Bitcoin

Primavera de Filippi

Bitcoin by Primavera De Filippi
in Haunter D. & Op den Kamp C. (eds). A History of Intellectual Property in 50 Objects. *Cambridge University Press*

On 12 January 2009 a pseudonymous entity signed a transaction that instructed a distributed network to transfer a small amount of digital currency to Hal Finney, one of the key figures of the cypherpunk movement. After a few minutes, the transaction was recorded on a distributed public ledger, permanently updating the balance of both parties. This transaction—the first Bitcoin transaction—marked the beginning of a new era of decentralized payment systems, ushering in a variety of new financial services that do not depend on any centralized clearinghouse or other financial middleman.

Bitcoin is regarded by many as a powerful technological innovation that could disrupt many sectors of activities, in the realm of finance and beyond. But the underlying technology on which the network operates, the Bitcoin *blockchain* can do much more than that. Just as the internet did in the early-'90s, blockchain technology carries with it a whole new range of promises concerning how decentralization can support and promote individual freedoms and autonomy. Blockchain proponents believe that Bitcoin and other cryptocurrency platforms will revolutionize mechanisms of value exchange in the same way that the internet transformed information sharing, by providing a platform for people to exchange digital resources, in a secure and decentralized manner, without the need to rely on any intermediary operator or trusted authority.

A blockchain is a decentralized database of transactions maintained by a distributed network of computers, which all contribute to the verification and the validation of transactions. Once accepted, these transactions are recorded inside a "block" of transactions, which incorporates a reference to the previous blocks. This creates a long chain of blocks —a "blockchain"— that stores the whole history of transactions in a chronological order. Every block contains information about a particular set of transactions, a reference to the preceding block in the blockchain, and the answer to a complex mathematical puzzle, which is used to validate the data associated with that block. A copy of the blockchain is stored on every computer in the network, making it virtually impossible for anyone to unilaterally modify the data stored on this decentralized database, because if anyone tries to modify even a single of these transactions, the fraud will be immediately detected by all other network participants. The initial implementation of the idea of a blockchain is found in the first Bitcoin whitepaper. Released on 31 October 2008, it was attributed to "Satoshi Nakamoto," a pseudonymous entity who has managed to keep his or her (or their) identity secret despite numerous attempts by the media to unravel this secret identity.

While no one owns the Bitcoin network, many people own *Bitcoins*, the virtual currency that enables this network to run and operate in an open and distributed manner. But what does it mean to "own" a Bitcoin? With cash, things are relatively simple: if you have a $10 bill in your wallet, you probably own it: as with many physical things, ownership is closely related to possession. Ownership of digital things is much more complicated, not because possession is more difficult to assess—it is relatively straightforward to determine whether or not I have a digital file stored on my device—but because in the digital world possession doesn't really line up neatly with ownership. I might possess a copy of an MP3 sound recording, but I may not have purchased it and even if I have it's not clear that I "own" it.

Intellectual property is a legal layer of artificial scarcity imposed over specific types of information, in order to facilitate the trading of these information goods. Its goal was to re-align the properties of information (a non-rival good) with the properties of the medium into which it had been embodied (a physical and therefore necessarily rival good).
The model broke down with the advent of Internet and digital technologies. Digital resources are—just like information—inherently non-rival: they can be held and consumed by multiple persons at the same time, without this affecting the opportunities for others to enjoy the same resource. The non-rivalry of the digital world is one of the wonders of the information age, and is fundamental to our ability to use the internet in order to share knowledge with one another. It also lies at the heart of the battles that have been waged over intellectual property in the digital age.

From the late 1990s and early 2000s, there emerged a growing wave of copyright infringement—sometimes called "online piracy"—where millions of copyrighted songs, videos and audiobooks were illegitimately reproduced and distributed over the internet. The pushback from the content industries led to lawsuits, new laws, and earnest public service announcements, along with a drop in the general perception of the legitimacy of copyright law in the digital environment. The law was regarded by many digital natives as a leftover from a previous era, or simply something that could be safely ignored.

Solving the digital scarcity problem is at the core of Bitcoin. Although a Bitcoin is nothing more than a series of bits stored on a decentralized public ledger that is associated with someone's Bitcoin account, because of the design

of the underlying blockchain network, no one has the ability to reproduce or multiply their Bitcoin in the same way as they could reproduce a digital file.
With the blockchain, we have gained the ability to create digital resources that are inherently scarce, in that they cannot be digitally copied or reproduced. Before, it was only possible to *reproduce* digital assets, since transferring a digital file over the internet still allows the original owner to keep a copy of the file. With Bitcoin, it is now possible to *transfer* digital assets, without copying them..

The development of Bitcoin thus marked the beginning of a new era: an era of digital scarcity, one where digital bits can be transferred over the internet, without losing their scarcity, and without recourse to intellectual property laws. The first great advance ushered in by Bitcoin is therefore that it enables us, for the first time, to apply the notion of property over digital assets. And we're not talking here of intellectual property over an information good, but of a real property right over digital goods.

But the significance of the blockchain is not limited to digital currency. Less than ten years after the first Bitcoin transaction, the blockchain protocol has inspired a large variety of new applications, many of which extend well beyond the realm of finance. From decentralized registries, recordation systems, marketplaces and peer-to-peer value exchanges, the blockchain protocol is currently being used for numerous applications that do not rely on any centralized intermediary or middleman. The blockchain can be used as the underlying transaction layer for the trading of many digital assets in a secure and decentralized manner.

