Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Blockchain's Potential Role In Admissibility Of Website Docs

By **Kelce Wilson**

Law360, New York (July 11, 2017, 11:49 AM EDT) --

Kelce Wilson

Attempting to use internet-sourced documents to resolve a dispute, whether in litigation or an administrative proceeding, you might just be inviting your opponent to bring evidentiary challenges. One of the issues with documents found on websites is that you can rarely have much certainty that the document had not just been altered and backdated by hackers, just a matter of minutes before you first encountered it.

This is not just a theoretical problem, it could affect the admissibility of documents that could otherwise be dispositive in settling a dispute. In St. Clair v. Johnny's Oyster & Shrimp Inc., a personal injury case in which the plaintiff attempted to use internet-sourced material, the court had rather harsh words:

There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No website monitored for accuracy and nothing contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on any website from any location at any time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules found in Fed R. Evid. 807. Instead of relying on the voodoo information taken from the Internet, Plaintiff must hunt for hard copy backup documentation in admissible form ... [1]

In a later seminal case on the admissibility and authentication of digital evidence, Lorraine v. Markel American Insurance Company, the court was more forgiving, but did comment on "the possibility that third persons other than the sponsor of the website were responsible for the content of the postings."[2] Cause for suspicion in digital evidence is likely well-deserved.

Consider the 2012 case of Paul Ceglia forging a purported 2003 contract with Mark Zuckerberg in a PDF file.[3] According to a criminal complaint filed in the Southern District of New York, Ceglia actually did have some contract with Zuckerberg, for a project unrelated to Facebook, but tampered with the contract by replacing one page with a new page that indicated a transfer of interest in Facebook.[4] Ceglia leveraged the admitted existence of a contract to introduce the forgery. Zuckerberg was unable to dispute the existence of the contract, so the issue for the civil lawsuit became: Which version of the contract — Ceglia's or Zuckerberg's — was the authentic one? Fortunately for Zuckerberg and Facebook, Ceglia was careless and left sufficient forensic evidence within the PDF file that the forgery could be detected. Zuckerberg was lucky. In other situations, however, a forger might be more skilled or careful, and the victim will not find such dispositive evidence so easily. This means that there could be significant risk that the forgery is accepted as genuine, while the genuine document is discounted.

And now that the “look and feel” of websites can constitute protectable trade dress,[5] it is only a matter of time before there is an authentication challenge with accusations that the purportedly earlier website page was backdated. Additionally, scientific and technically focused websites can have evidentiary value for their content that can affect administrative proceedings such as patent examinations and re-examinations.

It may therefore worth investigating whether there is any way to more reliably ascertain whether the material found on a website is actually intact and unchanged since prior to some date that is significant to a dispute. This seems to be a challenge, given the court’s commentary in St. Clair. However, the recent advent of blockchains has produced solutions to some long-standing problems — and it turns out that a blockchain can help with authenticating internet-sourced material in some situations, to improve admissibility.

With a properly capable internet browser, legally significant documents that are found on the internet can be trusted to be intact, and therefore likely have greater evidentiary value — provided they had earlier been registered in the right kind of blockchain. Although a large number of people have heard the term blockchain, fewer understand the mechanism that enables trust in one. That topic will be quickly addressed, followed by an explanation of how to leverage trust in a blockchain to prove that a document has remained intact, even though it may have been retrieved from one of the least trustworthy of all venues: the internet.

Some blockchains have the potential to help identify the genuine version of a document, when a forgery is presented in situations similar to the Ceglia/Zuckerberg dispute. This is because blockchains enable trust that certain documents are free from tampering or alteration. For the relatively famous cryptocurrency blockchains, such as Bitcoin and Etherium, the primary trust is in ledgers that enable verification of who has the right to spend certain units of the currency. However, the trust mechanism can extend beyond application to merely cryptocurrency ledgers.

