BERNSTEIN

LEGAL RESEARCH PAPER

INNOVATION EVIDENCE PLATFORM

Blockchain evidence in court

A cross-jurisdictional study of how courts and legislatures admit blockchain records and electronic timestamps as evidence - the frameworks, the doctrines, the case law, and what makes a certificate hold.

This paper surveys the admissibility and probative value of blockchain-anchored proof of existence, integrity and time across more than thirty jurisdictions. It sets out the four evidentiary questions every court asks, the three legal traditions that govern the answer, the international instruments that make an electronic record admissible, and the leading statutes and decisions - read from primary sources and secondary literature in English, Chinese, Korean, Japanese, German, Italian, Spanish, Portuguese, Dutch, Polish and the Nordic languages. It is a factual survey for information, not legal advice.

UPDATED	SCOPE	BASIS
July 2026 · v2	30+ jurisdictions	Primary law, case law & literature

ABSTRACT

What this paper finds

Across the common-law and civil-law worlds alike, courts do not, as a rule, reject a record simply because it is electronic or blockchain-based. The contested question has moved from admissibility to **weight** - and weight is decided by whether the proof is independently verifiable, qualified in time, and tied to an identity.

Three findings recur throughout the survey. First, no modern evidence system rejects a record merely for being electronic; the principle of functional equivalence and non-discrimination is written into UNCITRAL's model laws and the EU eIDAS Regulation and echoed in national codes, and blockchain records inherit that protection - with China and several US states naming blockchain expressly. Second, the strongest legal effect attaches not to a bare hash but to a *qualified* anchor - a qualified electronic timestamp under eIDAS, a court-recognised judicial chain in China, or a self-authenticating certified record in the United States. Third, courts everywhere draw the same honest line: a chain proves *what* existed, *when*, and *under whose key* - not authorship, originality, or legal identity, which remain for the party to establish.

THE THROUGH-LINE

Because the legal effect differs by jurisdiction, evidence anchored to a single authority is decisive in one forum and merely persuasive in another. The design conclusion of this paper is that court-grade digital evidence should carry **several independent anchors at once** - a public blockchain for a globally verifiable, permanent record, a qualified timestamp for regulator-grade time, and an identity layer for attribution - all independently verifiable without trusting the issuer.

Method and scope

Where available, primary sources were consulted in their original language and cross-checked against secondary legal literature and law-firm commentary. Case names, courts and dates are given where a decision is on point; statutes are cited by instrument and article. Where a proposition is contested, or where a court has limited or excluded blockchain evidence, the paper says so. Citations to the academic and institutional literature appear in the References at the end (§14).

1 · THE STARTING POINT

The four questions a court actually asks

No court admits or rejects evidence because it is 'on the blockchain.' It asks four ordinary questions - and a blockchain anchor answers three of them unusually well, while being candid about the fourth.

Admissibility

May the record come in at all? In most of the world an electronic record cannot be refused merely for being electronic - the functional-equivalence rule written into UNCITRAL and eIDAS (§4).

Authenticity and integrity

Is this the same data, unaltered? A cryptographic hash on a public chain makes any change detectable - the integrity question is answered by mathematics, corroborated by the ledger, not by testimony alone.

Time

When did it exist? A block fixes a cryptographically verifiable lower bound in time - existence no later than that block - and a qualified electronic timestamp adds a legal presumption of accurate date and time (§4).

Attribution

Who does it belong to? The honest limit: where the anchoring is signed with a key (as in Bernstein's multi-signature protocol), the record proves control of that key - not a legal name. Identity binding is a separate, complementary layer (§12).

WHAT BLOCKCHAIN PROVES, STATED PRECISELY

It proves that specific data existed, intact, at or before a specific time, under the control of a specific key. It does **not** prove who a person is, that content is original, or that it is lawful. Every credible framework below turns on exactly this distinction, and the most probative evidence pairs a blockchain anchor with a qualified timestamp and an identity layer.

2 · THE LEGAL TRADITIONS

Three models, one convergence

Whether blockchain evidence is admitted, and how it is weighed, depends less on the technology than on the evidentiary tradition of the forum. Three models cover most of the world; they arrive, by different routes, at the same practical destination.

