CFL ELECTRONIC EVIDENCE SERIES · GUIDE 7

SEPTEMBER 2026 EDITION

Cryptocurrency Assets: Investigation, Tracing, Attribution and Disclosure

A legal and technical reference for England and Wales practitioners: how crypto assets work, how they are traced across blockchains, how control is proved, and how to obtain and present the evidence.

Prepared by Computer Forensics Lab E-Discovery Team

For solicitors, barristers, litigation partners and associates, in-house counsel, disclosure lawyers, investigators, insolvency practitioners, expert witnesses and litigation-support professionals. Primarily England and Wales; differences in Scotland, Northern Ireland, arbitration, tribunals and criminal proceedings are identified. Cross-border and United States routes are covered in a dedicated section.

Computer Forensics Lab Ltd · Digital forensics and electronic disclosure laboratory · London

cflab.uk · e-discovery.uk · NPCC · ISO 17025 aligned practice

SCAN TO SAVE OUR CONTACT DETAILS

Contents

HOW TO READ THE STATUS LABELS USED IN THIS GUIDE

Established fact a technical or legal proposition that is settled and verifiable from primary sources.
Common practice what investigators and practitioners typically do; not mandated by any rule.
Jurisdiction-specific a rule that applies in England and Wales (or another named jurisdiction) and may differ elsewhere. **Uncertain** an area of live legal or technical uncertainty where the position may change or is contested.

Legal and technical positions are stated as at 4 September 2026. Online sources were accessed on 3 and 4 September 2026 unless otherwise stated. Cryptoasset technology and its regulation change quickly; check the current position before relying on any statement in this guide.

1 Executive summary

Crypto assets are now routine in English litigation, insolvency, fraud recovery and criminal work. The technology is unusual in one respect that matters enormously to lawyers: the record of every transfer is public, permanent and free to read, yet the record says nothing about who made it. This guide explains both halves of that sentence and what to do about the gap between them; it supports case assessment, disclosure planning, expert instruction and the drafting of requests, and it is not legal advice (section 29).

Ten points to take away

1. **Cryptoassets are property in England and Wales.** The Property (Digital Assets etc) Act 2025, in force from 2 December 2025, confirms that a thing is not prevented from being the object of personal property rights merely because it is neither a thing in possession nor a thing in action. It extends to England and Wales and Northern Ireland, not Scotland, and settles a threshold objection without defining which assets qualify; the case law (AA v Persons Unknown, D'Aloia, Smithers) does that work.
2. **Tracing and attribution are different exercises.** Tracing follows value between addresses on a ledger. Attribution identifies the human or legal person who controlled an address at a particular time. A tracing report that ends at an exchange deposit address is a lead, not a finding of ownership. Never let one be presented as the other.
3. **Methodology is now a merits issue.** In D'Aloia v Persons Unknown [2024] EWHC 2342 (Ch) the claimant lost against the exchange because his blockchain analyst's tracing method was unclear, changed during the case and favoured the claimant over other victims. Smithers v Persons Unknown [2026] EWHC 207 (Comm) recorded the risk of "false positive" freezing of innocent addresses when a fast method was used without telling the legal team. The method must match the ledger model, be stated in advance, applied consistently and reconciled at every hop.
4. **Analytics labels are intelligence, not evidence.** Commercial platforms attribute addresses to exchanges and services using heuristics and proprietary intelligence with published error rates. A label is a reason to send a disclosure request, not proof of who owns the address.
5. **The exchange holds the identity evidence.** Public ledgers stop at the exchange's deposit address. KYC files, internal ledgers, login IP addresses, device fingerprints and linked bank accounts sit with the exchange and are obtained through Norwich Pharmacal and Bankers Trust orders, CPR 31.17, criminal process, or (for US-resident providers) 28 USC 1782. UK-registered firms have also held Travel Rule originator and beneficiary data for in-scope transfers since 1 September 2023.
6. **Do not plead conversion.** Yuen v Li [2026] EWHC 532 (KB) held conversion unavailable for cryptoassets, following OBG v Allan. Plead proprietary claims, constructive trust, equitable proprietary restitution, unjust enrichment, deceit and unlawful means conspiracy.
7. **Speed and freezing come first.** Assets move in minutes. Interim proprietary injunctions, worldwide freezing orders, ancillary disclosure and service on the exchange (which triggers its own freeze) are the practical engine of recovery. Stablecoin issuers can also freeze on request, but that is a private act, not a court remedy.
8. **Private keys and seed phrases are the most sensitive evidence you will ever handle.** Whoever holds them can move the assets. Preserve them under restricted access, never type them into a networked device, never put them in an ordinary disclosure bundle, and record every access.
9. **The criminal toolkit has caught up.** The Economic Crime and Corporate Transparency Act 2023 inserted cryptoasset seizure, detention, crypto wallet freezing and forfeiture powers into Part 5 of the Proceeds of Crime Act 2002, in force since 26 April 2024, with a statutory code of practice for search powers.
10. **Date-stamp everything.** Block heights, token contract addresses, delegation status of Ethereum accounts, exchange labels, sanctions listings and regulatory perimeters all change. State the block number and date of every observation in every report.

2 The problem in plain English, and why it matters legally

A blockchain is a shared ledger that thousands of computers keep in step with one another. It records that value moved from one string of characters to another. It does not record names. Everything difficult about crypto evidence follows from that design choice.

2.1 The problem in plain English

Imagine a bank that publishes every account statement it has ever produced on a public website, in real time, but replaces every customer name with a random 34-character code. Anyone can see that code A sent money to code B, when, and how much. Nobody can see, from the website alone, who A and B are. Now imagine that anyone can create as many codes as they like, free, in seconds, without opening an account; that there are hundreds of such "banks" (blockchains), each with its own website and its own rules; and that some services exist whose sole function is to take money in under one code and pay it out under another with no visible link between the two. That is the environment in which crypto evidence has to be gathered.

Three practical consequences follow. First, the **movement** of value is usually provable to a high standard, from a permanent public record, without needing anything from the opponent. Second, the **identity** of the person behind a movement is almost never provable from the public record alone; it has to be built from off-chain sources, above all the records of regulated exchanges where crypto is turned into ordinary money. Third, the record is **brittle in unexpected ways**: a transfer through a mixer, a cross-chain swap, a privacy coin or a busy exchange hot wallet can end a trail that looked strong a moment earlier.

2.2 Why it matters legally

Context	Why crypto evidence matters	Typical legal question
Civil fraud and asset recovery	Victims of investment scams, "pig butchering", exchange account takeovers and wallet compromises need to locate assets fast and freeze them at an exchange before withdrawal. The claim is usually against persons unknown plus the exchange as a third party.	Is there a good arguable proprietary claim? Which exchange holds the traced assets and where is it incorporated? What tracing method was used and is it fair to other victims?
Commercial and shareholder disputes	Payments, loans and investments increasingly settle in stablecoins. Treasury movements, related-party transfers and misappropriation are visible on chain but need attribution.	Who authorised the transfer? Was the wallet a company wallet or a director's personal wallet? What do the exchange records show?
Insolvency	Office-holders must identify, secure and realise crypto held by the company or its directors, often across exchanges and self-custody, and trace antecedent transactions (Van Rooyen v Respondents [2026] EWHC 1286 (Ch)).	What did the company control at the relevant date? Are seed phrases recoverable? Which transfers are recoverable as preferences or transactions at an undervalue?
Family and private client	Non-disclosure of crypto holdings in financial remedy proceedings; estates where keys died with the deceased.	Does the disclosed wallet list match the on-chain and device evidence? Is a passphrase-protected wallet being concealed?
Criminal prosecution and defence	Money laundering, fraud, drugs and ransomware cases rely on tracing to and from exchanges; ECCTA 2023 seizure and freezing powers; CPIA disclosure of analytics working papers.	Does the prosecution's attribution survive scrutiny? Was the seizure and sweep of assets properly authorised and logged? Has the unused analytics material been disclosed?

Context	Why crypto evidence matters	Typical legal question
Regulatory and sanctions	FCA registration and (from 2027) authorisation; Travel Rule obligations; OFSI sanctions exposure via exchanges linked to designated entities.	Did the firm have exposure to a designated entity? What did its screening tool say at the time, and was that reliable?
Employment and internal investigations	Employees paid in or misappropriating tokens; salary diverted to personal wallets; insider access to corporate keys.	Which device signed the transaction? Who had the credentials at that time?

2.3 Five habits that separate good crypto evidence from bad

1. **Separate the ledger from the person.** Write "address X received Y" and "the evidence that Mr Z controlled address X is as follows" as two distinct findings, always.
2. **Name the chain, the asset standard, the contract and the block.** "USDT" on its own is ambiguous; USDT on Ethereum, USDT on TRON and legacy Omni USDT are different tokens with different records.
3. **Keep the source and the interpretation apart.** The raw transaction data (verifiable by anyone running a node) is source evidence. An analytics platform's graph, cluster or label is interpretation, and needs a stated method.
4. **Assume every timestamp needs explaining.** Block timestamps are set by miners and validators within tolerances; explorer displays convert to local time; exchange logs use their own clocks. State the time zone and the source of every time.
5. **Treat key material as a hazardous substance.** Restricted access, logged handling, never disclosed in the ordinary course.

