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

**WIPO Blockchain Whitepaper**

**Annex III: Use Cases**

Table of Contents

[POTENTIAL USE CASES FOR THE IP ECOSYSTEM 3](#_Toc84188340)

[**1. TIMESTAMPING** 3](#_Toc84188341)

[**2.** **DIGITAL IDENTITY** 17](#_Toc84188342)

[**3. IP REGISTER** 24](#_Toc84188343)

[**4. PROOF OF EXISTENCE** 37](#_Toc84188344)

[**5. EVIDENCE OF GENERATION** 48](#_Toc84188345)

[**6. ANTI-COUNTERFEITING** 55](#_Toc84188346)

[**7. IP RIGHTS ENFORCEMENT, SEIZURE ASSESSMENT** 62](#_Toc84188347)

[**8. PRIORITY DOCUMENT EXCHANGE** 70](#_Toc84188348)

[**9. CERTIFICATION MARK** 79](#_Toc84188349)

[**10. EVIDENCE OF TRADEMARK USE** 86](#_Toc84188350)

[**11. E-PVP MODULES** 92](#_Toc84188351)

[**12. IP RIGHTS TRANSFER/ASSIGNMENT** 102](#_Toc84188352)

[**13. IP LICENSING** 110](#_Toc84188353)

POTENTIAL USE CASES FOR THE IP ECOSYSTEM

# **1. TIMESTAMPING**

|  |  |
| --- | --- |
| **Topic** | **Timestamping** |
| **Summary** | A digital timestamp 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 timestamp 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 timestamp according to a given activity, the service provider will ensure trust (by means of a blockchain). The client will benefit from the trusted timestamp 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 timestamp.  Under [eIDAS regulation](https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014), a qualified timestamp 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. |
| **Relevant IP Value Chain phases** | Timestamping 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 * Priority Documents exchange. |
| **Business rationale** | A digital timestamp 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 timestamp provides electronic evidence of the existence of a document which 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.  Timestamp can provide complementary features to the existing IP system to reduce complexity, costs and time spent during the application process, at the same time so as to strengthen 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. * Research, development, and related data of pre-patent investigations. |
| **Potential Solution** | A blockchain-based digital timestamp service encrypts the code generated including the IP right 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 Timestamp Authority, the system instantly generates a unique timestamp, and the combination of the digital file and its unique timestamp 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 (digital signature delegation).  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).  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 timestamping of their document file (equivalent to the token in PKI-based solutions).  Even in case the user loses the transaction receipt, it is still possible to check the validity of the timestamp by examining the blockchain, especially if metadata is added to the transaction along with the timestamp.  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: 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 an HSM module placed in WIPO (for delegated digital signatures). * Client app: Client application (Web, Android, console, etc.) connecting to a blockchain network. * Blockchain network: Network of nodes building the blockchain (potentially thousands in public networks). |
| **Blockchain Rationale** | Current blockchain technologies compare and compete with existing PKI timestamping 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 a blockchain-based timestamping from a low-level technical point of view, and how similar features can be achieved with the current PKI are listed below.   * 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 timestamping, 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 node could manage to falsify its local clock, but not to rearrange the block order.  At the same time, timestamping data synchronization among such nodes would be provided for free. The current PKI can similarly add an absolute timestamp ordering by cryptographically linking timestamps to the previous ones forming timestamps 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 timestamps would provide extra legal value because parties could present the timestamp self-signed by its counter-party as legal proof to accept an obligation at a given time. Self-signed timestamps are technically possible with PKI-based solutions, but 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 timestamp 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 timestamp, for example using a ZFS filesystem. * Using token artefacts could allow in some contexts to automate or simplify billing and monetization of the timestamp 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 timestamp 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.  In order to have a proof of possession of a digital file at a specific date, the users can request a timestamp 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** | 1. The IP actor authenticates into the timestamp service. 2. The IP actor creates cryptographically a 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 timestamp 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 timestamp 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 timestamp 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 timestamped proof (the "proof token") on the blockchain. 7. The IP actor writes down/saves the proof token in a secure place.      1. A relying party requests a proof of previous existence of a digital file to the IP actor. 2. The IP actor shares the proof token (transaction receipt), the original file and his/her DID to requesting relying parties. 3. The relying party uses the receipt to fetch the hash in the blockchain. 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) timestamp of the block containing the timestamp and, optionally, the metadata from a trusted clock source with a more precise local timestamp.   **Actors** (or stakeholders) interacting in the use case and their role in the use case.   |  |  | | --- | --- | | **IP actor** | User that requests a new timestamp proof for a digital file to the timestamp 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 generation 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 digital signature is not delegated to the timestamp 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 timestamp 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 timestamp). | | **Registration in the blockchain** | A blockchain client registers the signed transaction on the blockchain. | | **Timestamping** | The blockchain creates a new block with the transaction. The timestamp of the blockchain block will be the official timestamp, 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 received) 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 timestamp returned by the block containing the transaction, and (optionally) the timestamp 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**   |  |  | | --- | --- | | **Document** | Original data to be timestamped. | | **Metadata** | Metadata related to the documents, to a timestamp, or to the timestamp 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 signed by the IP actor or the delegated service. | | **Cryptographic parameters** | Set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing. | | **Registers information** | Registers 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% 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[[1]](#footnote-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. | | DLT | RAFT[[2]](#footnote-3) | Complements an existing database adding blockchain functionality (immutable history of transaction, etc.) to provide a common vision among participants for a particular sub-state of information. Development is more similar to normal IT architectures supported by a database. | No current use outside the banking and financial industry. | |
| **Legal Assessment** | The **timestamping** 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 following regulatory framework for particular jurisdictions:   1. Digital Identity Regulation 2. Any Certified Authority/Trust Agent Regulation 3. Data Protection/Privacy Regulation   No specific regulation exists at the national or regional level to regulate a blockchain-provided timestamp, aside from eIDAS. **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[[3]](#footnote-4).  **In India, The Information Technology Act 2000** mandates that Certifying Authorities (CAs) shall provide Time Stamping Service for their subscribers. These timestamps 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[[4]](#footnote-5).  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)[[5]](#footnote-6); * The UK Data Protection Act (DPA 2018)[[6]](#footnote-7); and * The California Consumer Privacy Act (CCPA)[[7]](#footnote-8).   In terms of **Standards** and best practices, some examples are:   * ETSI Electronic Signature Format standards TS 101 733[[8]](#footnote-9), along with other ETSI standards; and * ISO/IEC 27002[[9]](#footnote-10) 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: (i) the legal consideration of these types of proofs; and (ii) 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 timestamping, especially if the goal is to compare it with another timestamping 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 timestamping system:   * Date and time of the transaction block commit; and * Date and time of the signing of the transaction. |
| **References and Contact Information** | <https://www.everis.co.uk/industries/banking/stampchain>  <https://khipus.io/en/?lang=true>  <https://www.stamping.io/indexEng.html>  <https://wipoproof.wipo.int/wdts/about-wipo-proof.xhtml>  <https://www.mondaq.com/china/copyright/926768/time-stamp--an-effective-solution-for-copyright-protection> |

