governing the use of the certification mark or the supervision measures to be applied by the certification mark owner. Blockchain offers trust, accountability and transparency. It allows checks to be made on whether the examination process has been performed following the indications defined within the certification mark process and it can be used as an immutable time-stamp on the application, the resolution and the maintenance of the rights in the use of the trademark. Blockchain ledgers are time-stamped records that cannot be altered and may store smart contracts that can be used as the authorization layer to stamp the products in accordance with the granted certification mark.
Potential outcome	A new system to manage the process of trademark certification, where the manufacturers can easily know the requirements to obtain a trademark certification and can apply to get the authorization of use of the trademark as well as where the owners of the trademark can have real-time knowledge of the fulfillment of the requirements by the manufactures in a secure, trustworthy way. The main benefits will be: • easy management of certification marks; • transparency in the certification evaluation process following the requirements for verification; and • simpler mark certification revocation procedures.

User stories

As a certification mark owner, to grant the use of a certification mark, the manufacturing process as well as any other characteristics concerning the conditions allowing the use of the mark can be recorded:

1. the certification mark owner creates the record for the certification mark in the system;
2. the certification mark owner describes the process and any other features that should be accomplished during the production of the goods or services;
3. the certification mark owner describes the verification process;
4. the certification mark owner includes the list of individuals or entities that can perform the verification of the request for use of the certification mark;
5. the hash is calculated with the provided data;
6. the hash is transmitted and stored to the blockchain nodes; and
7. the use of the certification mark is ready to be requested.

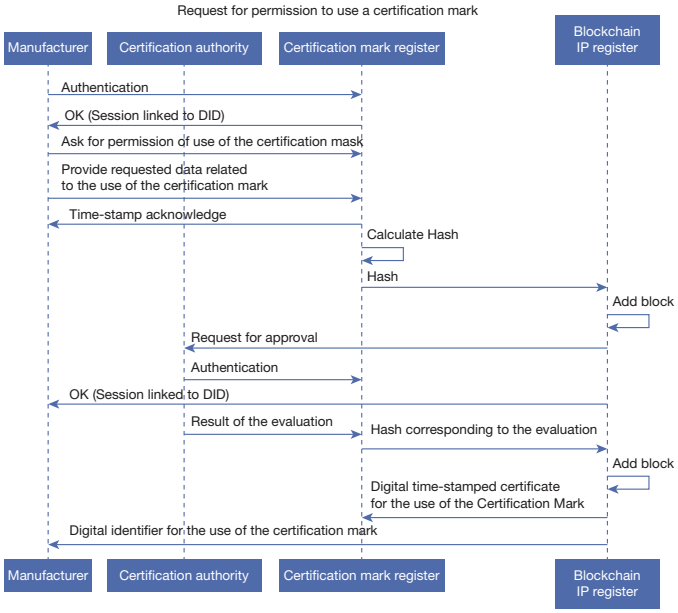
Figure 20. Certification mark registration



From the manufacturer's point of view, to use the certification mark, a request may be submitted and acceptance is subject to compliance with the requirements set by the certification owner:

1. the manufacturer requests use of an already existing certification mark in the system providing the required data;
2. the manufacturer can access the process and any other features that should be accomplished during the production of the goods or services;
3. the certification authority for the approval of the use accesses the data provided by the manufacturer;
4. the manufacturer accepts the terms of the verification process and the terms of condition to keep the use of the certification mark in case it is granted; and
5. the manufacturer gets the results of the verification process.

Figure 21. Request for permission to use a certification mark



Automatic revocation of a license

1. The system checks periodically when the terms and conditions are not met or the use of the certification mark should be revoked; and
2. when the conditions for expiration or revocation are met then the use of the certification mark is revoked automatically.

NOTE: The status of usage of the certification mark can be checked any time by all the parties and in case of dispute, an arbitrator can be appointed to resolve the terms.

Actors (or stakeholders) interacting in the use case and their role in the use case:

Certification mark owner	The user owns the certification mark and is responsible for the definition of the conditions to be accomplished by the products.
Manufacturer/service provider	The individuals or entities producing goods or delivering services for which the certification mark is requested.
Certification authority	The entity or individual authorized by the certification mark owner to grant the use of the trademark.

Interactions (general information applicable to other use cases):

Pre-set up	The manufacturer/provider must set up a wallet (if the signature is not delegated to the time-stamping service) containing its private key. This wallet can be a hardware wallet, a file protected by password or a remote service providing signature.
Connection to the application	The user authenticates to the time-stamping service establishing a new session.
Hash creation	A unique hash of the file is generated.
Transaction creation	The transaction will consist of the hash, plus any metadata requested by the blockchain protocol, as well as any user metadata considered appropriate (local clock time-stamp).
Registration in the blockchain	A blockchain client registers the signed transaction on the blockchain.

Time-stamping	The blockchain creates a new block with the transaction. The time-stamp of the blockchain block will be the official time-stamp, any local clock metadata will also be considered valid according to the origin of trust of the signer.
Proof token	The application generates a proof token with the transaction data related to the IP right.
Receive the data	The other participants (IP right holders, IP offices, importer/consignee and enforcement authorities) receive the notification in their wallets with the new data exchanged and can access it.
Verification	The relying party's local application compares the locally computed hash with the hash registered on the blockchain. It also checks the time-stamp returned by the block containing the transaction and (optionally) the time-stamp in the transaction metadata. It also checks that the signer was valid at the time of sending the transaction (this requires a parallel registry not described in this document). If all checks pass, the verification is valid.

Key data (general information applicable to other use cases):

Document	The original data to be time-stamped.
Metadata	The metadata related to the documents, to a time-stamp or to the time-stamp process.
Hash	The result of the hash algorithm processing of the document.
Transaction	The order to be submitted to the blockchain containing the hash plus the metadata.
Signed transaction	The transaction once signed by the registrar or the delegated service.
Cryptographic parameters	The set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing.
Register's information	The register's information.

Blockchain technical maturity	Initial: no exploration has been done.
Blockchain technical complexity	Medium: some uncertainty about the implementation needed and some components need to be designed from scratch, there is no common regulation.
Type of blockchain implementation	Trademark certification requires first a well-defined, controlled and monitored identity system, not available in public networks, as well as strict privacy of trademark information.

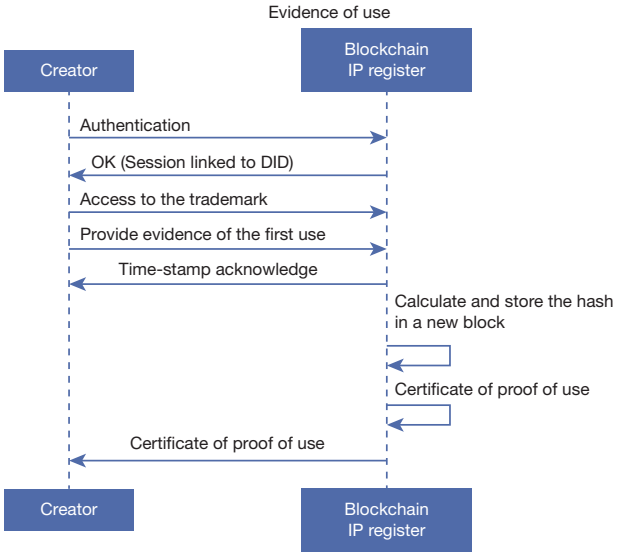
Blockchain type	Pros	Cons
Private permissioned (IBFT)	Allows fast synchronization of nodes.	Requires the deployment and maintenance of a custom infrastructure. To avoid governance issues, governance rules should be clearly agreed upon between all network participants.

Legal assessment	–
Challenges and risks of using blockchain	Although some jurisdictional courts allow blockchain as evidence, its full adoption into law is still far off and the presence of IP experts is still necessary for legal matters and examinations.

	With regard to a method to connect registries across the world through a single distributed ledger, this reality is far from simple. Successful management of IP rights using blockchain requires a mutually agreed, internationally supported platform. The problem with this is (and always will be) the issue of aligning multiple national and regional judicial frameworks and traditions.
References and contact information	–

10. Evidence of trademark use

Topic	Evidence of trademark use
Summary	Once a trademark has been registered in an IP office, in many jurisdictions, keeping the trademark-protected proof of first or genuine use is required. Similarly, further evidence may be required in disputes or any other proceeding involving recognition of well-known marks, or in defending a non-use revocation action. By way of example, collecting information on the use of a trademark in trade or commerce on a blockchain-based official trademark register may allow the relevant IP office to be notified almost immediately, for example, by appending the first "public" advertising or showing of the mark to the blockchain or by appending evidence of use (e.g., via a survey) to the blockchain. This would result in reliable and time-stamped 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, DLT could be used to publish technologies for defensive publication as prior art to prevent others from obtaining a patent over such technologies.
Relevant IP value chain phases	This use case may be applicable during the Protection phase mainly for trademarks, since to keep the trademark registered, it must be used in the market and dated evidence is needed to accredit such use. For patents, it may be used to protect the researchers as evidence of publication and defensive publications.
Business rationale	The use of a trademark is important to establish and maintain trademark rights. In many jurisdictions, trademark rights accrue to the first to use the relevant mark. In all jurisdictions, rights of trademark registration are dependent (with varying rules) on continued use of the trademark. Often, however, proving prior or continued use of a trademark is a difficult process involving the arduous collection of relevant records (which can prove to be unreliable and incomplete), and demonstrating use of a trademark, for example, via surveys, and can be a significant cost to right holders. If using a smart contract, which shows the time, date and circumstances of first or subsequent use is recorded on a blockchain, subject to the court accepting blockchain-based evidence as reliable (which is increasing as time passes), then a party may have a verifiable, immutable record to present as evidence. By circumventing the usual reliance on accounting records (which may not demonstrate sufficiently the actual use of the trademark) and archived paper records, the costs of proving use may be dramatically reduced, which could lead to a reduction in the risk of challenges to registration of trademarks. This solution may reduce the time and resources that right holders have to do in some jurisdictions.
Potential solution	Create a system able to issue trusted certificates in a public network, which contains the evidence of use or the trademark. This way of working results in an innovative form of digital recordation, which makes the data and files transparent, secure and irrevocable over time and provides proof of the use of the trademark in a digital, quick and easy way.

Blockchain rationale	Collecting information on the use of a trademark in trade on a blockchain ledger would allow the relevant IP office to be notified almost immediately on the occurrence of a verified event of this use. This means that reliable evidence and information of actual use of a trademark in trade, as well as the frequency of this use, could be readily shared and available on the official trademark register. Indeed, blockchain could have a knock-on effect on trademark specifications with the result that IP offices' trademark practices could move to a shorter and more concise specification of goods and services, as exists in the United States. If such a development were to prove legally acceptable, blockchain technology could simplify the process of providing evidence of use of a trademark and other evidence at an IP office or court; for example, in cases of proving first use, genuine use, acquired distinctiveness or secondary meaning or goodwill in a trademark. The newest generation of blockchain technology, which combines layered public and private elements, should help to address confidentiality issues.
Potential outcome	Easy and immutable tracking and automatic notification on the use of registered trademark to the owners of the brand and the trademark offices in the countries in which it is protected.
User stories	**Certification of use of trademark** 1. the trademark owner authenticates into the IP register with their digital identity; 2. the trademark owner accesses the trademark for which they want to provide the evidence of use; 3. the trademark owner uploads the evidence of use in the IP register; 4. the IP register calculates the hash with the provided evidence of use; 5. the hash is stored in the blockchain in a new block; and 6. the certificate of the use in the blockchain is now available in the IP register as a proof of use and a copy of the certificate is sent to the trademark owner. Figure 22. Evidence of use 

Actors (or stakeholders) interacting in the use case and their role in the use case:

Trademark owner	The user who owns the trademark.
IP office	The IP office that owns the blockchain-based official trademark register.
Trademark user	The user of the registered trademark.
Interactions	(general information applicable to other use cases):
Pre-set up	The registrar must set up a wallet (if signature is not delegated to the time-stamping service) containing its private key. This wallet can be a hardware wallet, a file protected by password or a remote service providing signature.
Connection to application	The user authenticates to the time-stamping service establishing a new session.
Hash creation	A unique hash of the file is generated.
Transaction creation	The transaction will consist of the hash, plus any metadata requested by the blockchain protocol, as well as any user metadata considered appropriate (local clock time-stamp).
Registration in the blockchain	A blockchain client registers the signed transaction on the blockchain.
Time-stamping	The blockchain creates a new block with the transaction. The time-stamp of the blockchain block will be the official time-stamp, any local clock metadata will also be considered valid according to the origin of trust of the signer.
Proof token	The application generates a proof token with the transaction data.
Proof token upload and file verification	The relying party uses the proof token (transaction receipt) to fetch the transaction data from the blockchain.
Verification	The relying party's local application compares the locally computed hash with the hash registered on the blockchain. It also checks the time-stamp returned by the block containing the transaction and (optionally) the time-stamp in the transaction metadata. It also checks that the signer was valid at the time of sending the transaction (this requires a parallel registry not described in this document). If all checks pass, the verification is valid.