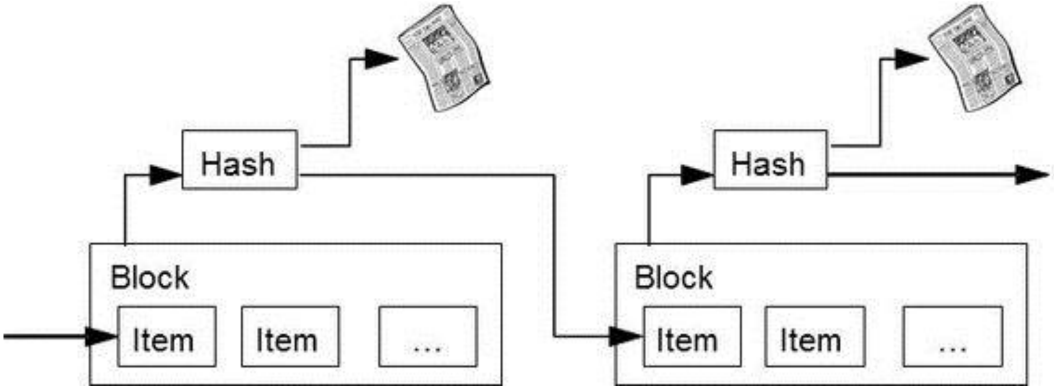
In simple terms, a blockchain is a set of information blocks with a self-evident unique sequential order. That is, given a set of information blocks, such as digital files, every honest observer will independently sort the set of blocks into the same unique sequence of occurrence, without requiring the observer to trust or defer to any other entity. The creation of a blockchain can be accomplished by iterative use of mathematical processes called hash functions that produce hash values. Hash values can be thought of as digital fingerprints for a computer file.

In the event that a block is forged, such as by adding deleting or modifying any information, that block’s hash value will be different, and anyone will be able to see that the forged block no longer fits within the sequence. This certainty of easy forgery detection is the foundation on which trust is built. Leveraged properly, a blockchain can enable trust, despite the absence of any trusted entity.

Bitcoin uses a hash function named SHA-256, although other hash functions could be used. Bitcoin and other cryptocurrency blockchains also use processes known as “proof of work” and distribute their ledgers only among a defined community of participants that vote on adding new blocks. Neither a proof of work process, nor community votes are required for the relatively easy task of verifying documents, such as ordinary contracts and estate planning material — and now website material.

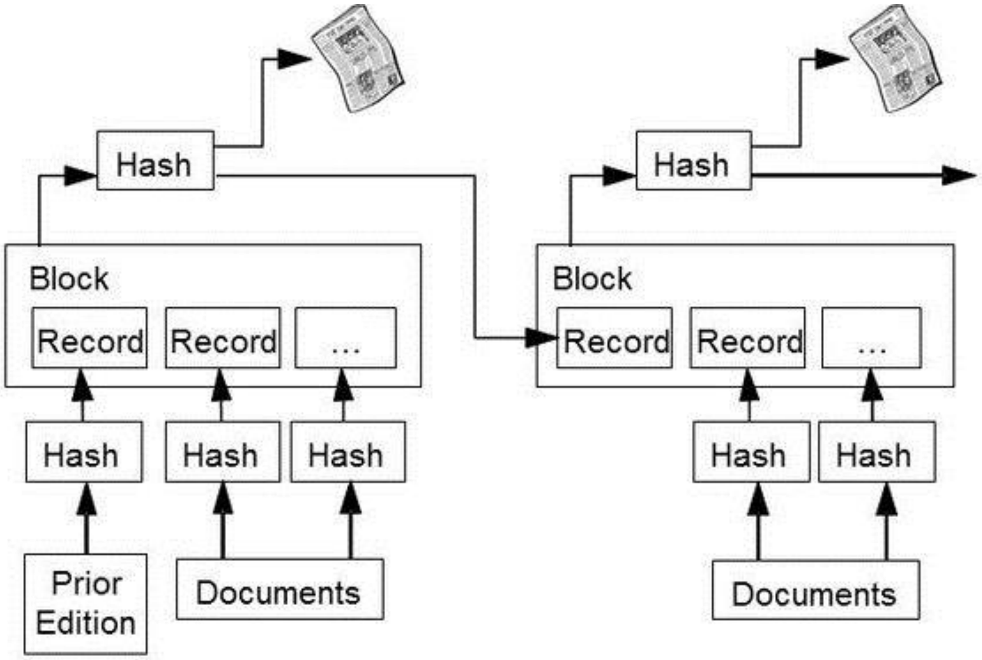
One useful improvement for the documents verification task is that the blockchain establishes not only just the sequencing of the blocks, but also establishes a no-later-than date-of-existence for each block. One such system is shown in Figure 1, which is a slight modification of the system originally shown in Figure 3 of the seminal Satoshi Nakamoto paper that introduced the world to Bitcoin [6]. As illustrated, Nakamoto's original system is modified by publishing the hash value of each block in a public venue, such as perhaps an ad in a widely-distributed newspaper.