# **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. 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.  With the eIDAS regulation[[10]](#footnote-11), 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.  In the same vein, the European Blockchain Services Infrastructure (EBSI) is a joint initiative from the European Commission and the [European Blockchain Partnership](https://ec.europa.eu/digital-single-market/en/news/european-countries-join-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 will be delivered and EBSI will become a [CEF Building Block](https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL), 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. |
| **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 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 more seamless and streamlined service experience, removing duplication, and making online transactions easier; * Standardized procedure of identification, agreed by network consensus (vs 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 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. * **Tools**:   + A wallet that allows users to register their own identity in several blockchain networks, as well as store and check their credentials, which can be shared with other users or institutions.   + A credential issuance platform allowing companies to issue verifiable credentials integrated into their own information systems.   **Decentralized Identity**  Implementing a generic decentralized identity capability allows entities to create and control their own identities 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.  The diagram below 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 sub-sets where 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 away 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 vision all nodes share the same information. Arrows represent claims that a 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 credential 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 make an order to Node A. Node A cannot remove the claim made by Node B.  d45e16af7fc2ef4b2dcab739ec9091c7  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 the previous diagram 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 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 meta-data about the identity. Claims, done by peer identity nodes, represent the real identity. |
| **Blockchain Rationale** | 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, 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. |
| **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 in mock-up document (Annex IV to the blockchain whitepaper).** |
| **Blockchain Technical Maturity** | Optimizing: Already exists in the production environment.  Examples include Hyperleder Indy, Sovrin, Ontology.  Up to 75 different solutions are registered in the [W3C DID Registry](https://w3c.github.io/did-spec-registries/#did-methods)[[11]](#footnote-12) 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 particular jurisdictions:   * Digital Identity Regulation * Data Protection/Privacy Regulation   For instance, the following regulation is applicable in the 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 [*eI*DAS Bridge](https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about) to reduce the regulatory gap between eIDAS and SSI models[[12]](#footnote-13). * The **General Data Protection Regulation** (**GDPR**)is the regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas.  Both the network architecture and the SSI data must comply with the GDPR[[13]](#footnote-14).   Thereafter, a regulatory assessment should be performed for compliance on a case-by-case basis according to the following levels on 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)[[14]](#footnote-15); * The UK Data Protection Act (DPA 2018)[[15]](#footnote-16); and * The California Consumer Privacy Act (CCPA)[[16]](#footnote-17). |
| **Challenges and Risks of using Blockchain** | The main challenges are: (i) the legal validity and characterization of these types of proofs; (ii) and 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: European Blockchain Service Infrastructure available at <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI> * eIDAS: electronic signature and trust services European regulation available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG>   Examples of existing solutions:   * KayTrust: Trusted platform to manage digital identities, available at  <https://www.kaytrust.id/> * SOVRIN: open source project creating a global public utility for self-sovereign identity, available at <https://sovrin.org/> * Serto: Identity Management services, available at 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 synchronizing and secured data exchange between Offices.  IP registries are currently separated across countries. Therefore, building a distributed ledger rather than traditional centralized databases could effectively turn 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 lifecycle 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 national level or at regional level (e.g. EU) or having worldwide coverage (WIPO). Nevertheless, they are in many cases represented in a national database and aggregated (using a limited set of attributes) in supra-national 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 like 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 whitepaper 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 the 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 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 immutable record 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 only once and it allows to record 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 onchain 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, 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 duplicities 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 timestamped 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 towards full tracking of the IP right life cycle. |
| **User stories** | **User story: IP right application for industrial property**  When a user (an applicant or IP legal representative) wants to apply for an IP right, s/he should be a user, with the role of applicant or representative in the IP Office in which s/he is going to apply for the IP right. The user will access the e-filing tool which will provide the details of the requested right.  In order 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 timestamped and it will be used as filing date evidence 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 timestamp proof with 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); 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. IP Office registers the result of the examination process in the blockchain; 12. The IP Office publishes the result of the examination process; 13. In case 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 DID&VC and it is made available for IP Offices in the IP Register network; 15. In case 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. In case the applicant wants to apply for the same IP right in another Office, the system will allow the applicant to recover already shared information in previous registrations.     **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** | Individual or the 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** | Individual or organization appointed by the innovator which has legal personality and which may, acting in its own name, exercise rights and be subject to obligations. | | **Receiving IP Office** | Official national IP Office in which the IP right application is filed. | | **Designated IP Office** | Official IP Office in which the IP right owner is asking for protection. |   **Activities or interaction or transaction**   |  |  | | --- | --- | | **Pre-set up** | 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 timestamp 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 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 Offices uploads the information related with 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, plus any user metadata considered appropriate (local clock timestamp). | | **Registration in the blockchain** | A blockchain client registers the signed transaction on the blockchain. | | **Timestamping** | The blockchain creates a new block with the transaction.  The timestamp of the blockchain block will be the official timestamp, 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 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 with the new data exchanged and 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 received) 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 timestamp returned by the block containing the transaction, and (optionally) the timestamp 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**   |  |  | | --- | --- | | **Documents** | Information provided by the applicant which 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 the data governance framework defined.  The information part of this IP Register 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 regulation. | | **Metadata** | 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** | Set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing. | | **Participants information** | 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 of this paper EUIPO has a system in production: the "IP Register in Blockchain" powering TM DS View where a blockchain solution based on Hyperledger Fabric stores already more than 3.5M IP rights. The solution incorporates nodes for 2 IPOs with 3 more to join by the end of 2021 and 27 by the end of 2025.  CMOs such as **Access Copyright or**the partnership composed by **ASCAP, the American Society for Composers, Authors and Publishers; SACEM, the Society of Authors, Composers and Publishers of Music;** and **PpRS** 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 uses cases in the market. |
| **Type of blockchain implementation** | |  |  |  | | --- | --- | --- | | **Blockchain Type** | **Pros** | **Cons** | | Private Permissioned | IPR Register 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 deploying and maintaining a custom infrastructure.  In order to avoid governance issues, governance rules should be clearly agreed between all network participants. | |
| **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 Register could create new gray areas in light of existing and inadequate regulations.  There are issues regarding the applicable laws and questions of jurisdiction, about the interoperability of blockchain solutions and lack of standardization, but also as to 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 the 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 blockchain-enabled IP Register. |
| **References and Contact Information** | Computer Law & Security Review, Volume 34, Issue 4, August 2018, 847-862, [doi.org/10.1016/j.clsr.2018.05.027](http://doi.org/10.1016/j.clsr.2018.05.027). Intellectual Property Law and Practice in the Blockchain Realm. Retrieved from <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285287>  European IPR Helpdesk. (n.d.). Your Guide to IP Commercialisation. Retrieved from <http://www.iprhelpdesk.eu/landing-page/ip-guides>  European IPR Helpdesk. (n.d.). *In a Nutshell: Blockchain and IP*  Retrieved from <http://iprhelpdesk.eu/ip-highlights/ip-special-blockchain/blockchain-in-a-nutshell>  ISO. (2020). ISO/DIS 56005(en) Innovation management — Tools and methods for intellectual property management — Guidance. Retrieved from <https://www.iso.org/obp/ui#iso:std:iso:56005:dis:ed-1:v1:en>  WIPO Magazine (February 2018). Blockchain and IP Law: A Match made in Crypto Heaven? Retrieved from <https://www.wipo.int/wipo_magazine/en/2018/01/article_0005.html>  WIPO Magazine (June 2020). *Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights.* Retrieved from <https://www.wipo.int/wipo_magazine_digital/en/2020/article_0002.html>  TaylordWessing (March 2017). Blockchain technology and IP. Retrieved from <https://www.taylorwessing.com/download/article-blockchain-technology-and-ip.html>  EUIPO (December 2016). IP in the Digital World Working Group (WG). Retrieved from <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>  COALA.  How blockchains can support, complement, or supplement intellectual property. Retrieved from <https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4307/529> |
