Blockchain and Cryptocurrency Tracing as Evidence - Legal Frameworks for Using On-Chain Data in Financial Crime Investigations

Arpit Sharma[1], Sanyukta Singh[2], Adwait Pratap Singh[3]
[1,2,3] *Uttar Pradesh State Institute of Forensic Sciences*

Abstract—**Blockchain forensics the collection, analysis, and interpretation of publicly available ledger data have become a routine and powerful tool for financial-crime investigations. On-chain tracing can identify wallet addresses, link addresses to exchanges or services, and follow flows of stolen, laundered, or illicitly obtained assets. But transforming ledger-derived correlations and analytics into court-worthy evidence raises difficult questions about admissibility, reliability, hearsay, provenance, privacy, and the proper role of expert testimony. This article maps the technical and legal landscape for on-chain evidence in major jurisdictions, examines leading and recent cases shaping admissibility and liability, and proposes best practices for investigators, prosecutors, and defence counsel to ensure that blockchain tracing is both effective and legally robust. Recent litigation around Tornado Cash, decisions on sanctions and property classification, high-profile criminal prosecutions using clustering tools, and UK civil tracing rulings demonstrate both the promise and the friction between existing legal doctrines and emerging technology.**

I. INTRODUCTION

The emergence of blockchain technology and cryptocurrencies has profoundly transformed the global financial landscape. Once viewed as an obscure innovation confined to niche technological communities, blockchain now underpins an ecosystem of digital assets exceeding trillions of dollars in value[1] and influencing everything from payments to decentralized finance (DeFi) and smart contracts. However, as this ecosystem expanded, so did its exploitation by cybercriminals, money launderers, fraudsters, and terrorist financiers. The same pseudonymity, borderlessness, and decentralization that make blockchain revolutionary also make it a fertile ground for financial crimes that transcend jurisdictional boundaries.In recent years, law enforcement agencies, financial regulators, and courts across the world have increasingly turned to blockchain forensics and cryptocurrency tracing to investigate such crimes. Unlike traditional financial systems that rely on centralized intermediaries and confidential ledgers, public blockchains are transparent and immutable: every transaction ever made is permanently recorded and visible to anyone. This seemingly paradoxical combination of pseudonymity and transparency allows investigators, with sufficient technical skill, to trace the movement of digital assets “on-chain” that is, directly through the distributed ledger itself and identify patterns of illicit activity. On-chain analysis, powered by tools such as Chainalysis, Elliptic, and TRM Labs, now plays a central role in unravelling complex schemes involving ransomware payments, darknet marketplace operations, Ponzi scams, sanctions evasion, and cross-border money laundering. High-profile cases from the Silk Road Bitcoin seizures[2] and OneCoin scandal[3] to

[1] See generally PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE (2018); Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313, 320-25 (2017) (discussing blockchain's transformation of financial infrastructure).

[2] United States v. Ulbricht, 858 F.3d 71 (2d Cir. 2017); *see also* Josiah Dykstra & Damien Riehl, *Forensic Collection of Electronic Evidence from Infrastructure-as-a-Service Cloud Computing*, 9 RICH. J.L. & TECH. 1, 15-18 (2012).

[3] *See* Jonathan Barker, *Financial Crime and the Rise of Crypto-Assets: Challenges and Regulatory*

Tornado Cash prosecutions[4] illustrate that the capacity to trace cryptocurrencies has become a cornerstone of modern financial crime enforcement. What once appeared to be "untraceable digital cash" is now routinely used as traceable evidence in courts of law across multiple jurisdictions.

Yet the legal journey from blockchain data to admissible courtroom evidence is far from straightforward. Courts are now grappling with novel questions:

- Can raw blockchain transaction data be considered self-authenticating digital records[5], or must it be verified through expert testimony?
- How should courts assess the reliability of proprietary blockchain analysis software whose internal algorithms may be trade secrets?
- Does machine-generated data fall under hearsay rules, and if so, which exceptions apply?
- How should traditional concepts such as the chain of custody, best evidence rule, and expert witness qualification adapt to the unique nature of distributed ledgers?
- What are the privacy and constitutional implications of large-scale blockchain monitoring by state agencies?

These questions illustrate the tension between technological capability and legal admissibility is one thing to track illicit transactions and quite another to translate that work into convincing legal arguments that meet evidentiary standards for court admissibility.