	How blockchain evidence is treated	Representative jurisdictions
Civil law - free evaluation of evidence	Electronic evidence is admissible by default; the judge weighs it freely (libre appréciation, freie Beweiswürdigung, libero convincimento). A qualified eIDAS timestamp adds a statutory presumption of integrity and time.	France, Italy, Spain, Germany, Netherlands, Poland, Nordics, Brazil, much of Latin America
Common law - authentication and reliability	The proponent must authenticate the record and, for expert analysis, show it reliable. Self-authentication rules and the Daubert/Frye standard do the work.	United States, United Kingdom, Singapore, Canada, Australia
Specific statute - codified presumption	Dedicated procedural rules give blockchain-stored data a named, rebuttable presumption against post-upload tampering, with a defined review test.	China (Internet Courts)

The convergence: almost everywhere, a blockchain record is admissible. The live question is weight - and that is where a qualified, independently verifiable anchor decides cases.

WHY THE DISTINCTION MATTERS COMMERCIALLY

In free-evaluation systems there is rarely a blockchain-specific statute, and none is needed: the record comes in and its weight is argued on the facts. In authentication systems, the same anchor is what satisfies the reliability test. In China, a specific rule shifts the burden onto the challenger. The technology requirement is identical in all three: proof a third party can re-derive and check.

3 · EVIDENTIARY DOCTRINES

The doctrines that decide the case

Underneath the jurisdictional detail sit a handful of evidentiary doctrines that recur in every common-law and civil-law system. Blockchain evidence succeeds or fails on how well it answers each.

Authentication

The proponent must show the item is what it claims to be. Common law does this by testimony, distinctive characteristics, or a process shown to produce a reliable result (US Federal Rule of Evidence 901(b)(9)); a hash matched to an on-chain record is close to self-proving. Civil law folds this into free evaluation, aided by an eIDAS qualified timestamp.

The best-evidence / original-document rule

Where the law prefers an 'original,' UNCITRAL's functional-equivalence rule treats a reliable electronic record as satisfying it. China's Supreme People's Procuratorate has expressly re-read the best-evidence rule for blockchain preservation, treating the on-chain hash as the authoritative reference for integrity.

Hearsay and the records exception

In common-law systems an out-of-court record is admitted as a business or machine record where it is generated reliably and kept in the ordinary course. A blockchain entry generated automatically by a system - as distinct from human-entered content - is machine-generated data, which many courts treat as outside the hearsay rule entirely.

Presumption of integrity

The strongest statutory lever. eIDAS Article 41 presumes the accuracy and integrity of a qualified timestamp (not identity or authorship); China's 2021 Online Litigation Rules presume on-chain data untampered after upload; Vermont deems a blockchain record accompanied by a qualifying declaration presumptively authentic. Each shifts the burden to the opponent.

Expert reliability - Daubert and Frye

For blockchain analysis offered as expert opinion, US courts apply Daubert: testability, error rate, peer acceptance. In United States v. Sterlingov (D.D.C., 2024) the court admitted blockchain-tracing testimony after a Daubert hearing - a holding on that specific methodology, not a blanket endorsement of blockchain evidence; the Fordham Law Review has catalogued the counter-arguments a litigant can raise to keep weak blockchain evidence out.

BURDEN OF PROOF - WHERE BLOCKCHAIN ACTUALLY SHIFTS IT

A distinction worth stating plainly. Blockchain reliably helps a party *prove* existence, integrity and chronology, but in most systems it does not alter the legal or evidential **burden of proof** - the record is simply good evidence the court weighs. The exceptions are decisive, and they are the ones that matter commercially: under China's Online Litigation Rules and eIDAS Article 41, a qualified anchor carries a rebuttable presumption, so the burden moves to the party challenging it. That is why a qualified timestamp and a court-recognised on-chain record are worth materially more than a bare hash.

4 · INTERNATIONAL FRAMEWORKS

The rules above the borders

Four bodies of international law do most of the heavy lifting. They do not mention Bitcoin - they establish the principles that make a blockchain record admissible and give an electronic timestamp legal weight.

UNCITRAL - electronic commerce (MLEC, 1996)

Two rules the world adopted: an electronic record cannot be denied legal effect for being electronic (non-discrimination), and it satisfies 'writing' and 'original' requirements where its integrity can be shown (functional equivalence). Enacted in over 80 States - one of the most widely adopted instruments in commercial law, and the basis for admitting electronic evidence across scores of jurisdictions.