| **Remarks** | This use case has been highly mentioned in answers received in the surveys performed during the preparation of the Blockchain Whitepaper. From these answers the following could be highlighted:   * Question "Categories for which you are using, or plan to use blockchain": 40% 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% 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% 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% of respondents selected: "We don't see any internal impact, but rather in the relationship with other Offices and with other ecosystem. " * 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% 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% 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 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 fulfil 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 which exist 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, e.g., 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 (1) IP asset life cycles (including, *but not limited to*, the illustrative commercialization-oriented IP asset life cycle described in Annex I to this Whitepaper); (2) multiple phases within those life cycles (e.g., generation, protection and management phases of the illustrative commercialization-oriented life cycle); (3) multiple vertical applications within some life cycle phases (e.g., trade secret protection and prior user rights recognition during the ‘management’ phase); and (4) within those vertical applications adding particular significance and value to some areas of subject matter because of the pre-existing distinctive properties of that subject matter (e.g., data characterizing natural material which 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 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* which the proof-of-existence function of blockchain fulfils 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 here 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[[17]](#footnote-18)** | **Legal function of proof-of-existence** | | Trade secret protection measures | Undis-closed | ‘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[[18]](#footnote-19);  2. Evidence of material scope of trade secret[[19]](#footnote-20); 3. Version management of trade secret protected know-how, information or data.[[20]](#footnote-21) | | 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 | Dis-closure | Act of public disclosure | E.g., GR databases | Time, scope, nature and version of technical disclosure | | Prior art recognition | Dis-closed | Disclosure of information to the public and making available to patent examiners | E.g., documented/ codified TK | Evidence that [information](https://en.wikipedia.org/wiki/Information) has been available to the public before a given date and might be relevant to a patent claims | | Prior public use recognition | Undocumented[[21]](#footnote-22) public use | E.g., undocumented/ uncodified TK | Evidence that knowledge or [information](https://en.wikipedia.org/wiki/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 to keep the documentation of the trade secret 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 nucloetide or amino acid level are disclosed in public databases currently most often four critical elements of IP information are lost: (i) the date of disclosure; (ii) the scope of disclosure (i.e., the originally disclosed sequence) (iii) the version of the sequence data (sequence data are continuously optimized and annotated); and (iv) 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 pubilc 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 (i)-(iv) 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 literature prior art wish to maintain that prior art 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 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.[[22]](#footnote-23) 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 which 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 the end relies on building a platform which generates a record of digital fingerprint or hash of the origin of intellectual asset with the timestamp 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, South 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 allowed to:   * Lower 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; * Strengthen information security for undisclosed information. It allows to register 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; * 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; * Undertake legally certain technical public disclosure of information, including the time, scope, nature and information version of the disclosure; * Provide 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; * Offer 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, s/he can register it into the blockchain, creating a transparent and immutable hash with a timestamp 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 artefact that could be created in relation with the same asset, ensuring that the data will remain unaltered and in 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 which is stored behind it. |
| **Potential Outcome** | 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 timestamp 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 timestamp 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** | **As an asset holder, I 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, e.g., 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 his/her disposal a document manager and a hash control for his/her internal organization.   **As a user,** I can verify the existence of an intellectual asset registered in the blockchain:  The user authenticates into the evidence storage service;   1. The user sends the document registered previously and the DID for verifying the authenticity; 2. The verification storage service provides an answer to authenticity; and 3. The user can verify the trade secret already registered. 4. The user can verify the existence of the intellectual asset if it has already been 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 timestamp 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 timestamp 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 timestamp). | | **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 timestamp of the blockchain block will be the official timestamp, 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 received) 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 timestamp returned by the block containing the transaction, and (optionally) the timestamp 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**   |  |  | | --- | --- | | **Document** | Original data including the description of the intellectual asset for which proof-of-existence is to be provided. | | **Metadata** | Metadata related to the Document(s), to a timestamp, or to the timestamp 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** | Set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing. | | **Registers information** | Registers 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 deploying and maintaining custom infrastructure.  In order 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% 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** | ClarkeModet: <https://sred.clarkemodet.com/>  *Blockchain and Trade Secrets: A Match Made in Heaven?,* Sindre Dyrhovden, King's College London, Retrieved  from <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 timestamped 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 timestamped record and trustable proof of generation. The owners can use this to commercialize, monetize and safeguard it from the potential misappropriation and infringement.  Blockchain makes it possible to store each creative work with a unique cryptographic identity, ensuring the 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 timestamping, 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, 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 middlemen taking profit with these "notarization" services with 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, but all the transactions will also be performed in the blockchain. Furthermore, the author is able to make direct agreements with 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 timestamped hash and supported by the immutability of the record, in case s/he is involved in any litigation process. |
| **Potential Solution** | The proposed solution is about 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 timestamping of their document. In the case that the user loses the transaction receipt, it is possible to check the validity of the timestamp and the digital file authenticity by examining the blockchain. * When needed or required, anyone with 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: (i) rights not being paid to the rightful owner because of not knowing who they are (publishers, CMOs, digital distributors, etc.); (ii) 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 timestamp 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 timestamping 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, e.g., by CMOs or other trusted authorities. |
| **Potential Outcome** | Blockchain-based platforms allow authors to make a record of 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** | As a creator of a creative work, I 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 timestamped proof of generation (the "proof token") on the blockchain.     As an IP User, I 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 timestamp of the block containing the timestamp and, optionally, the metadata from a trusted clock source with a more precise local timestamp.     **Actors**   |  |  | | --- | --- | | **Creator** | A user that requests a new timestamp proof for a document to the timestamp service. | | **Relying party** | A user that requests the registrant a proof of the file document of its generation. |   **Interactions**   |  |  | | --- | --- | | **Pre-set up** | The registrant must set up a wallet (if a signature is not delegated to the timestamp 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 timestamp 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 timestamp). | | **Registration in the blockchain** | A blockchain client registers the signed transaction on the blockchain. | | **Timestamping** | The blockchain creates a new block with the transaction. The timestamp of the blockchain block will be the official timestamp, 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 receive) 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 timestamp returned by the block containing the transaction, and (optionally) the timestamp 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** | Original data describing the creation timestamped as a proof of generation. | | **Metadata** | Metadata related to the documents proving the generation of the creative work, timestamped, or ready to be sent to the timestamp 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 signed by the creator. | | **Cryptographic parameters** | Set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing. | | **Registers information** | Registers 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 have 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** | <https://onlinelibrary.wiley.com/doi/full/10.1111/jwip.12069>  <https://www.sciencedirect.com/science/article/pii/S0267364920300066> |