3 Core concepts: coins, tokens and essential terminology

A crypto asset is a digital representation of value or rights whose ownership is recorded, and whose transfer is authorised, cryptographically on a distributed ledger. This section fixes the vocabulary used in the rest of the guide and draws the line between native coins, tokens and stablecoins that investigators must draw before they trace anything.

3.1 What crypto assets are and how they are used

The principal characteristics that distinguish crypto assets from ordinary bank money are: (a) there is no central ledger-keeper; a network of independent computers ("nodes") maintains identical copies of the ledger under a "consensus mechanism"; (b) control of an asset is exercised by whoever holds a cryptographic secret (the "private key"), not by whoever can prove identity to an institution; (c) transfers are irreversible once recorded, because no one has authority to reverse them; and (d) the ledger is, for most major networks, public. Crypto assets are used as speculative investments, as a means of payment (increasingly through stablecoins), as collateral and settlement instruments in "decentralised finance" (DeFi), as in-game and collectible items (NFTs), and, inevitably, as a laundering medium.

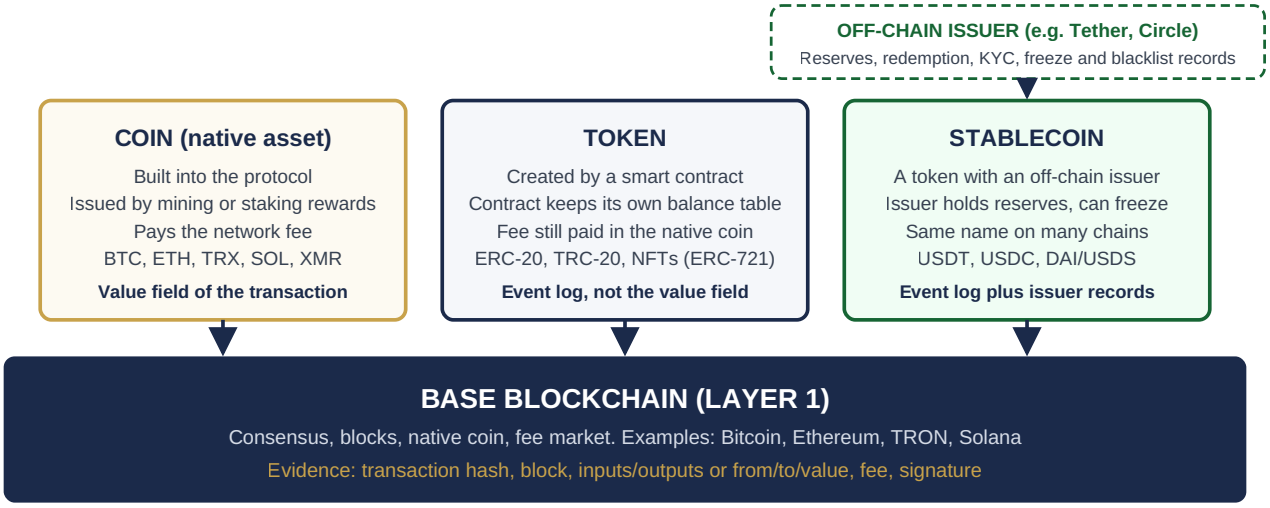
Transfer happens by "transaction": a signed instruction, broadcast to the network, that value at one address is to be re-assigned to another. Transfer can also happen entirely off chain, inside the books of an exchange, where a customer's balance is a contractual entitlement against the exchange rather than an on-chain holding. The distinction between on-chain and off-chain transfer runs through this whole guide.

3.2 Coins and tokens

A **coin** (or "native asset") is the unit of value built into a blockchain's own protocol: bitcoin (BTC) on the Bitcoin network, ether (ETH) on Ethereum, TRX on TRON, SOL on Solana. The protocol itself creates it (as a reward to miners or validators), tracks it and uses it to pay transaction fees. A **token** is an asset created on top of an existing blockchain by a program (a "smart contract") that keeps its own ledger of who holds how much. USDT and USDC on Ethereum, most DeFi governance tokens and all NFTs are tokens. The blockchain records calls to the token contract; the token contract records balances. The two are transferred differently, appear differently in explorers and generate different evidence.

Uncertain The coin/token distinction is technical. It does not map neatly onto legal or regulatory categories. The FCA's regime (section 13.6) turns on whether an asset is a "qualifying cryptoasset", a "qualifying stablecoin", a security token or an e-money token, not on whether it is native. The English courts have treated both native coins (AA v Persons Unknown) and tokens (D'Aloia, on USDT) as property, though Boonyaem v Persons Unknown [2023] EWHC 3180 (Comm) suggested that a stablecoin with an issuer redemption promise may be a thing in action rather than a "third category" asset. State which sense you are using whenever the distinction matters.

Figure 1 **Coins, tokens and stablecoins: where each one lives**



Coins are part of the base protocol; tokens and stablecoins are contracts running on top of it. A stablecoin adds a real-world issuer whose records exist entirely off chain.

Shows: why a token transfer is technically a call to a contract, and why stablecoin investigations have an extra evidence source (the issuer). **Limitation:** some networks (e.g. TRON, Solana) implement tokens differently from Ethereum; the layering principle holds but the record formats differ.

> **Text alternative:** Three boxes sit above one wide base box labelled "Base blockchain (layer 1)". Left box "Coin (native asset)": built into the protocol, issued by mining or staking, pays the network fee, examples BTC/ETH/TRX/SOL/XMR, appears in the transaction value field. Middle box "Token": created by a smart contract that keeps its own balance table, fee still paid in the native coin, examples ERC-20/TRC-20/NFTs, appears as an event log. Right box "Stablecoin": a token with an off-chain issuer that holds reserves and can freeze, same name on many chains, examples USDT/USDC/DAI, evidence is event log plus issuer records. A dashed box above the stablecoin, "Off-chain issuer", holds reserves, redemption, KYC and freeze records. Arrows connect each upper box to the base chain.

3.3 Comparison: coins, tokens and stablecoins

Feature	Coin (native asset)	Token	Stablecoin
Native blockchain	Its own (BTC on Bitcoin, ETH on Ethereum)	A host chain (Ethereum, TRON, BNB Chain, Solana, layer 2s)	Usually several host chains at once; each deployment is a separate contract
Function	Store of value, medium of exchange, fee payment, staking	Utility, governance, securities-like rights, collectibles, wrapped assets	Dollar-like settlement, trading pair, cross-border transfer, DeFi collateral
Method of issuance	Protocol rules: block rewards to miners or validators	Contract code: minted by deployer or by rule (e.g. wrapping)	Minted by issuer against fiat received (fiat-backed) or against locked collateral (crypto-backed)
Transaction processing	Native transfer; value field; consensus validates directly	Call to contract; contract updates balances; emits Transfer event; gas paid in coin	As token; issuer may also blacklist or freeze via contract admin functions
Examples	BTC, ETH, TRX, SOL, LTC, XMR, ZEC	UNI, LINK, WETH, ERC-721 NFTs, TRC-20 tokens	USDT (Tether), USDC (Circle), DAI/USDS (Sky), PYUSD
Typical legal and regulatory considerations (E&W)	Property (AA; 2025 Act). FCA "qualifying cryptoasset". MLR 2017 registration for exchanges and custodians.	May be a security token or specified investment; NFTs held to be property (Osbourne). Financial promotions regime applies.	Property (D'Aloia); possibly a thing in action (Boonyaem). "Qualifying stablecoin" issuance to be regulated by FCA from Oct 2027; BoE systemic regime for sterling stablecoins.
Common investigative evidence	Txid, inputs/outputs (UTXO) or from/to/value (account), block, fee, script/address type	Transaction to contract address, event logs, internal call traces, token contract address and decimals	All token evidence plus issuer freeze/blacklist records, mint/burn events, redemption records, issuer law-enforcement returns

3.4 Essential terminology

Term	Meaning for this guide
Blockchain / distributed ledger	A ledger replicated across many independent computers, arranged as a chain of blocks each of which cryptographically commits to the previous one, so that altering history requires redoing all later blocks. "Distributed ledger" is the wider term; not all distributed ledgers are chains of blocks.
Node	A computer running the network software, holding a copy of the ledger and relaying transactions and blocks. Anyone can run one on a public network.
Miner / validator	The participant that assembles transactions into a block and proposes it. Miners (proof of work, e.g. Bitcoin) compete by computation; validators (proof of stake, e.g. Ethereum since September 2022) are selected in proportion to staked coins and can be penalised ("slashed") for misbehaviour.
Consensus mechanism	The rule by which nodes agree which block is next. It determines how quickly a transaction becomes practically irreversible.
Transaction	A signed, broadcast instruction re-assigning value or invoking a contract. Identified by its hash (transaction ID).
Wallet	Software or hardware that generates and stores keys, derives addresses, builds and signs transactions and displays balances read from the chain. It does not "contain" coins.
Address	A public identifier, derived from a public key or script, to which value is assigned on the ledger. A person may control any number of addresses.
Private key / public key / digital signature	The secret number that authorises spending; its mathematically paired public counterpart; and the proof, generated with the private key, that a transaction was authorised by the key holder.
Smart contract	Program code deployed on a blockchain that executes automatically when called. Tokens, DeFi protocols, mixers and bridges are all smart contracts.
Decentralised finance (DeFi)	Lending, trading and derivatives implemented as smart contracts without an intermediary holding customer assets. Typically no KYC and no customer records.
Centralised exchange (CEX)	A company that takes custody of customer assets and runs an internal order book. Holds KYC and account records. Examples (illustrative only): Binance, Coinbase, Kraken, Crypto.com, Blockchain.com.
Decentralised exchange (DEX)	A smart contract that swaps tokens from pooled liquidity. No custody, no accounts, no KYC; all swaps are on chain.
Self-hosted (unhosted) wallet	A wallet whose private keys are held by the user, not by a service provider. The Travel Rule and FATF use "unhosted"; UK practice increasingly says "self-hosted".
Exchange-hosted (custodial) wallet	An address or balance controlled by an exchange on behalf of customers. Deposits are usually swept into pooled "hot" and "cold" wallets.
Stablecoin	A token designed to hold a stable value, usually against a fiat currency, by reserves, collateral or algorithm.
Confirmation / finality	A confirmation is a block built on top of the block containing a transaction. Finality is the point past which the protocol treats the block as irreversible; Ethereum has explicit finality (about 13 minutes), Bitcoin has only probabilistic settlement.

