Bloomberg BNA

Electronic Commerce & Law Report™

Authentication

Blockchain Technology Underpinning Bitcoin Used to Authenticate Documents, Digital Art

BY JOSEPH WRIGHT

"Don't trust but verify'' could be the motto of the virtual currency community, but the trustless verification permitted by the Bitcoin blockchain is being put to work authenticating digital objects that have nothing to do with the cryptocurrency itself.

Authentication is a natural application for the blockchain technology. Two inputs can be proven to be identical or not by any third party by comparing cryptographic outputs without revealing the contents of the inputs themselves. Because the blockchain expands at a consistent rate, adding an input to the blockchain also serves to timestamp the input within approximately an hour of certainty.

The blockchain offers a promising solutions for document authentication in legal disputes and for preventing digital art forgeries. The blockchain allows document authentication by creating evidence that a later-submitted document is identical to an earlier version. Providing a similar function for digital artworks, the technology not only has the potential to prevent theft but also to solve chain of title and marketability problems that have plagued the digital art market.

Authenticating Documents Via Blockchain. Several notary-type services have been created to take advantage of blockchain authentication. The most prominent of these resides at proofofexistence.com.

The Proof of Existence service does not retain a copy of submitted documents, except as a cryptographic output published to the blockchain. A perfectly identical document resubmitted later will create the same hash, but the hash itself cannot be reversed to recreate the document. Thus a subsequent submission will generate the same hash if, and only if, the document is identical to the first document.

Publishing the digest to the blockchain allows Proof of Existence to timestamp the document. A new block is added to the blockchain approximately every 10 minutes. Embedding the digest in a particular block creates a permanent record that the document was submitted during the creation of that block. The time the document was added to the blockchain can thereby be triangulated to a window of less than an hour.

Pamela Morgan of Empowered Law described the process of authenticating a document via Proof of Existence in a recent blog post. For example, Morgan submitted a document to Proof of Existence. Twenty days later she re-uploaded the same document. Using blockchain technology, Proof of Existence was able to detect that she had earlier submitted the identical document.

Morgan said she had to try the experiment twice, confessing that the first test failed because she uploaded a word processing document rather than a PDF. Because word processing documents contain metadata that change even as the contents of the document remain the same, the second upload of the word processing document did not create a match.

What Might Courts Say? While untested thus far in court, evidence provided by Proof of Existence could conceivably be used under existing evidentiary rules. Fed. R. Civ. Pro 901 provides that the proponent of evidence must show that the evidence is what the proponent purports it to be. Rule 901(b) provides a non-exhaustive list of examples of evidence that satisfy this requirement, include subsection (b)(9): ''Evidence describing a process or system and showing that it produces an accurate result.''

Rule 902 by contrast provides that 12 types of evidence are self-authenticating and require no extrinsic evidence as to their authenticity. These include certified copies of public records, newspaper and periodical articles, acknowledged or notarized documents and commercial paper.

Professor Colin Miller of University of South Carolina Law School told Bloomberg BNA that he can imagine Proof of Existence and similar services being used in court via Rule 901(b)(9), for instance in litigation related to a transaction where the timestamping of different versions of documents was at issue.

''If it's adopted by a few courts, it could become an established practice,'' Miller said.

Miller was less sanguine about whether the Federal Rules could someday be amended to allow self-authentication via Proof of Existence. ''I don't see them ever adding another example for blockchain services under Rule 902 for self-authentication,'' he said.

Arbitrators More Receptive? The first practical evidentiary applications of Proof of Existence might not be in U.S. courtrooms, Morgan told Bloomberg BNA, but in the international arbitration forums increasingly preferred in international commercial dispute resolution.

''In the U.S. we prefer witnesses to be called,'' Morgan said, ''but that's not necessarily the case everywhere in the world. In international commercial arbitration, for instance, many times witnesses aren't called at all. Many times the documents themselves are submitted as the evidence.'' This may particularly apply to witnesses routinely called in U.S. courts for very limited purposes to testify to document authenticity or chain of custody.

Because blockchain technology is independent of any government, Morgan said, it can lend validity to the submitted documents in international forums rather than relying on the validity of notaries in any particular country.

Is the Blockchain 'A Revolution For Digital Artists'? The digital inputs that can be validated via the blockchain are not limited to documents. A collaboration between New York University professor and artist Kevin McCoy and noted technologist and blogger Anil Dash is using the blockchain to authenticate — and perhaps create a more viable market for — digital artworks.

Monetized Graphics, or monegraph.com, provides a similar service to Proof of Existence but for digital images. Monegraph uses the blockchain technology of an alternative virtual currency, Namecoin, to create a digital signature and time-stamp for a particular image. The claimant inputs a URL containing the image and then signs into Twitter. Monegraph then tweets out a link to the image and creates a block of code to paste into a Namecoin client.

The claimant then creates a small Namecoin transaction — currently about four cents worth — using the block of code as the transaction key and value. That transaction encodes the image's time-stamped digital signature and a plain language assertion of ownership on the Namecoin blockchain. Any subsequent attempt to submit the same image will not pass Monegraph's validation system, as the work is already signed.

Monegraph provides two aspects that have been largely missing from the online digital art world, according to McCoy and Dash's presentation at the TechCrunch Disrupt NY 2014 event — verification and provenance. The time-stamped Twitter message and its encoding on the blockchain provide verification of authorship and that the artwork has not been changed. Permanent storage on the blockchain also provides provenance — a term traditionally referring to the proof of chain of title of a painting or historical document.

''The ownership title or the claim of that record can be traced or exchanged and a market can be created,'' McCoy said.

Dash showed an overhead photograph of what appears to be a parking lot, the image McCoy and Dash used for the initial trial run of Monegraph.

''This image that Kevin and his partner Jennifer created became the first digital image that was signed to a blockchain that could verify that it was a unique digital work and that we could establish provenance for it and that it could be transferred to another person to buy. In this case I actually was able to buy this artwork,'' Dash said.

''That's a revolution for digital artists.''

Putting Monegraph on Trial. For visual artworks, the legal test of authenticity has long involved stylistic inquiry, documentation, scientific verification or some combination of these elements, Robert Darwell, the head of Sheppard Mullin's art law practice, told Bloomberg BNA.

''Monegraph's attempt may be regarded as a combination of documentation and scientific verification,'' Darwell said, ''however certain issues regarding admissibility of Monegraph's authentication will have to be tested in the courts.''

Darwell said that the admissibility of Monegraph authentication will depend on whether and how widely known the technology becomes in the art industry.

He added that digital artworks reproduced on the Internet will likely be considered ''fine art multiples'' under California law, subjecting them to certificate of authenticity requirements before they can be sold by licensed art dealers. ''Complying with this law might also become an issue for digital art, but the authentication of the digital art by Monegraph may or may not suffice.''

To contact the reporter on this story: Joseph Wright in Washington at jwright@bna.com

To contact the editor responsible for this story: Thomas O'Toole at totoole@bna.com