From Blockchain to Courtroom: Preserving and Proving Digital Asset Evidence

Speakers:

Daniel B. Garrie, Esq., Founder, Law & Forensics; Neutral, JAMS; Adjunct Faculty, Harvard

Hon. Jackson Lucky, Mediator, Arbitrator, Neutral, JAMS

Justin Herring, Esq., Partner, Mayer Brown

Angus F. Ni, Esq., Partner, Morrow Ni LLP

(c) 2026 Lexeprint Inc. All Rights Reserved.

Disclaimer

- This is not legal advice, nor should it be considered legal advice.
- This presentation and the comments contained therein represent only the personal views of the participants, as spoken, and do not reflect those of their employers or clients.
- This presentation is offered for educational and informational uses only.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Speakers



Daniel B. Garrie, Esq.
Founder, Law & Forensics
Neutral, JAMS
Adjunct Faculty, Harvard



Hon. Jackson Lucky
Mediator, Arbitrator, Neutral,
JAMS



Justin Herring, Esq.
Partner, Mayer Brown



Angus F. Ni, Esq.
Partner, Morrow Ni LLP

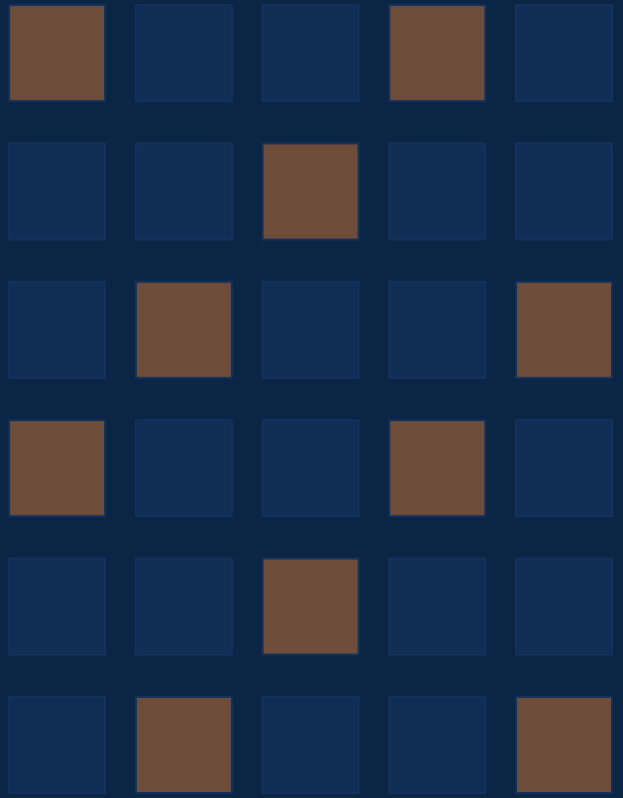
(c) 2026 Lexeprint Inc. All Rights Reserved.

Agenda

1. **Why This Matters Now**
2. **Blockchain Fundamentals for the Evidentiary Record**
3. **Preservation, Collection, and Authentication**
4. **Tracing, Attribution, and the Expert's Role**
5. **Discovery and ESI Protocol Design**
6. **Arbitration-Specific Considerations**

(c) 2026 Lexeprint Inc. All Rights Reserved.

Why This Matters Now



(c) 2026 Lexeprint Inc. All Rights Reserved.

From Novelty to Routine Docket Item

- Digital asset matters no longer arrive only as securities enforcement. They arrive as commercial breach, fraud, fiduciary, bankruptcy, matrimonial, and employment disputes.
- The 2023 to 2025 exchange and platform actions built a public record of how these entities keep books, custody assets, and describe their own controls. That record is now discoverable raw material in private disputes.
- The Binance and Ceffu custody dispute is the template. The contested question was not what the ledger said. It was who controlled the keys, and which records outside the chain proved it.
- Courts and tribunals are still calibrating. Many blockchain evidentiary questions remain unsettled, which means the party that frames the methodology first tends to set the terms.

The recurring failure is not understanding the technology. It is assuming the technology answers a question it was never built to answer.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Where Courts and Tribunals Get It Wrong

1 Immutability confused with authenticity

A tamper-resistant ledger proves the record was not altered after it was written. It says nothing about whether it was accurate when written, or who wrote it.

2 Pseudonymity confused with attribution

An address is not a person. Linking the two requires off-chain evidence and inference, and that inference is where the expert dispute lives.