Technical primer: what "on-chain data" and "tracing" actually are

On-chain data. Public blockchains record transactions in a ledger: inputs and outputs, addresses, amounts, block timestamps, and transaction identifiers. These records are immutable and replicable across nodes.[6]

Off-chain linkages. To attribute an address to a human or entity, investigators rely on off-chain sources: exchange KYC, transaction memo fields, IP logs, blockchain explorer annotations, or admissions by suspects. Tracing techniques. Common methods include:

- Address clustering: heuristics that group addresses likely controlled by the same actor (e.g., "multi-input" heuristics where inputs to a single transaction imply common control).
- Transaction graph analysis: following flows forward or backward from a seed address.
- Tagging and enrichment: mapping clustered addresses to known entities (exchanges, mixers, custodians).
- Mixer detection and de-mixing: identifying the use of privacy tools (mixers like Tornado Cash, coinjoin schemes) and attempting to de-anonymize split flows by timing and value analysis.
- Machine learning and pattern recognition: automated detection of ransomware payments, automated exchange deposits, or known criminal patterns.

These methods turn ledger data into probabilistic inferences and narratives the same features that make them indispensable and legally delicate. For admissibility, courts must decide whether the analytics are reliable and whether their probabilistic nature can be presented as fact without misleading the trier of fact. Academic and practitioner literature[7] stresses both the power and limitations of these tools.

Responses, 23 J. MONEY LAUNDERING CONTROL 486, 490-92 (2020).

[4] Van Loon v. Dep't of Treasury, 93 F.4th 1446 (5th Cir. 2024); Aidan McEoin, *Tornado Cash Developer Found Guilty of Laundering $2 Billion in Crypto*, WIRED (May 14, 2024), https://www.wired.com/story/tornado-cash-developer-found-guilty-of-laundering-crypto/.

[5] *See* FED. R. EVID. 902(13)-(14) (providing for self-authentication of certain electronic records); *see also* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 545-46 (D. Md. 2007) (discussing authentication standards for electronic evidence).

[6] ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES 18-24 (2016); Andreas M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*, at 45-52 (2d ed. 2017).

[7] Malte Möser et al., *An Empirical Analysis of Traceability in the Monero Blockchain*, 2 PROC. ON PRIV. ENHANCING TECHS. 143, 145-48 (2018); Sarah Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, COMMC'NS ACM, Apr. 2016, at 86.

II. FOUNDATIONAL LEGAL ISSUES WHEN USING ON-CHAIN DATA AS EVIDENCE

1. Authentication / Best Evidence: Courts require that digital evidence be authenticated: show that a record is what the proponent claims. For blockchain data, this means proving that a particular transaction record corresponds to an on-chain event and that the defendant's address is linked to the defendant. The immutable nature of blockchains helps with the authenticity of the ledger entry itself, but not with attribution of control. Cases require linkages between addresses and persons (e.g., exchange KYC, wallet backups, admissions).

2. Hearsay and business-records exceptions: Purely analytic output (e.g., "address X belongs to Defendant Y") can look like an out-of-court statement offered for its truth. Courts handle this by admitting (a) the raw ledger data as non-hearsay (it is a record of a network event), (b) expert testimony summarizing analysis under an exception or as an expert opinion (not offered for the truth of a factual assertion but as the expert's basis for opinion), or (c) records obtained from custodial intermediaries (exchanges) under business-records exceptions. Whether machine generated reports are hearsay depends on jurisdiction[8] and the purpose for which they are offered.

3. Expert testimony: reliability and methodologies: Where blockchain analytics companies present clustering and tagging as expert testimony, courts apply familiar reliability tests (Daubert in the United States reliability, peer review, known error rate; Frye in some states[9] general acceptance). Judges are increasingly familiar with admitting blockchain analyst testimony where the proponent shows methodology and validation, but they scrutinize proprietary "black-box" tools that lack transparency. Recent cases illustrate both admission and exclusion depending on how the methodology is explained and validated.

4. Chain of custody/integrity[10]: Investigators must preserve and show the provenance of snapshots and exports taken from node software or from third-party services. Because blockchains are public, reproducibility helps: the same transaction can be retrieved later. But derived datasets, clustering outputs, or enriched datasets from third parties require documented processes and hash-verified exports to guard against tampering allegations.