The same rules that apply to the transfer of Bitcoins can be applied to other digital resources—whether these are digital currencies, certificates, copyright licenses, or even titles to specific assets or commodities that subsist in the physical world. It can even be applied to revolutionize trademark law: rather than rely on brands and marks to distinguish the source of goods, companies can rely on a blockchain in order to prove the authenticity of their products, by associating them with a particular Bitcoin transaction. For instance, Armani or Louis Vuitton could transfer a small fraction of Bitcoins along with the purchase of any of their designer clothes, which would serve as a seal of authenticity to prove that these products are, indeed, authentic. When selling these products on the secondary market, the original purchaser would also need to transfer these Bitcoins to the new buyer—who would then be able to prove and verify that the product is not a counterfeit. Initiatives of this kind already exist to prevent the counterfeiting of luxury goods, in markets such as diamonds, for instance. Today, a diamond's authenticity is guaranteed by paper certificates, which can easily be forged. The company *Everledger* is using the Bitcoin blockchain to register diamonds, along with their unique identifier, that is, a digest of the diamond's features, including its color, clarity, and imperfections. This contributes to increasing the transparency and traceability of diamonds' supply chains, giving people the possibility to trace the movements of these diamonds as they pass from hands to hands.

Most relevant in the context of intellectual property is the use of Bitcoin and other blockchain-based applications to manage the dissemination of artistic works recorded in a digital format, and the transfer of limited editions of these works. It was, until now, impossible to create limited editions of a digital work, since anyone in possession of one of these editions could simply reproduce it into multiple identical copies. By recording the unique identifier of each legitimate copy of a work on the Bitcoin blockchain, the copy can become forever associated with a particular Bitcoin transaction—even if it is only worth a few cents—so that the ownership of that copy can be transferred in a secure and decentralized manner, just like one would make a Bitcoin transaction. Of course, people still retain the ability to reproduce the digital work and distribute it as they wish, but only the recipients of the relevant Bitcoin transactions will be able to prove that they are the legitimate owners of an authorized copy of the work.

This usage of the Bitcoin blockchain offers new opportunities to artists, eager to distribute their digital works over the internet while preserving the scarcity and authenticity of these works. Using the blockchain, digital objects can be imbued with a greater degree of rivalry and may be traded or exchanged in ways that are roughly equivalent to tangible property—i.e. claims to digital copies could be transferred from user to user, just like a book can be passed along from person to person. Secondary markets are likely to emerge, where copyright owners can transfer title to digital resources—e-books, digital movies, music files, and so on—which will potentially lower the price of these resources and increase their public availability.

The Bitcoin blockchain is, therefore, much more than a decentralized payment system. It is a decentralized ledger that makes it possible for anyone to exchange scarce digital resources—such as virtual currencies or unique digital copies of a creative work—in a secure and decentralized manner, without the need to rely on any trusted authority or centralized middleman.

At first glance, Bitcoin might thus appear to be a powerful tool for the enforcement of copyright in the digital world. Yet, Bitcoin's relationship with intellectual property laws is ultimately a double-edged sword. Depending

on the usage that is made of the technology, it could serve either as a friend or foe to the intellectual property regime–and copyright law in particular.

Indeed, the very same properties that make Bitcoin so valuable for exchanging value in secure and decentralized manner, also make it a powerful tool to publish and disseminate information in a way that cannot be retroactively deleted or modified by anyone. On the one hand, the Bitcoin blockchain can be, and has been, used by authors and artists to publish and license their works, in ways that might facilitate the enforcement of copyright law. On the other hand, the same technology is providing new means for people to disseminate information on a tamper-resistant and censor-resistant network, in ways that might easily run afoul of existing laws aimed at restricting the flow of information.

By recording data on the Bitcoin blockchain, a user can be sure that, as long as the blockchain exists, these data will remain permanently and persistently available to anyone who holds a valid copy of the blockchain. Any attempt by a third party to censor such information will be doomed to failure, since the network will simply ignore the request. The underlying protocol of the Bitcoin network makes it extremely difficult for censorship to occur in the first place, since it requires a coordinated action of more than 51% of the computational power of the network to retroactively alter the blockchain.

Because of the disintermediated nature of a blockchain, law enforcement authorities do not have the ability to restrict the flow of online communications using traditional means. In the context of most centralized online platforms, enforcement authorities can exert pressure on service providers or intermediary operators, who are responsible—upon notice—for taking down any illicit content from their platforms. In a decentralized network like Bitcoin, the lack of a central authority in charge of managing the network makes it virtually impossible for any single party to control the type of information that can be posted onto the network, or subsequently to censor or block that information. Whether it is copyright infringing material, cyber-bullying or hate speech, all information recorded on the Bitcoin blockchain will forever exist, outside the reach of the long arms of the law.

It is the dichotomy between blockchain technology as a *regulatory technology* and its potential use as an *unregulatable technology* that makes it so interesting from a legal perspective. The distinctive features of a blockchain—in terms of transparency, resiliency, and incorruptibility—can be regarded simultaneously as the greatest gift and as the greatest curse for intellectual property. While they might strengthen the ability for right holders to enforce their intellectual property rights, they may also lead to the demise of the current copyright regime, as well as other laws aimed at restricting the flow of information. ♦

Further Reading

Primavera De Filippi and Aaron Wright (2018). *Blockchain & The Law: The Rule of Code*. Cambridge: Harvard University Press.

Primavera De Filippi & Samer Hassan (2016). Blockchain technology as a regulatory technology: From code is law to law is code. *First Monday*, *21*(12)

Jessica Litman (2001). *Digital copyright*. Prometheus books.

Satoshi Nakamoto (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at: https://bitcoin.org/bitcoin.pdf

Don Tapscott and Alex Tapscott (2016) *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. New York: Portfolio Penguin.

Hal R. Varian (1999). *Markets for information goods* (Vol. 99). Institute for Monetary and Economic Studies, Bank of Japan