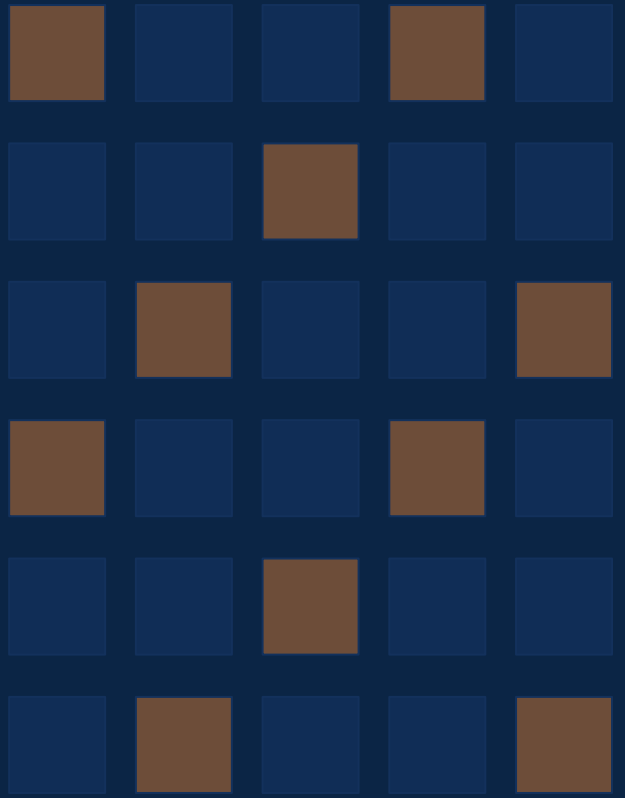
3 Transparency confused with completeness

Public chain data is only one layer. Exchange records, custody arrangements, and internal communications carry the facts the chain omits.

Practice point. Each error runs in both directions. A proponent overstates what the chain establishes; an opponent dismisses reliable ledger data because the attribution layer is weak. The disciplined position separates the two layers and concedes the gap in the weaker one.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Blockchain Fundamentals for the Evidentiary Record



(c) 2026 Lexeprint Inc. All Rights Reserved.

What a Blockchain Is, in Evidentiary Terms

The Technical Description

- A distributed ledger implemented without a central repository and usually without a central authority.
- Tamper evident and tamper resistant. Under normal network operation no transaction can be changed once published.
- Users hold public and private keys and digitally sign to transact.
- Consensus across nodes is what makes the record durable.

What That Means for Proof

- The ledger is a business record of the network, not of any party.
- There is no custodian to authenticate it in the ordinary sense, and no one to depose about how it was kept.
- A signature proves key control at signing time. It does not prove identity, authority, or consent.
- Consensus is a property of the network, not a warranty of the truth of any entry.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Not All Ledgers Produce the Same Record

Public permissionless *Bitcoin, Ethereum*	Anyone can read and write. Complete history is available to any party. No gatekeeper to subpoena, and no one to authenticate.
Permissioned *Enterprise consortium chains*	Access controlled by an operator. There is a custodian, which makes 902(11) and 902(13) far more workable.
UTXO model *Bitcoin and derivatives*	Value tracked as discrete unspent outputs. Supports coin-level tracing, which drives clustering heuristics.
Account model *Ethereum and most successors*	Balances held at addresses. Contract state matters as much as transfers. Tracing logic differs materially.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Digital Asset Types and the Disputes They Generate

- **Cryptocurrency and platform tokens** Fungible digital assets used as a medium of exchange or to power a decentralized application. Disputes: conversion, fraud, valuation, misappropriation, judgment enforcement.

- **Security tokens** On-chain representations of real-world securities. Disputes: registration, disclosure, and the Howey analysis that Ripple left unsettled.

- **Stablecoins** Tokens pegged to an external asset. Disputes: reserve adequacy, redemption, and misrepresentation about backing.

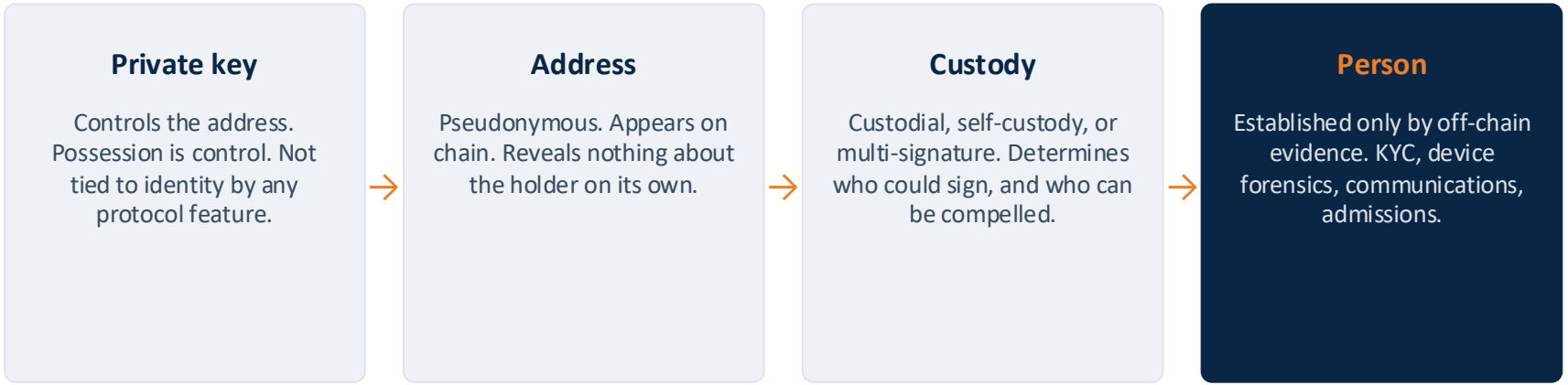
- **NFTs and tokenized rights** Unique tokens asserting ownership or license. Disputes: title, IP scope, and whether the token conveys anything off-chain at all.

