

What Criminal Defense Attorneys Need to Know about Cryptocurrency

Evidence, Forensics, and Tactical Defense in 2026

Robert Nordlander, CPA, CFE

Forensic Accountant | Former IRS-CI Senior Special Agent

ROBERT NORDLANDER, CPA, CFE

Principal, Nordlander CPA, PLLC — Forensic Accountant & Former IRS-CI Senior Special Agent

EXPERIENCE

- 20+ years as a Senior Special Agent, IRS-Criminal Investigation — federal tax and money-laundering investigations
 - Served as the agency's subject-matter expert on cryptocurrency
 - Member of the FBI Joint Terrorism Task Force; academy instructor
 - Since 2021, Principal of Nordlander CPA, PLLC — forensic accounting, financial analysis, and expert witness testimony for defense attorneys nationwide
-

CREDENTIALS & CONTACT

CREDENTIALS

CPA (North Carolina, 1996) · CFE (2021) · Certified Criminal Investigator (FLETC, 2000) · Chainalysis Reactor Certified in Cryptocurrency Tracing (2019)

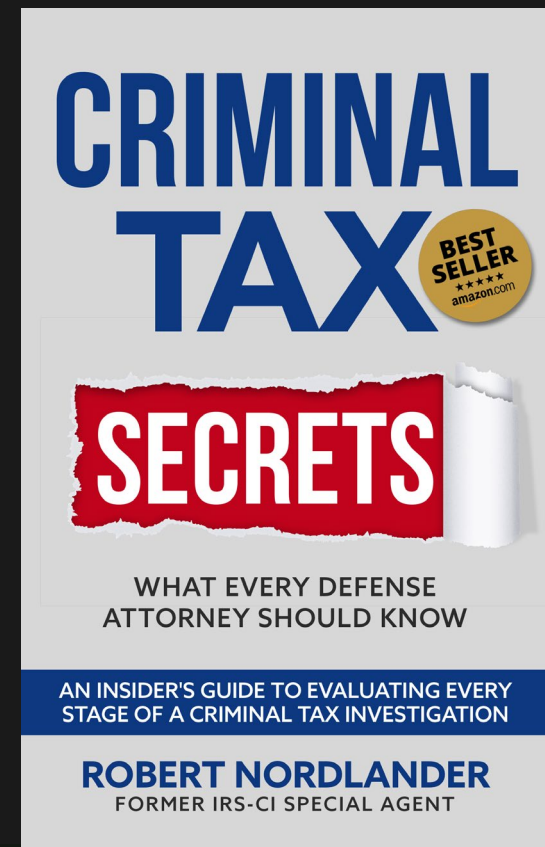
GET IN TOUCH

robert@nordlandercpa.com

(336) 421-2392

www.nordlandercpa.com

MY BOOK



LEARNING OBJECTIVES

By the end of this hour, you should be able to:

1

Explain the Mechanics

Describe how a Bitcoin transaction is signed, broadcast, mined, and confirmed — and how private keys, public keys, and addresses relate to identity.

2

Identify the Charges

Recognize how § 1960 rides alongside § 1956 and § 1957 money-laundering counts, and why courts treat crypto as a covered financial transaction.

3

Cross-Examine the Tracing Witness

Challenge how a tracing witness moves from a wallet address to a conclusion about your client — foundation, hearsay, and Daubert objections.

4

Build a Defense Strategy

Apply the custodial-vs-non-custodial distinction — the live question in the Tornado Cash and Samourai prosecutions — to a money-transmitting charge.

DEFINING THE ASSET

Bitcoin is the prototype. It is not the whole category.

Cryptocurrency is digital value that exists only as entries on a decentralized ledger — copied across thousands of independent computers instead of held by one bank. There is no central issuer; ownership is proven by a private key, not a bank account.

Legal Status

Treated as Property (IRS) or a Commodity (CFTC) — not legal tender in the United States.

The Control Gap

A private key grants authorization to move value, but offers zero evidence of the legal identity of the person who holds it.

OPEN SOURCE. OWNED BY NO ONE.

There is no company, no CEO, and no government behind the Bitcoin software

Anyone Can Read the Code

Bitcoin Core is open-source, published on GitHub. Anyone — including defense experts — can audit exactly what the software does. Nothing is proprietary or hidden.

Changes Require Consensus

Rule changes move through Bitcoin Improvement Proposals and need broad buy-in from node operators, miners, and developers. No single person can rewrite the rules.

WHY NO ONE “ISSUES” BITCOIN

No one “issues” Bitcoin the way a bank issues a product or a company issues stock. It is a voluntary, global agreement to run the same open software and follow the same rules.

Worth pressing a government witness on: if no one controls or issues the software, who exactly is the “financial institution,” and who is the “money transmitter”?

