Reuters Legal News

Trade secret metadata and blockchain evidence: a perfect combination

By R. Mark Halligan, Esq., FisherBroyles, LLP

SEPTEMBER 28, 2021

Using the term "blockchain" is a buzz word that most lawyers do not understand. It is often confused with things such as "Bitcoin" — a digital currency launched in 2009 by a mystical person known only by the pseudonym Satoshi Nakamato.

A blockchain and Bitcoin are different.

Visualize blockchain as an operating system like Microsoft Windows and "Bitcoin" as one of many applications that can be run on a blockchain.

Think of a blockchain as a computerized ledger that can record and translate information into an encrypted hash code with a digital timestamp called a "block" that then can be linked to other information in the next "block" going *forward* in chronological order.

> *A blockchain provides an efficient, cost-effective, reliable and secure system for managing trade secret metadata with a timestamp function built into the blockchain linking the blocks chronologically.*

Each individual block now provides a unique fingerprint which identifies the specific block (a "hash") in the chain, the "hash" code of the previous block in the chain, and a digital timestamp proving when the information was put into the specific block in the blockchain.

The key to understanding the functionality of a blockchain operating system requires understanding cryptographic hashing. MD5 stands for Message-Digest algorithm 5 invented by MIT Professor Ronald Rivest in 1991 to replace the MD4 standard. MD5 is a one-way hash function because there is no way to reverse the encryption. Today, MD5 is widely used to convert variable-length plain text into a 128-bit hash value represented as a 32-digit hexadecimal.

Hash codes create unique and immutable tamper-proof records. Digital forensic experts routinely use hashing methods to verify that copies of digital evidence match the original data from which the copies are made, *i.e.*, the hashes or "fingerprints" match. A blockchain provides an efficient, cost-effective, reliable and secure system for managing trade secret metadata with a timestamp function built into the blockchain linking the blocks chronologically.

There are no security risks because the blockchain captures only the trade secret metadata (not the actual trade secrets) and the trade secret metadata is then encrypted using one-way hash functions. The 32-character alpha-numerical hash code is indecipherable.

ec55d3e698d289f2afd663725127bace.

Evidentiary proofs — existence, ownership, notice and access

The plaintiff in a trade secret misappropriation lawsuit must prove existence, ownership, notice and access (the "EONA" proofs):

- Existence: The information qualifies as a trade secret, *i.e.*, a trade secret exists.
- Ownership: Plaintiff has ownership rights in the information.
- Notice: Defendant had actual, constructive or implied notice of the trade secret status of the information.
- Access: Defendant had access to the information, *i.e.*, did not independently develop the information.

These evidentiary proofs can be established by the testimony of witnesses and the admission of documents or other physical evidence, or now, as discussed in this article, the admission of blockchain evidence.

Admissibility of blockchain evidence

The litigation of trade secret disputes is fact-intensive. The existence of a trade secret is a question of fact; the ownership of an alleged trade secret is a question of fact; evidence of the defendant's notice and access to the alleged trade secret is a question of fact and evidence of misappropriation — the unauthorized acquisition, disclosure or use of a trade secret.

Blockchain evidence can drastically reduce or eliminate material issues of fact in a trade secret misappropriation lawsuit saving the parties millions of dollars in discovery costs.

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner. Nothing in this publication should be construed as legal advice or creating an attorney-client relationship. The views expressed in this publication by any contributor are not necessarily those of the publisher.

Authentication

It is a fundamental requirement in evidence law that a proponent of the evidence show the authenticity of the proposed evidence. Authentication requires the proponent of evidence to show that the evidence "is what the proponent claims it is."

However, there is a special rule for a "process or system." The rules of evidence allow for the authentication of a "process or system" with evidence describing the process or system and showing it produces an accurate result.

Blockchain evidence can drastically reduce or eliminate material issues of fact in a trade secret misappropriation lawsuit saving the parties millions of dollars in discovery costs.

Cryptography and hash codes have been used for years by digital forensic experts. Today there are thousands of applications using the blockchaining platform. Authentication of blockchain evidence will not be an issue in the trial courts. States are enacting special "blockchain" statutes.