- **Smart contracts and DeFi protocols** Self-executing code. Disputes: whether the code is the agreement, exploit versus intended behavior, and who bears the loss.

(c) 2026 Lexeprint Inc. All Rights Reserved.

The Attribution Gap

The single most contested question in digital asset litigation is rarely what happened on the chain. It is who was behind the key.



The chain proves the first two links. It never proves the last two. Every attribution opinion is therefore an inference built on off-chain evidence, and every attribution opinion is vulnerable at exactly that seam. Say so in the report before opposing counsel says it in cross.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Case Study: US*A v. Sterlingov* (No. 24-3161)



Admissibility of Blockchain Forensics

The court upheld the admission of proprietary blockchain-tracing software, Chainalysis Reactor. The court found no error in admitting expert testimony reliant on transaction clustering without requiring public peer review, a known error rate, or disclosure of the underlying proprietary source code

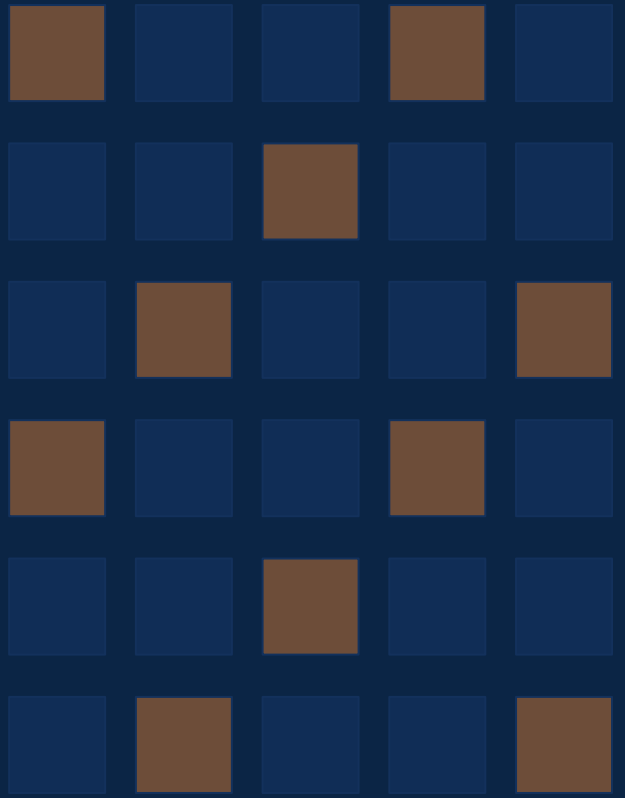


Lower Evidentiary Bar for Forensics

Defense challenges to commercial tracing heuristics face a steeper uphill battle. Prosecutors can rely heavily on commercial analytics tools (like Chainalysis) without opening the software's proprietary algorithms to deep cross-examination.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Preservation, Collection, and Authentication



(c) 2026 Lexeprint Inc. All Rights Reserved.

Immutability Is Not Authentication

The argument that fails. "The blockchain cannot be altered, so the record authenticates itself." This confuses the integrity of the ledger with the reliability of the process that produced the exhibit in the courtroom.

Three pathways, and what each actually requires

1 FRE 901(b)(9) Process or system

Describe the collection process and show it produces an accurate result. The workhorse for chain data. Needs a witness who can explain the node or explorer, the query, and the verification.

2 FRE 902(13) Certified machine record

Self-authentication by certification of a qualified person. Works where a custodian exists. Rarely available for public chain data.