# **6. ANTI-COUNTERFEITING**

|  |  |
| --- | --- |
| **Topic** | **Anti-counterfeiting** |
| **Summary** | This use case aims to use blockchain in order 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 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, to certify 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 the 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** | Worldwide industry is impacted by counterfeited goods. The impact is not only economic but it affects the consumer directly, by receiving poor-quality goods at an excessive price and sometimes exposing themselves to health and safety dangers.  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.  Not only IP right holders but also enforcement authorities in borders and internal market areas focus more and more on fighting against counterfeiting. Dedicated units for anti-counterfeiting matters have been created. Also, technical platforms are used by customs and police in order 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 via which counterfeiters can sell the products without direct contact with the final customer, who often is unaware that he is acquiring counterfeited goods.  If we look at the report published by the European Observatory on Infringements of Intellectual Property Report on the EU enforcement of intellectual property rights ([*Results at the EU borders and in Member States 2013-2017 (September 2019)*](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)), between 2013 and 2017 the EU detained approximately 438 million items with an estimated market value of 12 billion euros; 40% of seizures were made on borders and 60% 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. |
| **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[[23]](#footnote-24) 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; * Improve 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** | **User story consists of:**   * Tracing throughout the delivery chain  1. The IP owner authenticates as a user with his digital ID into 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 on the status of the transport (location, carry company, etc.), the new data is stored in the blockchain; 5. By scanning the container, customs' officers in 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.     **Actors** (or stakeholders) interacting in the use case and their role in the use case   |  |  | | --- | --- | | **IP Owner** | Owner of private legal rights that protect the generation of the human mind and seeks to protect it against counterfeiting. | | **Shipment carry companies** | Companies involved in the transport and delivery of the product. | | **IP enforcement authorities** | Fights against counterfeiting with the information provided by the IP right holders. | | **Customer** | Personal acquiring the product or legal entity selling the product/products. |   **Activities or interaction or transaction**   |  |  | | --- | --- | | **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 timestamp 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 registries, the enforcement services or the market place services establishing a new session. | | **Upload information** | 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. | | **Fulfil information** | The sender participants fulfil the request information about the data that is going to exchange and selects the receivers s/he wants 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, plus any user metadata considered appropriate (local clock timestamp).  The hash will track all the actions that occur in the product distribution process, timestamped by each of the actors. | | **Registration in the blockchain** | A blockchain stores the signed and timestamped transaction on the blockchain. | | **Timestamping** | The blockchain creates a new block with the transaction. The timestamp of the blockchain block will be the official timestamp, 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** | All the participants involved in the delivery process, receive in their wallets the notification with the new data exchanged and can access it. | | **Update the information** | All the parties can exchange as much as needed information they would need with new transactions. | | **Upload proof token and file to verify** | The viewers can use the proof token (transaction receive) 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 timestamp returned by the block containing the transaction, and (optionally) the timestamp 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**   |  |  | | --- | --- | | **Documents** | Encrypted information to share between the IP right holders and the enforcement authorities (carry companies, routes, packaging, etc.). | | **Metadata** | 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 with 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** | Set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing. | | **Participants information** | Participant’s information. | |
| **Blockchain Technical Maturity** | Optimizing: Already exists in the production environment.  At that moment IP Organizations such as EUIPO and DG TAXUD are involved in implementing solutions aimed to create a communication platform between IP right holders and the enforcement authorities.  Besides that, many industries are in sportswear, fashion or IP sectors using blockchain to protect their IP rights, the provenance of origin and to help with anti – counterfeiting procedures. |
| **Blockchain Technical Complexity** | Medium: Implementation can be inspired by solutions like iTrace, Compello, Circulor, Zertifier etc. |
| **Type of blockchain implementation** | |  |  |  | | --- | --- | --- | | **Blockchain Type** | **Pros** | **Cons** | | Consortium Permissioned (IBFT) | 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. | 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** | Anti-counterfeiting blockchain solutions must comply with national regulations about customs enforcement and, for WTO members which are not LDCs, the Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS Agreement). In the European Union is the Regulation (EU) No 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning customs enforcement of intellectual property rights.  The harmonization of copyright regulation around the world allows a 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. |
| **Challenges and risks of using blockchain** | Legal regulation between countries  High Data volumes needed to be stored  GDPR and confidentiality requirements must be respected  Upgrade of the devices in the involved stakeholders will be needed |
| **References and Contact Information** | <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>  <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> |