UNCITRAL - transferable records (MLETR, 2017)

Extends functional equivalence to negotiable and transferable documents (bills of lading, warehouse receipts), technology-neutral toward blockchain by design. Enacted in 13 jurisdictions, including the UK (2023), France (2024), Singapore (2021), Bahrain, ADGM and others.

EU - eIDAS Regulation 910/2014

Article 41: a qualified electronic timestamp enjoys a presumption of the accuracy of its date and time and the integrity of the bound data. Article 25 and Article 46: electronic signatures and electronic documents cannot be denied legal effect or admissibility for being electronic. In force across all 27 member states.

eIDAS 2.0 - Regulation (EU) 2024/1183

In force since 20 May 2024. It adds the European Digital Identity Wallet and, for the first time, 'qualified electronic ledgers' as a new qualified trust service (Articles 45k to 45l). Article 45k(2) grants a recorded ledger entry a presumption of accurate, sequential chronological ordering and of integrity; the reference technical standards are set by Commission Implementing Regulation (EU) 2025/2531 of 16 December 2025.

SUPPORTING INSTRUMENTS AND STANDARDS

UNIDROIT Principles on Digital Assets and Private Law (2023) harmonise the treatment of control and transfer of digital assets. **ISO/TC 307** is building the international blockchain standards family (vocabulary ISO 22739, security, governance). **RFC 3161** defines the trusted-timestamp protocol used by qualified authorities worldwide. The **WIPO White Paper on Blockchain and IP** and WIPO's Frontier Technologies programme map the use of ledgers for IP evidence; WIPO's own PROOF timestamp service ran from 2020 until it was discontinued in 2022 - a reminder that the durable anchor matters more than any single vendor.

80+	27	13
STATES: E-COMMERCE MODEL LAW	EU STATES: EIDAS TIMESTAMPS	JURISDICTIONS: MLETR ENACTED

5 · CHINA

The most developed blockchain-evidence law in the world

No jurisdiction has gone further, or faster. China moved from the world's first admitted blockchain evidence to a codified, rebuttable presumption of integrity, backed by state-run judicial blockchains, in three years - and has begun applying it in criminal as well as civil proceedings.

The first admission - Hangzhou Internet Court JUNE 2018

In Hangzhou Huatai Yimei Cultural Media Co. v. Shenzhen Daotong Technology, (2018) Zhe 0192 Min Chu No. 81, the court on 27 June 2018 accepted blockchain-preserved web evidence in a copyright dispute - widely recognised as the first court in the world to do so - assessing the third-party platform's neutrality and the technical credibility of the capture (curl and headless-browser tooling, hash on Factom and Bitcoin).

Supreme People's Court - Internet Court Provisions SEPT 2018

Article 11 of the SPC Provisions (6 September 2018) recognised that electronic data authenticated through electronic signature, trusted timestamp, hash verification or blockchain, and verified as authentic, shall be admitted by the Internet Courts (Hangzhou, Beijing, Guangzhou).

Beijing Internet Court - the judicial chain applied OCT 2019

In a short-video copyright dispute (ByteDance / Douyin line of cases), the Beijing Internet Court relied on blockchain-preserved evidence via its 'Tianping' (Balance) judicial chain - one of several court-run chains now holding vast volumes of preserved records.

Online Litigation Rules - a codified presumption AUG 2021

Article 16 of the SPC Online Litigation Rules (effective 1 August 2021) presumes blockchain-stored data has not been tampered with after upload, unless rebutted. Articles 17 to 19 set a 'Three Reviews' test of authenticity, with China's National Time Service Center as the binding time standard.

WHY THE CHINESE RULE IS THE BENCHMARK

It shifts the burden. Once data is shown technically consistent with its on-chain record, the court *presumes* integrity and the challenger must disprove it. The rule is paired with state infrastructure - the Hangzhou, Beijing and Guangzhou judicial chains - and China's Supreme People's Procuratorate has published analysis re-reading the 'best evidence rule' for blockchain preservation. Provincial guidance (for example the Jiangsu High Court's 2019 IP guidelines) points the same way.

