CA

Canada

Blockchain Timestamping and Creative Work Protection

Legal framework, electronic evidence admissibility and copyright law

March 2026

What is blockchain timestamping?

This guide presents the legal framework applicable in Canada to blockchain timestamping as proof of prior existence. Canada's existing framework for electronic records is well-established and supportive of blockchain-based proofs.

Blockchain timestamping creates permanent, tamper-proof evidence that a document existed at a specific point in time. It does not grant intellectual property rights — but it proves prior existence with mathematical certainty.

How it works (simplified)

1. Digital fingerprint: Your file is converted into a unique 64-character code (SHA-256 hash) — mathematically unique to that exact file.

2. Permanent record: That fingerprint is inscribed on Ethereum, a public ledger maintained by thousands of computers worldwide. Once recorded, it cannot be altered or deleted.

3. Timestamp: The blockchain automatically records the exact date and time — publicly verifiable by anyone, at any time, for free.

4. Your certificate: You receive a ZIP containing the PDF certificate, metadata, and a link to the Ethereum transaction.

Legal framework in Canada

Canada does not have specific blockchain evidence legislation, but the existing framework for electronic records is well-established and supportive. Both federal and provincial laws recognize electronic documents as valid evidence, and Canadian courts apply a pragmatic approach to authenticity and reliability.

Canada Evidence Act — Electronic Documents (ss. 31.1-31.8)

The Canada Evidence Act (CEA) governs the admissibility of electronic documents in federal proceedings. The key test is integrity: the court must be satisfied that the electronic records system produced a reliable record.

Canada Evidence Act — Key provisions

Section 31.1: a party must authenticate the electronic document — produce evidence sufficient to support a finding that it is what it purports to be.

Section 31.2: the best evidence rule is satisfied by producing the electronic document itself.

Section 31.3: the integrity of an electronic records system is presumed unless there is evidence to the contrary. Blockchain's immutable, cryptographically-secured architecture directly supports this presumption.

CGSB Standard CAN/CGSB-72.34-2024

Canada's national standard for electronic records as documentary evidence (updated 2024) provides detailed guidance on managing electronic records to ensure their future admissibility. The standard emphasises integrity, authenticity, reliability and usability — all properties that blockchain timestamping directly supports.

Uniform Electronic Evidence Act (UEEA)

All Canadian provinces and territories (except Quebec, which has its own framework) have adopted legislation based on the UEEA. These acts provide a technology-neutral framework that recognizes electronic documents as equivalent to paper documents, provided their integrity can be demonstrated. No specific technology is mandated — blockchain-based proofs are not disadvantaged.

Copyright Act (R.S.C., 1985, c. C-42)

Canadian copyright protects original works automatically from the moment of creation — no registration required. Protection lasts for the life of the author plus 70 years (extended under the 2022 CUSMA/USMCA implementation). Canada has been a Berne Convention member since 1928.

Canadian court approach — low authentication threshold

Canadian courts apply a relatively low standard for authentication of electronic evidence: all that is needed is 'some evidence' to support the conclusion that the document is what the party presenting it claims it to be (R v CL, 2017 ONSC).

Blockchain's immutable, time-ordered architecture — combined with the hash, the timestamp, and the Ethereum transaction — constitutes a strong authentication package under Canadian evidentiary standards.

Use cases for Canadian creators and businesses

Canada's creative industries — publishing, music, film, software, design, indigenous art — benefit directly from blockchain timestamping as a fast, affordable way to establish prior existence of their work.

Scenario	What the timestamp proves	Stake
Literary works — novels, scripts, articles	Final version before submission or publication	Copyright priority, plagiarism disputes
Music and sound recordings	Composition or recording before release or sharing	Authorship, prior art
Software and algorithms	Exact codebase state at a given date	Prior art, trade secret protection
Visual art and design	Existence of the work before public exhibition	Copyright, anti-counterfeiting
Academic research	Version before peer review or conference submission	Priority of ideas, protection against scooping
Business plans and proposals	Content shared with investors or partners	Trade secret, contractual disputes
Collaborations	Successive versions — who contributed what, and when	Co-author and co-founder disputes

Practical workflow — preparing your file(s)

The file(s) you timestamp must be preserved exactly as anchored. Even changing one character invalidates the proof.

Step	Action	Notes
1	Finalise your document	Make sure it is the version you want to protect — not a draft.
2	Prepare your file(s)	PDFs are stable. Word files modify their metadata when opened. For multiple files, drop them all at once — Etch will bundle them automatically. You may also ZIP them yourself if you prefer.
3	Name it clearly	E.g.: Smith_Work_FINAL_ANCHORED_2026-03-20.pdf
4	Make it read-only	Windows: right-click > Properties > Read-only. Mac: File > Get Info > Locked.
5	Timestamp it	Upload your file(s) to etchproof.eu — they never leave your browser, only their fingerprints are sent.
6	Store the ZIP	Keep your original file(s) and the proof ZIP together, in at least two locations.

File format stability

The hash changes if the file changes — even by a single bit. Always anchor the final version, in a format that does not modify itself when opened.

Format	Stability	Recommendation
PDF	**Ideal**	Stable when opened, universal, does not modify its metadata.
Plain text (.txt, .md)	**Ideal**	No hidden metadata, fully stable.
Source code	**Ideal**	Plain text, fully stable.
Video / Audio	Good	Stable if not re-encoded.
PNG / JPEG / WebP	Medium	EXIF metadata may change when re-saved. Make a dedicated copy.
SVG / AI / EPS	Medium	Stable if not re-saved in an editor.
PSD / Clip Studio	Medium	Stable if not re-saved. Also export a flattened PDF.
Word (.docx / .pages)	**Avoid**	Modifies metadata on every open — always export to PDF before anchoring.
Excel / Numbers	**Avoid**	Same issue as Word.

Important limitations — what timestamping does NOT do

It does NOT grant intellectual property rights. A timestamp proves existence, not ownership or authorship.

It does NOT prove you are the author. It proves you had the file at that date — additional evidence may still be needed.

It does NOT store your file(s). Only the fingerprint (hash) of each file is recorded. Without your original file(s), the proof is useless.

It does NOT constitute absolute proof. It is admissible evidence within a broader body of evidence.

The certificate alone is not sufficient. Verification requires both the certificate AND the original file(s).

Cost comparison

Blockchain timestamping offers permanent proof at a fraction of the cost of formal registration options available in Canada.

Method	Approximate cost	Duration
Blockchain timestamping (Etch)	~$2.70 CAD (~2 EUR) per anchoring	Permanent
Copyright registration (CIPO)	$50 CAD (online)	Life + 70 years (~1-3 months processing)
Notarised declaration	$100-300 CAD+	Permanent
Industrial design registration (CIPO)	$400 CAD+	10 years (renewable)
Patent application (CIPO)	$1,600-5,000+ CAD	20 years

How verification works

Anyone can verify your proof, at any time, for free — including Canadian courts, lawyers, and opposing parties:

• Calculate the SHA-256 hash of your original file using the verification tool at etchproof.eu.

• Look up the transaction on Etherscan.io — the public Ethereum blockchain explorer.

• Confirm that the hash in the blockchain matches your file's hash exactly.

For a multi-file bundle, each file can be verified individually using its own hash. The session hash (anchored on the blockchain) corresponds to the hash of the manifest listing all files.

Even if the Etch service were to cease operations, your proof remains permanently verifiable on the Ethereum blockchain — maintained by thousands of independent nodes worldwide, with no dependence on any company, government, or hardware.