# **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 supporting of enforcement authorities, right holders, and other parties involved in the lifecycle 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 rights holders, enforcement authorities such as Interpol, World Customs Organizations (WCO), Europol or DG Taxation and Customs Union, 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 phases of protection and commercialization. |
| **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, so will potentially counterfeiting. To counter this, new initiatives to fight counterfeiting and piracy are taken in which IP organizations and enforcement authorities are working closely together implementing 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 rights holders, it is necessary to ensure the confidentiality of 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 rights 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 rights holders to provide enough data to the enforcement authorities in order 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 current anti-counterfeiting challenges in the coming years with the following features.   * **Traceability and trust.** 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   + 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 favouring 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’ digital identities (DIDs) with a high Level of Assurance (LoA) identification tool, which also respects data privacy an 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 e.g. production facilities, points of entry/exit for import/export, 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, and whose 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 rights holder to determine if the goods are fake or genuine and decide 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 is overall, it is more related to the second stage.  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 rights holder through the platform. Encrypted data is shared and signed by the enforcer; 5. The IP rights holder authenticates into the platform using his/her digital identity; 6. The IP rights 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.     **Actors** (or stakeholders) interacting in the use case and their roles in the use case   |  |  | | --- | --- | | **IP rights holder** | Owner of IP rights seeking to protect his/her property. | | **IP Office** | Provide services for digital IPRs management. | | **Importer or Consignee** | Persons or entities who are the buyer or responsible for the receipt of a shipment | | **Enforcement authority** | Person in the relevant enforcement authority/institution fighting against counterfeiting. |   **Activities, interactions, or transactions** (general information applicable to other use cases)   |  |  | | --- | --- | | **Pre-setup** | The participants (the enforcement authority and the IP rights holder) must set up a wallet (if signature is not delegated to the timestamping 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** | Enforcement authorities and the IP rights holders upload the information they want to exchange. | | **Hash creation** | A unique hash of the files is generated. | | **Fulfill information request** | The sender participants fulfil the request for information about the data to be exchanged and selects the receivers he wants 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, plus any user metadata considered appropriate (local clock timestamp). | | **Registration on the blockchain** | A blockchain client registers the signed transaction on the blockchain. | | **Timestamping** | The blockchain creates a new block containing the transaction. The timestamp of the blockchain block will be the official timestamp, 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 rights 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 in order 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 timestamp returned by the block containing the transaction, and (optionally) the timestamp 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** | Encrypted information to share in different formats (documents, images, videos). | | **Metadata** | Metadata related to 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** | Set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing. | | **Participants information** | Participant’s information. | |
| **Blockchain technical maturity** | Optimizing: Already exists in the production environment.  At the moment IP organizations such as EUIPO and DG Taxation and Customs Union are involved in implementing solutions aimed at creating a communication platform between IP rights 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 components, which need to be designed from scratch. |
| **Type of blockchain implementation** | Type of blockchain implementation recommended: **Consortium (private) network formed by nodes from IP Offices, Member States and Custom 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.   |  |  |  | | --- | --- | --- | | **Blockchain Type** | **Pros** | **Cons** | | Consortium Permissioned (IBFT) | 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 transaction per seconds. | 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** | 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 12 June 2013 concerning customs enforcement of intellectual property rights. |
| **Challenges and risks of using blockchain** | National regulations.  High data volumes need to be stored.  Required upgrading of involved stakeholders devices. |
| **References and contact information** | <https://euipo.europa.eu/ohimportal/es/news/-/action/view/4963920>  <https://euipo.europa.eu/ohimportal/en/web/observatory/blockathon>  <https://www.wto.org/english/res_e/reser_e/session_2c_4_zahouani_saadaoui_dg_taxud_blockchain_v1.0.pdf> |