4 Keys, addresses and wallets

On a blockchain, ownership is not recorded against a name. Value is assigned to an address, and whoever can produce a valid digital signature for that address can move the value. Proving who could produce that signature, at the material time, is the central attribution question in every crypto case.

4.1 Private keys, public keys and addresses

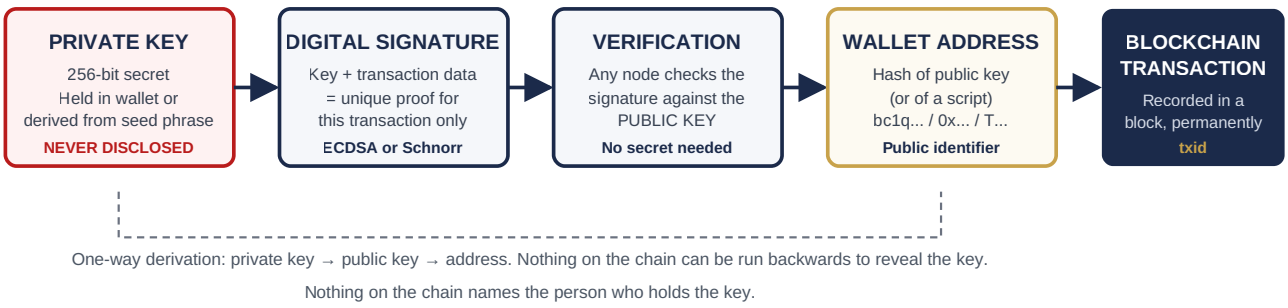
A **private key** is a very large random number (for Bitcoin and Ethereum, 256 bits) generated by the wallet. It is the secret that authorises spending. It is often compared to a password, and the comparison is useful as far as it goes: it must be kept secret, and whoever knows it has control. But a private key is not a password in three important respects. It is never sent to anyone to be checked; it cannot be reset or recovered by a provider if lost; and it is used to generate a mathematical proof (a signature) rather than to log in. The better analogy is a signature stamp that only ever exists in one place and that anyone can copy if they see it.

A **public key** is derived from the private key by a one-way mathematical operation (elliptic curve multiplication on the secp256k1 curve for Bitcoin and Ethereum). It can be published freely. Anyone holding the public key can verify that a signature was made with the corresponding private key, without learning the private key.

A **wallet address** is generally derived from the public key by further one-way operations (hashing) and then encoded for display, with a checksum so that typing errors are detected. For Bitcoin, the address encodes a hash of the public key or of a script; different address formats (beginning "1", "3", "bc1q" or "bc1p") correspond to different script types. For Ethereum, the address is the last 20 bytes of a hash of the public key, shown as "0x" followed by 40 hexadecimal characters. Because an address is a hash, an address is **not the same thing as a public key**: the public key is usually revealed only when the address first spends, in the signature data. Some address types (Ethereum contract accounts, Bitcoin script addresses, Taproot outputs) have no single public key behind them at all.

Established fact Control of the private key generally gives control of the assets assigned to the corresponding address. There is no other route (short of a contract-level freeze by a stablecoin issuer, or a court order enforced against a custodian who holds the key).

Figure 2 From private key to blockchain transaction



The private key never leaves the wallet. Only the signature, the public key (once spent from) and the address appear on the ledger.

Shows: why the ledger can prove that a transaction was authorised by the holder of a key, and cannot prove who that holder was. **Limitation:** simplified. Multi-signature, threshold (MPC) and smart-contract accounts replace the single key with several keys or with program logic; Ethereum's EIP-7702 (May 2025) lets an ordinary account delegate to contract code.

> **Text alternative:** Five boxes in a row joined by arrows: Private key (256-bit secret, never disclosed) → Digital signature (key plus transaction data produces a unique proof for this transaction only) → Verification (any node checks the signature against the public key, no secret needed) → Wallet address (hash of the public key or a script; public identifier) → Blockchain transaction (recorded in a block permanently, identified by txid). A dashed bracket beneath notes that derivation is one way and that nothing on the chain names the key holder.

4.2 Address, wallet, account and key: four things that are routinely confused

Term	What it is	What it is not
Address	A public identifier on the ledger to which value is assigned. Cheap and unlimited: a modern wallet generates a fresh one for every receipt.	Not a person, not an account with a provider, not a "wallet". One person typically controls dozens or thousands.
Wallet	Software or hardware that holds keys and manages addresses. Usually generated from one seed phrase, producing an unlimited tree of addresses (an "HD wallet", BIP-32/39/44).	Does not contain coins. The balance shown is read from the blockchain. Deleting the wallet does not delete the assets; losing the seed does.
Account	Two senses: (a) on Ethereum-type chains, an address with a balance and a transaction counter ("nonce"); (b) at an exchange, a customer relationship with a balance in the exchange's internal ledger.	An exchange account is not an on-chain address. Its balance is a contractual claim; movements inside it leave no on-chain trace.
Private key	The secret that signs. Held in the wallet, derived from the seed, or split (multisig, MPC).	Not the seed phrase (the seed generates many keys), not the address, not the exchange password.

4.3 Wallet types and what each means for evidence

Type	How it works	Where the key material is	Evidential points
Seed phrase (BIP-39)	12 to 24 English words encoding the master secret from which every key in the wallet is derived. Optional extra "passphrase" (sometimes called the 25th word) produces an entirely different wallet from the same words.	Paper, metal plate, photograph, notes app, password manager, cloud backup, email to self.	The single most valuable and dangerous artefact. A seed alone may open only a decoy wallet if a passphrase was used; the absence of evidence of a passphrase wallet is not evidence of its absence.
Software ("hot") wallet	App or browser extension (MetaMask, Trust Wallet, Exodus, Electrum, Phantom) holding an encrypted vault of keys.	Device storage (encrypted with a password), device backups, cloud sync.	Vault file proves existence and address list; keys are recoverable only with the password or from memory of a running system. Modern MetaMask vaults (600,000 PBKDF2 iterations) are effectively uncrackable without the password.
Hardware ("cold") wallet	Dedicated device (Ledger, Trezor, Coldcard) that signs internally; keys never leave the device; PIN-protected with wipe after repeated failures.	Secure element in the device; seed backup elsewhere.	Seize powered off, do not attempt PINs. Companion apps on the computer cache addresses and history. The device proves nothing about who used it without corroboration.
Custodial wallet	Exchange or custodian holds keys; customer sees a balance.	Provider's key infrastructure (usually MPC or HSM-based).	Customer never has the key. Evidence is the provider's account records, not on-chain data.
Multi-signature	Spending requires m of n keys (e.g. 2 of 3). Common for corporate treasuries and escrow.	Distributed across people, devices or providers.	Pre-Taproot Bitcoin multisig reveals all n public keys on spending; Taproot key-path multisig looks like a single signature. Ask who held each key and where.
MPC / threshold (key sharding)	The key never exists whole; parties hold shares and jointly compute a normal-looking signature.	Share files, devices, provider policy engine.	No seed phrase to seize; one device is insufficient to move funds. The provider's approval and policy logs are the real evidence of who authorised what.

Type	How it works	Where the key material is	Evidential points
Smart-contract wallet (ERC-4337, Safe)	An on-chain contract holds the assets and enforces rules (owners, limits, recovery).	Owner keys plus the contract code.	The on-chain sender is often a "bundler" or relayer, and gas may be paid by a "paymaster", so "the transaction came from address X" does not identify the actor. Establish the contract's owner set as at the material block.
Recovery mechanisms	Social recovery (guardians), custodial recovery, cloud-backed encrypted seeds (some mobile wallets), inheritance services.	Third parties, cloud accounts.	A route to assets when keys are lost, and a further attribution source (who were the guardians; who initiated recovery).

4.4 The legal significance of proving control of a key

English law now treats control, rather than possession, as the factual anchor for digital assets. The UK Jurisdiction Taskforce's Report on Control of Digital Assets (27 March 2026, chaired by Zacaroli LJ) explains control as the ability to exclude others from, and to permit or effect dealings with, the asset; it maps custody arrangements, multisig and MPC onto that test. In a dispute, the questions are therefore: *who* could sign for the address; *when*; whether they signed *personally or through an agent, custodian, employee or nominee*; and whether their control was *lawful* (a thief controls the stolen asset in the technical sense while the victim retains the proprietary claim).