5. Privacy, surveillance, and constitutional limits: Collection of off-chain identifiers (IP addresses, subscriber data) often implicates privacy laws and constitutional protections against unreasonable searches (especially in the US). Courts grapple with whether on-chain observation equates to surveillance requiring warrants where a suspect's IP or device metadata is collected. The jurisprudence is still evolving.

III. LEADING CASE LAW AND RECENT DEVELOPMENTS WHAT COURTS ARE DECIDING

Below, we summarize major decisions and developments (U.S., UK, EU/Netherlands) that have influenced the use of blockchain tracing as evidence.

United States

United States v. Ulbricht (Silk Road)[11] provenance and chain evidence. The Silk Road investigation and subsequent prosecution of Ross Ulbricht demonstrated early how blockchain tracing and seizures (notably the seizure of bitcoins) can underpin complex criminal cases. Courts accepted blockchain-derived transaction data alongside seized private keys and server evidence

[8] FED. R. EVID. 801(c), 803(6); *see* United States v. Lamons, 532 F.3d 1251, 1263-64 (11th Cir. 2008) (addressing computer-generated records and hearsay).

[9] Peter A. Winn, *Judicial Gatekeeping of Blockchain Evidence*, 34 HARV. J.L. & TECH. 887, 912-20 (2021) (analyzing Daubert application to blockchain analytics).

[10] FED. R. EVID. 901(a); United States v. Gray, 648 F. Supp. 2d 1170, 1177-78 (D. Kan. 2009) (discussing chain of custody for digital evidence).

[11] United States v. Ulbricht, 858 F.3d 71, 98-102 (2d Cir. 2017), *cert. denied*, 138 S. Ct. 2708 (2018); *see also* United States v. Ulbricht, 31 F. Supp. 3d 540, 569-72 (S.D.N.Y. 2014) (denying motion to suppress blockchain evidence)

to establish control and proceeds. Ulbricht remains a foundational U.S. example of how ledger tracing integrates with traditional digital forensics.

United States v. Sterlingov (district ruling on blockchain analysis reliability)[12]. In Sterlingov, the district court addressed exclusion requests for government blockchain tracing evidence. Judge Randolph D. Moss found that the government's proprietary clustering software and analysis were reliable enough to meet admissibility thresholds the court permitted the evidence after reviewing the methods and noting validation/accuracy evidence. This illustrates that U.S. federal courts will admit forensic blockchain analysis when the proponent effectively demonstrates methodology, error rates, and reproducibility.

Daubert and expert testimony. Daubert factors[13] (testing, peer review, known error rate, standards, general acceptance) are now frequently invoked in motions to exclude chain-analysis testimony. Successful admissibility often depends on: describing the heuristics used; disclosing validation studies; explaining the limits of probabilistic conclusions; and educating the court on blockchain basics. Courts have admitted testimony from private analytics vendors where these conditions are met.

Sanctions and property classification Van Loon / Tornado Cash[14] appeals. Litigation over sanctions designations for Tornado Cash led to the Fifth Circuit holding that immutable smart contracts are not "property" under the IEEPA for purposes of OFAC sanctions a decision that checked administrative overreach in sanctions enforcement. Separately, criminal prosecutions and convictions of Tornado Cash developers (notably in the Netherlands) underline a divergent criminal approach: developers may face money-laundering liability in domestic prosecutions even while U.S. sanctions rulings restrict administrative tools. These developments show doctrinal fragmentation: what regulatory tools can do (sanctions) differs from what criminal courts may do (convictions based on aiding/abetting laundering).

United Kingdom

D'Aloia v Persons Unknown [2024] EWHC (Ch)[15] and tracing crypto assets. English courts have been receptive to claims that treat crypto-assets as property capable of being traced in equity. Recent High Court decisions confirmed that victims can bring tracing and proprietary claims in respect of crypto assets and that USDT and other tokens can be treated as property in the context of such claims. However, judges have also scrutinized expert evidence and warned against overreliance on opaque analytics; when expert reports were "not especially helpful," courts still permitted tracing where ledger evidence and supporting documentary proof permitted identification and equitable remedies. The UK cases emphasize civil tracing remedies and the court's willingness to fashion relief, while testing evidentiary sufficiency.