BEYOND BITCOIN

Bitcoin is not the whole category — three families worth knowing

Ethereum

Account-based, not UTXO. Runs programmable code — DeFi, NFTs, and every token built on top.

Stablecoins

USDT / USDC, pegged 1:1 to the dollar. Borderless and stable — now the preferred rail for cross-border laundering.

BEYOND BITCOIN

(continued)

Privacy Coins

Monero, Zcash. Built to defeat address-tracing — ring signatures, shielded balances. Extra scrutiny in discovery.

Altcoins

Thousands more, many as ERC-20 tokens. Different rules, different case law — never assume “crypto” means Bitcoin.

84% of all illicit crypto transaction volume in 2025 moved in stablecoins — not Bitcoin.

Chainalysis, 2026 Crypto Crime Report

PUBLIC KEY VS. PRIVATE KEY

The pair that makes every transaction possible

The Private Key

A secret 256-bit number. It signs transactions to prove authorization to spend. Whoever holds this number — not whoever's name is on an account — controls the funds. It is never shared.

The Public Key & Address

Derived from the private key by one-way math. The address — a hash of the public key — is what gets published to receive funds. Safe to share; it reveals nothing about the private key.

HOW A KEY BECOMES AN ADDRESS

A one-way street — computable forward, unreversible with current computing

PRIVATE KEY → PUBLIC KEY → ADDRESS

One-way street. Each arrow is computationally trivial forward and, with current computing, impossible to reverse — you can prove you hold the key without ever exposing it.

PRIVATE KEYS: STATISTICAL IMPOSSIBILITY

Why brute-forcing a key isn't a real-world attack

The 256-Bit Number

A private key is a randomly generated number so vast (2^{256}) that replication is statistically impossible.

The Cosmic Analogy

There are more private key combinations than the estimated atoms in the observable universe (10^{78} to 10^{82}).



“To guess a specific private key is mathematically equivalent to picking a specific grain of sand out of every beach on Earth.”

THE BLOCKCHAIN LIFECYCLE

Four stages, Bitcoin-specific — each one matters in a tracing dispute

1

Sign

2

Broadcast

3

Mine

4

Confirm

STAGE 1–2: SIGN & BROADCAST

Sign & Broadcast

The private key signs the transaction, authorizing exactly which coins are being spent. That signature is broadcast to the network and sits in the “mempool” — a waiting room for unconfirmed transactions — until a miner picks it up, usually faster for a higher fee.

STAGE 3–4: MINE & CONFIRM

Mine & Confirm

Miners bundle pending transactions into a candidate block and race to solve a proof-of-work puzzle. Each block added afterward is one “confirmation” — 6 is the standard before treating a transfer as final.

Fewer than 6 confirmations means the transaction can still theoretically be reversed by a chain reorganization — relevant when a case's timeline turns on exactly when a transfer became final.

HOW BITCOIN KNOWS THE ADDRESS IS REAL

No one checks an ID. Every node re-runs the same one-way math that created the address: if the signature matches the public key behind it, the transaction is valid — full stop.

That shared math, independently verified by every node, is what stands in for a bank confirming an account is real.

THE RAW REALITY

A real Bitcoin transaction — the first peer-to-peer send, Block 170, Jan. 2009

TRANSACTION HASH (TXID)

f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16

FROM (INPUT)

12cbQLTFMXRnSzktFkuoG3eHoMeFtpTu3S

Satoshi's own address, spending a 50 BTC mining reward as the input.

OUTPUT #1 — TO

1Q2TWHE3GMdB6BZKafqwxXtWAWgFt5Jvm3

10 BTC sent to Hal Finney. The payment itself.

OUTPUT #2 — CHANGE

12cbQLTFMXRnSzktFkuoG3eHoMeFtpTu3S

40 BTC returned to Satoshi — same address as the input, this is the “change.”

No name, no bank — just a hash, two scripts, and two numbers. Everything beyond that is a witness's interpretation.

RAW VS. EXPLORER

What the chain actually says, versus what a witness says it means

The Immutable Record

Hexadecimal script. Anonymized addresses. This is admissible: it's exactly what every node on the network independently verified and agreed to.

The Explorer View

Interpretive labels (“Binance Hot Wallet,” “Darknet Market”) from a proprietary database. A private company's guess, not a blockchain fact — and what a witness usually reads from.

WORKED EXAMPLE

The chain itself only ever says: “Address X sent 0.5 BTC to Address Y.” A tracing witness testifies: “Address X belongs to the defendant, and Address Y is a known exchange deposit wallet.” Both labels come from a subscription database, not the blockchain.

That gap is a hearsay and foundation problem: an out-of-court assertion by a private vendor, offered for its truth, dressed up as expert observation.