# **8. PRIORITY DOCUMENT EXCHANGE**

|  |  |
| --- | --- |
| **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 IPO´s, 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) that allows to exchange 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 all the network. Additionally, accesses to documents may be controlled and restricted. |
| **Relevant IP Value Chain phases** | This is a vertical use case with a wide usage, e.g. used when an applicant asks to use the priority patent documents generated in the Office of First Filing (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 labour used in this 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 Office of First Filling (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 similar 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 legal value, security, and usability of the solution. * The IP Office will send the patent priority documents to the IP Office or Offices 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 timestamping 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 timestamp by examining the blockchain, especially if metadata is added to the transaction along with the timestamp. * The applicant selected by the IP Office or Offices 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 to automate the sending of priority patent documents from the OFF to Office 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 such node could manage to falsify its local clock, but not to rearrange the block order.  Agreed token artefacts could allow in some contexts to automate or simplify the process of the timestamp 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, easier and quicker 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, for sending OFF-certified patent documents to the offices for which the applicant is asking for granting the patent and 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** | **User story consists of: 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 in order to get the patent grant in a new patent office. The request includes DID1 and VC1; 3. OFF verifies the IP right ownership in the IP Register (DID1&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 timestamp proof.     **Actors** (or stakeholders) interacting in the use case and their role in the use case   | **Actors** | **Description** | | --- | --- | | **IP rights holder** | 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** | Official national or international bodies that are responsible for the grant, issue, or record of intellectual property rights. | | **IP legal representative** | Individual or organization appointed by the innovator which has legal personality and which may, acting in its own name, exercise rights and be subject to obligations. | | **Office First Filing (OFF)** | Official IP Office receiving the first application for a patent from which the applicant may ask for granting of the same patent in other countries. | | **Office Second Filing (OSF)** | Official IP Office receiving the application for a patent which is already registered in an OFF. |   **Activities or interaction or transaction**   |  |  | | --- | --- | | **Pre-setup** | The IP Offices must set up a wallet (if the signature is not delegated to the timestamp 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 fulfil the request information about the data to be shared and selects the IP Offices with which the IP right holder wants to share the documents with. | | **Transaction creation** | The transaction will consist of the hash, the required information, plus any metadata requested by the blockchain protocol, plus any user metadata considered appropriate (local clock timestamp). | | **Registration in the blockchain** | A blockchain client registers the signed transaction on the blockchain. | | **Timestamping** | The blockchain creates a new block containing the transaction. The timestamp of the blockchain block will be the official timestamp, 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**   |  |  | | --- | --- | | **Documents** | Information to share between OFF and OSF. | | **Metadata** | Metadata related to 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** | Set of cryptographic primitives, schemas, padding, method of operations, and procedures established for hashing and signing. | | **Participants information** | IP Offices 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 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 European Patent Office (EPO) has decided that as of 1 November 2018, the EPO will participate in the WIPO Digital Access Service (DAS) for the exchange of certified copies of patent applications (priority documents).  Currently, there are 21 participating Offices in total, including the other IP5 Offices (USPTO, JPO, KIPO and 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](http://www.wipo.int/das/en/participating_offices.html).  The United States Patent and Trademark Office (USPTO) transmits certain U.S. 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 World Intellectual Property Organization Digital Access Service (WIPO DAS) Exchange. |
| **Challenges and risks of using blockchain** | Technical, regulatory, and business challenges of adopting the technology for the use case. |
| **References and Contact Information** | <https://www.epo.org/law-practice/legal-texts/official-journal/2018/10/a79.html>  [https://www.wipo.int/das/en/#](https://www.wipo.int/das/en/)  <https://www.uspto.gov/patents-getting-started/international-protection/electronic-priority-document-exchange-pdx#:~:text=The%20European%20Patent%20Office%20(EPO,of%20exchange%20are%20mutually%20exclusive.> |

# 

# **9. CERTIFICATION MARK**

|  |  |
| --- | --- |
| **Topic** | **Certification mark** |
| **Summary** | A certification mark is a mark indicating that the goods or services protected by such 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 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 USPTO and EUIPO having a similar registration process to process for a 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 difficulties to obtain the trademark as it is not always clear where to request the trademark certification. On the other side, the trademark certification owners must be sure that the users comply with all pre-established 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 allows to 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 allowing to check whether the examination process has been performed following the indications defined within the certification mark process as well as it can be used as immutable timestamp on the application, the resolution, and the maintenance of the rights in the use of the trademark.  Blockchain ledgers are timestamped records that cannot be altered and may store smart contracts which 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 manufactures 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 fulfilment 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, in order 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.     **From the manufacturer’s point of view, in order to use the certification mark, a request may be submitted and acceptance is subject the compliance of the requirements set by the certification owner:**   1. Manufacturer requests use of an already existing certification mark in the system providing the required data; 2. 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. Manufacturer accepts the terms of the verification process and the terms of condition to keep the use of certification mark in case it is granted; and 5. The manufacturer gets the results of the verification process.     **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 anytime 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** | User owns the certification mark and is responsible for the definition of the conditions to be accomplished by the products. | | **Manufacturer/Service Provider** | Individuals or entities producing goods or delivering services for which the certification mark is requested. | | **Certification authority** | 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 signature is not delegated to the timestamp 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 timestamp 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 timestamp). | | **Registration in the blockchain** | A blockchain client registers the signed transaction on the blockchain. | | **Timestamping** | The blockchain creates a new block with the transaction. The timestamp of the blockchain block will be the official timestamp, 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 receive) 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 timestamp returned by the block containing the transaction, and (optionally) the timestamp 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** | Original data to be timestamped. | | **Metadata** | Metadata related to the documents, to a timestamp, or to the timestamp 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** | Set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing. | | **Registers information** | Registers 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 deploying and maintaining custom infrastructure.  In order 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 virtually immediately, e.g. 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 timestamped evidence of actual use and frequency of use of a trademark in trade, both of which are relevant in proving first use, genuine use, acquired distinctiveness/secondary meaning or goodwill in a trademark. Similarly, distributed ledger technology 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 in order to keep the trademark registered, it must be used in the market and dated evidence is needed in order 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 in order 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 arduous collection of relevant records (which can prove to be unreliable and incomplete), and demonstrating use of a trademark, e.g. via surveys, and can be a significant cost to rights 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 allows to prove the use of the trademark in a digital, easy and quick 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 virtually 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 US.  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 track 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 IP register with his digital identity; 2. The trademark owner accesses the trademark for which s/he wants 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 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.     **Actors** (or stakeholders) interacting in the use case and their role in the use case.   |  |  | | --- | --- | | **Trademark owner** | User owns the trademark. | | **IP Office** | IP Office owning the blockchain-based official trademark register | | **Trademark user** | 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 timestamp 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 timestamp 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 timestamp). | | **Registration in the blockchain** | A blockchain client registers the signed transaction on the blockchain. | | **Timestamping** | The blockchain creates a new block with the transaction. The timestamp of the blockchain block will be the official timestamp, 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 receive) 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 timestamp returned by the block containing the transaction, and (optionally) the timestamp 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** | Original data to be timestamped. | | **Metadata** | Metadata related to the documents, to a timestamp, or to the timestamp 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** | Set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing. | | **Registers information** | Registers 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. |
| **Type of blockchain implementation** | |  |  |  | | --- | --- | --- | | **Blockchain Type** | **Pros** | **Cons** | | **Public/Private Permissionless/Permissioned** Consensus recommended: PoW/PoS for public networks, IBFT for private networks. | 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. |  | |
| **Legal Assessment** | **Timestamping** is the core solution in this use case.  As it was mentioned in the **timestamping** 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:   1. Digital Identity Regulation 2. Any Certified Authority/Trust Agent Regulation 3. Data Protection/Privacy Regulation   In terms of s**tandards** and best practices: All of the current standards and best practices applied to an existing **timestamping**, 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. |
| **Challenges and risks of using blockchain** |  |
| **References and Contact Information** | <https://www.wipo.int/wipo_magazine_digital/en/2020/article_0002.html> |