> **PRACTICE POINT: CONTROL IS PROVED BY EVIDENCE, NOT BY ASSERTION**
>
> Direct proof of control includes: a seed phrase or key found in the person's possession; a signed message from the address (a wallet can sign an arbitrary text such as "I control this address, [date]" which anyone can verify); a hardware wallet in their custody whose companion app lists the address; exchange KYC records tying a withdrawal address to their account; and wallet software on their device containing the address. Circumstantial proof includes transaction patterns matching their known activity, communications referring to the address, and IP or device correlation. None of the circumstantial items alone establishes sole control (section 12).

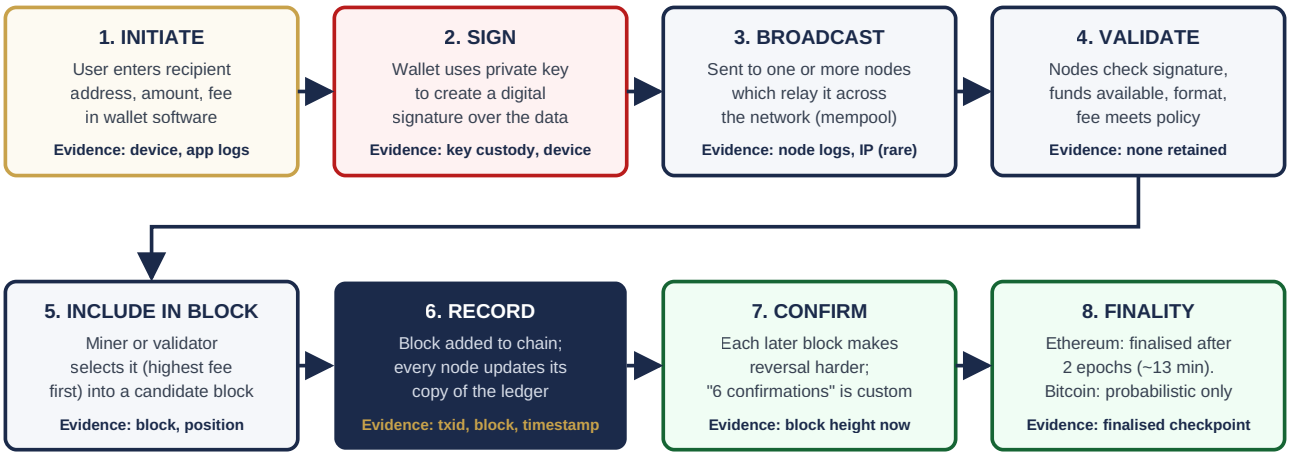
Jurisdiction-specific In criminal proceedings a suspect may be served with a notice under section 49 of the Regulation of Investigatory Powers Act 2000 requiring disclosure of a key or password; failure to comply is an offence under section 53. The notice cannot compel production of a passphrase whose existence cannot be shown, which is exactly the problem the BIP-39 passphrase creates.

5 How a cryptocurrency transaction works

A transaction passes through eight stages between the moment a user presses "send" and the moment it is safe to treat the transfer as settled. Each stage leaves, or fails to leave, a particular kind of evidence.

5.1 The eight stages

Figure 3 Life cycle of a cryptocurrency transaction



Stages 1 and 2 happen on the user's device and leave device evidence only. Stages 3 and 4 leave almost nothing.

Stages 5 to 8 are the permanent public record. Unconfirmed transactions (between 3 and 5) can be replaced or dropped.

Only the last four stages produce durable public evidence. The first two are where attribution evidence lives.

Shows: the separation between the private act of authorising a transaction and the public act of recording it. **Limitation:** stage timings vary by network (Bitcoin blocks about every 10 minutes; Ethereum slots every 12 seconds; TRON and Solana faster still). Layer-2 networks add a further stage in which batches are posted to the base chain.

> **Text alternative:** Eight numbered boxes in two rows. Row one: 1 Initiate (user enters recipient, amount and fee in wallet; evidence is the device and app logs); 2 Sign (wallet uses the private key to create a digital signature; evidence is key custody and the device); 3 Broadcast (sent to nodes which relay it into the mempool; evidence is node logs and rarely an IP address); 4 Validate (nodes check signature, funds, format and fee; no evidence retained). Row two: 5 Include in block (miner or validator selects it, highest fee first; evidence is the block and position); 6 Record (block added to the chain and every node updates; evidence is txid, block and timestamp); 7 Confirm (each later block makes reversal harder; six confirmations is a custom not a rule; evidence is current block height); 8 Finality (Ethereum finalises after two epochs, about 13 minutes; Bitcoin is probabilistic only). Footnote: stages 1 and 2 leave device evidence only; stages 5 to 8 are the permanent public record; unconfirmed transactions can be replaced or dropped.

5.2 Two ledger models: UTXO and account

Transaction structures differ between blockchains, and the difference dictates how tracing must be done (section 11) and, as the English courts have now recognised, what remedy is available (section 13.3).

	Bitcoin: unspent transaction output (UTXO) model	Ethereum (and TRON, BNB Chain, Solana): account model
Basic unit	Discrete "coins" (outputs) of arbitrary size. An address's balance is the sum of the unspent outputs locked to it.	An account with a balance and a transaction counter (nonce). A transfer debits one balance and credits another.
Inputs and outputs	A transaction consumes whole prior outputs as inputs and creates new outputs. Inputs must be spent in full, so a payment smaller than the input generates a **change output** back to an address the payer controls.	One sender, one recipient (or contract), one value, no change. Multiple recipients require multiple transactions or a contract.

	Bitcoin: unspent transaction output (UTXO) model	Ethereum (and TRON, BNB Chain, Solana): account model
Identifying traceable units	Each output keeps its identity until spent. Smithers v Persons Unknown [2026] EWHC 1907 (Comm): outputs "resemble distinct assets that coexist without losing their individual identity".	Balances merge on receipt. The same court held that account-model assets (ETH, USDC) lose individual identity on transfer, so the remedy tends to be compensatory rather than delivery up of the original tokens.
Fees	Implicit: the difference between input total and output total goes to the miner.	Explicit "gas": gas used multiplied by gas price, deducted from the sender's balance (section 8).
Ordering	No per-address counter; outputs reference earlier transactions.	Nonce is strictly sequential per account, so gaps or ordering anomalies are provable.
Tokens	Rare on Bitcoin itself (legacy Omni USDT, Ordinals/ Runes).	Central: tokens are contracts; transfers appear as event logs, not value movements.

Figure 4 A Bitcoin transaction: inputs, outputs and change

The ledger does not say which output is "change". Analysts infer it (fresh address, odd amount, same script type). Both inputs being spent together suggests one controller ("common input ownership"), unless the transaction is a CoinJoin.

A hypothetical payment of 1.00 BTC to an exchange, funded from two earlier outputs, with change returned to a fresh address.

Shows: the UTXO structure that makes Bitcoin traceable output by output, and the two inferences (change identification, common-input ownership) on which clustering rests. **Limitation:** addresses, txid and block are illustrative. Real transactions may have dozens of inputs and outputs; exchanges batch withdrawals; CoinJoins deliberately defeat both inferences.

> **Text alternative:** On the left, two input boxes: Input 0 of 0.80 BTC from an earlier transaction output at address bc1q…k7x2, and Input 1 of 0.45 BTC from another at bc1q…p9r4; each signed; total in 1.25 BTC. In the centre, a transaction box with txid e4b1c0…7d2f, block 965,112, timestamp 14 August 2026 09:41:52 UTC, size 372 vB at 18 sat/vB, two signatures, fee 0.00007 BTC (inputs minus outputs). On the right, two outputs: Output 0 of 1.00 BTC to an exchange deposit address, and Output 1 of 0.24993 BTC to a new address marked "change? inferred, not labelled"; total out 1.24993 BTC. A note states that the ledger does not label change and that spending two inputs together suggests one controller unless the transaction is a CoinJoin.

5.3 Anatomy of a transaction record

The table below shows the fields a lawyer should expect to see, and should ask for, in any transaction relied on. The values are hypothetical.

Field	Bitcoin example	Ethereum example (USDT transfer)
Sender address(es)	bc1q…k7x2 and bc1q…p9r4 (one per input)	0x3fA2…9c1e (the "from" account)
Recipient address	bc1q…exch (output 0)	"To" field is the USDT contract 0xdAC17F958D2ee523a2206206994597C13D831ec7; the true recipient 0x81B0…44d7 appears only in the Transfer event log
Asset and amount	1.00 BTC (100,000,000 satoshis)	25,000 USDT, recorded as 25,000,000,000 raw units (USDT has 6 decimals, not 18); "value" field is 0 ETH

Field	Bitcoin example	Ethereum example (USDT transfer)
Transaction fee	0.00007 BTC (implicit: inputs minus outputs)	Gas used 63,209 × effective gas price 4.2 gwei = 0.000265 ETH, paid in ETH by the sender
Transaction hash	e4b1c0…7d2f (64 hex characters)	0x7c19…a3e0 (66 characters with 0x)
Block number	965,112	24,118,430
Digital signature	One ECDSA or Schnorr signature per input, in the witness data	One ECDSA signature (v, r, s fields) over the whole transaction
Change output	0.24993 BTC to bc1q…n3v8 (inferred)	Not applicable
Smart-contract interaction	Not applicable	Call data: transfer(0x81B0…44d7, 25000000000); status "success"; log index 142
Nonce	Not applicable	Sender nonce 87 (its 88th transaction)
Confirmation status	Included at block 965,112; 143 confirmations at time of capture (block 965,255, 2026-08-15 10:02 UTC)	Included in slot 12,914,022; finalised (epoch 403,563); captured 2026-08-15 10:02 UTC

A TRANSACTION HASH IDENTIFIES A TRANSACTION, NOT A PERSON

The hash is a fingerprint of the transaction data. Quoting it proves that a specific transfer exists and allows anyone to look it up. It does not identify who pressed "send", who held the key, or whether the key holder acted for someone else. Statements such as "the defendant's transaction, hash 0x7c19…" assume the very thing that has to be proved; write "the transaction with hash 0x7c19…, sent from address 0x3fA2…, which the claimant contends was controlled by the defendant for the reasons at paragraph […]".