6 · EUROPEAN UNION & WIDER EUROPE

eIDAS as backbone, national courts as proof

Europe runs on a shared spine - eIDAS - under which electronic evidence is admissible and a qualified timestamp carries a presumption of integrity. National courts and statutes then supply the case law. Nearly all these systems use free evaluation of evidence, so a blockchain record is admitted and its weight judged on the facts.

Italy

STATUTE

Law 12/2019 · Art 8-ter

The first EU state to legislate directly: storing a document via distributed ledger produces the legal effect of an electronic timestamp under eIDAS. In force February 2019, though the enabling AgID technical standards were slow to arrive, so its practical scope was debated for years.

France

CASE LAW

T. jud. Marseille · 20 Mar 2025

In a March 2025 design-and-copyright dispute the court accepted a SHA-256 hash anchored on a public blockchain as evidence of existence and anteriority under Civil Code Art 1366 to 1367. Commentators read the decision as turning on four cumulative considerations: integrity, objective dating, no later change, and an identity link.

Spain

STATUTE + CASE LAW

Ley 6/2020 · Art 1227 CC

The electronic trust-services law and the 'fecha cierta' rule of Civil Code Art 1227 give blockchain timestamps probative value; Spanish courts have weighed blockchain as a medio de prueba under free evaluation.

Germany

DOCTRINE

§371a / §371b ZPO

Electronic documents and qualified-timestamp records are handled under the Code of Civil Procedure; German scholarship expressly frames a blockchain timestamp as an author's proof of priority (Prioritätsnachweis).

Netherlands

DOCTRINE

Vrije bewijsleer · eIDAS

Dutch civil procedure evaluates evidence freely; legal commentary (NJB, IE-Forum) treats the blockchain timestamp as carrying real evidentiary weight (bewijskracht) in copyright disputes.

Poland

DOCTRINE

Kwalifikowany znacznik czasu

Polish practice relies on the eIDAS qualified timestamp for date-certainty; scholarship examines Bitcoin's evidentiary force (moc dowodowa) in civil and criminal process.

SWITZERLAND, LIECHTENSTEIN AND THE NORDICS

Switzerland enacted its DLT Act (a blanket amendment to nine federal statutes), in force through 2021, giving ledger-based rights and records a clear legal home. **Liechtenstein's** Token and Trusted Technology Service Providers Act (TVTG, the 'Blockchain Act') has been in force since January 2020. The **Nordic** systems (Sweden, Denmark, Finland) apply free evaluation with no formal admissibility bar - a 2025 study in Svensk Juristtidning on the courts' duty to investigate digital manipulation underlines why a tamper-evident anchor now matters.

7 · UNITED STATES

Self-authentication and the reliability test

US law has no single blockchain-evidence statute. It has something more useful: rules of evidence that already fit. Digital records self-authenticate by certification, machine-generated data sidesteps hearsay, and the reliability of blockchain analysis has now been tested and upheld under Daubert.

FRE 902(13)

A record generated by an electronic process or system is self-authenticating on a qualified person's certification - no live witness needed. Effective December 2017.

FRE 902(14)

Data copied from an electronic device, storage medium or file is self-authenticating when a hash value or equivalent confirms it is unaltered - a rule written for exactly this kind of proof.

FRE 901(b)(9)

Evidence describing a process or system that produces an accurate result - the classic route for admitting the output of a verifiable technical process.

THE LEADING FEDERAL DECISIONS

In *United States v. Sterlingov*, 2024 WL 860983 (D.D.C. 2024) - the Bitcoin Fog prosecution - the court held, after a Daubert hearing, that the specific blockchain-tracing methodology was sufficiently reliable for expert testimony to reach the jury (a ruling on that methodology, not a blanket endorsement of blockchain evidence). In *United States v. Gratkowski*, 964 F.3d 307 (5th Cir. 2020), the court treated the Bitcoin blockchain as a public ledger for Fourth Amendment purposes. Together they establish that the chain is public, and that rigorous analysis of it meets the federal reliability standard.