IDENTITY VS. AUTHORIZATION

Traditional Banking

Verification of the **Human Identity** (KYC) occurs *before* any value moves.

The Blockchain

Verification of the **Cryptographic Signature** (Math) is all that occurs. Identity remains off-chain.

HOW PEOPLE BUY BITCOIN

Three on-ramps — only two of them create an identity record



Centralized Exchange

Coinbase, Kraken, and similar.
Government ID, linked bank card,
often an SSN for 1099 reporting.
This is the paper trail that shows
up in subpoena returns.



Bitcoin ATM / Kiosk

Cash-to-BTC at a physical kiosk.
ID is required above federal/state
thresholds; smaller cash
purchases can be far lighter-
touch.

HOW PEOPLE BUY BITCOIN

(continued)



Peer-to-Peer / OTC

Direct wallet-to-wallet transfer — cash, trade, or a broker who arranges it off-platform. No exchange KYC layer at all.

Every on-ramp except true peer-to-peer creates an identity record somewhere. That's usually where the government's chain of custody starts — and where cross-examination should test it.

MINING & CONSENSUS

10

Minutes (Avg Block Time)

Mining secures the order and validity of entries, but it provides zero proof of the actor's legal authorization or state of mind.

WHAT MINERS DO & HOW THEY'RE PAID

The Job

Miners collect pending transactions into a candidate block and race to solve a computationally-hard puzzle. Whoever solves it first adds the next block to the chain.

The Paycheck

The winning miner receives the block subsidy (newly-created coins) plus every transaction fee in that block — paid automatically by the protocol. No employer, no invoice, no W-2.

THE BLOCK SUBSIDY

3.125 BTC

Current block subsidy — halves roughly every 4 years; next halving $\approx$ March 2028

No entity “employs” a miner. Payment is protocol-enforced code, not a business relationship — worth making explicit when the government calls a miner a financial institution.

PART 2

DEFENSE & ENFORCEMENT STRATEGY

APPLIED TO CODE, NOT CUSTODIANS

The 2025 Cases

Tornado Cash (U.S. v. Storm) — convicted Aug. 2025 of §1960 conspiracy; jury deadlocked on the money-laundering/IEEPA counts, retrial set for Oct. 2026. Samurai Wallet (U.S. v. Rodriguez) — pleaded guilty; sentenced Nov. 2025 to the statutory max, \$6.3M forfeiture.

WHY THESE CASES MATTER — TORNADO CASH

An Untested, Live Theory

Storm's code was fully non-custodial — he could never freeze or control a single transaction that ran through it. The jury convicted on the §1960 conspiracy count alone but deadlocked on money laundering and the IEEPA sanctions counts — proof the “no custody required” theory doesn't automatically win every count. A retrial on the deadlocked counts is set for October 2026. This is not settled law yet.

WHY THESE CASES MATTER — SAMOURAI

The Distinguishing Line

Samourai ran a coordinator server that actively facilitated every mixing transaction, and prosecutors had evidence the founders marketed the tool for laundering. Much closer to “operating a business” than Tornado Cash's hands-off contract.

Push the government to prove how custodial the code was and whether there's real evidence of intent — before conceding your client is a “money transmitter” at all.

HOW CRYPTO GETS LAUNDERED

The mechanics prosecutors point to alongside the predicate offense



Mixers & Tumblers

Pool many users' coins together and redistribute them, breaking the on-chain link between source and destination.



Chain-Hopping

Swap between cryptocurrencies or blockchains — through a DEX, bridge, or swap service — to break a trail that only follows one chain.

HOW CRYPTO GETS LAUNDERED

(continued)



Structuring Across Wallets

Split funds across many addresses and small transactions to stay under reporting thresholds.



Exchange Layering

Route funds through a chain of exchanges — especially weak-KYC jurisdictions — before cashing out to fiat.

Stablecoins — not anonymity coins — made up roughly 84% of the ~\$154B in illicit on-chain volume identified in 2025.

Chainalysis, 2026 Crypto Crime Report

CHARGES THAT RIDE WITH § 1960

§1960 rarely stands alone

§

§ 1956 — Money Laundering

Conducting a financial transaction knowing the funds are proceeds of unlawful activity, intending to promote it or conceal its source. Up to 20 years.

§

§ 1957 — Monetary Transactions

Simply spending or depositing over \$10,000 in criminally derived property — no intent to conceal required. Up to 10 years.

CRYPTO IS A “FINANCIAL TRANSACTION”

§1956(c)(4) reaches the movement of “funds by wire or other means.” Courts have read “funds” by its ordinary meaning to include crypto ever since U.S. v. Faiella (2014), reaffirmed in Murgio, Ulbricht, and — as recently as April 2026 — U.S. v. Goklu. Every reported challenge has lost.