# **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 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 also resolve the practicalities of collating, storing and providing such evidence. 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 either at national level or at 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 supra-national and international databases. Current practices make that applicants are required to file for protection for their varieties in each UPOV member they wish to obtain protection and therefore provide the same information at 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 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 distributed ledger technology 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. * 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 to 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 real-time. * Have an immutable track of data history. It will create 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, it allows to record 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 DUS examination processes and their results.  This common register contains shared information of 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 lifecycle 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 in order to give a high degree of security to all operations.  Blockchain technology brings 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:   * Monitor their application during the full life cycle; * Save time thanks to the information shared between PVP Offices; and * Decentralized information timestamped valid in case of legal disputes.   The PVP Office will receive the following benefits:   * Digital framework for standardized data sharing among PVP Offices; * Better service to the applicants, a simpler process could increase the number of applications; * Eliminate mistakes and typos in the examination process; and * The first step to full tracking of the PBR life cycle. |
| **User stories** | **User story: Plant Breeder’s right application**  When a user (an applicant or a legal representative) wants to protect his/her variety, s/he should be a user, with the role of applicant or representative, in the PVP Office in which s/he is going to apply. The user will access the online filing tool UPOV PRISMA or the national filing system.  In order 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 timestamped 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 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 case of regional mechanism (e-PVP Asia), only one form is completed and the application data is distributed to designated PVP Offices; 3. The encrypted application data as well as the related meta data is recorded in 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. In case the Plant Breeder’s Right is granted, the PVP Office provides the Plant Breeder’s Right certificate to the IP right owner; and 13. C:\Users\chavas\Pictures\EPVP.pngMatters after grant: this includes payment of fees for keeping the right in force, renunciation, nullity and cancelation.   **Actors** (or stakeholders) interacting in the use case and their role in the use case   |  |  | | --- | --- | | **PVP Offices** | Official national or regional bodies responsible for the management of PVP. | | **Applicant** | 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** | Natural or legal person appointed by the breeder and authorized to act on behalf of the breeder. | | **Receiving PVP Office** | PVP Office in which the PVP application is filed. |   **Activities or interaction or transaction**   |  |  | | --- | --- | | **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, plus any user metadata considered appropriate (local clock timestamp). | | **Registration in the blockchain** | A blockchain client registers the signed transaction on the blockchain. | | **Timestamping** | The blockchain creates a new block with the transaction.  The timestamp of the blockchain block will be the official timestamp, 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 users) can use the proof token (transaction received) 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 timestamp returned by the block containing the transaction, and (optionally) the timestamp 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**   |  |  | | --- | --- | | **Documents** | Encrypted information to share in different formats (documents, images). | | **Metadata** | Metadata related to 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** | Set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing. | | **Participants information** | Data shared between the PVP Office and the Applicant or the 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 Hyper ledger 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 transaction-per-seconds. | Requires to deploy and maintain 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 does 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 Breeders’ rights.  Interoperability between Blockchain initiatives is another important matter to be addressed at an early stage (e.g. authorities, interested in using Blockchain technology, that in addition to PBR they administer other intellectual property rights). |