The Illinois Blockchain Technology Act [205 ILCS 730]

Take Illinois as an example. On Jan. 1, 2020, the Illinois Blockchain Technology Act became effective.

Review these statutory definitions in Section 5 of the Act:

> Sec. 5. Definitions. As used in this Act:
>
> - "Blockchain" means an electronic record created by a decentralized method by multiple parties to verify and store a digital record of transactions which is secured by the use of a cryptographic hash of previous transaction information.
> - "Cryptographic hash" means a mathematical algorithm which performs a one-way conversion of input data into output data of a specified size to verify the integrity of the data.
> - "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
> - "Electronic record" means a record created, generated, sent, communicated, received, or stored by electronic means, including a blockchain or a smart contract.
> - "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.
> - "Smart contract" means a contract stored as an electronic record which is verified by the use of a blockchain.

Applying these statutory definitions, the Illinois Legislature sets forth the following permitted uses of blockchain in Section 10 of the Act:

> Sec. 10. Permitted use of blockchain.
>
> (a) A smart contract, record, or signature may not be denied legal effect or enforceability solely because a blockchain was used to create, store, or verify the smart contract, record, or signature.
>
> (b) In a proceeding, evidence of a smart contract, record, or signature must not be excluded solely because a blockchain was used to create, store, or verify the smart contract, record, or signature.
>
> (c) If a law requires a record to be in writing, submission of a blockchain which electronically contains the record satisfies the law.
>
> (d) If a law requires a signature, submission of a blockchain which electronically contains the signature or verifies the intent of a person to provide the signature satisfies the law.

Rule 902 of the Illinois Rules of Evidence

Illinois addresses the admissibility of a certified record generated by an electronic process or system in Rule 902(12) – a record generated by an *electronic process or system* that produces an accurate result, as shown by a certification of a qualified person. The blockchain technology complies with these statutory requirements.

International developments: China is moving forward with blockchain evidence

For years, China has been criticized for failing to protect trade secrets in Chinese courts.

The vexing issues for China relate to the difference between a civil law system and a common law system.

China is a civil law system and the legal provisions for trade secret protection are scattered among various laws and regulations. In a civil law system, there is no discovery.

Contrast China to the United States which is a common law system with robust pretrial discovery: interrogatories, document production requests, depositions, request for admissions, common law precedents.

This distinction is critical because the protection of trade secrets often requires the trade secret holder (with the burden of proof) to ferret out evidence of trade secret misappropriation using the evidence obtained from pretrial discovery.

With no right of discovery—no interrogatories, no document production requests, no depositions—the plaintiff in a Chinese court could not meet its evidentiary burden of proof to prove trade secret misappropriation by a preponderance of the evidence.

The discrepancy in the U.S. and Chinese legal systems appeared intractable but China has recently changed its system for the judicial protection of trade secrets in two major ways: (1) accepting blockchain evidence to prove the existence and misappropriation of trade secrets and (2) shifting the burden of proof to the defendant when certain presumptions are met.

Using a blockchain system, the trade secret holder can preserve trade secret evidence on the blockchain of the required elements of proof: existence, ownership, notice and access. The trade secret holder can now enforce and protect trade secrets in China more effectively and efficiently *without* discovery.

Coupled with these evidentiary proofs established using blockchain evidence, recent amendments to the PRC Anti-Unfair Competition Law (AUCL) also provide that if the evidentiary proofs reasonably indicate that the trade secret has been infringed upon, the burden of proof shifts to the accused party to show that the no trade secret misappropriation exists.

Blockchain technology is a game changer both in the United States and internationally.

About the author

R. Mark Halligan is a partner at **FisherBroyles, LLP** and is based in Chicago. He focuses his practice on intellectual property litigation and is recognized as a leading practitioner in the development of automated trade secret asset management blockchain systems. He has taught Advanced Trade Secrets Law in the LLM program at UIC John Marshall Law School for the past 26 years and is the lead author of the "Defend Trade Secrets Act Handbook," 3rd Edition, published by Wolters Kluwer. He can be reached at rmark.halligan@fisherbroyles.com.

This article was first published on Reuters Legal News and Westlaw Today on September 28, 2021.