Figure 1: Modified Blockchain With Date-of-Existence Proof



Since some people may wish to keep their documents private, unless disclosure is later needed to settle some dispute, so another improvement may be desirable: rather than inserting the documents themselves into the blockchain, generating hash values for the documents ("hashing the documents") and inserting those value into each of the blocks. This approach has the added benefit of enabling large documents to be protected by the blockchain, without the blockchain growing too rapidly. This type of system is illustrated in Figure 2. Another potential improvement is the use of a permissioned blockchain, in which some entity acts as a gatekeeper for blockchain entries, to ensure that the blockchain does not become bloated with material unrelated to its purpose.

Figure 2: Blockchain With Date-of-Existence Proof, Suitable for Large or Confidential Documents



Using the system of Figure 2 for website material is not difficult. The proof process for website documents requires a minimum of two steps, registration and later verification, shown in Figures 3 and 5. An optional process, shown in Figure 4, involves a search engine identifying that a website document is registered in a blockchain and then enabling users to specify website age or date as search criteria.

Initially, when a document is put on the internet, the website publisher also hashes that document and then inserts the hash value into a blockchain that permits anyone — not just community members — to search within the blockchain's contents. A useful blockchain system will return information to the website publisher that indicates which of the blocks contains the hash value, where within that block it can be located, and the provable no-later-than date-of-existence for that block. The website publisher then puts this information into a predefined folder on the website, where it can be easily located along with the document. Perhaps the folder is the same one containing the registered documents, or perhaps the website has a set location for the information regarding all documents in the same section of the website domain.

In many situations, though, a website publisher may have a webpage containing a mixture of information that will not change ("static content") with some information that could change often ("dynamic content"). For example, a webpage may have legally significant information about a person, product or service — which is intended to remain unchanged — along with advertisements that change continually. In such a situation, the website publisher can simply demark the static content with html tags, so it can be identified later, and send only the hash of the demarked content to the blockchain. This is illustrated in Figure 3. Additionally, many webpages are constructed from multiple files, such as textual material and images (perhaps in GIF or JPEG format) contained in different files. Each of these different files should probably be hashed separately. For versioning information, different revisions each require their own hash.

Figure 3: Registering Website Material in a Blockchain

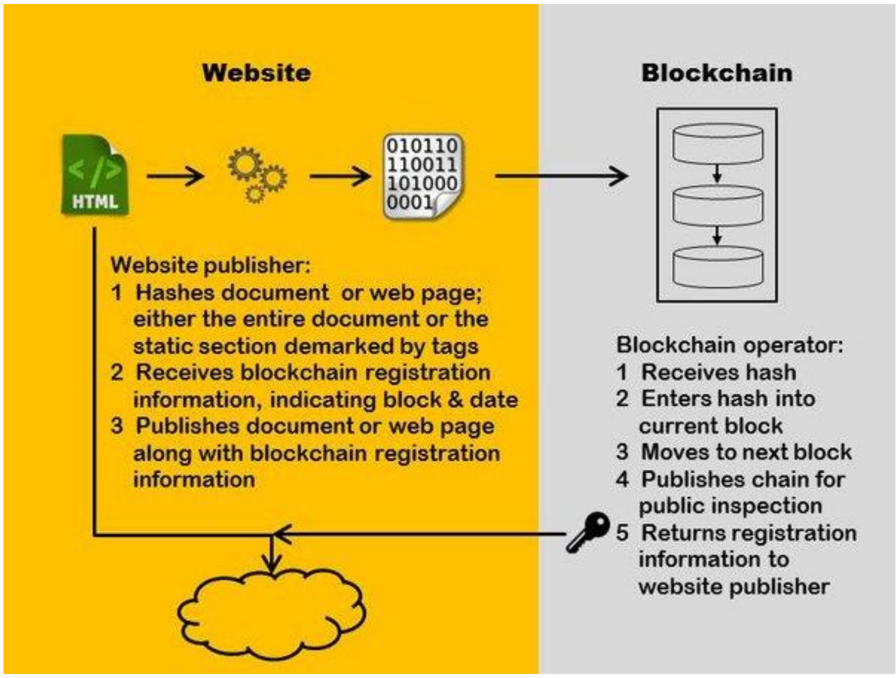
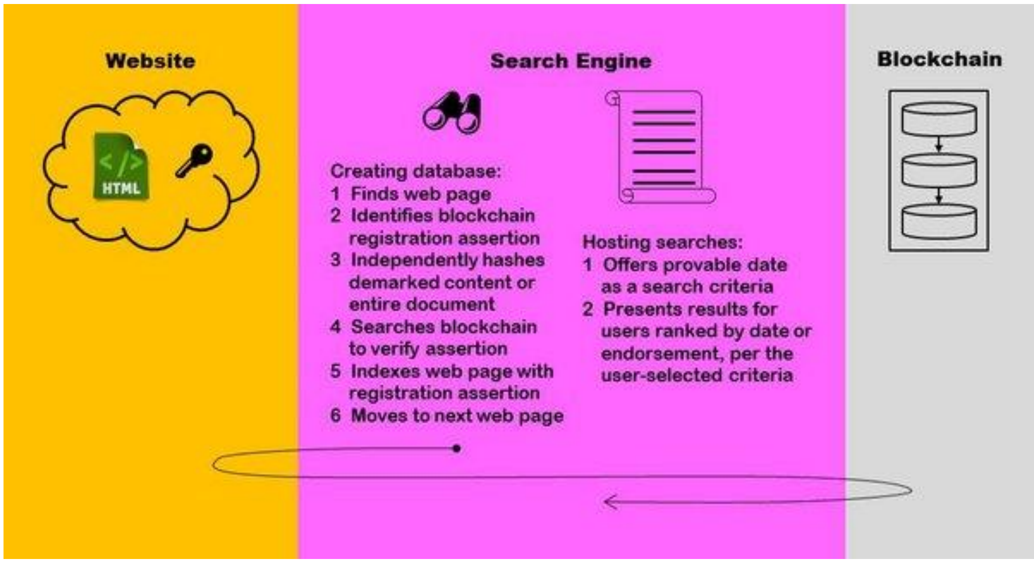