3 FRE 902(14) Certified copy by hash

Hash verification against the original. Strong for wallet images and exchange exports. Proves the copy matches, not that the original was accurate.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Collection Methodology and Its Failure Points

Full node	Highest fidelity. Independent verification of consensus. Slow, expensive, and requires a witness who can explain it.
Block explorer	Fast and cheap, and used constantly. A third-party interpretation layer, not the ledger. Screenshots of an explorer are hearsay about a business record.
Exchange records	Where attribution usually lives. KYC files, IP logs, internal ledgers. Off-chain, custodial, and subject to normal subpoena and authentication practice.
Wallet imaging	Device forensics on the key material and application artifacts. Conventional digital forensics, and conventional chain of custody applies in full.
Smart contract state	Historical state at a specific block. Requires archive node access. Frequently overlooked until it is too late to obtain.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Hashing, Timestamps, and the Two Clocks

On-chain time

Block timestamps are asserted by the producer within a consensus-tolerated window. Ordering within a block is not chronological. Confirmation is probabilistic before finality.

Wall-clock time

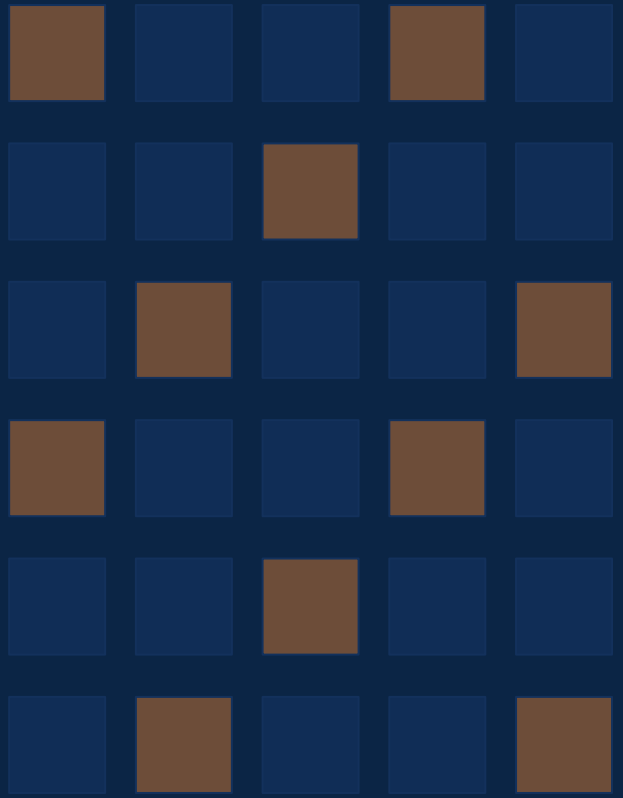
Exchange logs, device artifacts, emails, and messages. Subject to time zone handling, clock drift, and system configuration, all of which are provable and all of which get contested.

The reconciliation is the opinion. Any narrative that a person did something at a time requires binding an on-chain event to an off-chain one. That binding is an expert conclusion with a stated margin, not a lookup. Cases turn on whether the margin was disclosed or buried.

Hashing serves a narrower purpose than counsel often assume. It proves a copy matches a source. It does not timestamp the source, prove the source was accurate, or establish who created it.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Tracing, Attribution, and the Expert's Role



(c) 2026 Lexeprint Inc. All Rights Reserved.

Tracing Methods and the Assumptions Inside Them

Common-input clustering *Inputs to one transaction share an owner*	Fails against CoinJoin and any collaborative spend. The foundational heuristic, and the most widely assumed.
Change-address detection *One output returns to the sender*	Pattern-based and wallet-software dependent. Error compounds across every subsequent hop.
Taint and poison analysis *Illicit value is traceable through mixing*	Competing accounting conventions (FIFO, LIFO, haircut) produce materially different answers on identical facts.
Mixers and tumblers *Deliberate severance of the trail*	Statistical inference only. Confidence degrades sharply with pool size and time.
Cross-chain bridges *Value continues on another ledger*	The link is an inference across two ledgers with no shared consensus. The weakest joint in most tracing chains.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Daubert Exposure in Blockchain Tracing Opinions

1	**Testing**	Has the method been tested against ground truth? Commercial vendors rarely publish validation data, and the licence usually forecloses independent testing.
2	**Error rate**	Clustering heuristics have measurable false-positive rates. If the report states no rate, the omission is the vulnerability.
3	**Peer review**	Academic literature on clustering is real and substantial. Proprietary vendor scoring is not peer reviewed, and the distinction matters.
4	**Standards**	There is no controlling standard for attribution methodology. Both sides can exploit this, which is precisely why methodology should be fixed in the protocol.
5	**General acceptance**	Wide use in industry is not general acceptance for the specific opinion offered. Widely-used tools produce inadmissible opinions when stretched past their design.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Separating Inference from Fact in the Report

Established fact

- A transaction with these inputs and outputs was included in block N.
- The block header hash is X and it is confirmed by the network.
- The image of the device produced hash Y, matching the source.
- Exchange records show an account opened with these KYC documents.

