docproof.org
protège vos idées !

Présentation

docproof.org est une solution **innovante** de **consignation numérique**, basée sur la **cryptographie** et la **technologie *blockchain***, issue de Bitcoin, permettant d'enregistrer une **preuve d'antériorité** pour tout objet numérique, indépendamment de tout tiers de confiance et pour un coût dérisoire.

docproof.org est un projet académique, développé à l'Institut de Biologie Structurale[1] (IBS). Il est actuellement disponible sous la forme d'un **démonstrateur**, disponible en version beta.

Principe

L'article L.111-1 du Code de propriété intellectuelle stipule que *« L'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous. »*

Le créateur d'une œuvre sera celui qui pourra présenter la plus ancienne **preuve d'antériorité**.

docproof.org permet **l'enregistrement de ces preuves d'antériorité** en consignant une **empreinte numérique** du document à protéger au sein de la **blockchain** Bitcoin.

Une **empreinte** est une sorte de résumé cryptographique, propre à un document. L'algorithme utilisé est SHA256. Compte-tenu des moyens connus dont nous disposons aujourd'hui, il est **matériellement impossible** de fabriquer deux documents produisant une même empreinte. Une empreinte SHA256 ressemble à cela :

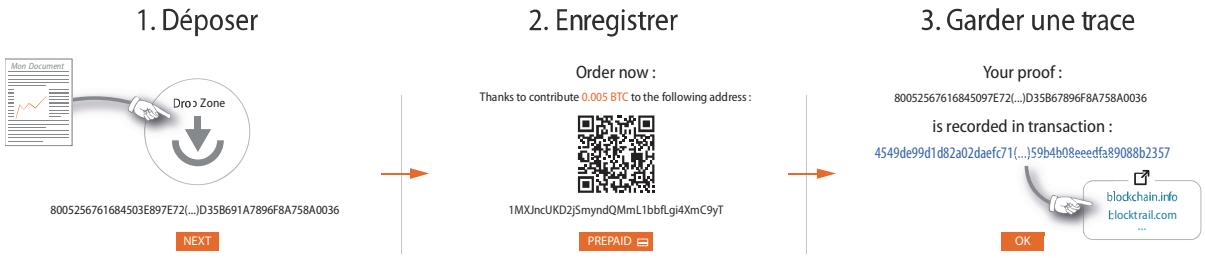
37C81A099B21FB60E59A9F695A1288BA313A4BF635F8A79E2EB56E653B760E3A

Une **blockchain**, telle que celle de Bitcoin, est une sorte de base de données redondée, composée de milliers de copies, dont les contenus sont à la fois **très difficilement falsifiables** et **consultables par tous**. Modifier une blockchain sans que cela ne soit détecté est par conception impossible. Par ailleurs, cela demanderait une puissance de calcul très difficilement accessible.

Toute écriture dans la blockchain est **datée de manière infalsifiable**. Il est ainsi possible d'enregistrer la preuve d'existence d'un document à une date donné.

Utilisation pratique

docproof.org permet d'enregistrer une **preuve d'existence** depuis un simple navigateur, en simplement 3 étapes :



1/ **Calcul de l'empreinte**, via un simple « drag & drop ». Votre navigateur calcule alors localement l'empreinte du document.

2/ **Enregistrement** de l'empreinte au sein de la blockchain, **via un compte prépayé** ou une transaction Bitcoin.

3/ **Archivage** de l'identifiant de votre transaction, permettant de retrouver votre preuve d'antériorité au sein de la blockchain.

Le processus complet d'un enregistrement ne prend que **quelques minutes** et ne nécessite aucune installation de logiciel. Le coût effectif de l'enregistrement est de **quelques centimes d'euros**.

docproof.org est accessible depuis Windows, MacOS, Linux, Android et IOS !

Contexte légal

Les technologies utilisées par **docproof.org** sont très récentes et la **jurisprudence n'est pas encore établie**. En cas de litige, deux questions seront susceptibles d'être posées aux experts :

- Est-ce que cet « enregistrement » prouve l'existence du document à la date annoncée ?
- Est-ce que cette « prétendue preuve » est authentique ?

L'enregistrement comporte une **empreinte** SHA256, **totalement spécifique du document déposé**. En l'état actuel de la cryptographie, il n'est pas possible de générer un second document possédant cette même empreinte. Par ailleurs le dépôt est **horodaté via la technologie blockchain** du réseau Bitcoin.

La réponse à la première question est donc : **OUI**

La blockchain Bitcoin, de par sa conception et l'importance de la communauté qui la maintient, **ne peut-être falsifiée sans que cela ne soit détecté** or aucune falsification n'a été constatée à ce jour.

La réponse à la seconde question est donc : **OUI**.

Note : en l'absence de jurisprudence établie, en cas d'enjeux importants, un double enregistrement via des organismes traditionnels peut être un choix pragmatique.

Bénéficiaires potentiels du service

Potentiellement tout le monde :-)

La preuve d'antériorité est le meilleur moyen de **protéger une création intellectuelle**, qu'elle soit **artistique**, **scientifique** ou de **tout autre domaine**. Tout document électronique peut être protégé via **docproof.org** ; photographie, texte, pdf, vidéo, mp3, etc.

Les usages possibles sont donc innombrables ; protection industrielle, artistique ou scientifique, consignation de diplômes, cadastre, journal officiel, preuve de dépôt, etc.

Les bénéficiaires sont de fait tout aussi nombreux : scientifiques, artistes, acteurs économiques ou juridiques, administrations, etc.

Bénéfices

En utilisant la technologie **blockchain** de Bitcoin[2] **docproof.org** est **indépendant de tout organisme** ou **tiers de confiance**.

La **confidentialité des documents est totale**. Seule l'empreinte du document est enregistrée et le calcul de cette dernière est effectué localement. En aucun cas **docproof.org** ne peut donc connaître les documents protégés.

docproof.org est un service d'enregistrement **indépendant du service de séquestre utilisé**. Si **docproof.org** venait à disparaître, les preuves déposées, enregistrées au sein de la blockchain, demeureraient totalement accessibles et consultables par tous.

docproof.org n'effectuant que l'enregistrement, la **vérification** d'une preuve peut être effectuée **en toute indépendance** et de manière **publique**, via de nombreux services en ligne, indépendants de **docproof.org**.

docproof.org ne nécessite **aucun prérequis** ni **aucune installation de logiciel**. L'enregistrement d'une preuve ne demande que **quelques minutes** et ne coûte que **quelques centimes d'euros**.

Il est en outre possible **d'automatiser l'enregistrement** via des **API**, en backoffice de processus métiers existants.

Alternatives

docproof.org s'appuie sur des développements et extensions récentes de l'infrastructure Bitcoin et reprend les principes de **proofofexistence.com**[3]. Très peu de solutions alternatives sont actuellement disponibles.

---

[1] UMR 5075 / Unité Mixte de Recherche CNRS, CEA, UGA – Grenoble, par Jean-Luc Parouty, Équipe informatique IBS
[2] Bitcoin est un projet open-source et communautaire, n'appartenant à aucune organisation publique ou privée, ni aucun état.
[3] https://proofofexistence.com, développé par Manuel Araoz