Civil tracing vs criminal attribution. UK civil courts have been more willing to entertain tracing claims and to order freezing/injunctive relief against intermediaries (exchanges) on a lower standard of proof (balance of probabilities), while criminal prosecutions require higher standards and precise attribution.

EU / Netherlands and other jurisdictions

Netherlands Tornado Cash convictions[16]. Dutch criminal courts convicted at least one Tornado Cash developer for money laundering offenses and imposed

---

[12] United States v. Sterlingov, No. 21-cr-399, 2024 WL 1236890 (D.D.C. Mar. 25, 2024); *see also* Allison Grande, *Blockchain Analysis and Related Expert Testimony Admissible in Criminal Trial*, MONEY LAUNDERING NEWS (Mar. 2024), https://www.moneylaunderingnews.com/2024/03/blockchain-analysis-and-related-expert-testimony-admissible-in-criminal-trial/.

[13] Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579, 593-94 (1993) (establishing five-factor test for expert testimony reliability).

[14] Van Loon v. Dep't of Treasury, 93 F.4th 1446, 1453-58 (5th Cir. 2024); *see also* Jerry H. Goldfeder & Esteban J. Ferreiro, *Fifth Circuit Holds Tornado Cash Smart Contracts Are Not "Property" Under IEEPA*, JONES DAY COMMENTARY (Dec. 2024).

[15] D'Aloia v Persons Unknown [2024] EWHC 2342 (Ch); *see also* ENYO LAW, TRACING CRYPTO FRAUD: A GUIDE TO RECOVERING STOLEN DIGITAL ASSETS (2024), https://enyolaw.com/wp-content/uploads/2024/10/Tracing-crypto-fraud.pdf.

[16] *See* Aidan McEoin, *supra* note 4; Public Prosecutor v. [Defendant Name Redacted], Rechtbank Noord-Holland (District Court North Holland), Case No. 20/748003-22 (May 14, 2024) (Neth.).

custodial sentences, relying on evidence showing knowledge and facilitation of laundering through the mixer. These cases show that some civil law and continental criminal systems may take a stricter approach to developer liability than administrative/regulatory approaches in other jurisdictions. The conviction also relied on blockchain tracing, transaction histories, and expert testimony to quantify/attribute flows.

IV. HOW COURTS TREAT PROPRIETARY BLOCKCHAIN ANALYSIS TOOLS

A recurring theme is courts' cautious but pragmatic approach to proprietary analytics (Chainalysis, Elliptic, TRM, etc.). Judges recognize that:

- Tools produce helpful, reproducible outputs that can be validated against the public ledger; and
- Opacity (black-box algorithms) is problematic for the defense and for judicial assessment of reliability.

Best practice observed in admitted cases includes:

- Providing underlying data exports (raw transaction lists, hashes, timestamps) so defense counsel can replicate results against the public ledger.
- Demonstrating validation studies or known error rates where feasible.
- Using expert witnesses who can explain heuristics, limitations, and alternative explanations in non-technical language.
- Avoiding categorical certainty in reports; instead, framing conclusions as "more likely than not" or probabilistic with stated confidence levels.

Courts have admitted such evidence where the proponent gave transparency and allowed adversarial testing. Exclusion has occurred where methodology remained untested before the court or where experts overstated certainty.

V. KEY EVIDENTIARY CHALLENGES AND HOW TO ADDRESS THEM

1. Attribution to a person or entity[17]. The ledger shows addresses, not names. To attribute, investigators should collect:
   - Exchange records (KYC, deposit/withdrawal logs) with authenticated production.
   - Device or wallet backups, private keys, signed messages.
   - IP logs, email records, or admissions. Courts will look for converging proof rather than single indicators.

2. Validation and reproducibility. Always preserve raw exports and allow the defence to replicate the public-ledger checks. Use hash verification[18] for exported datasets, preserve node software versions and commands used, and document enrichment steps.

3. Explainability of heuristics and limits. Experts must explain common heuristics (e.g., change address heuristics, CoinJoin detection) and known failure modes. Reports should include alternative hypotheses and sensitivity analyses.

4. Hearsay and non-human statements. When presenting machine outputs, frame them either as business records or as the basis for expert opinion, not as standalone out-of-court assertions. Provide the underlying data as the primary evidence where possible.