Key data (general information applicable to other use cases):

Document	The original data to be time-stamped.
Metadata	The metadata related to the documents, to a time-stamp or to the time-stamp process.
Hash	The result of the hash algorithm processing of the document.
Transaction	The order to be submitted to the blockchain containing the hash plus the metadata.
Signed transaction	The transaction once signed by the registrar or the delegated service.
Cryptographic parameters	The set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing.
Register's information	The register's information.

Blockchain technical maturity	Initial: no exploration has been done.
Blockchain technical complexity	Medium: some uncertainty of the implementation needed and some components need to be designed from scratch; there is no common regulation.

<table>
<tr><td>Type of blockchain implementation</td><td>
<table>
<tr><th>Blockchain type</th><th>Pros</th><th>Cons</th></tr>
<tr><td>Public/private permissionless/ permissioned
consensus recommended: PoW/ PoS for public networks, IBFT for private networks.</td><td>Due to the expected low transaction rate (one single transaction after first usage) and the need to make the notarization of the “proof of first usage” valid in legal disputes, any blockchain that can be accepted as valid in legal procedures will suit the need.</td><td></td></tr>
</table>
</td></tr>
<tr><td>Legal assessment</td><td>Time-stamping proof is the core part of this use case. As it was mentioned above in the time-stamping use case, the final implementation should ensure the alignment with best practices, standards and regulations at all times.
In terms of regulation, it should be compliant with, at least, the following regulatory framework as per the particular jurisdiction or the specific jurisdiction where the IP office owns the blockchain-based official trademark register:
• digital identity regulation;
• any certified authority/trust agent regulation; and
• data protection/privacy regulation.

In terms of standards and best practices: all of the current standards and best practices are applied to an existing time-stamping, ensuring minimum security and quality requirements. These standards and best practices already exist regardless of the use of DLT and can be implemented.
Some examples are:
• ETSI Electronic Signature Format standards TS 101 733, along with other ETSI standards.
• ISO/IEC 27002 is an international standard used as a reference for controls when implementing an information security management system, cryptographic control of sensitive data and key management.</td></tr>
<tr><td>Challenges and risks of using blockchain</td><td>–</td></tr>
<tr><td>References and contact information</td><td>WIPO Magazine (2020). Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights. June. www.wipo.int/wipo_magazine_digital/en/2020/article_0002.html</td></tr>
</table>

11. E-PVP modules

Topic	E-PVP modules
Summary	Plant variety protection (PVP) applications are examined and plant breeders' rights (PBR) are granted by authorities of members of the International Union for the Protection of New Varieties of Plants (UPOV). It is hard for applicants to have a global overview of their varieties and their status in different authorities and difficult for those authorities (PVP offices) to exchange information. This use case proposes the creation of an electronic PVP administration system. The system will allow PVP offices to exchange data securely between the UPOV PRISMA PBR Application Tool, PVP office systems and applicants. Therefore, building a distributed ledger rather than a traditional centralized database could effectively turn e-PVP into a ledger that incorporates rights without geographic barriers, interconnecting the offices' data. This solution would create an immutable record of "events" in the life of a protected variety, globally. It includes the moment when a PVP application is filed, examined and granted; it would resolve the practicalities of collating, storing and providing such evidence as well. It is also relevant for the PVP matters after grant (e.g., keeping the rights in force, nullity and cancellation).
Relevant IP value chain phases	The most relevant phase of the IP value chain for this use case is the Protection phase.
Business rationale	Given the applicable legislation, varieties are protected at either national or regional level (e.g., EU, OAPI). Nevertheless, they are in many cases represented in a national database and then aggregated (using a limited set of attributes) in supranational and international databases. Current practices require applicants to file for protection for their varieties in each UPOV member they wish to obtain protection and therefore they provide the same information in several instances, which are not always interconnected. At the same time, PVP offices can exchange documents using emails, but there is no common place where they can share information provided by the applicant. This use case focuses on the simplification of the application processes for the applicants and the connection between different PVP offices by interconnecting the PVP offices with a common tool and improving the information exchange. This use case represents one of the steps for the achievement of the "Once Only" principle applied to the IP value chain: in a generic way it entails that natural and legal persons provide diverse data only once in contact with public administrations, while public administration bodies take actions to internally share and reuse the data – even across borders – always in respect of data protection regulations and other constraints. Translated to the IP value chain, it will allow the applicants and legal representatives to provide the data only once, which can be implemented in the form of a blockchain.

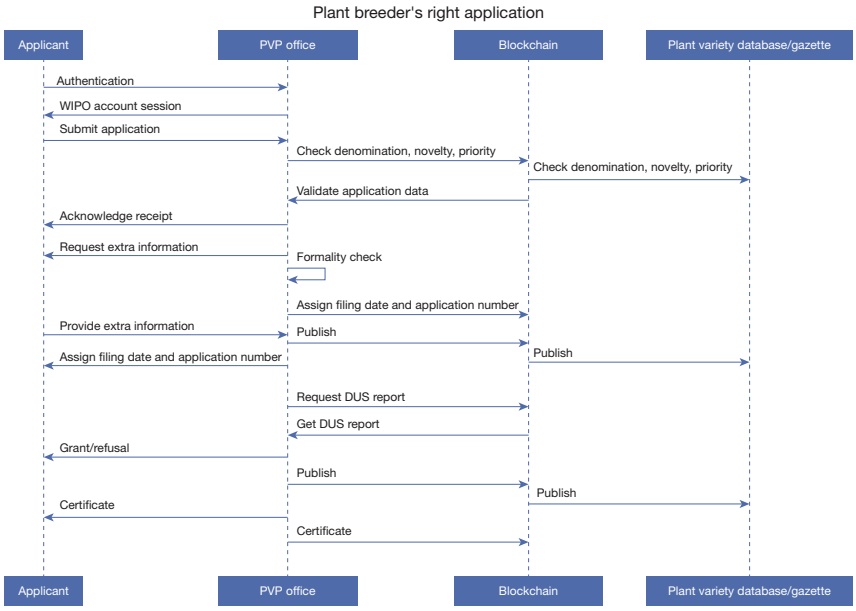
	When the plant breeder's right (PBR) holder decides to ask for protection in several UPOV members there is limited synchronization between the systems and the data provided in each system may be different. In addition, the cost for the applicants is high, not only during the application of the PBR but also the maintenance. This is due to the fact that each process requires that all the documentation is provided as many times as UPOV members are selected, and each of them has its own fee to be paid. A common decentralized system should mitigate the reiterative process and enhance the efficiency of the process.

Potential solution	The solution is to create a common register using DLT managed by the PVP offices – using an agreed consensus model – and to allow:
	• the applicants and legal representatives to submit their application data: this step defines the creation of the blockchain asset; and
	• the PVP offices (administrative and Distinctness, Uniformity and Stability [DUS] examiners) to report on the different examination steps in the process.
	
	This common register is the first step to connect PVP offices and interconnect their data. Such an approach reduces the duplication of data and creates further opportunities for the harmonization of examination practices.
	
	Additionally, different services could be created around this solution:
	• Exchanging data in real time: the e-PVP applicant monitoring module will offer the possibility to know the application status in real time. On the other hand, the e-PVP DUS exchange module will make the cooperation between PVP offices more efficient as the access to the needed data is in real time.
	• Having an immutable track of data history. It will create an immutable record of PVP applications on the chain tracking all the activities performed with each of them during the PBR grant process, stamping each of the transactions performed and using trust data sharing among all the actors involved. A smart contract provides a self-executed agreement between:
	  • breeders and PVP offices; and
	  • between PVP offices.
	
	It can be used during the whole IP value chain, from filing an application to the termination of the right including publication.
	
	By replacing centralized administration systems with decentralized ones, there is a record of the complete application grant process including the filing application date, plus the different activities performed during the formality examination, the examination of denomination and novelty, and the DUS examination processes and their results.
	
	This common register contains shared information of the PBR application data between PVP offices, so the applicant will be the first provider of the information at the time of submission, and then the different PVP offices can share this information in a secure way. This is applicable to the documents provided during the whole life cycle as well.

Blockchain rationale	The decentralized nature of blockchain disintermediates central authorities and reduces the amount of trust required among the participants in the system. The participants' motives are fully aligned with the goals of the register mechanism because the participants are both users (applicants/title holders) and operators (examiners) of the system. Blockchain, by definition, is a decentralized register. With a blockchain-based system, different PVP offices will have an opportunity to do their own customizations on top of the shared ledger, so even having a decentralized and unique register, PVP offices could have different rules: data classification levels, delegation/cooperation rules. There are many advantages of using blockchain-based registries: • the records are immutable: once a record is published, no one can remove it; • the records are completely traceable: they are publicly available to anyone to search for and consult the public information; • it is totally digital: papers and signature checks are not needed anymore; and • there is no central point of failure since the whole infrastructure is decentralized. Blockchain technology does not guarantee data confidentiality. Cryptographic algorithms should be added on the top to give a high degree of security to all operations. Blockchain technology provides the opportunity to make the PVP application examination more efficient and accurate and to make the publication faster.
Potential outcome	Blockchain-based decentralized e-PVP modules among PVP offices allow the applicants and legal representatives to provide the information at the time of submission. It eliminates duplicities and enables the sharing of information between PVP offices. The applicant/title holder will receive the following benefits: • monitoring of their application during its full life cycle; • saving of time thanks to the information shared between PVP offices; and • decentralizing of information that is time-stamped and therefore valid in case of legal disputes. The PVP office will receive the following benefits: • a digital framework for standardized data sharing among PVP offices; • better service to the applicants: a simpler process could increase the number of applications; • elimination of mistakes and typos in the examination process; and • the first step to full tracking of the PBR life cycle.

User stories	**Plant breeder's right application** When a user (an applicant or a legal representative) wants to protect their variety, they should be a user, with the role of applicant or representative, in the PVP office in which they are going to apply. The user will access the online filing tool UPOV PRISMA or the national filing system. To ensure the confidentiality of the data provided by the user, once the data is submitted, it will be automatically encrypted creating a hash that will be recorded, time-stamped and stored in the blockchain ledger with a unique identifier. At this moment the plant breeder's right grant process will start and all the transactions will be stored and linked to this unique identifier on the blockchain. 1. the applicant or the legal representative logs in to the PBR application tool (UPOV PRISMA or the receiving filing system) through a secure mechanism (WIPO account in the case of UPOV PRISMA); 2. the applicant or the legal representative fills in all pertinent data and submits it to the receiving PVP office(s). In the case of regional mechanism (e-PVP Asia), only one form is completed and the application data is distributed to the designated PVP offices; 3. the encrypted application data as well as the related metadata is recorded by the receiving PVP office; 4. the transaction ID is created on the chain; 5. the PVP office acknowledges receipt of the application (optional); 6. the PVP office reviews the application and proceeds with any established procedures to check the provided data; 7. data exchange is established between the PVP office and the applicant or the legal representative in case any clarification is needed during the formality and/or denomination/novelty examination phase; 8. the PVP office assigns a filing date and application number and updates the blockchain (before recording the transaction and creating the new entry on the register, the consensus mechanism is activated to validate the mentioned transaction); 9. the PVP office proceeds with the denomination (if not done at step 7), novelty (if not done at step 7) and DUS examination process of the application, if needed; 10. the PVP office provides the applicant or the legal representative with the result of the examination process; 11. the PVP office publishes information concerning PBR applications for grants, proposed and approved denominations, and matters after the grant; 12. where the plant breeder's right is granted, the PVP office provides the plant breeder's right certificate to the IP right owner; and 13. matters after grant: this includes payment of fees for keeping the right in force, renunciation, nullity and cancelation.