That fight is over — save your credibility for custody and knowledge, where the law is still genuinely unsettled.

THE BLANCHE MEMO (APRIL 2025)

-  Ends "**Regulation by Prosecution**" of devs.
-  Mandates **Victim-Centric** enforcement strategy.
-  Tactical Use: Motion to dismiss charges lacking specific fraudulent intent.

ATTACKING TRACING FORENSICS



Heuristics

Clustering tools "guess" links. These are probabilistic, not scientific fact.
Subpoena error rates.



Dusting

Third-party "dusting" can associate a wallet with criminal activity without the owner's knowledge.

CROSS-EXAMINING THE WITNESS

Foundation — before you ever get to “my client”



What Tool, Exactly?

Name the software — Chainalysis, TRM, Elliptic. Is it open-source or a black box? Has the methodology been published or peer-reviewed?



What's Your Error Rate?

Every clustering heuristic has a false-positive rate. Ask for it. If the witness doesn't know it, they cannot vouch for the result.

CROSS-EXAMINING THE WITNESS

Foundation — (continued)



Are You Qualified to Say This?

Separate the fact witness (“I ran the software”) from the expert opinion (“this address belongs to my client”). Object under Daubert / Rule 702 if reliability was never established.



Show Me the Underlying Data.

Demand the raw on-chain data and the proprietary label database separately. The “conclusion” is often someone else's guess, relabeled as fact.

CROSS-EXAMINING THE WITNESS

The attribution gap — an address is not a person



Control, Not Just Custody

An exchange address can be an omnibus wallet holding thousands of users' funds. Did the witness confirm your client alone held the private key?



Confidence Score $\neq$ Certainty

Push the tool's own confidence percentage into the record. Make the witness admit “probable” is not “proven beyond a reasonable doubt.”

CROSS-EXAMINING THE WITNESS

The attribution gap — (continued)



Dusting & Address Reuse

Could a third party have sent dust to link this address into a cluster? Was the address ever reused or exposed publicly?



The KYC Chain of Custody

Attribution to a human ultimately rests on an exchange's KYC file, not the blockchain. Subpoena and stress-test that record for gaps.

5TH AMENDMENT & PRIVATE KEYS

Compelled Decryption

Challenge the "Foregone Conclusion" doctrine for memorized seed phrases. Are they

Testimonial?

- FaceID (Physical) vs. PIN (Testimonial).
- The "Act of Production" immunity defense.



LEARNING OBJECTIVES — RECAP

You should now be able to:



Explain the Mechanics

How a Bitcoin transaction actually moves — and why an address is not a person.



Identify the Charges

The money-transmitting and money-laundering charges prosecutors reach for, and how they get charged together.



Cross-Examine the Tracing Witness

On foundation, error rates, and the gap between a wallet address and a human identity.



Build a Defense Strategy

A custody-based defense to a crypto money-transmitting or money-laundering charge.

QUESTIONS?

Robert Nordlander, CPA, CFE

robert@nordlandercpa.com

(336) 421-2392

www.nordlandercpa.com

IMAGE SOURCES



<https://www.preposterousuniverse.com/wp-content/uploads/bb-plugin/cache/AI-thinks-different-square.jpeg>

Source: www.preposterousuniverse.com



https://miro.medium.com/1*C7myfMglf_bG9skxdmeGVg.png

Source: [mahdidarabi.medium.com](https://miro.medium.com/1*C7myfMglf_bG9skxdmeGVg.png)



<https://www.lbank.com/static-nasbak-backend/image/landingpage/20250919232351015.png?x-oss-process=image/format,webp>

Source: www.lbank.com



<https://i.ebayimg.com/images/g/QkMAAOSwcZlbNFnQ/s-l400.jpg>

Source: [www.ebay.com](https://i.ebayimg.com/images/g/QkMAAOSwcZlbNFnQ/s-l400.jpg)



https://ledger.com/cdn-cgi/image/width=828,format=auto/https://images.ctfassets.net/ge894kijvls/1vW3SaD5FFQVoWe6qg8oHk/c90648af0bcea39da4e6f11c60587685/Encrypted_digital_backup.webp

Source: [shop.ledger.com](https://ledger.com/cdn-cgi/image/width=828,format=auto/https://images.ctfassets.net/ge894kijvls/1vW3SaD5FFQVoWe6qg8oHk/c90648af0bcea39da4e6f11c60587685/Encrypted_digital_backup.webp)



https://png.pngtree.com/png-vector/20260630/ourlarge/pngtree-secure-digital-safe-with-cryptocurrency-symbols-and-lock-png-image_19668974.webp

Source: [pngtree.com](https://png.pngtree.com/png-vector/20260630/ourlarge/pngtree-secure-digital-safe-with-cryptocurrency-symbols-and-lock-png-image_19668974.webp)