State-level statutes

	Instrument	Effect
Vermont	12 V.S.A. §1913 (2016)	A blockchain record accompanied by a qualifying declaration is admissible as a business record and presumptively authentic (date, sender, recipient)
Arizona	HB 2417 (2017)	Blockchain signatures and records given legal effect; smart contracts recognised
Illinois	Blockchain Technology Act, HB 3575 (in force 2020)	A record or signature may not be denied legal effect solely because a blockchain was used
Ohio	SB 220 (2018), amending UETA	Records and signatures secured through blockchain are electronic records and signatures
Washington	SB 5638 (2019)	Electronic records via distributed ledger cannot be denied legal effect or enforceability

The pattern across states: blockchain is folded into existing electronic-records and business-records law - the UETA and the business-records exception - not treated as a novelty. Similar bills are pending in further states.

8 · UK, COMMONWEALTH & THE GULF

Common law modernises for digital assets

The common-law world outside the US has moved decisively since 2019 - a taskforce statement, then statutes on electronic trade documents and digital-asset property, and a growing body of decisions in which courts weigh blockchain evidence directly.

United Kingdom

STATUTE + CASE LAW

ETDA 2023 · Property Act 2025

The Electronic Trade Documents Act 2023 (in force Sept 2023) gives electronic trade documents parity with paper; the Property (Digital Assets etc) Act 2025 confirms digital assets as a distinct category of personal property (a property-law reform, not an evidence rule). The UKJT Legal Statement (2019) underpins both.

UK - crypto case law

CASE LAW

AA · D'Aloia

AA v Persons Unknown [2019] EWHC 3556 (Comm) recognised cryptoassets as property; D'Aloia v Persons Unknown [2024] EWHC 2342 (Ch) examined, and scrutinised, blockchain-tracing expert evidence in a fraud-recovery claim.

Singapore

STATUTE + CASE LAW

ETA · MLETR · case law

Singapore adopted MLETR into its Electronic Transactions Act (2021); B2C2 v Quoine [2019]-[2020] and ByBit v Ho Kai Xin [2023] SGHC 199 confirm crypto as property and rely on on-chain records.

New Zealand

CASE LAW

Ruscoe v Cryptopia

Ruscoe v Cryptopia Ltd (in liq) [2020] NZHC 728 held cryptoassets to be property capable of being held on trust - a widely-cited common-law precedent.

ADGM & DIFC (UAE)

STATUTE + COURT PRACTICE

MLETR · digital custody

The ADGM enacted MLETR-based rules (2021); the DIFC Courts have moved to permit digital-custodian and blockchain-intelligence capabilities for court users.

Canada & Australia

DOCTRINE

Evidence Acts · integrity

The Canada Evidence Act admits electronic documents where the integrity of the record system is shown; Australia's Evidence Acts and Electronic Transactions Acts admit electronic records subject to reliability.

9 · ASIA, LATIN AMERICA & THE MIDDLE EAST

The frameworks spread outward

Beyond the headline jurisdictions, the same two ideas - admit electronic evidence, weigh it on integrity - are being written into national codes and tested by national courts, often with a distinctive local doctrine of certification or chain of custody.

India

STATUTE + CASE LAW

BSA 2023 · s.63 · s.63(4)

The Bharatiya Sakshya Adhiniyam 2023 (in force July 2024) replaced the 1872 Act; Section 63 admits electronic records with a certificate (formerly s.65B). Anvar P.V. v P.K. Basheer (2014) and Arjun Panditrao Khotkar (2020) made the certificate mandatory; a 2026 Supreme Court ruling clarified the role of the hash value.

South Korea

DOCTRINE

Digital evidence rules

Korean criminal and civil procedure admit digital evidence subject to authenticity (jinjeongseong) and integrity; academic and policy work studies blockchain systems for tamper-proofing judicial digital evidence.

Japan

STATUTE + PRACTICE

Accredited timestamps

Japan placed its established time-business timestamp accreditation on a national statutory footing in 2021; courts assess the authenticity (shinseisei) of electronic files, with accredited timestamps as core support.

Brazil

DOCTRINE

Cadeia de custódia · CPP 158-A

Brazilian scholarship and emerging judicial practice treat blockchain as a means of securing the chain of custody of digital evidence and guaranteeing temporal integrity in civil and criminal process.

UAE (Federal)

STATUTE

Evidence Law 35/2022

The federal Evidence Law expressly recognises digital and electronic evidence, giving the Gulf's largest civil-law system a clear statutory basis for blockchain-anchored records.