Figure 23. Plant breeder's right application



Actors (or stakeholders) interacting in the use case and their role in the use case:

PVP offices	The official national or regional bodies responsible for the management of PVP.
Applicant	The natural or legal person who files an application for PBR with the relevant PVP office. The applicant will become the holder of the plant breeder's right once it is granted upon the conclusion of the application process.
Breeder	The person who bred, or discovered and developed, a variety – the person who is the employer of the aforementioned person or who has commissioned the latter's work, or – the successor in title of the first or second aforementioned person, as the case may be.
Legal representative	The natural or legal person appointed by the breeder and authorized to act on behalf of the breeder.
Receiving PVP office	The PVP office in which the PVP application is filed.

Interactions (general information applicable to other use cases):

Pre-set up	The users (applicants, legal representatives and PVP officers) must set up a WIPO account (with strong authentication options).
Connects application	The users authenticate to the e-PVP modules.
Upload information	When applicants/legal representatives submit their application data using UPOV PRISMA (or other compatible filing system), they instantiate the blockchain and upload the information related to their application including the attachments. During the grant process, PVP offices upload the information related with the grant process. Matters after grant are also covered.
Hash creation	A unique hash of the files is generated.
Fulfill information	The applicant/legal representative fills out the requested information with the data as well as any required attachments.

Transaction creation	The transaction will consist of the hash, the required information, plus any metadata requested by the blockchain protocol, as well as any user metadata considered appropriate (local clock time-stamp).
Registration in the blockchain	A blockchain client registers the signed transaction on the blockchain.
Time-stamping	The blockchain creates a new block with the transaction. The time-stamp of the blockchain block will be the official time-stamp, any local clock metadata will also be considered valid according to the origin of trust of the signer.
Proof token	The application generates a proof token with the transaction data to the participant.
Receive the data	The relevant PVP offices receive the notification in their accounts with the new data exchanged and can access it.
Update the information	The relevant PVP offices and the applicants/legal representatives can exchange as much information as they need with a new transaction.
Upload proof token and file to verify	The viewers (i.e., any entity wishing to access the public data, e.g., Pluto Digital users) can use the proof token (transaction receipt) to fetch the transaction data from the blockchain.
Verification	The e-PVP module compares the locally computed hash with the hash registered on the blockchain. It also checks the time-stamp returned by the block containing the transaction and (optionally) the time-stamp in the transaction metadata. It also checks that the signer (i.e., the entity that triggers the data exchange through the e-PVP module) was valid at the time of sending the transaction (this requires a parallel register not described in this document). If all checks pass, the verification is valid.

Key data (general information applicable to other use cases):

Documents	The encrypted information to be shared in different formats (documents, images).
Metadata	The metadata related to the shared information (application number, applicant data, denomination, filing date, etc.).
Hash	The result of the hash algorithm processing of the document.
Transaction	The order to be submitted to the blockchain containing the hash plus the metadata.
Signed transaction	The transaction once signed by the entity that triggers the data exchange through the e-PVP module.
Cryptographic parameters	The set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing.
Participant's information	The data shared between the PVP office and the applicant/representative related to the application.

Blockchain technical maturity	Basic: some conceptual definition or analysis has been done by UPOV in the context of e-PVP Asia. E-PVP is a platform for creating distributed registers under development by UPOV on top of the Hyperledger platform.
Blockchain technical complexity	High: complex technical development due to the fact that there is no reference in the market of real use cases.

Type of blockchain implementation

Blockchain type	Pros	Cons
Private permissioned	e-PVP requires first a well-defined, controlled and monitored identity system, not available in public networks, as well as strict governance rules that need to be defined by a central institution. Allows fast synchronization of nodes and a high number of transactions per second.	Requires the deployment and maintenance of a custom infrastructure. Blockchain implementation matters: in the beginning, UPOV is the entity responsible for running the blockchain nodes; in the future, this responsibility will be shared with other authorities.

Legal assessment

The use of e-PVP modules, including the technology for their deployment (e.g., blockchain) is optional and the use by the participating UPOV members is done in accordance with their applicable legislation. Therefore, e-PVP modules are used to report decisions in a digital way and do not interfere in the way the decision is taken or its contents. This is valid in all steps during the examination process and after grant.

E-PVP modules are a set of services provided to facilitate communication, access to and implementation of decisions including any related evidence.

Challenges and considerations

It is crucial for the PVP system to ensure that the identity of the different actors involved in a potential e-PVP is trustable to ensure the authenticity of the ownership of the plant breeder's rights.

Interoperability between blockchain initiatives is another important matter to be addressed at an early stage (e.g., authorities, interested in using blockchain technology, administer other intellectual property rights in addition to PBR).

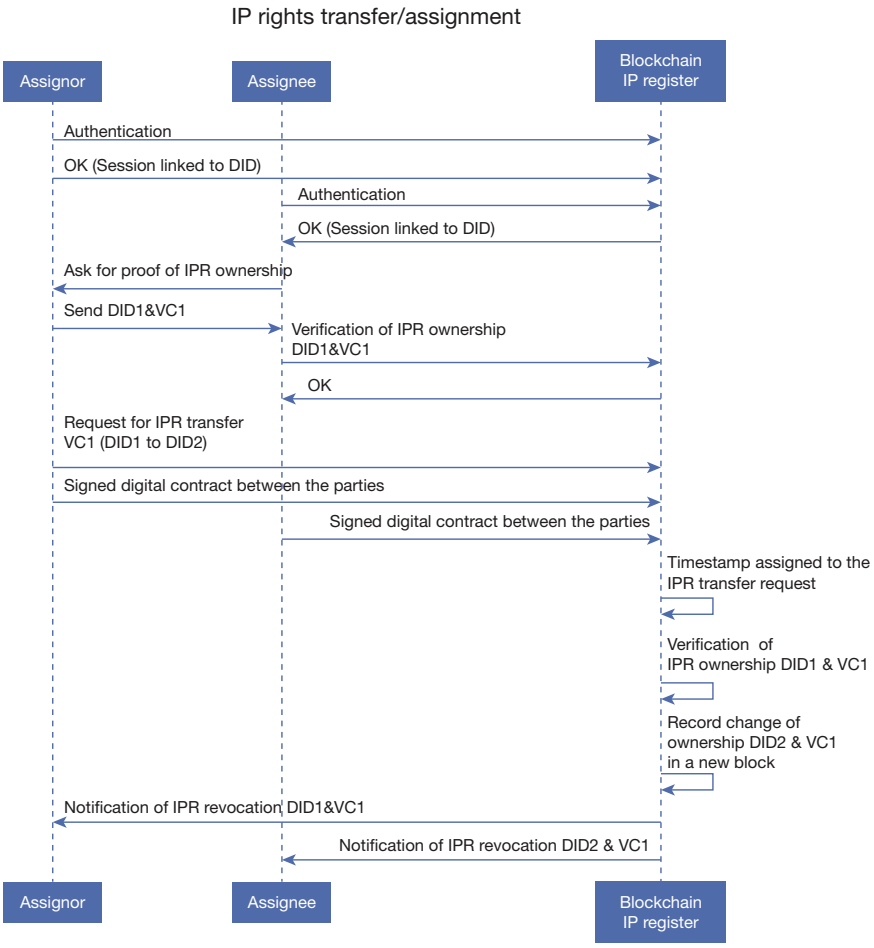
12. IP rights transfer/assignment

Topic	IP rights transfer/assignment
Summary	The transfer of IP rights, known as IP assignment, is the change of ownership of the IP rights from the ownership (the assignor) to another party (the assignee) who becomes the new owner of the IP right. For a transfer of rights to be managed by an IP office, written evidence of the agreement signed by the parties has to be delivered, which will be reviewed by the IP office, and if there are no deficiencies, the transfer will be recorded in the office's register with effect from the date on which the request, the supporting evidence or the fee was paid, whichever is the latest. Before starting the transfer of rights, the parties sign a non-disclosure agreement to ensure the confidentiality of the information shared. This agreement is beneficial for both parties because during the Negotiation phase most probably the assignee will need to perform an IP due diligence, accessing confidential information to ensure the ownership of the IP right, which must be protected to avoid any kind of data leak, even though the assignment may not be reached in the end. Blockchain has the potential to support both parties involved in the process: • making the evidence of the agreement clearer between the assignee and the assignor for the transfer of the IP right; • time-stamping the change of ownership of the transferred IP right; and • exchanging all encrypted data between the parties in the blockchain and tracing the access to this data to avoid any potential data leak.
Relevant IP value chain phases	This use case is related to the IP Right Management phase for all the patents, trademarks, industrial designs and copyright that can benefit from another supportive horizontal use case – capabilities like time-stamping, trust data sharing and digital identity.
Business rationale	IP rights transfer is one of the most basic and fundamental capabilities in IP rights management. After the application for an IP right, during the examination phase or once the right has been granted, the owner of the IP application or IP right may transfer ownership to another party. This change should be performed through the IP register, which would verify the authenticity of the parties and the IP asset ownership. The current systems require many human interventions, which are time-consuming and in many cases require IP professional advice that makes the process more expensive. Besides that, the parties will exchange confidential data before the acquisition, and protection measures are needed to avoid losing strategic information. Before requesting the transfer of IP rights to the IP register, the assignee may be interested in performing an IP due diligence to verify the validity and the ownership of the IP rights or the legal requirements concerning the assignment of the IP rights concerned. This activity needs information related to the rights, which could include prior assignment agreements, employment contracts, status of the registration and the record history, something that currently obliges the IP right holder to have all the information securely stored and when it is shared, the information is out of the control of the assignee. The tool that the parties are currently using to protect the confidentiality of the data is the written signature of a non-disclosure agreement between the parties.

	Other problems with the current IPR transfer processes are related to the fact that many IP offices, to proceed with the IP rights transfer, need a written contract or document signed by both parties, otherwise the agreement is invalid and non-binding. Here is where blockchain could improve the process using digital identity mechanisms. The application number or registration number should be clearly indicated in the agreement. To proceed with the registration of the IP right transfer, some IP offices require the assignee to register the new ownership, otherwise they may lose the transferred rights; this is how the time-stamping feature plays a key role in using blockchain in the IP transfer process.
Potential solution	The potential solution will be a distributed platform based on blockchain technology, a single place where the different IP owners and customers can identify and manage their own digital identity to make the different IPR transactions. The trust via blockchain enables new agile ways to transact with IPR, with public smart contracts that can manage the transaction clauses in a transparent, automated and auditable way. The system will allow for tracking and checking the end-to-end life cycle of the IP rights, and smart contracts can be used for compliance verification.
Blockchain rationale	Many of the transfer or assignment processes could be improved by recording all the data related to the IP right in the blockchain as well as the transactions performed with the data. Having the records of relevant data will allow the assignor to grant access to the assignee to perform their IP due diligence without the necessity to send any information on paper or even to exchange data in a non-protected way. Blockchain can streamline the validity process of an assignment in providing various features, for example, the validity of IP ownership, identification of the parties to the assignment (assignor and assignee), digital signature and time-stamping of documents. In addition, all the activities performed with the data can be traced and stored in the blockchain, giving the IP right holder another tool to protect the confidential data. Using blockchain technology may allow: • protection against unauthorized access to the database (e.g., cryptographic protection); • use of smart contracts to automate processes; • traceability of the transfer of IPRs that streamlines audit processes; • a platform providing an IPR marketplace without the need for traditional intermediaries; • selection of IPR and drawing up an offer; • finding a buyer; • automatic generation of application; and • record of ownership change in the state register. In this use case the blockchain will be used as the distributed ledger where the different IP assets are registered. Every transfer will be made through a blockchain transaction that will change the status of ownership of the IPR. Smart contracts can be used to automate certain processes such as the verification of the compliance or the generation of an application to register the change in IP ownership.