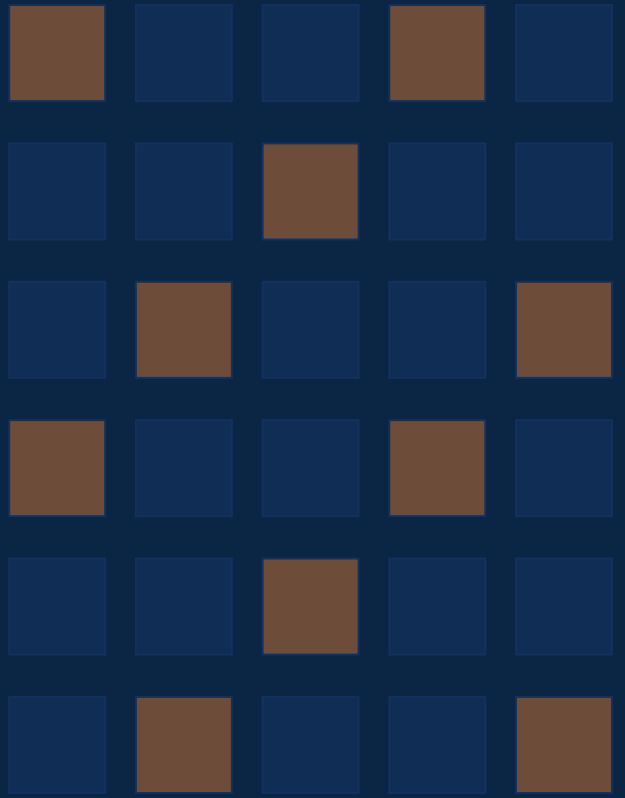
Analytical inference

- These addresses are controlled by a single entity.
- This output is the change address, so the counterparty is that one.
- The funds that left address A are the funds that arrived at address C.
- The person who holds the exchange account controlled the wallet.

An expert who labels the right column as fact has handed the other side its Daubert motion and its cross. Label the inference, state the confidence, and name what would falsify it.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Discovery and ESI Protocol Design



(c) 2026 Lexeprint Inc. All Rights Reserved.

Possession, Custody, or Control of What, Exactly

- Private keys. A party who holds keys controls the assets and can produce signed proof of control. A party who has lost or destroyed keys can produce nothing, and the distinction is a factual question, not a technical one.
- Custodial accounts. Assets held at an exchange are the exchange's records about the party. The party may have control over the account without possession of any key. Rule 34 reaches the account records through the party; Rule 45 reaches the exchange.
- Node access. Running a node is not possessing the chain. The chain is public. What a party's node holds that the public chain does not is the party's own query history, configuration, and logs.
- Smart contract control. Admin keys, upgrade rights, and pause functions are control, and they are visible on chain. Contract deployment records answer questions parties often decline to answer.
- Off-chain infrastructure. Key management systems, hardware wallet backups, seed phrase storage, and multi-signature policy documents. This is ordinary ESI and it is where the answers usually are.

The Binance and Ceffu dispute was a control question dressed as a technical one. Whether a custody provider was an independent third party or an affiliate determined who could be compelled, and the chain data was silent on it.

(c) 2026 Lexeprint Inc. All Rights Reserved.

What the ESI Protocol Should Actually Say

Scope of chain data	Which chains, which addresses, which block range, and who bears the cost of archive node access.
Collection method	Node versus explorer, and the verification step required for either. Fix this before collection, not at the motion.
Production format	Raw transaction data with block references, not screenshots. Native format with hashes, and a load file that survives the exhibit.
Tracing methodology	Which heuristics, which tool, which version, and whether the parties will exchange the underlying analysis or only the conclusions.
Off-chain custodians	Named exchanges and custodians, the subpoena sequencing, and who initiates cross-border process.
Preservation of keys	An affirmative obligation not to destroy, transfer, or abandon key material, stated as a term rather than assumed.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Spoliation in a Self-Executing Environment

1 Key destruction

Deleting a private key destroys access permanently and leaves an artifact trail on the device. The chain is untouched. The assets are unreachable. Whether that is spoliation or destruction of the res is a live question.

2 Wallet abandonment

A party stops using an address and claims no knowledge of it. The chain shows dormancy, not lost control. Device forensics and backup artifacts usually resolve it.