Latin America (broad)

DOCTRINE

UNCITRAL-aligned

Civil codes with 'fecha cierta' rules and UNCITRAL-based e-commerce statutes give blockchain timestamps a recognised evidentiary role across the region.

THE COMMON THREAD

In free-evaluation systems - most of Europe, Latin America, Japan, Korea - the record is admissible and a qualified, independently verifiable anchor is what carries weight. In authentication systems - the US, UK, Commonwealth - the same anchor satisfies the reliability test. In China, a specific rule shifts the burden onto the challenger. The technology requirement is identical everywhere: proof a third party can re-derive and check.

10 · CASE-LAW DIGEST

Landmark decisions at a glance

A digest of the decisions most often cited when a court weighs blockchain or cryptographic evidence. The list is illustrative, not exhaustive; holdings are summarised and should be read against the full judgment.

	Court · year	What it established
Hangzhou Huatai Yimei v. Shenzhen Daotong	Hangzhou Internet Court · 2018	First judicial admission of blockchain-preserved evidence; test of platform neutrality and technical credibility
ByteDance / Douyin short-video line	Beijing Internet Court · 2019	Blockchain-preserved evidence via the 'Tianping' judicial chain accepted in copyright infringement
United States v. Sterlingov	D.D.C. · 2024	Blockchain-tracing expert testimony admitted after a Daubert reliability hearing
United States v. Gratkowski	5th Cir. · 2020	Bitcoin blockchain treated as a public ledger for Fourth Amendment purposes
AA v Persons Unknown	EWHC (Comm) · 2019	Cryptoassets recognised as property under English law
D'Aloia v Persons Unknown	EWHC (Ch) · 2024	Blockchain-tracing expert methodology scrutinised in a crypto-fraud recovery claim
Ruscoe v Cryptopia Ltd (in liq)	NZHC · 2020	Cryptoassets are property capable of being held on trust
B2C2 v Quoine	SGHC(I) / SGCA(I) · 2019-2020	On-chain records and code relied on to resolve a digital-asset trading dispute
ByBit Fintech v Ho Kai Xin	SGHC · 2023	Cryptoassets held to be property; on-chain evidence central to tracing
Arjun Panditrao Khotkar v Kailash Gorantyal	Supreme Court of India · 2020	Certificate for electronic records (then s.65B) held mandatory - now carried into s.63(4) BSA
Tribunal judiciaire de Marseille	France · 2025	Public-blockchain hash accepted as proof of existence and anteriority, on cumulative conditions

Direction of travel: from recognising cryptoassets as property, to admitting on-chain records, to scrutinising the reliability of blockchain analysis. Courts are now engaging with cryptographic proof on its technical merits.

11 · THE LAST TWO YEARS

What changed in 2024 to 2026

The legal ground has moved faster in the last twenty-four months than in the prior decade. The direction is uniform: from tolerating electronic evidence to giving verifiable digital records named legal standing.

eIDAS 2.0 enters into force MAY 2024

Regulation 2024/1183 adds ‘qualified electronic ledgers’ as a trust service and launches the EU Digital Identity Wallet - the first time a distributed-ledger record is named in EU trust-services law.

France and Timor-Leste enact MLETR 2024

France adopts electronic transferable records; the MLETR count reaches 13 jurisdictions, with China (bills of lading) and Mauritius following in 2025.

India’s Bharatiya Sakshya Adhiniyam in force JULY 2024

India’s new evidence code replaces the 1872 Act, modernising electronic-record admissibility and the certificate-and-hash regime under Section 63.

France - Marseille blockchain-anteriority decision MARCH 2025

A French court accepts a blockchain-anchored hash as evidence of existence and prior creation; commentators read it as turning on cumulative conditions other courts can apply.

UK Property (Digital Assets etc) Act LATE 2025

Royal Assent confirms digital assets as a distinct category of personal property in English law - closing a question open since the UKJT statement.

India Supreme Court clarifies hash-value evidence 2026

The Court explains how hash values authenticate electronic records under the new code - a signal that apex courts now engage with cryptographic proof directly.

12 · THE HONEST LIMITS

Where blockchain evidence is challenged

A credible paper states the limits as plainly as the strengths. Blockchain evidence is powerful and widely admitted - but it is not self-executing, and courts and commentators have been clear about what it does not do.