Potential outcome	A new platform that improves the IPR transfer or assignment process and facilitates the procedures to IPR holders and potential assignees with less manual work and time spent in sending and certificating different information. With full data transparency for audit and supervision executed by companies and users. And an opportunity for both assignor and assignee to conduct reliable operations, sign a deal on IPRs transfer and then verify the deal at the IP register online in almost real time and without the need to spend a great amount of resources and time.
User stories	**Transfer/assignment of IP rights** To transfer an IP asset, the owner should register it in the IP register, for example, an IPO's register, as explained in Use Case III. IP Register. For this registration process, the verifiable credential (VC1) will be linked to the assignor DID, which will serve as a proof of ownership. The assignor DID and the VC1 will be used alongside both the assignee and the IP office to verify the ownership of the IPR. 1. the assignor authenticates into the service; 2. the assignee authenticates into the service: 3. the assignee requests that the assignor provide the proof of ownership (DID1 and VC1); 4. the assignor provides the ownership proof, which should be verified against the data stored in the IP registry, for example, the IP office; 5. the assignee verifies the IP asset ownership in the IP register; 6. the assignor makes a request to the IP office for a change of IPR ownership. This request is composed by the DID1, VC1 and the smart contract signed by both parties; 7. the IP registry time-stamps the request for the IPR transfer and verifies the IPR ownership in the IP register (DID1 and VC1); 8. the IP registry records the ownership transfer into the IP register and confirms the new assignment to the parties; and 9. the IP register issues a new ownership certificate to the assignee. *[Notes: The assignor and assignee can use the same protocol to exchange secure information, for example, a written contract or document, which must be signed by both parties. The hash of the contract can then be recorded on the blockchain as the record of the change of ownership in the IP registry. For example, https://github.com/hyperledger/aries-rfcs/tree/master/features/0160-connection-protocol]*

Figure 24. IP rights transfer/assignment



Actors (or stakeholders) interacting in the use case and their role in the use case:

Assignor	The owner of the IPR aiming to transfer it to the assignee. The assignor will exchange information with the assignee and the IP register to prove the ownership of the IPR.
Assignee	The purchaser of the IPR, who tracks the IP assets to verify their ownership and will be notified with the change of the ownership at the end of the process by the IP register. The assignee verifies the ownership of the IP assets through the DID1 and VC1 against the IP register.
IP register	The blockchain network where the IPRs are recorded and where the assignment will be managed. The IP register will be in charge of the verification of the parties involved in the commercial transaction, and the ownership of IPRs as well as the notification to the parties at the end of the process.

Activities or interaction or transaction

Pre-set up	The actors must set up a wallet (if signature is not delegated to the time-stamping service) containing its private key. This wallet can be a hardware wallet, a file protected by password or a remote service-providing signature.
Connection to application	The user authenticates to the time-stamping service establishing a new session.
Registration of an IPR	The owner registers an IPR in the platform, a unique digital identifier is generated for the IPR and is linked to the owner identity, the owner receives a proof of ownership, which can be shared with potential customers.
Proof of ownership	The customer logs in to the system and checks if the owner is the legitimate owner of the IPR that they want to purchase.
IPR transfer	The owner or a logistic entity transfers the IPR from the owner to the customer, a blockchain transaction is generated and the ownership of the IPR asset is changed.
Audit	A third party can see the different transferences on an IPR and checks all the operations were made in the right way.

Key data (general information applicable to other use cases):

IP right data	The IP identification, IP right information, customer identifiers and IPRs transfer status.
Product data	The product information.
Customer data	The customer information.
Supply data	The event, entity and documents.

Blockchain technical maturity

Optimization: already existing in the production environment.

Blockchain technical complexity

Medium: some uncertainty on the implementation needed and some components (Identity) need to be designed from scratch.

Type of blockchain implementation

Blockchain type	Pros	Cons
Private permissioned (IBFT)	IP right transfer requires first a well-defined, controlled and monitored identity system, not available in public networks, as well as strict governance rules that need to be defined by a central institution. Allows fast synchronization of nodes.	Requires the deployment and maintenance of a custom infrastructure. To avoid governance issues, governance rules should be clearly agreed between all network participants.

Legal assessment

The legal requirements regarding the necessity to send written and signed proof of agreements in the IP transfers must be checked for each type of IPR concerned. In some countries, for example, the law may require a written form for the assignment of a trademark, but not for the assignment of copyright.

Challenges and risks of using blockchain

Technical challenges regarding regulations, to accept the smart contracts between the assignor and the assignee as evidence of the commercial transaction, and business challenges of adopting the technology for the use case.

References and contact information

European IPR Helpdesk (2013). *Fact Sheet Commercialising Intellectual Property: Assignment agreement.* September. www.iprhelpdesk.eu/sites/default/files/newsdocuments/Assignment_Agreements_0.pdf

13. IP licensing

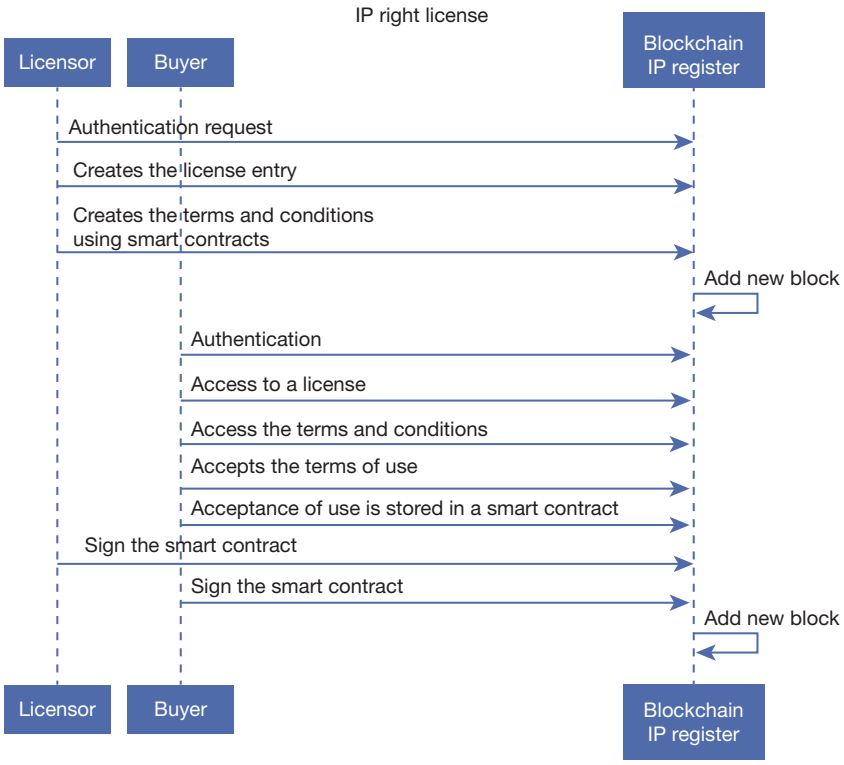
Topic	IP licensing
Summary	A license is a consent by the owner of IP (licensor) to the use of that IP by another party (licensee) in exchange for money or other value (e.g., cross-license). There may be more than one licensor or more than one licensee in a license agreement. The management and licensing of the different IPRs is crucial to the success of a company's business. For instance, in the context of copyright, licenses are signed by the creative work owner and the CMO or the final user. Each license includes contractual information related to the licensed content, who may use the IP right and under what conditions, the duration and the termination of the agreement and the economic conditions. Real-time tracking of all the events concerning the use of an IPR-protected product, requires the identification of the parties as well as the ownership of creative works and will allow: • the calculation of the payment based on the use; • a reduction of the necessity of conventional auditing of the use; and • automatic termination of the contract in case of breach of terms.
Relevant IP value chain phases	Vertical use case mainly focused on the Commercialization phase, in particular in the process in which the licenses are granted and managed. The use case is also related to time-stamping.
Business rationale	One of the main current IPR issues is the lack of protection in the digital environment. Blockchain can provide trustable information in matters of ownership, licensing and the tracking of the usage of the digital content. Thus, it might prove beneficial for a fairer compensation of authors. Blockchain could bring a secure, reliable and scalable distributed transaction processing to licensing works. It could introduce traceable and verifiable ownership and an accurate distribution of royalties, allowing the possibility to pay directly to the right holders, reducing or even eliminating the use of intermediaries. Blockchain may allow creators or collectors to document and verify the authenticity of digital content to secure their commercial value. This use case aims to identify a scenario where the IPR holder is able to directly manage in an automated way a transparent, fair and immediate licensing of their IPRs (i.e., less transaction costs). Furthermore, the use of blockchain might not just benefit one side (the IPR holder) but also the other side (the licensee), as in some instances the licensee will benefit from a more accurate and transparent licensing process.
Potential solution	Creating a secure and traceable register of licenses of creative works in which the terms and conditions of use are stored and may be used to grant certificates of trust between the IP right owner to the CMOs authorizing them for the commercialization of creations, and the subsequent public exposure by the licensees, ensuring the immutability of the content for each user.

	The register by means of a smart contract might be able to automatically enforce clauses that are raised under agreed and transparent circumstances: payments, revocations of licenses, renovation of licenses, etc.
Blockchain rationale	Blockchain technology can be used as a tool to manage and store IP licenses on a decentralized ledger, which can easily track the status and the use of protected work. Blockchain offers trust, accountability and transparency allowing to check whether the license is valid or to manage the clauses related to the correct use of the license. Blockchain ledgers are time-stamped immutable records suitable for storing licenses and related information. Smart contracts might prove useful in automating the execution and enforcement of licensing terms. A consequence could be the reduction of the number of intermediaries involved in the commercialization of creative works. Smart contracts will help CMOs to manage digital rights and to allocate shares to the different contributors, permitting the payment of creators in a more open and transparent way.
Potential outcome	This blockchain system should allow for the management and tracking of the licensing process and the use of licenses with: • easy management of license use; • automatic revocation and payment procedures; • transparency in the licensing process and terms and conditions; • possible traceability of the use of the license; and • less intermediaries.

User stories

How can a licensor register a license in the system to grant its use?

Figure 25. IP right license



1. the licensor creates the license entry in the system;
2. the licensor creates the terms and conditions using smart contracts; and
3. the license is ready to be accepted by a licensee.

For a licensee to access the IPR, they can accept the terms of use and get the license as follows:

1. the licensee can access a license already existing in the system;
2. the licensee can access the terms and conditions of use;
3. the licensee accepts the terms of use for using the license; and
4. the licensee gets permission to use the protected material by the IPR.

Automatic revocation of a license

1. The system checks when the terms and conditions are not met or the license can be revoked. In a blockchain license system, the check should be implemented by oracles in charge of communicating events to the smart contract so as to trigger it if anything is altered (e.g., unauthorized sub-license).
2. When the conditions for expiration or revocation are met, the license is automatically revoked.

Note: The status of the license can be checked anytime by the licensor or the licensee. In case of dispute, an arbitrator can be appointed to resolve the terms.