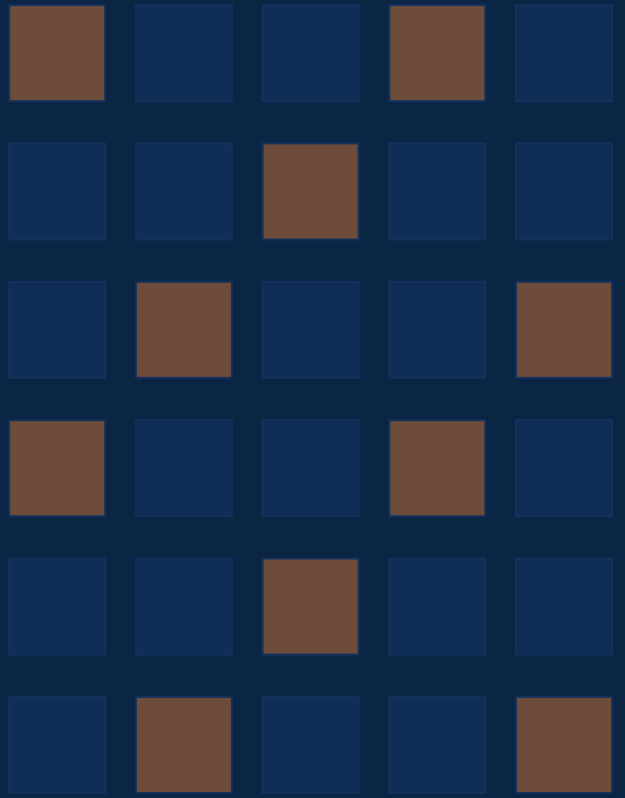
3 Self-executing loss

A contract moves or burns assets by its own terms after the duty to preserve attaches. No human acted. Whether preservation extends to disabling deployed code is unsettled.

The asymmetry worth naming. Blockchain preserves the transaction record perfectly and preserves access not at all. A party can comply with every preservation instruction and still put the assets permanently beyond reach. Address it in the litigation hold, not the sanctions motion.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Arbitration-Specific Considerations



(c) 2026 Lexeprint Inc. All Rights Reserved.

Why These Disputes Land in Arbitration

What draws parties in

- Technical competence in the decision-maker, selected rather than assigned.
- Confidentiality over key management and custody architecture.
- Cross-border enforceability under the New York Convention.
- Speed, where asset dissipation is the live risk.
- Arbitration clauses already embedded in exchange and protocol terms of service.

What they give up

- No subpoena power over non-party exchanges in most seats.
- Limited discovery against the counterparty and none against third parties.
- No published authority, so the same methodology questions get relitigated privately.
- Interim relief that binds parties but not the ledger, and not a foreign custodian.
- Narrow review, which raises the cost of a tribunal that misunderstands the technology.

The consent-to-arbitrate question is itself contested where the clause sits in click-through terms and the party is a retail holder. Expect challenges to the agreement before any tribunal reaches the chain data.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Getting Technical Competence onto the Panel

Party-appointed experts	The default. Two opposed opinions, no independent validation, and a tribunal left to choose between methodologies it may not be equipped to assess.
Tribunal-appointed expert	Available under most institutional rules. Effective for methodology questions. Raises due process concerns about how the parties test that expert's assumptions.
Special Master or discovery neutral	Resolves protocol disputes and methodology fights without consuming merits hearing time. Well suited to the collection and format questions that dominate early.
Technical advisor to the tribunal	Advises without deciding. Useful for a panel that needs to follow the evidence rather than resolve a dispute about it. Scope must be defined in the terms of reference.

The JAMS AI Dispute Resolution Rules provide a template worth borrowing here. Verify the current text and scope before citing it as applicable to a digital asset matter.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Interim Relief and the Limits of an Award

An order binds a person. It does not bind a ledger.

Asset freeze against a party	Enforceable against a person who holds keys. Compliance is voluntary in the first instance and verifiable on chain after the fact.
Freeze against a custodian	Effective where the custodian is within reach. This is why identifying the exchange early determines whether relief means anything.
Wallet preservation order	Prohibits transfer and destruction of key material. Compliance is auditable on chain, which makes violation provable and sanctionable.
Stablecoin issuer freeze	Some issuers can freeze tokens at the contract level. This is a genuine chokepoint and depends entirely on the issuer's cooperation.
Award enforcement	New York Convention enforcement reaches the party, not the assets. Converting an award into recovered assets is a separate exercise requiring a custodian or a key.

The practical consequence: relief that arrives after self-custodied assets move is a paper victory. Sequencing custodian identification ahead of the relief application is the whole game.

(c) 2026 Lexeprint Inc. All Rights Reserved.