WHAT IT RELIABLY PROVES

- **Existence and integrity.** That specific data existed and has not changed - the strongest, least contestable part of the proof.
- **Time.** That the data existed no later than a given block, corroborated to the second by a qualified eIDAS timestamp.
- **Independent verifiability.** That anyone can re-derive and check the proof from the original files, with open tools, without trusting the issuer.
- **Control.** That the holder of a private key controlled the record at the time it was anchored.

WHAT IT DOES NOT SETTLE

- **Authorship or originality.** A hash proves what and when, not that content is original or lawful - that stays for the party to assert.
- **Identity.** A chain proves control of a key, not a legal name; identity binding is a separate layer courts still require (as Marseille did).
- **Garbage in.** The ledger faithfully records whatever was submitted; it cannot cure a falsehood recorded truthfully.
- **Foundation still matters.** The Fordham Law Review catalogues how a litigant can challenge weak blockchain evidence; Italian commentators caution that a bare hash needs forensic certification to carry at trial.

THE DESIGN ANSWER TO EVERY LIMITATION

Each limit points to the same fix: pair a public, immutable anchor (existence, time, integrity) with a qualified timestamp (regulator-grade time), an identity layer (attribution), and independent verifiability (no trust in the issuer). That combination is not a wish-list - it is how Bernstein certificates are built.

13 · WHAT THIS MEANS

One certificate, built for every framework

The survey has a practical conclusion. Because the frameworks differ by jurisdiction, evidence anchored to only one authority is strong in one forum and merely persuasive in another. Bernstein anchors every certificate to several at once.

Bitcoin blockchain

LIVE

Global · permissionless

Public, immutable, timestamped by proof-of-work; operating continuously since 2009. Needs no authority and nothing to renew - the borderless backbone of the proof, and a public ledger the US courts have expressly recognised.

EU qualified timestamp

LIVE

eIDAS · Art 41

A qualified electronic timestamp carrying the eIDAS presumption of accurate time and data integrity across all 27 EU member states - to-the-second, regulator-grade time.

China Timestamp Authority

LIVE

China TSA

A parallel timestamp from a recognised Chinese authority - aligning with the jurisdiction that has the most developed blockchain-evidence rules in the world.

Global RFC 3161

LIVE

ISO / RFC 3161

A standards-based trusted timestamp recognised internationally, so the certificate speaks the common language of digital-evidence standards everywhere.

WHY MULTI-ANCHOR IS THE POINT

A French court wants Art 1366 integrity and objective dating; a US court wants a reliable, self-authenticating record; a Chinese court wants an on-chain record it can presume intact; an EU regulator wants a qualified timestamp. A Bernstein certificate satisfies all of them *from a single act of certification* - Bitcoin for borderless permanence, qualified timestamps for regulatory weight, and zero-knowledge client-side encryption so only a hash is ever exposed. The proof is independently verifiable by anyone, with open tools, without trusting Bernstein. Final weight is always assessed case by case; what a multi-anchor certificate does is meet the threshold each framework asks for - integrity, qualified time, a public record, a presumption - at once.

4	30+	0
INDEPENDENT ANCHORS PER CERTIFICATE	JURISDICTIONS SURVEYED HERE	TRUST IN THE ISSUER REQUIRED

14 · REFERENCES & FURTHER READING

Sources

Where available, primary legislation and court decisions were consulted in their original language; the secondary, national and academic literature below informed the analysis. Some decisions (notably at first-instance level) are known through official gazettes and reputable legal commentary rather than an officially published docket. This paper is a factual survey for information, not legal advice.

International instruments & standards

- UNCITRAL, Model Law on Electronic Commerce (1996, with 1998 additional article) and Guide to Enactment.
- UNCITRAL, Model Law on Electronic Transferable Records (MLETR, 2017) and adoption status table.
- Regulation (EU) No 910/2014 (eIDAS), in particular Articles 25, 41 and 46.
- Regulation (EU) 2024/1183 (eIDAS 2.0), Articles 45k to 45l on qualified electronic ledgers, and Commission Implementing Regulation (EU) 2025/2531 (technical standards).
- UNIDROIT, Principles on Digital Assets and Private Law (2023).
- ISO/TC 307 blockchain and distributed ledger technologies standards (incl. ISO 22739); IETF RFC 3161 (trusted timestamping).
- WIPO, White Paper on Blockchain Technologies and IP Ecosystems; WIPO Frontier Technologies programme.