Actors (or stakeholders) interacting in the use case and their role in the use case:

Licensor	The user holding IPRs.
Licensee	The user accessing the IPRs by means of a license.

Interactions (general information applicable to other use cases):

Pre-set up	The registrar must set up a wallet (if signature is not delegated to the time-stamping service) containing its private key. This wallet can be a hardware wallet, a file protected by password or a remote service providing signature.
Connects application	The user authenticates to the time-stamping service establishing a new session.
Hash creation	A unique hash of the file is generated.
Transaction creation	The transaction will consist of the hash, plus any metadata requested by the blockchain protocol, as well as any user metadata considered appropriate (local clock time-stamp).
Registration in the blockchain	A blockchain client registers the signed transaction on the blockchain.
Time-stamping	The blockchain creates a new block with the transaction. The time-stamp of the blockchain block will be the official time-stamp, any local clock metadata will also be considered valid according to the origin of trust of the signer.
Proof token	The application generates a proof token with the transaction data.
Upload proof token and file to verify	The relying party uses the proof token (transaction receipt) to fetch the transaction data from the blockchain.
Verification	The relying party's local application compares the locally computed hash with the hash registered on the blockchain. It also checks the time-stamp returned by the block containing the transaction and (optionally) the time-stamp in the transaction metadata. It also checks that the signer was valid when performing the transaction (this requires a parallel registry not described in this document). If all checks pass, the verification is valid.

Key data (general information applicable to other use cases):

Document	The original data to be time-stamped.
Metadata	The metadata related to the documents, to a time-stamp or to the time-stamp process.
Hash	The result of the hash algorithm processing of the document.
Transaction	The order to be submitted to the blockchain containing the hash plus the metadata.
Signed transaction	The transaction once signed by the registrar or the delegated service.
Cryptographic parameters	The set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing.
Register's information	The register's information.

Blockchain technical maturity

Advanced: several proofs of concept are, or a real project is, being developed.

Blockchain technical complexity

Medium: some uncertainty on the implementation needed and some components (digital identity) need to be designed from scratch.

Type of blockchain implementation

Blockchain type	Pros	Cons
Private permissioned (IBFT)	IP licensing management requires firstly a well-defined, controlled and monitored identity system not available in public networks as well as strict governance rules that need to be defined by a central institution. Allows fast synchronization of nodes.	Requires the deployment and maintenance of a custom infrastructure. To avoid governance issues, governance rules should be clearly agreed upon between all network participants.

Legal assessment

–

Challenges and risks of using blockchain	Possible regulatory challenges for the licensing cross-countries. Possible legal challenges using smart contracts to reflect the terms of use when a dispute arrives. Technical challenges related to the implementation of smart contracts for the license agreement, etc.
References and contact information	CEDro (n.d.). Cedro: Para las licencias de uso. https://citymis.co/cedro/guides/blockchain/certificado ConsenSys Mesh (n.d.). About ConsenSys Mesh. https://ujomusic.com

Notes

1. eIDAS Regulation (2014). https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014
2. See definition at https://consensys.net/blog/enterprise-blockchain/scaling-consensus-for-enterprise-explaining-the-ibft-algorithm/
3. Europa (n.d.). European Blockchain Partnership. https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership
4. https://www.epa.ee/en/general-info/requirements-documents-related-application-its-processing-and-registrations-filed-e
5. https://e-estonia.com/solutions/security-and-safety
6. https://guardtime.com/vaccineguard
7. European Union Intellectual Property Office (2019). Report on the EU Enforcement of Intellectual Property Rights: Results at the EU borders and in Member States 2013–2017. September. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Report_on_Enforcement_of_IPR_at_EU_borders_and_in_MS_2013_2017/2019_Report_on_enforcement_of_IPR_at_EU_borders_and_in_MS_2013_2017_Full_en.pdf

Annex IV
Mockup – decentralized identifiers

Blockchain white paper mock-up

This document is prepared for the mock-up of the Blockchain White Paper as an example to explain how blockchain technology could be used to address one of the long-standing issues in identifying an actor or a participant in IP ecosystems at the global level.

I. Self-sovereign identities and decentralized identifiers

An identity, which corresponds to an entity or an individual, consists of attributes and/or identifiers. This mock-up has been built around the concept of using decentralized identifiers of a legal entity or an individual to demonstrate the suitability of blockchain-based technologies for the use of identifiers in the life cycle of an IP asset.

By using a self-sovereign identity (SSI), the owner of the identity can fully and without intervention from an outside governing body use and manage such identity. The owner of the identity has full control over his verifiable credentials (VC) and how his personal data is made available and used. The solution provides the means to generate, store and control identity information of an individual – namely, a natural person – or another legal entity such as an institution or enterprise.

However, within the context of this mock-up, the objective is to use a subset of these capabilities and to ensure that the user has a globally unique digital identifier, controlled by a centralized body (e.g., WIPO) within a permissioned blockchain network. The centralized body acts as the coordinator of the blockchain and manages access permissions to it. Further details on how the unique digital identifier can be created and used as well as its potential implications are explained below in the Section II Mock-Up Business Case.

For a user to own and control their identifier, it needs to be issued by an issuing body. This issuer is a trusted body, also known as the claim issuer.[1] In the context of this mock-up, a centralized body, namely, WIPO, will attribute the user a globally unique identifier, trusting the user. The participating parties, for example, IP offices (IPOs) and applicants, need to trust the identifier issued by the claim issuers, for example, WIPO and IPOs, whereby such an identifier can be verified within a blockchain network.

Decentralized identifiers (DIDs), implemented via blockchain, enable a verifiable decentralized identity (credentials) to allow an object – defined by the owner of the identity – (person, company, abstract identity, etc.) to be identified.

Examples of DIDs could be the following:

DID	Remarks
did:btc:1d7faChpbnbpP Jd9Xu5kd4J7qhRnLz6FZ	subject managed in a Bitcoin blockchain
did:ontology:1234567 89abcdefghi	subject managed in an Ontology blockchain
did:ldap:user1234	subject managed in an LDAP (lightweight) directory
did:custom:user1234	subject managed by custom system (internal database, etc.)

DIDs allow the decoupling of the identity from centralized registries, identity providers and certification authorities, while still retaining their services. Additionally, DIDs enable personas and companies to trust a system that generates globally unique identifiers and authenticates such identifiers using digital and cryptographic proofs based on, for example, digital signatures and biometrics.

The creation of a verifiable identity and the verification thereof implies three types of personas, namely the Holder, the Issuer and the Verifier. These three personas interact with each other within a decentralized blockchain implementation system.

The following process is implemented within a distributed blockchain representing decentralized identities. The Holder is the owner of objects that must be identifiable by the interested party. They therefore request an Issuer to issue a signed claim to the Holder. The Holder, on their part, will on-demand allow the Verifier to access the claim issued by the Issuer. It might be necessary to provide a sign-in password to grant access to the claim payload or just to provide the Verifier with a one-time password to some external storage where the claim is being stored.

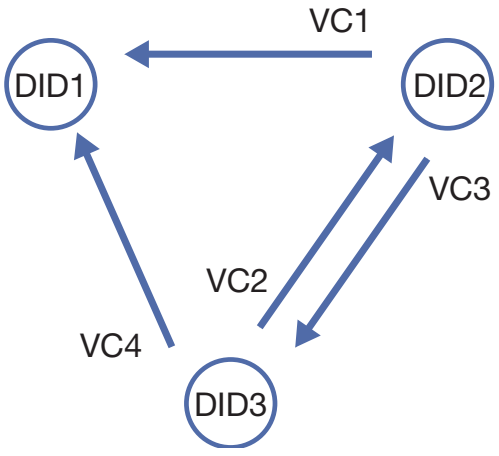
A DID is associated with a public key/private key pair that allows the owner to protect its identifier and to use this key pair to send a signed VC to another subject. The receiver uses the sender's public key to verify that the sending is legitimate. The DIDs will be kept in a digital wallet controlled by the Holder. Such a wallet can be kept by the owner in safe storage or they can alternatively decide to have an external party securely store it on their behalf.

Verifiable credentials

Once a DID identity has been established, VCs can be created and managed in a decentralized way. We might think of a VC as the equivalent of a driver's license, passport, ID card, etc. However, the main difference with traditional credentials is that DIDs can create VCs against other DIDs, creating a graph/vector of linked VCs. As VCs are agnostic of the underlying credential storage or transport, this effectively allows for an on-demand disclosure of the identity's credentials in a self-controlled manner, in compliance with existing or future regulations. Figure 26 illustrates the relationship between DIDs and VCs. The effective identity of a natural person or a legal entity such as an enterprise and organization, which could be identified by a DID, is the sum of the VCs pointing to the DID of the natural person or legal entity. Note that VCs can also include information that can be claimed by the owner of the DID (e.g., ownership of an item or asset).

The diagram shows DID1's identity being identified by DID2 via a verifiable credential VC1, with VC2 as the verifiable credential provided by DID3. DID2 and DID3 have paired credentials set up. Each of the VCs provides specific objects that complete the identity of DID1.

Figure 26. Relationship between DIDs and VCs



The DIDs and VCs model enables a governance model that is agnostic of the underlying objects, giving a high degree of flexibility in the choice of blockchain implementation, namely, for permissioned or permissionless ledgers and for users' freedom in creating DIDs and VCs.

Therefore, DIDs and VCs are neutral to the final identity governance model, allowing involved parties to decide by whom DIDs and VCs can be created and managed (or in what circumstances and what types of VCs should be created). For example, in a public permissionless blockchain network, most participants are expected to be free to create their own DIDs and VCs at will, whereas, in a public-permissioned or private blockchain, a certain degree of control by central actors managing the infrastructure will apply.

DID use cases and degree of adoption

Many different active projects exist. The DID Method Registry[2] includes more than 75 compatible implementations, most of them based on Ethereum and Bitcoin public networks.

Microsoft has published white papers on DID and is actively participating in the creation of an open-source blockchain solution within its Azure service platform. This includes a blockchain-based royalty remuneration system within their Xbox gaming ecosystem.

Other important projects using their own underlying blockchain technology include Sovrin (based on Indy tech stack), Ontology (based on the Ontology network), Tangle ID (based on IOTA) and Gataca (offering support for different underlying blockchain technologies – Ethereum, Fabric and derivates). Initiatives in the identity standardization field, such as Identity Foundation, have also opted for a W3C DID approach. Identity Foundation's current work targets mostly Ethereum and Bitcoin stacks as well as Sidetree (blockchain/ledger agnostic DID scaling protocol), according to Github activity.[3]

II. Mock-up business case

One of the long-standing issues in the IP community is whether it is possible to use an identity that is verifiable by participants across systems at national, regional and international levels. DIDs

could be a potential model for addressing the long-standing issue of applicant name standardization in IP ecosystems.

There are multiple ongoing projects that are working on DIDs based on blockchain along with different technologies and protocols. There are some wallets that already allow the user to manage Identities and DIDs from different blockchain networks. However, it is still not possible to use a credential issued in one blockchain network to make a presentation to an agent in a different network. Legal and functional agreements should be made between the standardization groups from different ecosystems to work together and go beyond the strictly technical challenges. This would enable full interoperability of VCs and DIDs between different Blockchain networks.

Due to the above reasons the mock-up assumes that all IP offices will participate in a common blockchain-based DID network (called hereafter "WIPO BC network"). In this way, all the offices will be able to register and see information in the blockchain, issue VCs and DIDs, and verify DIDs and VCs issued by other offices.

Several technical challenges will need to be overcome to turn the following mock-up use cases into a widely accepted solution. There are commonly recognized challenges, including:

- interoperability among multiple blockchain solutions that also use DIDs addressing trust and interoperability requirements;
- scalability, sustainability and operational transaction costs of blockchain technology, specifically computing power, energy consumption;
- usability of blockchain systems and digital wallets (essentially a secure central service for maintaining keys);
- internationally coherent legal recognition of blockchain transactions within national and regional legal systems, namely, regarding the legal standing of DIDs.