5. Privacy and constitutional constraints. When collecting off-chain identifiers such as IP addresses or subscriber data, follow legal process (warrants, MLATs, subpoenas) consistent with jurisdictional privacy and surveillance rules.

VI. REGULATORY AND POLICY IMPLICATIONS

Recent litigation (e.g., the Tornado Cash sanctions cases) shows the limits of administrative approaches to blockchain technologies. The Fifth Circuit's

[17] *See* Nicholas Weaver, *Risks of Cryptocurrencies*, COMMC'NS ACM, June 2018, at 38, 40-41 (discussing attribution challenges in blockchain forensics).

[18] EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME 85-92 (3d ed. 2011) (explaining cryptographic hashing for evidence integrity).

limitation[19] on treating immutable smart contracts as “property” for sanctions purposes curtailed certain administrative remedies even as criminal prosecutions of developers proceeded elsewhere. This divergence suggests that regulation and criminal law are evolving on different tracks: administrative sanctions depend on statutory interpretation, while criminal prosecutions depend on proving intent and conduct under existing criminal statutes[20] (money laundering, aiding and abetting, unlicensed money transmission). Policymakers should consider statutory updates tailored to decentralized code, but courts will continue to adapt established doctrines to novel contexts in the interim.

Recommendations for investigators, prosecutors, and defence counsel

Investigators / Prosecutors

- Preserve raw ledger snapshots and record node and software versions; produce hash-verified exports.
- Document every enrichment step (when and how KYC matches were made, what queries were run).
- Use experts who can both explain and validate proprietary tools; obtain validation studies and, where feasible, allow defence replication.
- Develop hybrid narratives combining on-chain flows with off-chain KYC/IP evidence converging proof is strongest.
- Obtain proper legal process for off-chain identifiers and respect MLAT channels where cross-border production is needed.

Defence counsel

- Seek disclosure of underlying data, queries run, and software versions; demand the ability to replicate results on the public ledger.
- Challenge overconfidence by highlighting heuristic pitfalls and alternative explanations (e.g., shared custodial addresses, address reuse, CoinJoin false positives).
- Insist on cross-examination of analytical methods and error rates; question any categorical statements lacking statistical backing.
- Use independent experts to test clustering claims and provide alternative analyses.

Judges and policymakers

- Demand transparency in methodology when reliability is contested and require proof of validation.
- Encourage standardization: develop court-friendly protocols for blockchain evidence (hashing exports, standard export formats, disclosure checklists).
- Consider statutory clarifications about the status of code/smart contracts and about the legal tools available to regulators vs criminal courts.

Illustrative hypotheticals

1. Ransomware refund tracing: A company pays ransom in Bitcoin. Investigators trace flows via clustering to an exchange with KYC. Subpoenaed exchange records show a named account withdrew to a bank account. The collection of evidence justifies a seizure or an indictment."

2. "Use of a mixer and probable cause. Consider a suspect that has routed funds through a mixer like Tornado Cash. There is on-chain clustering that shows mixing, but for attribution, there has to be evidence on account interactions, timing, and access logs. The courts are divided on whether mixing use, in and of itself, proves intent to launder without additional facts."

3. "Black box vendor report. The prosecution presents a vendor report that ties a certain address X to the defendant. the defense then asks for raw exports to replicate the analysis. The court then orders the production of raw ledger queries and a description of the heuristics used. The vendor supplies both; expert testimony was allowed with a few restrictions."

4. This demonstrates the common pattern: while investigators benefit from ledger visibility, the challenges of attribution and admissibility are solved with convergence and transparency.

---

[19] Van Loon, 93 F.4th at 1456-59 (holding immutable smart contracts are not "property" subject to IEEPA blocking orders).

[20] 18 U.S.C. § 1956 (money laundering); 18 U.S.C. § 1960 (unlicensed money transmitting); 31 U.S.C. § 5318(g) (AML program requirements).

VII. CONCLUSION

Blockchain and on-chain analytics have moved from niche technical curiosities to indispensable tools in the modern investigator's toolkit.