Website
Blockchain
HTML
010110
110011
101000
0001
Website publisher:
1 Hashes document or web page; either the entire document or the static section demarked by tags
2 Receives blockchain registration information, indicating block & date
3 Publishes document or web page along with blockchain registration information
Blockchain operator:
1 Receives hash
2 Enters hash into current block
3 Moves to next block
4 Publishes chain for public inspection
5 Returns registration information to website publisher

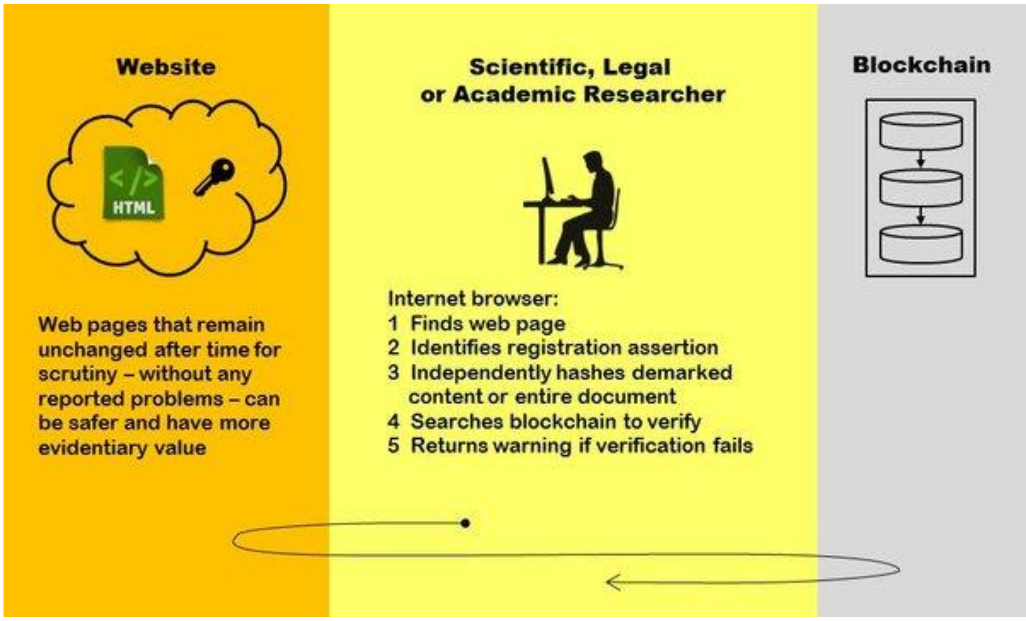
Figure 4 shows the optional step of a search engine compiling its database of internet resources. The search engine indexes the webpage, identifies the blockchain registration information, and adds this to its database. As a further option, the search engine may independently verify the blockchain registration, to avoid passing along incorrect information to users. The verification process is effectively the same as what will be described for an internet browser in the next step. Next, when a user performs a search, the provable date-of-existence is presented as a possible search criteria, and used to rank the results. Not shown, but possibly part of the system, is some trusted entity operating similarly as a certificate authority, that endorses claimed calendar dates and furnishes copies of the blocks for searching.

