Cryptocurrencies beyond transactions. How they can evolve to a technological platform for digital content certification

by Yiorgos Lykidis

01/03/2015

The technology behind the digital cryptocurrencies can have revolutionary applications which do not necessarily relate to money or currency transactions.

Recording of information on the decentralized public ledger of cryptocurrencies may become an alternative platform for record keeping that is traditionally carried out by centralized private or public organizations/authorities.

The Blockchain

Cryptocurrencies are based on the recording of all transactions in a public book/ledger, also known as the “blockchain”. For Bitcoin, the blockchain is updated every 10 minutes with an additional block of new transactions. This public ledger is not saved on a centralized server but is maintained on a vast peer to peer network with thousands of nodes around the world. Ensuring consensus between the nodes regarding which of the new circulating blocks of transactions will become the new unquestionable record on the public ledger is accomplished through the "mining" process based on a proof of work concept (http://en.wikipedia.org/wiki/Proof-of-work_system).

To summarize, a cryptocurrency’s public ledger (blockchain) has the following characteristics:

1) It is completely decentralized and its existence is based on the consensus of all the nodes in the peer to peer network.

2) Its records are undeniable and irrevocable.

3) It is public and can be read by anyone having access to the internet and the peer to peer network.

Bearing in mind the above, it has been proposed that the technology behind the blockchain may have various applications in replacing book keeping services that have been traditionally provided by centralized organizations/authorities, not necessarily publicly accessible and always susceptible to illegitimate record amendments (due to their centralized nature). For example, it has been proposed that the Blockchain could become an ideal platform for the recording of property, personal identification, contracts and other.

Proof of existence, possession and ownership

One of such possible applications, is the time stamping of digital content of any type (documents, creative artwork, photos, scientific papers etc) on the blockchain ledger. By blockchain time stamping, one could, at any time in the future, prove the existence of the content at the time of the stamping.

A few such blockchain time stamping services have recently emerged on the internet, acting as the middle part between the end user and the bitcoin blockchain network. When a user of these services time stamps digital content, its unique hash 32-byte imprint (derived through a

cryptographic hash algorithm named SHA256) is publicly linked with the current date and time. Given that the imprint can easily be derived from the content itself, the user who made the stamping, will be able to prove in the future that the content itself existed at the time of the stamping with the argument that the imprint is publicly and unquestionably linked to the particular point in time.

It is noted that due to the nature of the SHA256 cryptographic algorithm, it is not possible for the digital content to be derived from the imprint itself (only the other way around is possible and also with a zero possibility of two human-created digital creations having the same imprint). Therefore, it depends on the user when he will express in public which digital content corresponds to the imprint he has time stamped on the Blockchain.

If the user time stamps digital material which is a product of authentic original work/creation and if he has included a statement or signature within the content itself, then the publicly stated time stamping of the imprint could potentially be used in the future to argue that the content was at the user's disposal at the time of the stamping.

Obviously if the content has not be stolen and if it is not possible to find a prior public record of intellectual property related to it (including the literature, newspapers, public authorities etc), then in that case the user can claim a solid ownership of the content.

Still, given that the blockchain technology is very recent, there is no experience on how the above concept could be used in a court of law. But one would normally expect that any specialized IT expert witness could certify the above facts and confirm the credibility of the blockchain time stamping. We may not be very far from the time where the above technology could be used as an unquestionable argument on intellectual property against court.

Example

As an example, let's assume that someone creates a movie script. Before sharing it with others, he signs it and includes a statement of ownership. He then proceeds with a blockchain time stamping according to the above procedure. The signed script's imprint is publicly recorded on bitcoin's public ledger and is linked with that certain point of time. In the same time the script remains exclusively in the possession of its author, as only its imprint is public. It is at the author's discretion when he will disclose the script which corresponds to the publicly stated imprint.

Having in mind the above, the user can distribute his script to others for their consideration. He is fully covered against theft as he can at any time prove that he was the first to have the script in his possession by referring to the appropriate blockchain public time stamping record. As he is the first to have publicly stated possession of the script he is also its undeniable owner.