5.4 Other terms in the transaction record

Blocks and timestamps. The block timestamp is set by the miner or validator who built the block, within protocol tolerances (Bitcoin allows roughly two hours of drift against network time; Ethereum's slot times are fixed at 12-second intervals). It records approximately when the block was built, not when the user signed. Explorers display it converted to the viewer's local time; always record UTC and the block number. **Confirmations** are the count of blocks after the containing block; treat "6 confirmations" as an industry convention and not a legal or protocol threshold. **Nonces** on account-based chains are strictly sequential; on Bitcoin the word means something else (a mining field) and should not be confused. **Gas** is explained in section 8. **Replace-by-fee:** an unconfirmed Bitcoin transaction can be replaced by a higher-fee version spending the same inputs; since Bitcoin Core 28.0 (2024) most nodes accept such replacements whether or not the original signalled it. An expert who describes an unconfirmed transaction as "pending and irreversible" is wrong.

6 Blockchains, transaction visibility and technical limits

Transfers between addresses are recorded on a blockchain: a distributed public ledger whose history is, for practical purposes, impossible to alter once buried under later blocks. Because the record is public, anyone can follow the movement of value with a free "block explorer" or a commercial analytics platform. Following value is not the same as identifying people, and not all blockchains are equally visible.

6.1 Five distinctions that change what evidence exists

Distinction	Meaning	Investigative consequence
Public v private blockchain	Public: anyone may read the ledger (Bitcoin, Ethereum, TRON). Private: read access restricted to members (some enterprise and bank consortium ledgers).	Public chains can be evidenced from your own node or a reputable explorer. Private ledgers require disclosure from the operator, like any other database.
Permissionless v permissioned	Permissionless: anyone may run a node, transact or validate. Permissioned: participation requires approval by a gatekeeper.	Permissioned networks have an operator who holds identity records and can be served. Permissionless networks have no one to serve; evidence about identity must come from the edges (exchanges, devices).
Transparent v privacy-enhanced	Transparent: sender, recipient and amount are visible (Bitcoin, Ethereum). Privacy-enhanced: one or more of those is hidden by cryptography (Monero; Zcash shielded pool; mixers).	Tracing through privacy-enhanced systems on chain is generally impossible; the tractable points are the entry and exit boundaries and the services on either side.
On-chain v off-chain records	On-chain: written to the ledger. Off-chain: exchange internal ledgers, Lightning channel payments, layer-2 batches before posting, custodian records, chat messages.	Most identity evidence and much of the movement evidence is off-chain. A tracing exercise that stops at the chain boundary is incomplete.
Finality v confirmation	Confirmation: blocks built on top. Finality: protocol-defined irreversibility (Ethereum, after two epochs). Bitcoin has no finality, only diminishing probability of reversal.	State confirmation count or finality status at the time of capture. A "reorganised" transaction may vanish from the canonical chain.

6.2 Technical limitations every report should acknowledge

Limitation	What happens	How to deal with it
Chain reorganisation	Two blocks are found at nearly the same time; one branch is later abandoned. Natural reorgs on Bitcoin are almost always one block deep; the deepest incident (March 2013, a software bug) was resolved by coordinated rollback with at least one double spend.	Rely only on transactions with substantial confirmations or finality. Record the block hash, not just height, at capture.
Bridges	Assets are locked on chain A and an equivalent minted on chain B (or burned and released). The A-side and B-side transactions are linked by the bridge's own event logs, not by a shared identifier.	Obtain the bridge contract's events for both sides; correlate by amount, time and destination; request bridge operator records where a company exists.
Mixers and CoinJoin	Many users' funds are pooled and redistributed so that inputs cannot be matched to outputs on chain. Tornado Cash (Ethereum) uses zero-knowledge proofs; Bitcoin CoinJoins produce equal-value outputs.	Trace to the mixer entry and from candidate exits; use timing and amount analysis (probabilistic only); seek the coordinator's records where a service operator existed (Samourai's founders were sentenced in November 2025 in the US).

Limitation	What happens	How to deal with it
Privacy coins	Monero hides sender (ring signatures), amount (RingCT) and recipient (stealth addresses). Zcash shielded pools hide all three; about 30% of ZEC supply was shielded by mid-2026.	Trace to the exchange where the privacy coin was bought or sold; exchanges' internal records replace the chain. Do not rely on claims of on-chain Monero tracing without validated method.
Layer-2 networks	Transactions occur on a separate network (Arbitrum, Optimism, Base, Polygon; Lightning for Bitcoin) and only batches or channel opens/closes reach the base chain. Since Ethereum's Dencun upgrade (March 2024) the batch data ("blobs") is pruned from Ethereum nodes after about 18 days.	Use the layer-2's own explorer and archive; obtain data from the rollup operator; for Lightning, evidence comes from node operators and custodial wallet providers, not the chain.
Decentralised exchanges and cross-chain swaps	Token-for-token swaps within one chain are fully visible. Cross-chain swap services (THORChain; the eXch service shut down by German authorities in May 2025) substitute their own liquidity, so the inbound and outbound legs have no cryptographic link.	DEX swaps: read the router and pool events. Cross-chain: correlate by time and value; seek service records; state that the link is inferred.
Lost keys	Assets remain on the ledger but cannot be moved. "Burn" addresses and lost seeds account for a material share of Bitcoin supply.	An asset that cannot move is preserved by default but cannot be recovered. Check whether the "dormant" address has any history of spending.
Address reuse	Older wallets and many exchange deposit systems reuse one address for many receipts, which aids clustering; modern wallets generate a fresh address per receipt, which defeats naive linkage.	Do not assume that one address equals one person, nor that a fresh address is a different person.
Commercial attribution labels	Analytics platforms label addresses ("Binance hot wallet", "Garantex") from heuristics, scraped data and undisclosed intelligence. Labels are incomplete, sometimes wrong, and change over time.	Treat as leads. Corroborate by disclosure from the labelled entity. Record the platform, version and date of the label, and cross-check between platforms (D'Aloia found outputs from two platforms irreconcilable).
Explorer-derived views	"Internal transactions" on Ethereum explorers are reconstructed by re-executing the transaction; they are not stored on chain and can differ between explorers.	Ask how the view was generated; where it matters, reproduce from an archive node with a stated tracer.

7 Stablecoins and USDT

A stablecoin is a crypto asset designed to hold a stable value, usually by tracking a fiat currency, most often the US dollar. Stablecoins now dominate illicit crypto flows (Chainalysis and TRM Labs each estimated that stablecoins made up the large majority of illicit volume in 2025) precisely because they behave like dollars but move like tokens. They also introduce an actor that Bitcoin never had: an issuer that keeps records and can freeze.

7.1 Categories

Category	Mechanism	Examples	Investigative significance
Fiat-reserve backed	Issuer receives dollars, mints tokens, holds reserves (Treasury bills, cash, repo) and redeems on request from verified customers.	USDT (Tether), USDC (Circle), PYUSD	Issuer holds KYC on direct customers (usually institutions and exchanges, not end users), mint/burn records and freeze capability.
Crypto-collateralised	Users lock crypto collateral worth more than the tokens minted; a protocol liquidates if collateral falls.	DAI and USDS (Sky, formerly MakerDAO)	No issuer KYC; collateral positions are on chain and traceable; governance may have limited freeze powers.
Algorithmic / uncollateralised	Peg maintained by incentives and a paired volatile token rather than reserves.	TerraUSD (UST), which collapsed in May 2022; its founder was sentenced to 15 years in the US in December 2025	High collapse risk; losses are typically total; the "algorithm" may in fact have been covert market-making, as in Terra.
Other asset-backed and hybrid	Tokenised money-market funds, gold-backed tokens, partially collateralised designs.	Tokenised fund shares; XAUT, PAXG	May be regulated as securities or funds; issuer and transfer-agent records exist.

7.2 The four-party relationship

Every stablecoin transaction involves an **issuer** (who created the token and holds the reserves), a **blockchain** (which records transfers of the token), a **wallet holder** (who controls an address holding the token) and, very often, an **exchange** (through which the holder acquired or will dispose of the token). The token's on-chain transfer and its underlying fiat value are distinct: a transfer of 1,000 USDT on TRON moves a ledger entry in a contract on TRON; the dollar value depends on Tether's reserves and willingness to redeem, and only Tether's verified customers can redeem directly. A court order affecting the token (a freeze, delivery up) operates on the ledger entry; it does not reach the reserves.