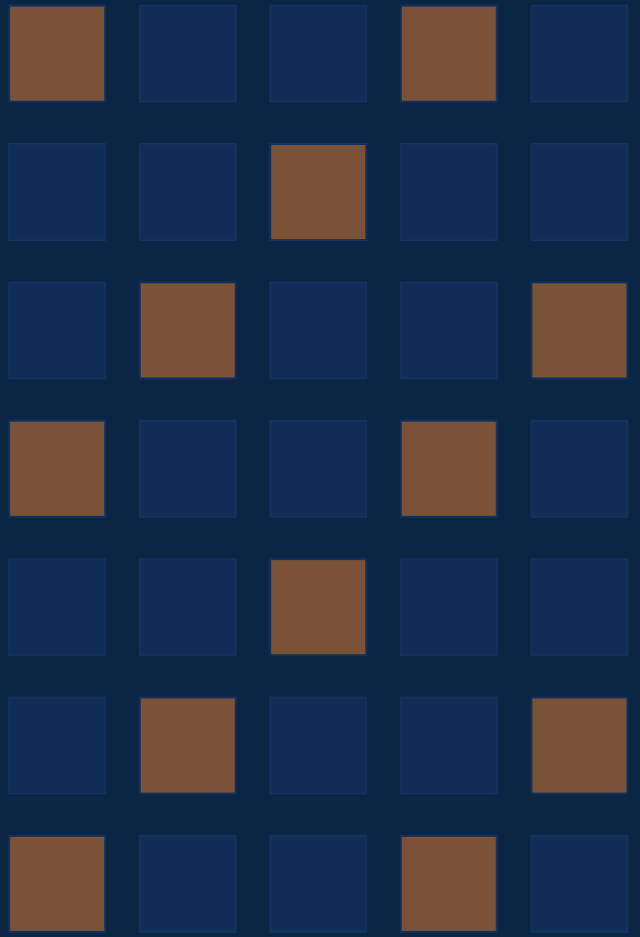
Ten Questions for Any Blockchain Expert

1. How was the chain data collected, and can you reproduce the query?
2. Did you verify against a node, or rely on a third-party explorer?
3. Which clustering heuristics did you apply, and what is their error rate?
4. Which tool, which version, and have you tested its output independently?
5. Which facts are on-chain, and which are inferences from off-chain evidence?
6. What accounting convention did your taint analysis use, and why that one?
7. How did you reconcile block timestamps with wall-clock evidence?
8. What is the confidence interval on your attribution conclusion?
9. What evidence would falsify your opinion?
10. What did you not have access to, and how does that limit the opinion?

The same ten questions discipline your own expert's report before it is served.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Questions?



(c) 2026 Lexeprint Inc. All Rights Reserved.



Daniel B. Garrie, Esq.
Law & Forensics LLC – Founder
JAMS – Neutral
Harvard – Adjunct Faculty
Contact:
W: (855) 529-2466
E: daniel@lawandforensics.com
W: https://www.lawandforensics.com/

LAW & FORENSICS
A Global Legal Engineering Firm

B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel Garrie, Esq. is the Co-Founder of Law & Forensics LLC, where he heads the Computer Forensics and digital discovery Cybersecurity teams. Daniel has been a dominant voice in the computer forensic and cybersecurity space for the past 20 years, as an attorney and technologist. He is an adjunct professor at Harvard for Computer Forensics and prior to Law & Forensics, he successfully built and sold several technology start-up companies.

Since co-founding Law & Forensics LLC in 2008, Daniel has built it into one of the leading boutique cybersecurity forensic engineering firms in the industry. He is a mediator, arbitrator, and e-discovery special master for JAMS and is a partner and head of the Cybersecurity at Zeichner, Ellman & Krause LLP. Daniel has both a Bachelor's and a Master's degree in computer science from Brandeis University, as well as a J.D. from Rutgers Law School.

Daniel has led cyber and forensic teams in some of the most visible and sensitive cyber incidents in the United States. He and his team have worked for two of the top five banks in the globe, and dozens of the largest private and public companies in the world. In addition, Daniel has been awarded several patents for advanced cybersecurity and forensic platform he built with his team that is currently used in the industry, TableTop.AI, CustodyTrack.IO, and Forensic Scan.

Daniel is also well-published in the cybersecurity space and has authored more than 200 articles and books. His work is cited by Black's Law Dictionary 10th Ed. In defining the terms "software", "internet", and "algorithm." Lastly, he has been recognized by several United States Supreme Court Justices for his legal scholarship and is a trusted source and thought leader for cybersecurity articles and opinions, being cited over 500 times to date.

(c) 2026 Lexeprint Inc. All Rights Reserved.



Hon. Jackson Lucky
Mediator, Arbitrator, Neutral—JAMS

Contact:
E: jlucky@jamsadr.com
W: https://www.jamsadr.com/neutrals/lucky

Hon. Jackson Lucky (Ret.) is a mediator, arbitrator, and neutral resolving business, entertainment, cannabis, institutional liability, and complex family and civil disputes. He brings a deep understanding of technology, extensive subject-matter knowledge, and decades of trial advocacy insight to help parties achieve resolution. He has handled thousands of lawsuits and hundreds of ADR proceedings across diverse practice areas. In addition to his judicial experience, he has taught and coached trial advocacy for three decades, including with the Stanford Law School Trial Advocacy Workshop, as a coach and lecturer in law at UCLA Law School, and as a coach at UC Davis Law School.