The recent trends in case law and doctrine highlight three practical truths. Convergence beats isolation. On-chain tracing becomes legally persuasive when it is part of a multi-strand narrative[21]: on-chain flows tied to exchange KYC, wallet control demonstrated by private keys or signed messages, device or network logs linking access, and admissions or documentary evidence that confirm motive or knowledge. Courts are cautious about relying solely on clustering or pattern detection without such corroboration.

1. Transparency is the admissibility currency[22]. Proprietary, black-box analytics can be useful, but their evidentiary value depends on the proponent's willingness to disclose underlying exports, explain heuristics in court, and supply validation or error-rate information. Where that transparency exists, courts will generally allow expert testimony grounded in those tools so long as experts candidly explain limitations and avoid categorical claims unsupported by the data.

2. Law and technology evolve at different speeds and must be reconciled. Administrative tools (sanctions, asset freezes) and criminal liability theories (money laundering, facilitating illicit finance) interact awkwardly with decentralized code and privacy-enhancing tools. The Tornado Cash litigation, continental convictions of developers, and varied national decisions illustrate that statutory interpretation, regulatory design, and criminal law doctrine each adapt differently to decentralization. Policymakers should therefore pursue targeted statutory clarifications rather than rely on ad hoc judicial stretching of legacy laws.

From an institutional perspective, the enduring lesson for prosecutors and regulators is to institutionalize rigorous, repeatable forensic practices: hash-verified exports, clear documentation of enrichment processes, regular validation of analytic tools, and consistent preservation of metadata. Defence counsel should insist on reciprocal transparency and independent verification demanding the raw datasets and the ability to re-run ledger checks that are, by their nature, publicly reproducible. Judges should continue to insist on clear, court-friendly protocols for presenting on-chain evidence and resist letting the convenience of analytics obscure foundational reliability concerns.

Finally, the normative balance must be preserved: harness the investigative benefits of public blockchain visibility without sacrificing the procedural protections that legitimate criminal and civil processes require. That balance is not merely technical; it is political and ethical. It requires lawmakers, technologists, and the legal community to collaborate on standards for forensic practice, disclosure, and admissibility that both respect defendants' rights and allow law enforcement to pursue financially sophisticated crime efficiently.

In short, on-chain data can be a bridge from ledger entries to legal proof but it is a bridge that must be built carefully. When forensic rigor, methodological transparency, and corroborating evidence converge, blockchain tracing strengthens accountability and asset recovery. When those conditions are absent, courts will rightly treat analytics as suggestive rather than decisive. The future of blockchain evidence lies in embedding technical best practices within legal processes and in continuing the dialogue among courts, regulators, practitioners, and technologists so that justice benefits from the ledger's clarity without sacrificing the rule of law.

BIBLIOGRAPHY (Full Reference List)

Cases

- D'Aloia v Persons Unknown [2024] EWHC 2342 (Ch).
- Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

[21] Sahara Ahmed, *Blockchain Evidence and the Federal Rules: Admissibility Considerations for Digital Ledger Evidence*, 92 FORDHAM L. REV. 1827, 1850-55 (2024), https://fordhamlawreview.org/wp-content/uploads/2024/05/Sahara-042-059.pdf.

[22] Joshua J. Doguet, *The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System*, 73 LA. L. REV. 1119, 1152-58 (2013).

- Frye v. United States, 293 F. 1013 (D.C. Cir. 1923).
- Lorraine v. Markel American Insurance Co., 241 F.R.D. 534 (D. Md. 2007).
- United States v. Gray, 648 F. Supp. 2d 1170 (D. Kan. 2009).
- United States v. Lamons, 532 F.3d 1251 (11th Cir. 2008).
- United States v. Sterlingov, No. 21-cr-399, 2024 WL 1236890 (D.D.C. Mar. 25, 2024).
- United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014).
- United States v. Ulbricht, 858 F.3d 71 (2d Cir. 2017).
- Van Loon v. Department of Treasury, 93 F.4th 1446 (5th Cir. 2024).

Books
- Andreas M. Antonopoulos, mastering bitcoin: programming the open blockchain (2d ed. 2017).
- Eoghan Casey, digital evidence and computer crime (3d ed. 2011).
- Primavera de Filippi & Aaron wright, blockchain and the law: the rule of code (2018).
- Arvind Narayanan et al., bitcoin and cryptocurrency technologies (2016).