7.3 Investigative and legal significance

- **Payments and settlement.** Stablecoins are used to settle trades between exchanges and OTC brokers, to pay suppliers across borders, and increasingly for wages. Many "crypto" frauds are in substance stablecoin frauds.
- **Trading and cross-border transfer.** USDT on TRON has become the default rail for cheap, fast dollar transfers in parts of Asia, Africa and Latin America, and in sanctioned economies.
- **Issuer records and compliance data.** Issuers keep mint and redemption records for direct customers, blacklist and freeze logs, and law-enforcement request records. Tether publicises cooperation with law enforcement; Circle acts on court or regulatory order.
- **Freezes and blacklisting.** The USDT contract lets Tether add an address to a blacklist, blocking transfers from it, and to destroy and reissue frozen funds. USDC uses a deny-list; the tokens remain in place and cannot move. Industry compilations reported several thousand USDT addresses frozen by mid-2026, with a value in the billions of dollars. **Uncertain** An issuer freeze is a private act by a private company, obtainable quickly on a credible law-

enforcement or (sometimes) legal request, but it is not a proprietary remedy, it can be lifted, and issuers have faced litigation over freezes made ahead of formal process. Use it alongside, not instead of, court relief.

- **Redemption and reserves.** Tether announced in August 2026 that KPMG had issued an unqualified audit opinion on its 2025 financial statements, though press reported that the full statements were not published. Circle publishes monthly attestations. Reserve adequacy matters to the value of a judgment denominated in stablecoins.
- **Regulation.** Jurisdiction-specific In the UK, issuing a "qualifying stablecoin" and safeguarding cryptoassets become FSMA-regulated activities from 25 October 2027 under the Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 (SI 2026/102), with FCA rules in PS26/10 and PS26/11 (June 2026) and the FCA authorisation gateway opening on 30 September 2026. The Bank of England is finalising a separate regime for systemic sterling stablecoins. In the EU, MiCA led major exchanges to delist USDT for EEA spot trading in early 2025, which changes where a suspect can trade and therefore where evidence sits. In the US the GENIUS Act (July 2025) created a federal stablecoin regime with rules proposed in February 2026.

7.4 USDT in particular

USDT is a dollar-denominated stablecoin issued by Tether. It is available on multiple blockchains, including Ethereum (as an ERC-20 token), TRON (TRC-20), Solana, Avalanche and others. Each deployment is a separate contract with a separate address, a separate transaction history and separate freeze administration. "USDT" without a chain name is therefore ambiguous, and USDT on one chain cannot be sent to an address on another.

Network	Standard	Contract identifier (verify against Tether's published list before use)	Notes
Ethereum	ERC-20	`0xdAC17F958D2ee523a2206206994597C13D831ec7`	6 decimals. Raw values must be divided by 10^6; dividing by 10^{18} (the ETH convention) understates by a factor of a trillion.
TRON	TRC-20	`TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t`	Largest USDT supply by chain in 2026 (about half of tracked supply). Very low fees; favoured by OTC brokers and scam operations.
Bitcoin (Omni Layer)	Omni	Property ID 31	The original 2014 USDT. Tether ended issuance and redemption on Omni and four other legacy chains from 2025 but did not freeze the contracts, so historic tokens remain transferable. Requires Omni-aware tooling; a plain Bitcoin explorer shows only the carrier transaction.

WHAT TO PIN DOWN IN EVERY USDT CASE

(1) The network; (2) the token contract address on that network; (3) the transaction hash; (4) the asset standard (ERC-20, TRC-20, Omni); (5) the decimals used in the raw figures; (6) whether the sending or receiving address was on Tether's blacklist at the material time, and if so from when. A schedule of loss that mixes networks or mis-scales decimals will not survive cross-examination.

8 Ethereum, gas fees and smart contracts

Ether (ETH) is the native coin of the Ethereum blockchain. Every transaction on Ethereum, including a transfer of someone else's token, is paid for in ETH. That single fact generates some of the most useful attribution evidence in token cases.

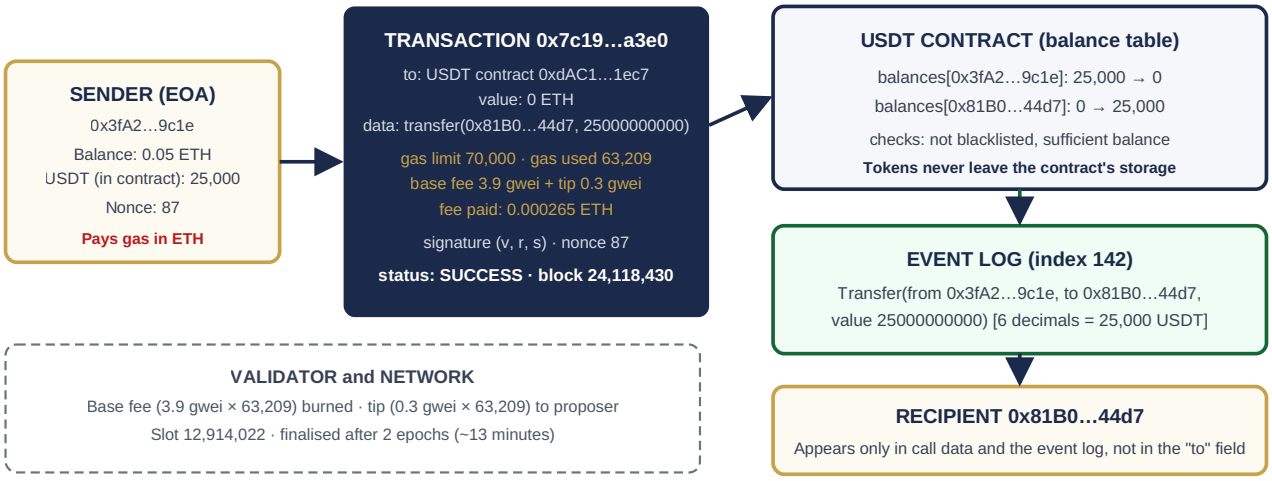
8.1 Gas: what it is and why it matters

Ethereum charges for computation. Each operation costs a fixed number of "gas" units; the sender sets a **gas limit** (the maximum they will pay for) and the network charges **gas used** multiplied by a price. Since the London upgrade (EIP-1559, 2021) the price has two parts: a protocol-set **base fee**, which rises and falls with demand and is destroyed ("burned"), and a **priority fee** or tip, which goes to the validator. The sender also specifies a **maximum fee**; any excess over base fee plus tip is refunded. A plain ETH transfer costs 21,000 gas; a USDT transfer around 50,000 to 65,000; a complex DeFi interaction can cost several hundred thousand.

Gas is paid in ETH even when the transaction moves another token. A wallet holding 100,000 USDT and no ETH cannot send the USDT. That is why investigators look for the small ETH deposit that "funds gas" before a token wallet becomes active: the source of that ETH is frequently an exchange withdrawal tied to a KYC'd account, and it links the token wallet to a person. Sponsored-gas mechanisms (ERC-4337 paymasters; EIP-7702 delegated accounts since May 2025) are exceptions and must be checked.

Failed transactions still consume gas. A transaction that reverts (wrong parameters, insufficient token balance, blacklisted address) is recorded on chain with status "failed" and the gas is charged. Failed transactions are evidence of attempts, and often of intent; never filter them out of an analysis.

Figure 5 An Ethereum token transfer: gas, the contract call and the event log



A 25,000 USDT transfer. The transaction's "to" is the token contract; the ETH value is zero; the movement of tokens exists only as a change in the contract's balance table and an emitted event.

Shows: why an ETH-only view of an address is blind to stablecoin movements, why the sender must hold ETH for gas, and where the true recipient is recorded. **Limitation:** figures illustrative. A malicious contract can emit a Transfer event without moving value ("fake token" scams), so a log is not proof of value movement unless the contract is genuine.

> **Text alternative:** Left: sender account 0x3fA2…9c1e with 0.05 ETH, 25,000 USDT held in the contract and nonce 87; it pays gas in ETH. Centre: transaction 0x7c19…a3e0 addressed to the USDT contract with value 0 ETH, data calling transfer to 0x81B0…44d7 for 25,000,000,000 raw units; gas limit 70,000, gas used 63,209, base fee 3.9 gwei plus tip 0.3 gwei, fee 0.000265 ETH; status success in block 24,118,430. Right top: USDT contract balance table changes sender from 25,000 to 0 and recipient from 0 to 25,000 after checking blacklist and balance; tokens never leave the contract's storage. Right middle: event log index 142 records Transfer(from, to, value). Right bottom: recipient 0x81B0…44d7 appears only in call data and the log. Bottom left dashed box: the validator and network burn the base fee, pay the tip to the proposer, and finalise after two epochs.