Figure 4: Search Engine Indexing a Website and Verifying a Blockchain Registration


Website
HTML
Search Engine
Creating database:
1 Finds web page
2 Identifies blockchain registration assertion
3 Independently hashes demarked content or entire document
4 Searches blockchain to verify assertion
5 Indexes web page with registration assertion
6 Moves to next web page
Hosting searches:
1 Offers provable date as a search criteria
2 Presents results for users ranked by date or endorsement, per the user-selected criteria
Blockchain

The proof step is illustrated in Figure 5. When an academic, legal or scientific researcher visits the website, the researcher's internet browser identifies the blockchain registration information. The browser then independently hashes the material — either an entire document or demarked static content. The browser locates a copy of blockchain to search, perhaps via a simple website address or through an equivalent of a domain name service to find the proper address and search within in the specified block. The researcher is advised of the verification results, whether a pass or a failure, or a mixture in the event of multiple files used within a single web page.

Figure 5: Using a Blockchain to Verify Website Documents


Website
HTML
Web pages that remain unchanged after time for scrutiny – without any reported problems – can be safer and have more evidentiary value
Scientific, Legal or Academic Researcher
Internet browser:
1 Finds web page
2 Identifies registration assertion
3 Independently hashes demarked content or entire document
4 Searches blockchain to verify
5 Returns warning if verification fails
Blockchain

At this point, if all verification tests succeed, the researcher can have confidence that the documentation found on the internet has the exact same content as some documentation that had been registered in the blockchain by the claimed no-later-than date. For webpages in which only static content is hashed, the browser might optionally highlight the verified content to alert the researcher. It might also permit saving only those files and portions of files that have been verified.

One additional new use of this capability is improving internet security and safety for some users. Consider the situation of parental controls on internet browsers. If a particular website is catering to children, they may register their website material in a “whitelisting” blockchain that only registers website material after performing a security and content-suitability evaluation. So, it would need to be a permissioned blockchain. The parental controls on the browser can be set to only display only those portions of a webpage that pass the verification tests, or block the entire page if any portion fails. In the event that a hacker had compromised the website, and inserted either malware or objectionable content, the browsers will fail at the verification step will fail, refuse to display the affected content, and thus automatically protect the child from potentially harmful exposure. It should be noted that, in comparison, parental control systems that whitelist by domain name, rather than the newer blockchain verification method, are susceptible to displaying malicious or objectionable content in the event that the website had been compromised by hackers.

This new capability, of establishing trust and evidentiary value in webpages and other internet-sourced documentation can be used in a myriad of other ways yet to be discovered.

Kelce S. Wilson, Ph.D., is the data privacy compliance and intellectual property counsel for Tenet3, a cybersecurity consulting firm serving both military contractors and civilian companies. Prior to beginning his legal career, he worked as a security penetration tester for the U.S. military. His patent work includes prosecution, litigation and license negotiation.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] St. Clair v. Johnny’s Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774–75 (S.D. Tex. 1999)

[2] Lorraine v. Markel American Insurance Company, 241 F.R.D. 534 (D.Md. May 4, 2007)

[3] FoxNews.com, Facebook files ‘smoking gun’ evidence in ownership lawsuit, March 26, 2012, available at http://www.foxnews.com/tech/2012/03/26/for-facebook-ownership-lawsuit-end-is-near.html.

[4] Criminal complaint in United States of America v. Paul Ceglia, SD NY, October 25, 2012, available at https://www.justice.gov/archive/usao/nys/pressreleases/October12/CegliaPaulCharges/Ceglia,%20Paul%20Complaint.pdf

[5] Ingrid & Isabel, LLC. v. Baby Be Mine, LLC., 70 F.Supp.3d 1105 (2014)

[6] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, available at https://bitcoin.org/bitcoin.pdf.