Introduction to the mock-up

The objective of the mock-up is to illustrate the potential use, benefits and challenges of a DID model based on blockchain technology. To this end, the different phases of the IP value chain have been covered in this model. There are several user stories designed to create a small journey in which it is explained how the DID of a natural person or legal entity could be used for protecting, managing and commercializing IP assets:

- during the Generation phase, an inventor registers his own "Lab Notes" and related research data before applying for a patent;
- during the Protection phase, an applicant files an international patent application for two countries where the application is evaluated by a competent authority to grant the patent;
- during the Management phase, a patent owner could consider the transfer of ownership of his patent; and
- during the Commercialization phase, a patent can be licensed to other parties.

Additionally, user stories illustrate how a new global unique DID is assigned to an actor, be it an applicant, inventor or legal representative, and how the management of the DID is done.

The mock-up reflects the usage of a public-permissioned approach in which all participants will have access to:

- all VCs (claims that a natural person or a legal entity makes over other subjects, both identified with a DID);
- all registered identities;
- a permissioned blockchain with the ability to create new or subsets of claims (attributes that will be part of the VC and therefore of the digital identity);
- new identities that are automatically created under the control of competent authorities such as WIPO and IPOs; and
- permissioned access to the blockchain platform through a front-end web application.

The mock-up will show how DIDs and VCs can be used to manage a digital identity. In the context of this mock-up, only competent IP offices and their representatives can act as Issuers of DIDs and manage their life cycle. Verifiable claims can be issued either by IPO staff or IP applicants depending on the use cases. IPO staff will generally have higher freedom to assign VCs to any targeted DID, while IP applicants will be allowed to issue only specific claims, for example, to request the delegation of permissions to another DID.

While not explicitly shown in use cases, the cryptographic artifacts associated with a DID of a natural person or legal entity are stored, protected and managed by WIPO or any competent authority. This is a governance decision, not a technical constraint. W3C DIDs and VCs standards do not require it. The reference architecture explains in more detail the complexity of secret storage and management and why in practice applicants are preferably not in charge of secret artifacts, considering that many of them are not security experts and may lack the experience to protect complex cryptographic secrets, such as private keys used for digital signatures.

The management of a real claim payload associated with VCs is left unspecified in the mock-up, considering that, due to compliance with privacy regulation in different jurisdictions, management of private data will be complex and such complexity would make use case flows difficult to illustrate.

Different types of claims can be stored in different encrypted storage systems and protected with different levels of privacy and security. Public-related claims can be directly stored in the blockchain to simplify the management of such data.

The mock-up assumes that a mechanism exists by which communication and integration of different identity systems used in different jurisdictions, regions or countries are established. In reality, this is a technical challenge yet to be overcome.

The mock-up further assumes that it is possible for a user to have multiple identities (duplicates) to use for different purposes and that adequate mechanisms exist to govern this usage, detect and avoid the erroneous or malicious creation and usage of duplicates.

Implementation and use of the mock-up

To use and demonstrate this mock-up, two different users from two different IP offices will be accessing the user interface of the mock-up representing Issuer and Verifier. This implies the necessity of a mock back-end, which will show that credentials are issued by one party and verified by another.

Roles

The following roles will be used within the mock-up:

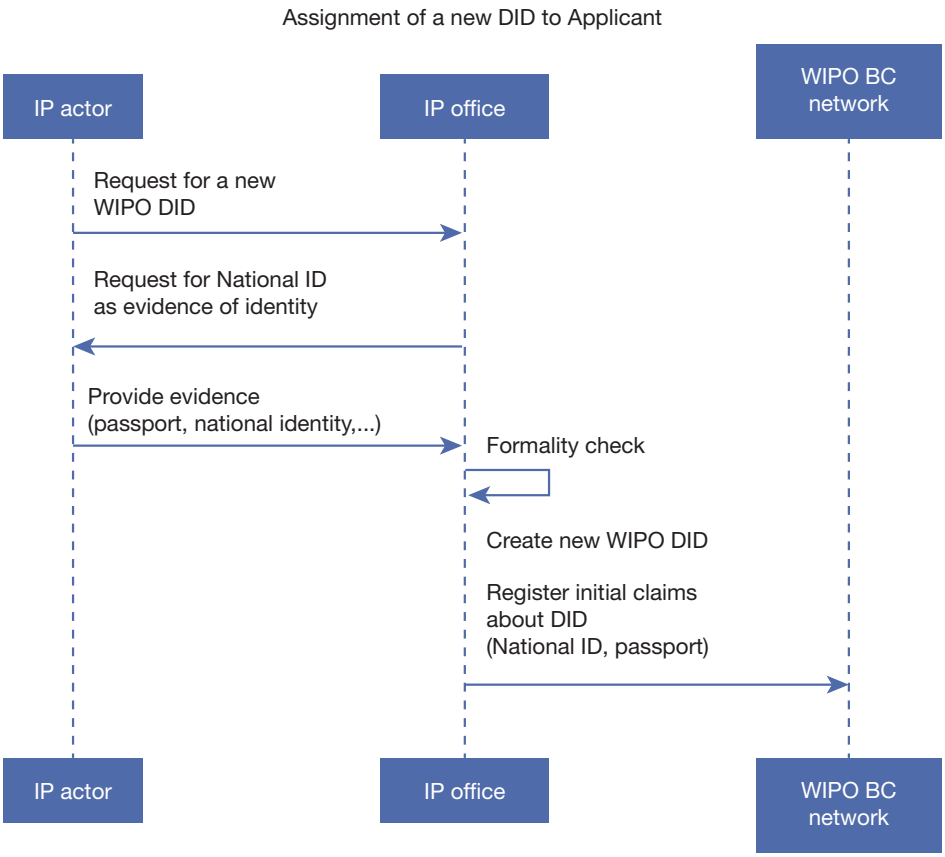
Issuer	WIPO/IB and IP offices
Verifier	Any stakeholders and service providers, including IP offices
Holder	Applicants, IPO staff
Blockchain-based DID network (WIPO BC-network)	Provided by WIPO/IB *[Note that for this mock-up, the BC-network is not based on blockchain, and the behavior of a potential BC DID management system is simulated.]*

User stories related to the assignment and management of DID (USD)

USD1: Issue of a new DID to applicant

Role(s)	Holder: the IP applicant as Holder of a new DID; Issuer: the IP office acting as Issuer of the new DID and WIPO blockchain network.
Background	The applicant wants to obtain a new Digital ID in the WIPO chain (WIPO DID) through an IP office that will allow them to identify themselves in future management tasks within that IP office or any other parties that are in the WIPO blockchain network.
Objective	Upon request, the competent IP office will provide the applicant with a new WIPO DID after appropriate checks. The applicant will be given a new WIPO DID similar to "did:WIPO**:**Name_FamilyName_0x12345..." [*Note: the Name and Family Name are added in the mock-up to provide a more human-readable view of the otherwise numeric and hard to remember WIPO DID.*] Furthermore, the collected information should allow for the detection of unintended duplicates.
Narrative	• the applicant requests a new WIPO DID from the regional IP office; • the IP office requests any suitable information according to national laws to identify the applicant. As for individuals, such information can include a passport, driving license, email, etc. In the case of legal actors representing a corporation, the registration certificate at the commercial registry office and other documents could be requested. *[Note: the required information and procedure should be discussed and agreed for harmonization and standardization under the Governance topic.]*; • the applicant provides all of the requested data; • a set of minimum data is to be agreed upon as part of the governance model (e.g., full name, data regarding birth, email address, company or social security registration, etc.) to allow for detection of the duplicates and to determine under which conditions duplicates may be allowed; • the IP office checks that the applicant is not erroneously duplicated in the IP office database, runs any other necessary tests and sends a request to the WIPO Digital ID System to create and register a new WIPO DID (did:WIPO: ...), adding all known real identity data (identity claims); • the WIPO Digital ID System uses a blockchain that within a short time synchronizes the information (i.e., the new blocks) to all blockchain nodes distributed worldwide; and • existing applications in different IP offices can connect to a blockchain node to get updates on new events of interest (new WIPO DID or VC added) and react accordingly. Non-sensitive data is registered directly on the blockchain, while confidential data is stored off-chain and a corresponding VC pointing to the off-chain storage location is registered on the blockchain.

Figure 27. Assignment of a new DID to applicant



In case a duplicate is found, two possible scenarios are considered:

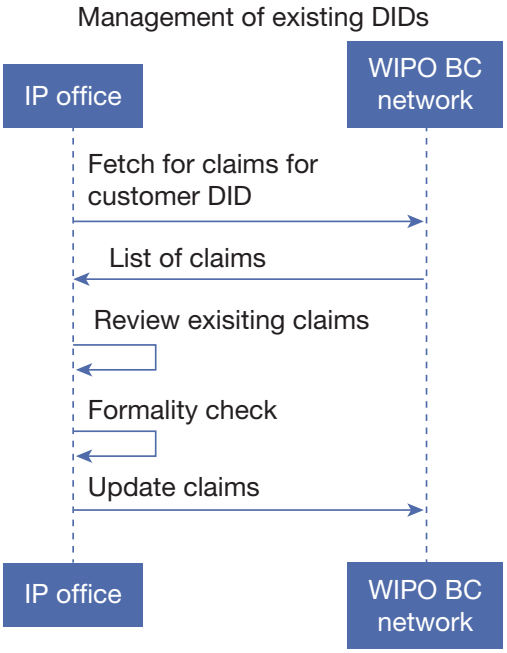
1. A well-intentioned user decides to inform an IP office of their already existing WIPO DID. In that case, the IP office searches for claims related to that WIPO DID to see if the requested information has already been added by another IP office. The user can then create a new claim, duplicating and confirming the same information, or just skip this step if confirmation from the local office is not considered relevant. This scenario should also consider the possibility that the user already owns a WIPO DID but may have forgotten. Moreover, the user may have legitimate reasons (e.g., taxation purposes, etc.) for wanting multiple DIDs and using them for specific purposes (these could be reflected via specific VCs).

2. A malicious user wants to create a different identity for each IP office. In that case, IP offices can perform other necessary tests and further investigate the information provided to discover an existing WIPO DID. If the search returns a positive result (there was already a previously registered DID and the user acted with a potentially malicious intent), the affected IP office will abort the WIPO DID creation flow and will create a claim against an existing WIPO DID, warning about the so-called Byzantine behavior. The other IP offices will then be able to analyze such messages and act appropriately by removing the claims or marking them as tampered/non-valid.

USD2: IP offices' management of existing WIPO DIDs

Role(s)	Holder: the IP applicant as the Holder of a new DID, an IP office as the Issuer of new claims and the WIPO blockchain network.
Background	In case a WIPO DID has already been assigned to a given customer and an update is required, the following can occur: • the customer contacts the IP office requesting a change to some of their claims providing a previously registered WIPO DID; • the IP office runs periodic checks on outdated data after N weeks or months for already assigned WIPO DIDs and takes appropriate actions; • some existing external service provides warnings about potentially updated information (e.g., the legal status of a corporation, providing its Fiscal Identification Number). A search for claims related to the WIPO DID is done and the update is registered (e.g., a search against Fiscal Identification Numbers is done to retrieve the original affected WIPO DIDs and claims involved and the update is registered); and • an IP office detects through an internal process that the identity information associated with a WIPO DID is outdated or invalid and takes appropriate action (e.g., a given claim was registered providing some information about the correct legal status of a corporation; later on the corporation ceases its activity and the claim needs to be updated).
Objective	An IP office wants to update the existing information about a given WIPO DID.
Narrative	• an IP office retrieves the information about a given customer's WIPO DID; • an IP office reviews the data through any established internal process; and • an IP office updates (or create new) claims pointing to the given WIPO DID.