# 

# **12. IP RIGHTS TRANSFER/ASSIGNMENT**

|  |  |
| --- | --- |
| **Topic** | **IP rights transfer or assignment** |
| **Summary** | **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.  In order for a transfer of rights to be managed by the IP Office, a 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 use to sign a non-disclosure agreement between them 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 in order 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:   1. Making the evidence of the agreement clearer between the assignee and the assignor for the transfer of the IP right; 2. Timestamping the change of ownership of the transferred IP rights; and 3. 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 with the IP right management phase for all the patents, trademarks, industrial designs and copyright that can benefit from another supportive horizontal use cases capabilities like Timestamping, 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 in order 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 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, in order 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.  In order to proceed with the registration of the IP right transfer, some IP Offices require the assignee to register the new ownership, otherwise s/he may lose the transferred rights, reason why the timestamping 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 to track and check the end-to-end lifecycle 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 with 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 the 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, e.g., the validity of IP ownership, identification of the parties to the assignment (assignor and assignee), digital signature and timestamping 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); * Using smart contracts to automate processes; * Traceability of IPRs transfer that streamlines the audit processes; * A platform providing an IPR marketplace without the need for traditional intermediaries; * Selecting IPR and drawing up an offer; * Finding buyer; * Automatic generation of application; and * Record of ownership change in 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 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** | **User story Transfer/Assignment of IP Rights**  In order to transfer an IP asset, the owner should register it in the IP Register, e.g. an Office’s Register, as explained in Use Case III. IP Register. For this registration process, 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 along by both the assignee and the IP Office to verify the ownership of the IPR.   1. Assignor authenticates into the service; 2. Assignee authenticates into the service: 3. Assignee requests the Assignor to provide the proof of ownership (DID1&VC1); 4. Assignor provides the ownership proof, which should be verified against the data stored in the IP Registry, e.g., the Office. 5. Assignee verifies the IP asset ownership in the IP register; 6. Assignor request for change of IPR ownership to the IP Office. This request is composed by the DID1, VC1 and the smart contract signed by both parties; 7. IP Registry timestamps the request for IPR transfer and verifies the IPR ownership in the IP register (DID1&VC1); 8. IP Registry records the ownership transfer into the IP Register and confirms the new assignment to the parties; and 9. IP Register issues a new ownership certificate to the assignee   *[Notes: Assignor and assignee can use some protocol to exchange secure information, e.g. 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*](https://github.com/hyperledger/aries-rfcs/tree/master/features/0160-connection-protocol)*.]*    **Actors (or stakeholders)** interacting in the use case and their role in the use case.   |  |  | | --- | --- | | **Assignor** | Owner of the IPR aiming to transfer it to the assignee. The assignor will exchange information with assignee and IP Register in order to prove the ownership of the IPR. | | Assignee | Purchasing and tracking IP assets who will verify the ownership of the IPR 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&VC1 against the IP Register. | | **IP Register** | 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 timestamp 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 timestamp 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 s/he wants 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 check all the operations were made in the right way. |   **Key data**   |  |  | | --- | --- | | **IP Right data** | IP identification, IP Right information, Customer Identifiers, IPRs transfer status | | **Product data** | Product information | | **Customer data** | Customer information | | **Supply data** | Event, Entity, 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 to deploy and maintain custom infrastructure.  In order 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 intellectual property right concerned. In some countries for example, the law may require a written form for an assignment of trademarks, however, not for an assignment of copyright. |
| **Challenges and risks of using blockchain** | Technical, regulatory in order 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, September 2013. *Fact Sheet Commercialising Intellectual Property: Assignment agreement.*  <http://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 IP by other 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, licences are signed by the creative work owner and the CMO or the final user. Each licence 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 to ensure the identification of the parties as well as the ownership of creative works and will allow:   * To calculate the payment based on the use; * To reduce 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 with Timestamping. |
| **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 middlemen.  Blockchain may allow creators or collectors to document and verify the authenticity of digital content in order 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 his/her 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** | The use of blockchain technology as a tool allows to manage and store IP Licenses on a decentralized ledger and 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 timestamped 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 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 to manage and track 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** | **As a licensor, how can I register a license in the system in order to grant its use?**     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.   **As a licensee, in order to access the IPR, I 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** | User holding IPRs. | | **Licensee** | 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 timestamp 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 timestamp 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 timestamp). | | **Registration in the blockchain** | A blockchain client registers the signed transaction on the blockchain. | | **Timestamping** | The blockchain creates a new block with the transaction. The timestamp of the blockchain block will be the official timestamp, 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 receive) 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 timestamp returned by the block containing the transaction, and (optionally) the timestamp 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** | Original data to be timestamped. | | **Metadata** | Metadata related to the documents, to a timestamp, or to the timestamp 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** | Set of cryptographic primitives, schemas, padding, method of operations and procedures established for hashing and signing. | | **Registers information** | Registers 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 needs to be defined by a central institution.  Allows fast synchronization of nodes. | 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** |  |
| **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** | <https://citymis.co/cedro/guides/blockchain/certificado>  <https://ujomusic.com/> |

[Annex IV follows]

1. See definition at <https://consensys.net/blog/enterprise-blockchain/scaling-consensus-for-enterprise-explaining-the-ibft-algorithm/> [↑](#footnote-ref-2)
2. See definition at <https://raft.github.io/> [↑](#footnote-ref-3)
3. 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 [↑](#footnote-ref-4)
4. <http://cca.gov.in/index.php> [↑](#footnote-ref-5)
5. <https://diacc.ca/trust-framework/> [↑](#footnote-ref-6)
6. <https://www.gov.uk/data-protection> [↑](#footnote-ref-7)
7. https://oag.ca.gov/privacy/ccpa [↑](#footnote-ref-8)
8. https://www.etsi.org/deliver/etsi\_ts/101700\_101799/101733/02.02.01\_60/ts\_101733v020201p.pdf [↑](#footnote-ref-9)
9. https://www.iso.org/standard/54533.html [↑](#footnote-ref-10)
10. https://ec.europa.eu/futurium/en/system/files/ged/eidas\_regulation.pdf [↑](#footnote-ref-11)
11. https://www.w3.org/TR/did-spec-registries/ [↑](#footnote-ref-12)
12. [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/AUTO/?uri=CELEX:32014R0910&qid=1591808619409&rid=1)  [↑](#footnote-ref-13)
13. [Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC](https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1591808798287&uri=CELEX:32016R0679) [↑](#footnote-ref-14)
14. <https://diacc.ca/trust-framework/> [↑](#footnote-ref-15)
15. https://www.gov.uk/data-protection [↑](#footnote-ref-16)
16. https://oag.ca.gov/privacy/ccpa [↑](#footnote-ref-17)
17. Purely illustrative examples from past technical work undertaken by the International Bureau at the request of WIPO Member States. [↑](#footnote-ref-18)
18. In this case, the obtaining of ‘proof-of-existence’ *with* encryption on blockchain could *itself* be considered one possible, legally recognized ‘reasonable step under the circumstances by the person lawfully in control of the information to keep the information secret’ (cf. Art. 39.2(c) TRIPS Agreement). [↑](#footnote-ref-19)
19. The body of information which itself constitutes the trade secret would never be processed or uploaded on chain, but would remain exclusively in the possession of the trade secret holder. [↑](#footnote-ref-20)
20. This is particularly relevant for data sets which are repeatedly annotated, revised and reannotated, such as e.g. trade secret protected genomic sequence data of GRs, which are continuously resequenced and reannotated. [↑](#footnote-ref-21)
21. i.e., unwritten and otherwise un-‘fixed’/recorded use [↑](#footnote-ref-22)
22. WIPO/GRTKF/IC/9/13, WIPO/GRTKF/IC/11/11 [↑](#footnote-ref-23)
23. Petersson Nielsen, C (2020), “Digital Twins and Blockchain – Proof of Concept”, available at https://www.sciencedirect.com/science/article/pii/S2212827120307381 [↑](#footnote-ref-24)