

Blockchains for Copyright

Making Use of Bitcoin's Technology to Protect, Track and Monetize Digital Works

Submitted by Mathijs Koenraadt on Thu, 11/12/2015 - 09:45 · Essay · 6 min read

The very nature of the internet that allows content creators to disseminate their work globally and instantly also allows for anyone to pirate near-free copies of identical quality. Content creators that broadcast their work online give up control, hoping that the benefits of internet dissemination outweigh its potential loss of income due to piracy.

Anti-piracy efforts have come a long way since early attempts at disabling the 'Right click...' functionality in web browsers. Looking into Bitcoin's underlying blockchain technology, we must recognize that it too can not help to fully prevent copyright infringement, but the technology offers several applications that may support copyright holders in enforcing, tracking or monetizing their works.

Such applications include validating a proof-of-existence, a proof-of-authorship and -identity, as well as proving the existence of a physical work of art, the creation of digital scarcity and, in the future, possibly even the tracking and tracing each individual copy and derivative of a digital work.

Blockchain Dilemmas

Bitcoin's creators imagined a fully decentralized technology that generates a global yet trust-less consensus on the validity of transactions made to a certain public ledger. Almost by definition, such true decentralization involves great inefficiency, as embodied by Bitcoin's proof-of-work mining algorithm required to validate these transactions.

Such inefficiency comes at ridiculous cost: at current **conversion rates** and **mining rewards** (3600 Bitcoin per day), Bitcoin investors pay approximately **\$850k per day** to secure the network, or over **\$300 million per year**. That's a lot of money wasted on mining hardware, maintenance, operating fees, mining pool middle-men, electricity and personal gain.

Design Flaws and Private Blockchains

Due to its high security cost that will only make CFO's frown, the Bitcoin blockchain

has no commercial use case. And then there's a host of design flaws setting Bitcoin up for failure. The so-called [longest-chain rule](#) may some day potentially undo every transaction ever made. Bitcoin's native reward halving will lead to a *programmed death* as miners eventually switch to more rewarding coins. Bitcoin transactions could have been [100 times faster](#) if its anonymous creator hadn't forgotten or neglected to add time stamps.

Even a most-promising alternative created by [Ripple Labs](#) was recently exposed to contain a [major design flaw](#). The “workable” solution lies in *semi-decentralization*: the private blockchain, also called a “shared database”. A private blockchain can be hosted by multiple publicly trusted parties who make their ledger available as a public service. For example, Creative Commons could ally with the MPAA and other copyright organizations to host a single public copyright ledger, a *Blockchain-as-a-Public-Service* (BAAPS), for content creators to register their copyrights with.

Blockchain Applications for Copyright

Using such a private blockchain, or shared database, as a public service, we can identify several applications for copyright holders. The following applications are possible today:

I—Proof of Existence

Artists, writers and other content creators can use a public blockchain service to self copyright their work. Using the blockchain, they can prove their work existed at a certain point in time, and at the same time apply a copyright license of choosing. This protects the content creator against third party claims over earlier authorship. If everyone would have their digital work signed on the blockchain, we could easily identify or prevent plagiarized works.

Such a proof-of-existence relies on a digital signature consisting of the digital work of art itself. The content owner keeps a private part of the signature. This private key can be used to prove that the work really existed at some point in time. To ease the self-copyrighting process, and perhaps allow for changing licenses, such a blockchain solution would require real-time branching and versioning, just like [GitHub for code](#).

II—Proof of Authorship and/or Identity

Next, the content creator can prove his own authorship of the work, because he/she alone owns the private key proving the work existed. But we can extend this proof-of-authorship with a separate blockchain service on which content authors prove *they* exist. Note that in the future content creators may not be human beings, but machines, e.g. “smart artists”, self copyrighting their own machine-made work.

(Machines can own the copyrights to their smart output.)

III—Digital Scarcity

A different angle at copyrighting digital works makes the work itself a digitally scarce object, of which only a certain number of copies exists on a given blockchain. For example, imagine a blockchain for artworks where the public key itself contains the artwork, which can be traded online (like Bitcoin). Art collectors would own the private key(s) that accesses their digital collections.

This may sound far-fetched, but simpler applications of digital scarcity already have viable use cases. Blockchain technology allows for digitally scarce concert or movie tickets, or gift cards, that users redeem upon consumption, thereby voiding all other copies. For example, a holder of a unique digital movie ticket—or “ticketcoin” in the Bitcoin parlance—sends his ticketcoin to a revolving “smart door” granting him access to the cinema. Although he sent his friends a copy of his private key, the already redeemed ticketcoin is now no longer available to them. In other words: digital scarcity on a blockchain solves the problem of forged paper tickets.

Note that ‘digital scarcity’ does not imply a work of art can only exist once. Artists may choose to disseminate unlimited copies of their work, but each embedded with a unique serial number tied to a blockchain ledger. Pirated copies would show up as illegitimate copies, because would have duplicate serial numbers.

A Blockchain-Based Internet?

In the future, the entire internet might be built on top of a blockchain, whereby Internet Service Providers (ISPs) act as trusted nodes. This next-generation internet could track the whereabouts of each and every bit of information. Each copy of a file would be stored in a global public ledger. This would allow content creators to track each and every copy, whether pirated or not, and potentially identify the users.

Such an internet, of course, would be a digital police state, but the obvious commercial benefit to control what information users access might allocate the funding to build it. In the future, I suspect the rise of quantum computing (and quantum storage) may spur the development of such a blockchain-based, “quantum-traceable internet”.

This Quantum Web offers content creators the power to enforce their copyrights, track and trace content usage, and value and monetize their content, while still enjoying the benefits of global dissemination.

Tags:

[blockchain](#)

[Bitcoin](#)

[copyright](#)

[ledgers](#)



Blockchains for Copyright by [Mathijs Koenraadt](#) is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](#).