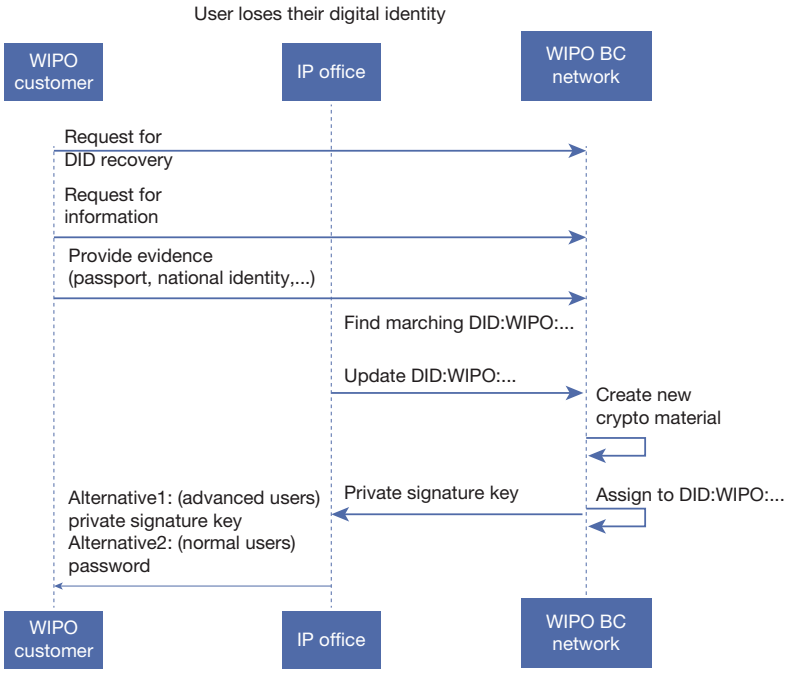
Figure 28. Management of existing DIDs



USD3: A user loses their digital identity

Role(s)	Holder: the IP applicant as the Holder of a new DID1, an IP office as the Verifier and Issuer of new digital artifacts and the WIPO blockchain network
Background	An applicant (natural or legal person) has been assigned a WIPO DID and has some IP rights linked to their WIPO DID. This actor loses the cryptographic secrets that allowed them to identify themselves as the subject associated with a WIPO DID in the identity blockchain.
Objective	An IP applicant, owner of a WIPO DID, wants to recover their WIPO identity.
Narrative	• an IP applicant owning a WIPO DID contacts an IP office where the WIPO DID was created, providing as much information as possible (requested time, passport number, etc.); • WIPO, in a best-effort mode, will try to retrieve the WIPO DID, reset the password to access the front-end web app (for standard users delegating management of blockchain private keys) or associate new public keys to an existing WIPO DID (advanced users or corporations managing private keys on their own); and • the security measures to restore the ID can be extended based on already existing claims for a given WIPO DID; • if a VC has already been assigned to the WIPO DID node, WIPO can request from the user a proof matching the credential. For example, the user can send WIPO the original file associated with a given hash proof.

Figure 29. User loses their digital identity

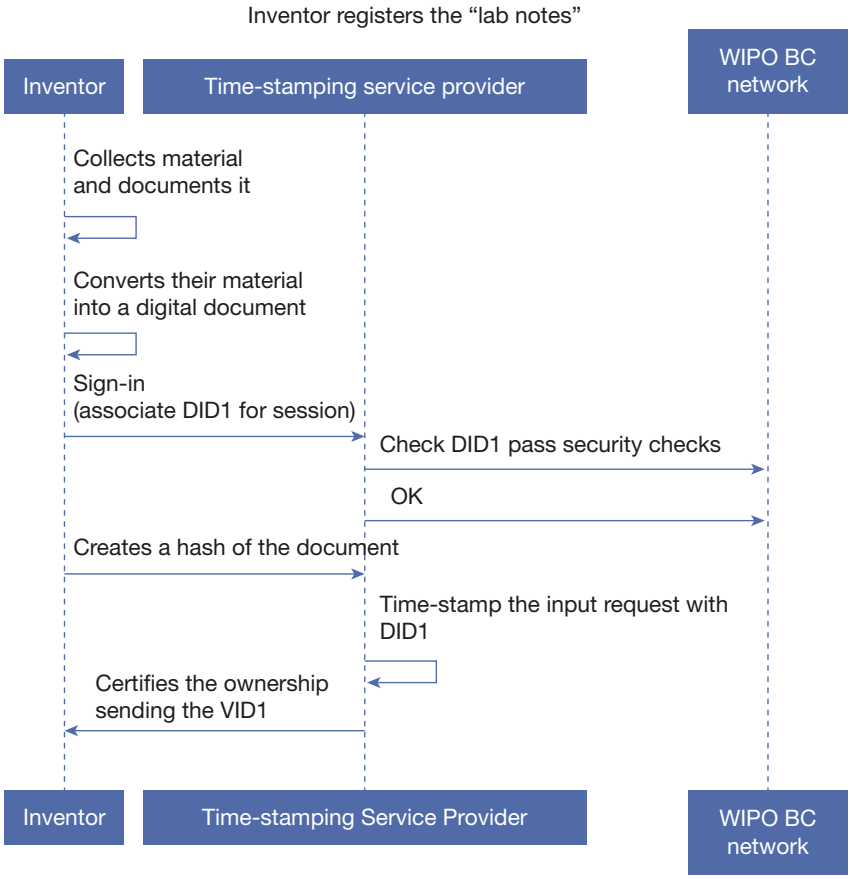


User stories related to patent life cycle (USP)

USP1: Time-stamping on pre-filing data lab notes.

Role(s)	The inventor as the Holder of a current WIPO DID, a time-stamping service provider such as WIPO PROOF as the Verifier of the WIPO DID and the WIPO blockchain network.
Background	An inventor, who has already been assigned a WIPO DID, wants to get time-stamping on a set of data such as “lab notes” or nucleotide or amino acid sequence listings to be used in a future patent application. This data describes the idea and outcome of ideation and experimentation that lead to the intention of patenting. Potentially, the idea may be turned into a trade secret, should patenting not be a possibility. In any case, proof of work on an idea and potential innovation or novelty has been recorded without divulging the content, demonstrating that the inventor is in possession of the idea or trade secret. This is of particular value where “lab notes” or research data are continuously annotated and reannotated. Version management and version verification is therefore particularly important to provide legal certainty from an IP point of view. This is particularly the case, for example, with nucleotide, amino acid sequence data and other characterization data of biological and genetic resource and associated traditional knowledge, as has been addressed by WIPO’s work on GRs and associated traditional knowledge. The recording of a transaction in the blockchain network inherently carries the time-stamp of the time that the transaction was written. This information is part of the immutable log of the ledger.
Objective	The data is turned into a unique hash, registered and/or time-stamped as a reference to the initial intention of filing a patent application, serving as evidence of possession also for further works.
Narrative	• the inventor collects materials (formula, process, research or sequence data, etc.) and documents them for IP assets, for example, a trade secret or a patent; • the inventor transforms the collected materials into a digital form, if needed; • the inventor starts the process of time-stamping with a time-stamping service provider using their WIPO-DID and creates a hash of the documents via the time-stamping service; and • the time-stamping provider registers the hash and time-stamps it on the WIPO Blockchain Network, adding information about the requesting WIPO DID.

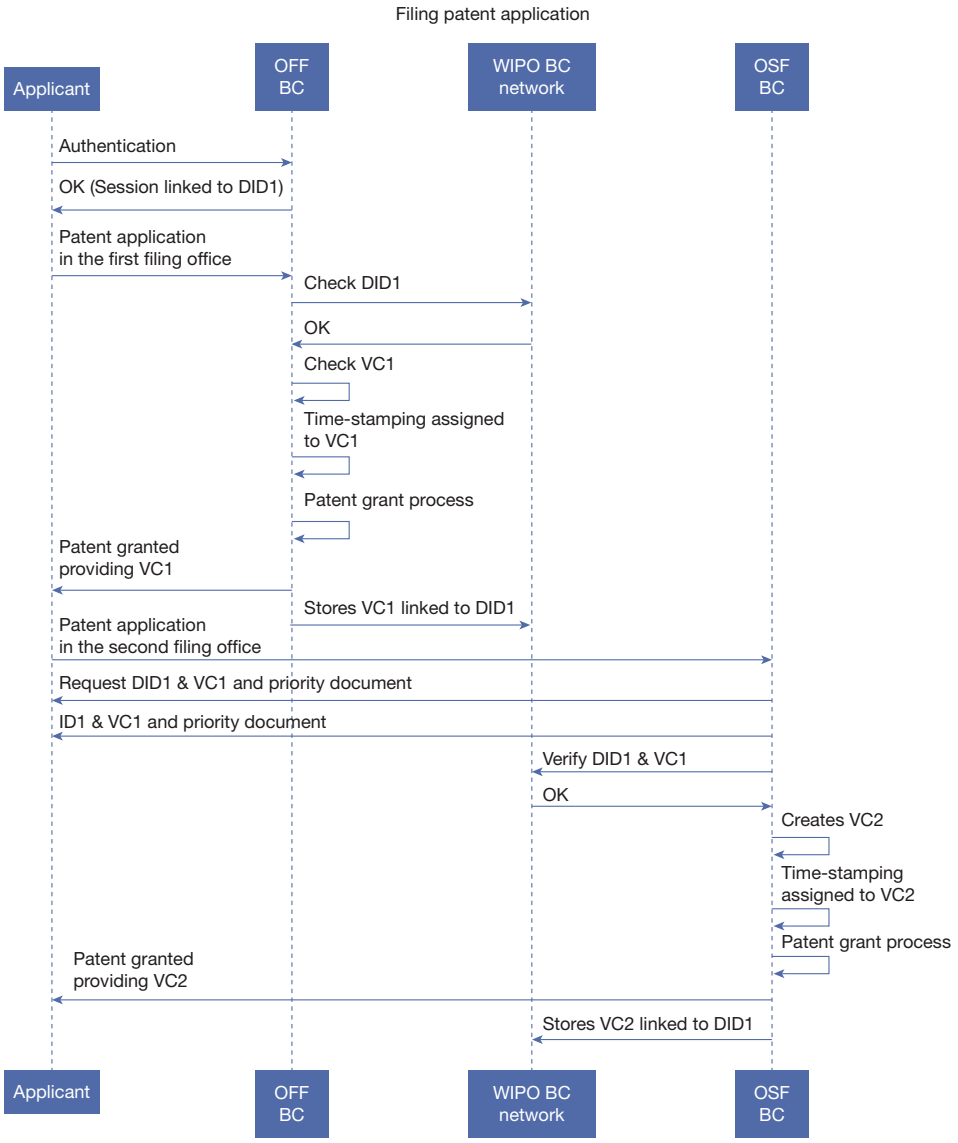
Figure 30. Inventor registers the “lab notes”



USP2: Filing patent application

Role(s)	A patent applicant holding a WIPO DID1, an IP office (holding DID2) as the Verifier of DID2, the WIPO Blockchain Network and another IP office DID3.
Background	The applicant submits a patent application first to an IP office (called the Office of First Filing [OFF]). After the first filing, the applicant submits their application to the other office (called the Office of Second Filing [OSF]) with a priority claim of the first filing. There is a single blockchain network in which the IP offices participate. Each IP office has its own network node through which it interacts in the network. Through this node it has access to a copy of the ledger and the global status of the ledger.
Objective	The applicant will submit the initial patent application to the OFF using an already assigned globally unique WIPO DID1. The OFF (DID2) will proceed with a patent filing process and will inform the outcome of the proceeding to the applicant with the application number and filing date. This process is out of the scope of this mock-up, which is focused on the management of the identities and the verifiable credentials. Based on the result of the filing process with the OFF, the applicant applies for a patent to the OSF (DID3) providing the DID1 and the VC1 and the priority document issued by the OFF. The OFF (DID2) will verify the DID1 and proceed with their patenting filing acceptance process, creating a specifically assigned VC2(id) during the application process using this VC2(id).
Narrative	• the patent applicant logs into the OFF's online front-end and is assigned a session linked to their DID1; • the applicant submits a patent application to the OFF (DID2); • the OFF (DID2) receives a notification of the application; • the OFF checks DID1 in the WIPO BC network; • the OFF (DID2) creates VC1 and a time-stamp is automatically assigned; • the OFF (DID2) proceeds with the formality check process; • the OFF (DID2) sends VC1 to the patent applicant linked to DID1; • the applicant applies for a patent in the OSF (DID3); • the OSF (DID3) asks the patent applicant for the unique tuple DID1 and VC1 and the priority document provided by the OFF; • the OSF (DID3) verifies DID1 and VC1 in the WIPO BC network; • the OSF (DID3) performs their national patent examination and granting process; • the OSF (DID3) creates VC2 for the granted patent at national level; • the OSF (DID3) stores the granted patent data into their national blockchain node; and • the OSF (DID3) sends the VC2 linked to the DID1 to the patent applicant.

