Blockchain certificates for securing intellectual property assets

Moscow, 16.04.2018
A public blockchain is the universal **public registry** that humanity has been waiting for.
Public blockchains
- Decentralized
- Permissionless
- Uncensorable
- Resilient

Private blockchains
- Distributed
- Permissioned
- Trust based

ethereum
bitcoin
MultiChain
HYPERLEDGER
Public blockchains are a new common

{Common: a resource accessible to all members of a society, including natural materials such as air, water and a habitable earth. These resources are held in common, not owned privately.}
A public blockchain is a public registry with very unique features.
Bernstein is a gateway to blockchain-based registries for innovators
Bernstein approach to IP management

Multifaceted and complex:
- Securing trade secrets
- Claiming copyrights
- Proving prior use
- Make defensive disclosures
- Confidentiality agreements
- Technology licenses
- ...

**Risks**: product delays, wasting R&D money, legal costs, going out of business, litigations, ...

The blockchain allows companies to create solid foundations to neutralize these risks.

At **low effort** and **low cost**.
Bernstein is a web service that allows innovators to register IP assets on the blockchain.

Bernstein’s unique protocol will create blockchain certificates that can prove: **existence**, **integrity** and **ownership**.

**Specific targets**
- Industrial and scientific IP
- Small and mid-size companies

**Unique advantages**
- Perfect confidentiality
- Unlimited encrypted data storage

Bernstein is a **gateway** to multiple certification infrastructures.
Disclose inventions on a decentralized file system (IPFS).
Three **use cases** for blockchain certificates
Bernstein blockchain certificates

BLOCKCHAIN CERTIFICATE

The file or collection of files referred hereunder existed and was presented in the date and time printed down below by the entry identified as Project Owner:

Aperture Science Handheld Portal Device

Project Owner: Aperture Laboratories
Registration Date: 23.06.2016 18:05:38 UTC

Project Hash: 28299503635d9d500ac21e3eb6e99952b26e7336c908712f25677dc3fa0bc

TX: 02b082113e35d5362685094c2829e7e2963fa0b5369fb7f4b79c4c908777dc3d3
Block: 266484
Use case

Enhanced confidentiality agreements

The NDA dilemma:
- broad ⇒ unenforceable
- specific ⇒ complex, discloses trade secrets

Blockchain enhanced NDA:
- simple, strong, private

---

**NONDISCLOSURE AGREEMENT**

1. This Non-Disclosure Agreement (the "Agreement") is entered into by and between

('Disclosing Party')

and

('Receiving Party')

for the purpose of preventing the unauthorized disclosure of Confidential Information as defined below. The parties agree to enter into a confidential relationship with respect to the disclosure of certain proprietary and confidential information ('Confidential Information').

For purposes of this Agreement, "Confidential Information" shall include trade secrets and confidential information designated as such by the Disclosing Party prior or at the time any such trade secret or confidential information is transmitted to the Receiving Party. Notwithstanding the foregoing, any information transmitted by the Disclosing Party to the Receiving Party concerning:

shall constitute Confidential Information.

3. Receiving Party's obligations under this Agreement do not extend to information that is: (a) publicly known at the time of disclosure or subsequently becomes publicly known through no fault of the Receiving Party; (b) discovered or created by the Receiving Party before disclosure by Disclosing Party; (c) learned by the Receiving Party through legitimate means other than from the Disclosing Party or Disclosing Party's representatives; or (d) disclosed by Receiving Party with Disclosing Party's prior written approval.

4. Receiving Party shall hold and maintain the Confidential Information in strictest confidence for the sole and exclusive use for Receiving Party's own benefit, which may or otherwise disclose to others, except the use by others for their

---

**Blockchain-enhanced NDA**

Between "Legal person or entity A" hereinafter referred to as "Inventor" and "Legal person or entity B" hereinafter referred to as "Recipient"

Whereas:

Inventor and Recipient intend to collaborate on a joint project and, in order to define the nature and content of the collaboration, the Inventor wishes to share technical and/or commercial information of a confidential nature with the Recipient that will ensure that the same remain confidential. Now, therefore, it is hereby agreed as follows:

1. For the purposes of this Agreement "Confidential Information" shall mean such technical and/or commercial information as univocally identified by Annex A, a blockchain certificate issued via Bernstein Technologies GmbH, the specific certificate number being xxxx-yyyy-wwww-zzz.

2. Additional information disclosed by the Inventor to the Recipient during the collaboration should be considered part of the Confidential Information only if:
   a. the new information is identified by a new blockchain certificate logically linked to the one mentioned in 1. (see Annex 2 for technical details)
   b. the new blockchain certificate is transmitted to the Recipient along with the new information.
Use case

Securing 3D models

Copyright claims: the traditional way

- Slow and inconvenient
- Reveal trade secrets
- Expensive
- Limited geographies

Copyright claims: the blockchain way

- No need to redact files
- Perfect confidentiality
- Strong ownership claim
- Convenient, quick, global.

Consistent enforcement and **statutory damages** may dissuade infringers (anyone with a 3D printer). But strong copyright claims are required.

---

**IndustryWeek**

3D Printing May Lead to Increased Copyright Litigation

Mar 13, 2017
Use case
Better defensive publishing

Defensive publishing is getting more popular, but it is not trivial neither cheap to execute in a robust and indisputable way.

In-house
- publication date can be challenged
- public availability is hard to prove

Commercial services
- expensive
- limited visibility, for paid access

Blockchain registration + IPFS publishing
- robust and indisputable timestamp
- proven public availability
- optionally anonymous
- convenient and inexpensive
- always secures the largest perimeter
- not just for documents (datasets, visuals, ...)
- freely available to anyone

Disclosure certificate
October 2017
Team & Contacts

Marco Barulli
Managing Director

Paul Reboh
Chief Technology Officer

Jean-Maxime Rivière
Business Development

Andy Goldstein
Deloitte Digital - LMU

Tankred Hase
Lightning Labs

Sevim Süzeroglu
Dennemeyer

Bernstein Technologies GmbH
Maximilianstr. 52
80538 Munich - Germany

web: www.bernstein.io
email: info@bernstein.io