Statutes & procedural rules

- China: SPC Provisions on Internet Courts (2018), Art 11; SPC Online Litigation Rules (2021), Arts 16 to 19.
- United States: Federal Rules of Evidence 901(b)(9), 902(13), 902(14); Vermont 12 V.S.A. §1913; Arizona HB 2417; Illinois Blockchain Technology Act; Ohio SB 220; Washington SB 5638.
- European Union: Italy Law 12/2019, Art 8-ter; Spain Ley 6/2020 and Código Civil Art 1227; Germany ZPO §§371a to 371b; Switzerland DLT Act; Liechtenstein TVTG.
- United Kingdom: Electronic Trade Documents Act 2023; Property (Digital Assets etc) Act 2025; UKJT Legal Statement on Cryptoassets and Smart Contracts (2019).
- India: Bharatiya Sakshya Adhiniyam 2023, Section 63 and 63(4); UAE Federal Evidence Law No. 35/2022; Singapore Electronic Transactions Act (MLETR, 2021).

Case law

- Hangzhou Huatai Yimei Cultural Media Co. v. Shenzhen Daotong Technology, (2018) Zhe 0192 Min Chu No. 81 (Hangzhou Internet Court).
- United States v. Sterlingov, 2024 WL 860983 (D.D.C. 2024); United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020).
- AA v Persons Unknown [2019] EWHC 3556 (Comm); D'Aloia v Persons Unknown [2024] EWHC 2342 (Ch).
- Ruscoe v Cryptopia Ltd (in liq) [2020] NZHC 728; B2C2 v Quoine [2019] SGHC(I) 03; ByBit Fintech v Ho Kai Xin [2023] SGHC 199.
- Anvar P.V. v P.K. Basheer (2014) 10 SCC 473; Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1.
- Tribunal judiciaire de Marseille, 20 March 2025 (design/copyright; reported in the French legal and specialist press, docket not officially published); Beijing Internet Court short-video copyright line, 2019 (via the 'Tianping' judicial chain).

Academic & professional literature

- Z. Su, 'Evidentiary value and evidentiary status of blockchain evidence,' The International Journal of Evidence & Proof (2025).
- 'Blockchain in the courtroom: evidentiary significance and procedural implications in U.S. judicial processes,' Frontiers in Blockchain (2024).
- 'The evidentiary value of blockchain in civil litigation: comparative insights and future directions,' Frontiers in Blockchain (2026).
- R. Sahara, 'Blockchain Evidence: How Smart Litigators Can Keep It Out at Trial,' Fordham Law Review (2024).
- Norton Rose Fulbright, 'When blockchain analytics meet the Daubert test,' New York Law Journal (2024).

National commentary consulted (by language)

- Chinese: Supreme People's Procuratorate commentary on the best-evidence rule under blockchain preservation (spp.gov.cn); China Justice Observer analyses of the Internet Courts.
- French: usine-digitale.fr and Village-Justice analyses of the Tribunal judiciaire de Marseille decision (2025); commentary on Civil Code Art 1366 to 1367.
- Italian: Agenda Digitale and practitioner commentary on Law 12/2019 Art 8-ter and the AgID technical standards.
- German: 'Prioritätsnachweis des Urhebers durch blockchainbasierten Zeitstempel' (2019); ZPO §§371a to 371b commentary.
- Spanish: commentary on Ley 6/2020 and Código Civil Art 1227; Economist & Jurist on blockchain como medio de prueba.
- Dutch: NJB and IE-Forum on the bewijskracht of the blockchain timestamp in copyright disputes.
- Polish and Nordic: commentary on the eIDAS qualified timestamp (kwalifikowany znacznik czasu) and Bitcoin's moc dowodowa; Svensk Juristtidning (2025) on courts and digital manipulation.
- Japanese, Korean and Portuguese: national timestamp-accreditation guidance; KCI studies on blockchain tamper-proofing of judicial evidence; Brazilian scholarship on cadeia de custódia (EMERJ, IBCCRIM).

Want this paper tailored to a specific jurisdiction, deepened on a single forum, or folded into a procurement or litigation-support pack? Contact your Bernstein partner - www.bernstein.io.