8.2 Ethereum concepts the lawyer needs

Concept	Explanation
Externally owned account (EOA) v contract account	An EOA is controlled by a private key and can initiate transactions; a contract account holds code and cannot. **Uncertain** Since the Pectra upgrade (7 May 2025, EIP-7702) an EOA can delegate to contract code and later revoke, so "is this address a person or a program?" must be answered as at a specific block.
Nonce	Per-account count of transactions sent, strictly sequential. Useful for proving the order of a wallet's activity and that a transaction could not have been sent at an alleged time.
Smart-contract execution	Deterministic: every node re-executes the call and must reach the same result. The call data (function and arguments) is public and decodable if the contract's interface is known.
Internal transactions	Calls made by contracts during execution (for example a DEX router moving tokens between pools). Not stored on chain; reconstructed by explorers using a "tracer". Different explorers can show different internal transactions for the same hash.
Account abstraction (ERC-4337)	Users sign "UserOperations" which a "bundler" submits in one outer transaction to an "EntryPoint" contract. The on-chain "from" is the bundler; the user's account appears inside the operation and its events. Gas may be paid by a "paymaster".
Proof of stake and finality	Since the Merge (15 September 2022), validators propose blocks in 12-second slots; 32 slots form an epoch; a block is finalised after two epochs. Reversal after finality would require destroying a third of all staked ETH.
Upgrades	Dencun (March 2024) added blob storage for layer 2s, pruned after about 18 days; Pectra (May 2025) added EIP-7702; Fusaka (December 2025) added data-availability sampling and a passkey-signature precompile. The "Glamsterdam" upgrade was expected in the second half of 2026 but had not activated as at 4 September 2026. Reports should state which upgrade was in force at the material block.
Other chains	TRON charges "energy" and "bandwidth" rather than gas, and TRX can be staked to obtain them, so a TRON wallet may send USDT with no visible fee payment. Solana charges lamports per signature. The evidential logic is the same: find who funded the fees.

9 Exchanges, hosted and self-hosted addresses, and exchange records

Crypto assets are converted into pounds or dollars, or exchanged for other digital assets, through exchanges. The centralised exchange is the point at which pseudonymous ledger activity meets verified identity, regulated banking and retained records. It is therefore the most important single evidence source in almost every case.

9.1 Centralised and decentralised, custodial and non-custodial

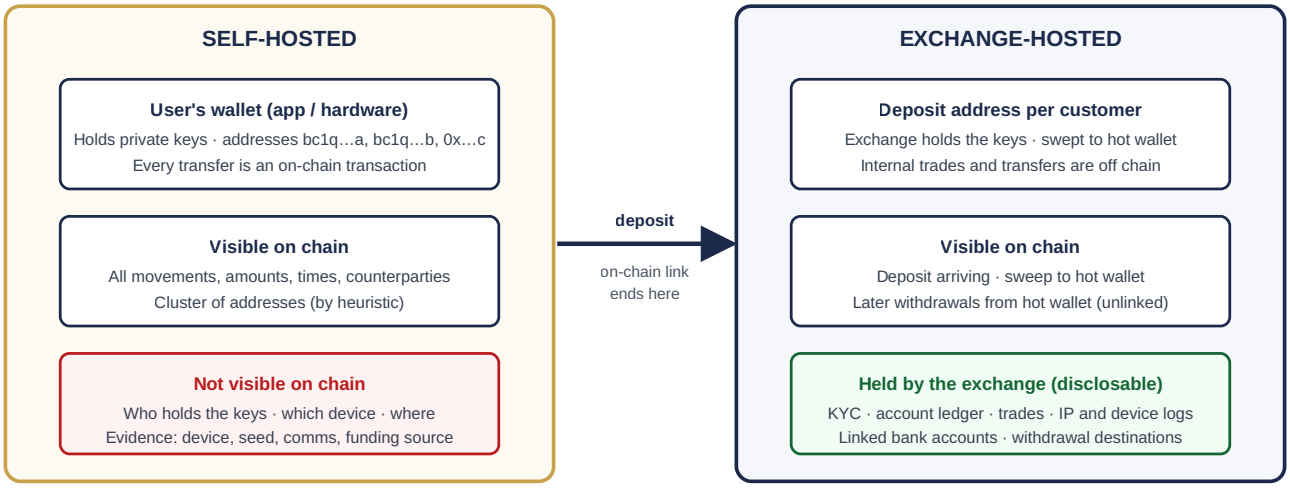
A **centralised exchange** operates much like a traditional financial institution. Customers open an account, verify their identity, deposit fiat (by bank transfer or card) or crypto (by sending it to a deposit address the exchange assigns to them), trade on the exchange's internal order book, and withdraw fiat to a bank account or crypto to an external address. The exchange, not the customer, controls the private keys of the addresses that hold deposited crypto; customer deposits are typically swept into pooled "hot" wallets (online, for liquidity) and "cold" wallets (offline, for reserves). The customer's balance is an entry in the exchange's database.

Distinction	Explanation	Records and legal position
Custodial v non-custodial service	Custodial: the provider holds the keys (exchanges, custodians, most "earn" products). Non-custodial: the user holds the keys and the provider supplies software or routing (self-hosted wallets, DEX front-ends).	Custodial providers hold account and KYC records and can freeze; in the UK they must register with the FCA under MLR 2017. Non-custodial providers may hold little beyond app telemetry and IP logs.
Centralised v decentralised exchange	CEX: company, order book, custody, KYC. DEX: smart contract (Uniswap, PancakeSwap, Curve) that swaps tokens from liquidity pools; no custody, no accounts.	DEX swaps are fully on chain and traceable; there is no one to serve for identity, though front-end operators may hold IP logs.
Broker v trading platform	Broker: buys and sells as principal or agent with the customer at a quoted price (many "buy crypto" apps, OTC desks). Platform: matches customers with each other.	Both hold customer records. UK regulation from October 2027 distinguishes "dealing as principal/agent" and "operating a trading platform" (SI 2026/102).
Hosted v self-hosted wallet	Hosted: an address or balance controlled by a service on the customer's behalf. Self-hosted (unhosted): controlled by the user's own keys.	Travel Rule information attaches to transfers involving hosted wallets; UK firms must also collect information on transfers to and from self-hosted wallets on a risk basis.
Exchange account v on-chain address	An account is a customer relationship with an internal balance; an address is a ledger identifier. One account may be assigned many deposit addresses; one hot wallet serves thousands of accounts.	On-chain evidence ends at the deposit address. Account evidence is obtained only from the exchange.

Examples of centralised exchanges commonly encountered in UK matters include Binance, Coinbase, Kraken, Crypto.com, Blockchain.com, Bybit, OKX, HTX (formerly Huobi), Gate.io and KuCoin. These examples are illustrative only. Platforms differ in their corporate structure, jurisdiction, record-keeping, retention periods and willingness to respond to civil process, and nothing in this guide implies that any two have identical procedures or obligations.

9.2 Exchange-hosted and self-hosted addresses

Figure 6 **Exchange-hosted and self-hosted wallets: what the chain shows and what it hides**



The chain shows everything a self-hosted wallet does but nothing about who runs it. The chain shows almost nothing of what happens inside an exchange, but the exchange knows who its customer is.

Shows: why tracing to an exchange deposit address is a milestone, not a conclusion, and why the two wallet types call for different evidence-gathering routes. **Limitation:** some exchanges use one shared deposit address plus a memo or tag (common for XRP, XLM and some TRON deposits); some "nested" or unregistered services operate inside a larger exchange's account, so the labelled exchange may itself be one step removed from the real customer.

> **Text alternative:** Two panels. Self-hosted: the user's wallet holds the private keys and several addresses and every transfer is on chain; visible on chain are all movements, amounts, times, counterparties and heuristic clusters; not visible are who holds the keys, which device, and where; evidence comes from the device, seed, communications and funding source. Exchange-hosted: a deposit address assigned per customer whose keys the exchange holds and which is swept to a hot wallet; internal trades are off chain; visible on chain are the deposit arriving, the sweep, and later unlinked withdrawals from the hot wallet; held by the exchange and disclosable are KYC, account ledger, trades, IP and device logs, linked bank accounts and withdrawal destinations. An arrow labelled "deposit" joins the panels with the note "on-chain link ends here".

Blockchain explorers and analytics tools label many addresses as belonging to a particular exchange. The label may come from the exchange itself, from test deposits, from clustering, or from scraped or purchased intelligence. **Common practice** Investigators treat a label as a reason to write to the exchange, and treat the exchange's confirmation (or its production of the account file) as the evidence. Where the label is disputed, the analytics provider's methodology and date of labelling should be obtained; where it cannot be corroborated it should be described in any report as an unverified attribution.

9.3 Why exchange records are indispensable

Blockchain data may show that funds reached an exchange. It cannot show what happened next: whether they were credited to one account or split; traded into another asset; transferred to another customer of the same exchange (an "internal transfer" that never touches the chain); withdrawn to a bank; or withdrawn on chain from a hot wallet that also serves thousands of other customers. Only the exchange's records answer those questions.

Record type	What it shows	Why it matters
On-chain deposit and withdrawal records	Which customer account a deposit address belongs to; which account requested each withdrawal and to which external address.	Ties the chain to the account at both ends.
Internal ledger entries	Every credit and debit to the account: deposits, trades, fees, internal transfers, staking rewards.	The only record of movement inside the exchange.
Trades and conversions	Orders and fills, pair, price, time.	Shows chain-hopping and conversion to stablecoin or fiat.

Record type	What it shows	Why it matters
Account-to-account transfers	Off-chain transfers between customers (by email, phone or user ID).	A frequent laundering step invisible on chain; identifies the counterparty account.
Fiat deposits and withdrawals	Bank account numbers, card details, payment processor references, faster-payments references.	Connects to the banking system and to a name.
KYC and enhanced due diligence	Identity documents, selfie or liveness checks, address proof, source-of-funds declarations, occupation and income, risk rating.	The core identity evidence; note that documents may be stolen or synthetic.
Technical and session data	Registration IP and date, login IP history, device identifiers, user agent, 2FA method, API keys, session cookies.	Corroborates or undermines attribution; links multiple accounts to one operator.
Communications and compliance	Support tickets, chat logs, compliance alerts, account restrictions, freeze and closure records, internal investigation notes.	Shows what the exchange knew and when (relevant to constructive trust and to D'Aloia-type findings about notice).