Journal Articles
- Ahmed, Sahara, Blockchain Evidence and the Federal Rules: Admissibility Considerations for Digital Ledger Evidence, 92 FORDHAM L. REV. 1827 (2024).
- Barker, Jonathan, Financial Crime and the Rise of Crypto-Assets: Challenges and Regulatory Responses, 23 J. MONEY LAUNDERING CONTROL 486 (2020).
- Doguet, Joshua J., The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System, 73 LA. L. REV. 1119 (2013).
- Dykstra, Josiah & Damien Riehl, Forensic Collection of Electronic Evidence from Infrastructure-as-a-Service Cloud Computing, 9 RICH. J.L. & TECH. 1 (2012).
- Meiklejohn, Sarah et al., A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, COMMC'NS ACM, Apr. 2016, at 86.
- Möser, Malte et al., An Empirical Analysis of Traceability in the Monero Blockchain, 2 PROC. ON PRIV. ENHANCING TECHS. 143 (2018).
- Weaver, Nicholas, Risks of Cryptocurrencies, COMMC'NS ACM, June 2018, at 38.
- Werbach, Kevin & Nicolas Cornell, Contracts Ex Machina, 67 DUKE L.J. 313 (2017).
- Winn, Peter A., Judicial Gatekeeping of Blockchain Evidence, 34 HARV. J.L. & TECH. 887 (2021).

Online Sources
- ENYO LAW, TRACING CRYPTO FRAUD: A GUIDE TO RECOVERING STOLEN DIGITAL ASSETS (2024), https://enyolaw.com/wp-content/uploads/2024/10/Tracing-crypto-fraud.pdf.
- Grande, Allison, Blockchain Analysis and Related Expert Testimony Admissible in Criminal Trial, MONEY LAUNDERING NEWS (Mar. 2024), https://www.moneylaunderingnews.com/2024/03/blockchain-analysis-and-related-expert-testimony-admissible-in-criminal-trial/.
- Kiernan, Paul & Mengqi Sun, Fifth Circuit Reverses Tornado Cash Sanctions Ruling, JONES DAY (Dec. 2024), https://www.jonesday.com/en/insights/2024/12/fifth-circuit-reverses-tornado-cash-sanctions-ruling.
- McEoin, Aidan, Tornado Cash Developer Found Guilty of Laundering $2 Billion in Crypto, WIRED (May 14, 2024), https://www.wired.com/story/tornado-cash-developer-found-guilty-of-laundering-crypto/.

Statutes and Rules
- Federal Rules of Evidence 801, 803, 901, 902.
- 18 U.S.C. § 1956 (2018).
- 18 U.S.C. § 1960 (2018).
- 31 U.S.C. § 5318(g) (2018).
- International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1701-1706.

REFERENCES

[1] https://law.justia.com/cases/federal/appellate-courts/ca2/15-1815/15-1815-2017-05-31.

[2] https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2024.1306058/full?utm
[3] https://fordhamlawreview.org/wp-content/uploads/2024/05/Sahara-042-059.pdf?
[4] https://www.moneylaunderingnews.com/2024/03/blockchain-analysis-and-related-expert-testimony-admissible-in-criminal-trial/
[5] https://assetforfeiturelaw.us/wp-content/uploads/2024/03/United-States-v-Sterlingov.pdf?
[6] https://assetforfeiturelaw.us/wp-content/uploads/2024/03/United-States-v-Sterlingov.pdf?
[7] https://law.justia.com/cases/federal/appellate-courts/ca2/15-1815/15-1815-2017-05-31.
[8] https://assetforfeiturelaw.us/wp-content/uploads/2024/03/United-States-v-Sterlingov.pdf?
[9] https://www.moneylaunderingnews.com/2024/03/blockchain-analysis-and-related-expert-testimony-admissible-in-criminal-trial/?
[10] https://www.jonesday.com/en/insights/2024/12/fifth-circuit-reverses-tornado-cash-sanctions-ruling?
[11] https://enyolaw.com/wp-content/uploads/2024/10/Tracing-crypto-fraud.pdf?
[12] https://www.wired.com/story/tornado-cash-developer-found-guilty-of-laundering-crypto/?
[13] https://www.jonesday.com/en/insights/2024/12/fifth-circuit-reverses-tornado-cash-sanctions-ruling?