During his 13 years on the Riverside County Superior Court bench, Judge Lucky served in both family law and unlimited civil divisions. As supervising judge of the family law division for four years, he developed innovative ADR programs that consistently achieved 90% settlement rates. His judicial service earned numerous honors, including the Outstanding Jurist Award from the Leo A. Deegan Inn of Court and Judicial Officer of the Year from the Riverside County Barristers. As the first Korean American and first AAPI judge in Riverside County, he received the Trailblazer Award from the Asian Pacific American Lawyers of the Inland Empire.

Judge Lucky has decades of programming experience, ranking him in the top 11% of contributors to Stack Overflow, a computer programming website with over 14 million users. He pioneered digital education for judges through his Digital Judge podcast series—one of the Center for Judicial Education and Research's most downloaded resources. As a member of the California Chief Justice's Pretrial Reform Operations Workgroup, he taught judges about best practices for algorithmic pretrial risk assessment tools. Known for his clear, practical teaching style, technical expertise, and legal experience, Judge Lucky is a sought-after instructor on evidence, ethics, AI, and virtual ADR for judges and attorneys nationwide.



Angus F. Ni
Morrow Ni LLP – Partner

Contact:
E: angus@moni.law
W: https://www.moni.law/angus-ni

MORROW NI / LLP

Mr. Ni has extensive experience litigating for and advising individuals and companies in complex, cross-boarder disputes, with particular expertise in securities litigation. Because his experience spans the spectrum of cases, Mr. Ni has become the "go-to", trusted consigilieri to many businesses requiring high-touch, strategic advise to navigate everything from multi-jurisdictional commercial disputes, to asset protection (or enforcement) issues, to civil and criminal investigations. Mr. Ni is known for thinking many steps ahead while giving concrete, direct, and actionable advice. He is also one of a handful of U.S. attorneys practicing complex commercial litigation who is also fluent in Mandarin.

Prior to co-founding Morrow Ni LLP, Mr. Ni was a litigator at Bernstein Litowitz Berger & Grossman LLP, the top shareholder rights law firm in the U.S., where he prosecuted numerous securities class actions against U.S. listed corporations on behalf of hedge fund and pension fund investors. These actions ranged across a multitude of industries, were before diverse jurisdictions throughout the U.S., and involved both domestic and international discovery.
Earlier in his career, Mr. Ni also practiced as an associate in the litigation department of Debevoise & Plimpton LLP, a major transnational law firm, where he participated in complex arbitrations before the International Chamber of Commerce (ICC) and World Bank Investment Treaty (ICSID) Tribunals, and in large-scale corporate investigations in several jurisdictions.



Justin Herring
Mayer Brown– Partner

Contact:
E: jherring@mayerbrown.com
W: https://www.mayerbrown.com/en/people/h/justin-herring

MAYER | BROWN

Justin Herring provides clients with comprehensive representation and counseling on sophisticated cybersecurity matters, including global incident response, enforcement actions and related litigation, cyber monitorships and regulatory compliance. He also advises individuals and entities in the crypto and fintech sectors.

Prior to joining Mayer Brown, Justin was Executive Deputy Superintendent of the Cybersecurity Division at the New York State Department of Financial Services (NYDFS). At NYDFS, he served as the first leader of the agency's Cybersecurity Division, itself a first-of-its-kind unit at a financial services regulator. NYDFS issued the nation's first cybersecurity regulation for financial services, which has since become a model for other regulators such as the Federal Trade Commission, the Securities and Exchange Commission, and dozens of state banking and insurance regulators. Under Justin's leadership, NYDFS' Cybersecurity Division became a go-to source for guidance on novel and emerging cyber challenges. Among the influential regulation developed during his tenure was the nation's first cybersecurity regulation for financial services, and others adopted by the Federal Trade Commission and dozens of state banking and insurance regulators.

Prior to NYDFS, Justin served as the inaugural chief of the Cybercrimes Unit at the US Attorney's Office for the District of New Jersey, where he led several of the most consequential cyber prosecutions, including the first major insider trading and hacking cases (Newswire & SEC EDGAR Hacks) as well as the prosecution of the first ransomware ring focused on corporate extortion (Samsam). He served for nine years as an Assistant United States Attorney in New Jersey and in the District of Maryland. In addition to complex cybercrimes prosecutions, Justin prosecuted financial crimes such as securities fraud and tax evasion. He draws on his extensive courtroom experience when serving clients and has tried seven cases to verdict.

Justin served on the New York Governor's Cybersecurity Advisory Board from 2019 to 2022, where he developed guidance and solutions related to election security, critical infrastructure protection and pandemic benefits fraud.