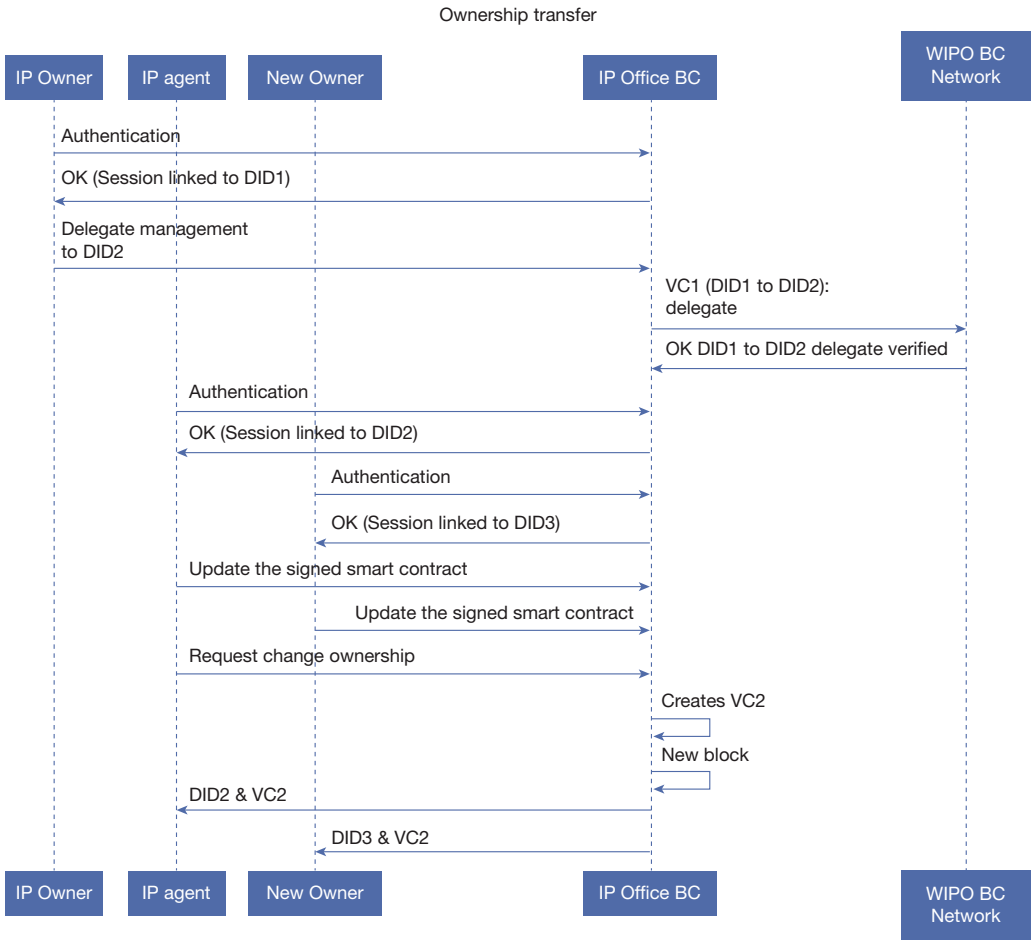
Figure 31. Filing patent application



USP3: Change of ownership of an IP right

Role(s)	The patent owner as the Holder of WIPO DID1, the IP legal representative as the Holder of WIPO DID2, the new patent owner as the Holder of WIPO DID3, the IP office DID as the Verifier of DID and the Issuer of new claims, the blockchain and the WIPO BC network
Background	This user story is applicable to any IP rights, but in this case we will refer to a patent that a patent owner wants to sell (transfer ownership) by delegating an agent.
Objective	The change of ownership of a patent will be registered using a digital contract stored in the blockchain. The two parties store the undersigned smart contract using the WIPO DID and the VC, which facilitate the change of ownership by adding them into the blockchain.
Narrative	• the patent owner logs into the online blockchain front-end app and is assigned a session linked to their WIPO DID1; • the patent owner creates a new entry VC1 DID1→DID2 into the identity system (a new VC) confirming that they delegate its management to an agent identified by WIPO DID2; • the IP agent logs into the online blockchain front-end app linked to their WIPO DID2; • the new patent owner logs into the online blockchain front-end app and is assigned a session linked to their WIPO DID3; • both parties store the undersigned smart contract into the IP office blockchain; • the agent gets in charge of selling the patent to a new owner and then initiates the ownership transfer by requesting that the IP office change the ownership; • the IP office creates VC2 for the transfer of the rights; • the IP office stores the change of ownership into the blockchain; • the IP office sends DID2 and VC2 to the IP agent; and • the IP office sends DID3 and VC2 to the new IP owner.

Figure 32. Ownership transfer

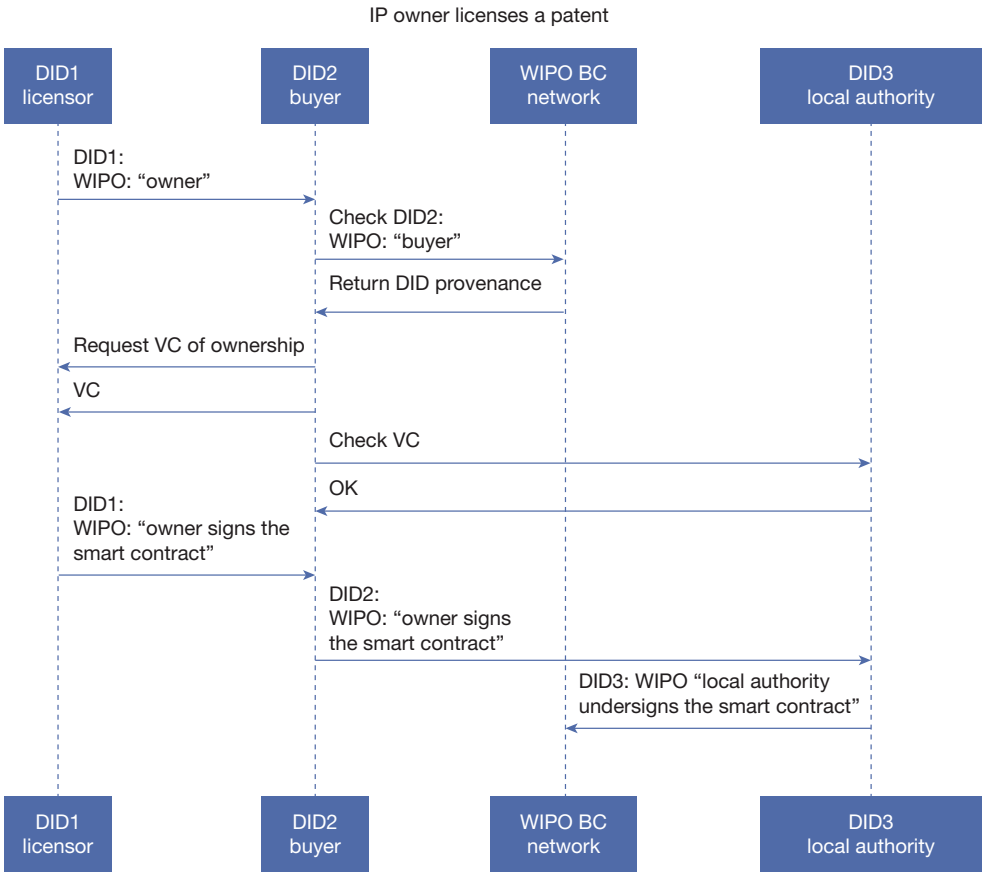


USP4: IP owner licenses a patent

Role(s)	The licensor owns the IP identified by the WIPO DID1 and VCs; the licensee, identified by the WIPO DID2, takes a license on the IP held by the licensor; the WIPO blockchain network verifies the WIPO DIDs and credentials; a competent authority or institution, such as an IP office, verifies the parties, claims and undersigns the transaction using WIPO DID3 and VCs.
Background	An IP owner (licensor) has acquired some IP rights and wants to monetize them. An IP buyer (licensee) intends to pay to be licensed the IP rights. Both the IP licensor and licensee already have a WIPO DID in place. The IP licensor and IP licensee can reside in different countries and have no previous knowledge of each other.
Objective	The IP licensor and IP licensee want to transact their contract on blockchain.
Narrative	• the IP licensor informs the licensee of their WIPO DID1; and • the IP licensee can check all VCs associated with the WIPO DID1 in the blockchain, and those related to IP rights held by the WIPO DID1 in particular. VCs can be signed by an IP office, court or government authority, and the buyer can verify the provenance of all VCs: there is a VC from a government authority (WIPO DID3) asserting that an IP licensor (WIPO DID1) owns the IP, and there is a VC issued by WIPO asserting that DID3 is in fact a recognized government authority. The above assumes that a trust relationship has been established (through a formal service contract, smart contract, etc.), so that a competent authority is allowed to create/ modify a subset of claims in the WIPO blockchain network and that designated agents can act on behalf of the WIPO DID licensor to update the WIPO blockchain network. The Licensee can also request the help of an auditor, IP licensor and/or online services to verify the VCs stored in the blockchain. *[Note: in W3C VC specs, the VC itself does not always contain the real credential information, but only the minimal subset of information needed to verify the credential on demand, such as public keys against some service.* *It should be decided whether the VCs stored in the blockchain should be free up to some limit per month, or a subscription fee should be imposed, as well as if the service should be provided to anonymous users only or also to registered users.]* • in the process where a licensee aims to acquire an IP right, they may request that the licensor verify the current state of ownership; • the IP licensor sends the information back to the licensee; • the licensee, after having made the appropriate checks, agrees to accept the terms of the license, including payment and; • the current licensor creates a new verifiable credential (VC) – DID Licensor→DID Licensee – asserting the IP rights according to some established terms, then they notify the licensee. Afterwards, the licensee can present the issued VC to third parties as a proof of the agreed license over the licensed IP rights.

- This licensing process can be further strengthened with extra security measures (initial pre-payment, delivery vs. payment, etc.). Such measures have been ignored in this mock-up to avoid unnecessary complexity not directly related to identity management.

Figure 33. IP owner licenses a patent



Notes

1. W3C (2019). User Roles. In *Verifiable Credentials Use Cases*. W3C Working Group Note, September 24. www.w3.org/TR/vc-use-cases/#user-roles
2. W3C (2021). DID Specification Registries: The interoperability registry for Decentralized Identifiers. September 24. https://w3c.github.io/did-spec-registries
3. Decentralized Identity Foundation (n.d.). https://github.com/decentralized-identity

World Intellectual Property Organization
34, chemin des Colombettes
P.O. Box 18
CH-1211 Geneva 20
Switzerland

Tel: +41 22 338 91 11
Fax: +41 22 733 54 28

For contact details of WIPO's
External Offices visit:
www.wipo.int/about-wipo/en/offices

Cover: Getty Images / AF-studio

WIPO Reference No. RN2022-2E
DOI: 10.34667/tind.44950