TRAVEL RULE DATA: AN UNDER-USED SEAM

Jurisdiction-specific Since 1 September 2023, UK-registered cryptoasset businesses must collect, verify and (where the counterparty is another cryptoasset business) transmit originator and beneficiary information on cryptoasset transfers, with additional identity details for transfers of €1,000 or more (MLR 2017, regs 64A to 64G, inserted by SI 2022/860). Information must be collected for transfers to and from self-hosted wallets as well. A UK firm should therefore hold, for every in-scope transfer since that date, structured records naming the originator and beneficiary. Disclosure requests and Bankers Trust applications against UK firms should refer to these regulations expressly.

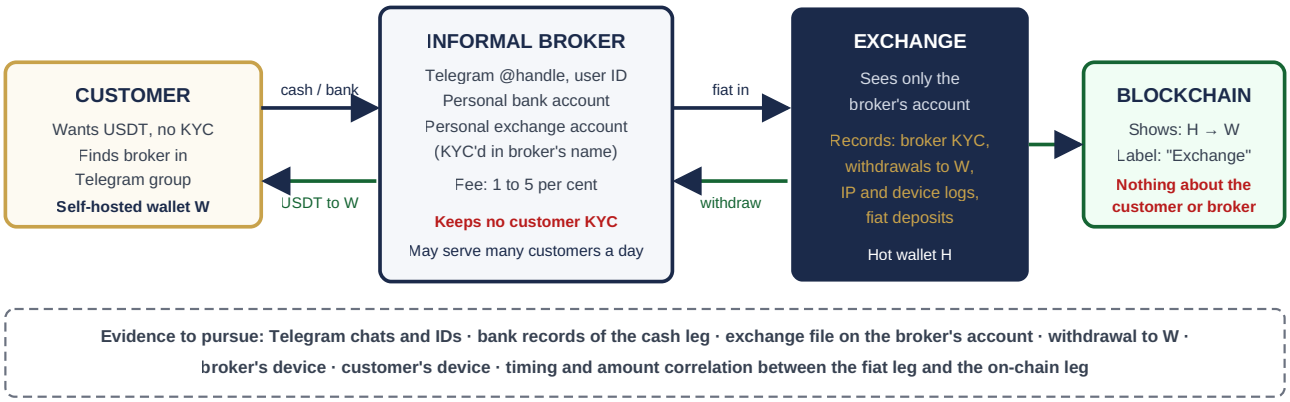
10 OTC brokers, Telegram and laundering typologies

Over-the-counter (OTC) brokers sit between users and exchanges. At one end are the institutional OTC desks of major exchanges, fully KYC'd and record-keeping. At the other are individuals who rent out their own exchange accounts through Telegram. The second kind is a recurring feature of fraud, laundering and sanctions-evasion cases and a recurring gap in tracing.

10.1 What OTC brokers do

An OTC broker facilitates a transaction outside an exchange's public order book. Formal OTC desks (offered by Coinbase, Kraken, Binance and specialist firms) handle large trades for verified institutional clients and keep full records. Informal OTC brokers, by contrast, typically use personal accounts at one or more centralised exchanges; operate without the exchange's authorisation and in breach of its terms; collect no KYC from their own customers; and serve customers who do not want, or cannot pass, KYC at an exchange. Through such a broker a customer can convert cash or bank money into crypto, swap one crypto asset for another, or cash out crypto, all through an account that bears the broker's name, not the customer's.

Figure 7 An informal OTC broker transaction and the evidence it leaves



The exchange's records identify the broker, not the customer. The customer is found through the broker's communications, the cash leg, and correlation.

Shows: how an intermediary account breaks the direct link between an exchange's KYC and the person actually acquiring or disposing of the asset. **Limitation:** some brokers use multiple exchange accounts, "money mule" accounts or nested exchanges, adding further hops; some are themselves unwitting mules.

> **Text alternative:** Four boxes left to right. Customer: wants USDT without KYC, finds a broker in a Telegram group, holds self-hosted wallet W. Informal broker: Telegram handle and user ID, personal bank account, personal exchange account KYC'd in the broker's own name, fee 1 to 5 per cent, keeps no customer KYC, may serve many customers a day. Exchange: sees only the broker's account; its records are the broker's KYC, withdrawals to W, IP and device logs and fiat deposits; it holds hot wallet H. Blockchain: shows H to W, labelled "Exchange", nothing about the customer or broker. Arrows: cash or bank from customer to broker; fiat in from broker to exchange; withdrawal from exchange to broker; USDT to W. A dashed bar lists the evidence to pursue: Telegram chats and IDs, bank records of the cash leg, the exchange file on the broker's account, the withdrawal to W, both devices, and timing and amount correlation between the fiat leg and the on-chain leg.

10.2 Telegram-based OTC services

Informal brokers advertise in large Telegram groups devoted to crypto swaps and "P2P" trading, often organised by city or currency. A prospective customer identifies a broker from group posts and contacts them privately; terms are agreed by message; the customer pays in cash, by bank transfer or in crypto; the broker delivers the other side from their own exchange account. Customers commonly deal with several brokers in different countries, and brokers commonly act as "guarantors" or escrow agents for one another. **Established fact** Since 23 September 2024 Telegram's privacy policy states that it will disclose a user's IP address and phone number to authorities on receipt

of a valid legal order confirming that the user is a suspect in a criminal case; previously it did so only for terrorism suspects. Telegram does not respond to private civil requests; the practical route is through law enforcement or through the counterpart's device.

Evidence type	Where it is found and what it proves
Telegram usernames, user IDs, phone numbers	In chat exports, device extractions and the Telegram API; the numeric user ID is stable even when the username changes. Proves the account, not the person.
Group messages, private messages, channel records	On the participant's device (Telegram "cloud chats" are also on Telegram's servers; "secret chats" are device-only). Shows the offer, terms, addresses and payment instructions.
Payment instructions and receipts	Bank details, cash-drop arrangements, screenshots of transfers. Connects the fiat leg to the crypto leg.
Exchange deposit addresses and wallet addresses	Quoted in messages; matchable to on-chain transactions by time and amount.
Screenshots and exported chats	Easy to fabricate. Authenticate against the device or the counterpart's copy (section 18).
Device data and application artefacts	Telegram databases, media cache, contact lists, deleted message remnants; wallet apps on the same device.
Records from Telegram, exchanges, payment processors, telecoms	Telegram (criminal process only); exchanges (broker's account file); banks and PSPs (the fiat leg); telecoms (subscriber for the phone number, subject to lawful process).

10.3 OTC brokers and money laundering

As in the traditional financial system, some users of crypto seek to hide where money came from or where it is going. An OTC broker can help them convert fiat into crypto, one crypto into another, or crypto back into fiat, all through the broker's exchange account rather than an account in the customer's name. The effect is to insert a KYC'd stranger between the exchange's records and the true party. Typologies seen in UK and international cases include the following; none is proof of criminality on its own, and legitimate users (including people in jurisdictions with poor banking access) use informal brokers too.

Typology	Pattern	On-chain and off-chain indicators
Layering and rapid transfers	Funds split and moved through many fresh addresses in minutes.	Peel chains; many one-use addresses; transfers within seconds of receipt.
Chain hopping	BTC to ETH to USDT on TRON via bridges, DEXs or swap services.	Bridge and router events; timing correlation across chains; use of swap services with no KYC.
Multiple exchanges and nested services	Deposits to several exchanges, or to an unregistered "nested" service operating inside a large exchange's account.	Exchange labels on many outputs; deposit addresses belonging to a single large account.
Mixers, tumblers and privacy tools	Tornado Cash, CoinJoin, Monero conversion.	Fixed-denomination deposits; equal-value outputs; exchange trade into XMR followed by silence.
Structuring	Amounts kept below reporting or Travel Rule thresholds; many small fiat deposits.	Repeated round amounts just under €1,000 or £/$ thresholds; many bank accounts feeding one exchange account.
Use of intermediaries and mules	Recruited account holders lend exchange or bank accounts.	Account activity inconsistent with declared income (the Bitkub account holder in D'Aloia declared monthly income of THB 15,000 to 29,999 and withdrew THB 33 million in three days).
Investment fraud and "pig butchering"	Victims induced to send stablecoins to fake trading platforms; consolidated and cashed out through OTC brokers in South-East Asia.	Many victim deposits to a few consolidation addresses; USDT on TRON; large OTC cash-outs.

Typology	Pattern	On-chain and off-chain indicators
Ransomware	Bitcoin demanded; proceeds consolidated, mixed, swapped and cashed out at high-risk exchanges.	Payment addresses from ransom notes; known ransomware clusters; mixer use.
Darknet markets	Escrow wallets, vendor withdrawals, Monero preference.	Market-labelled clusters; conversion to XMR.
Sanctions evasion	Russian-linked exchanges (Garantex, its successor Grinex, the A7 network) and the ruble-pegged A7A5 stablecoin; UK designations of cryptoasset exchanges under the Russia regulations in May 2026.	Exposure to designated addresses; OFSI reported that over 90% of crypto-related suspected breach reports involved Russian entities (July 2025 assessment).
Conversion through OTC brokers	Any of the above ending in a Telegram-arranged cash-out.	Withdrawal from a hot wallet to a self-hosted address shortly after a matching fiat receipt in a personal bank account.

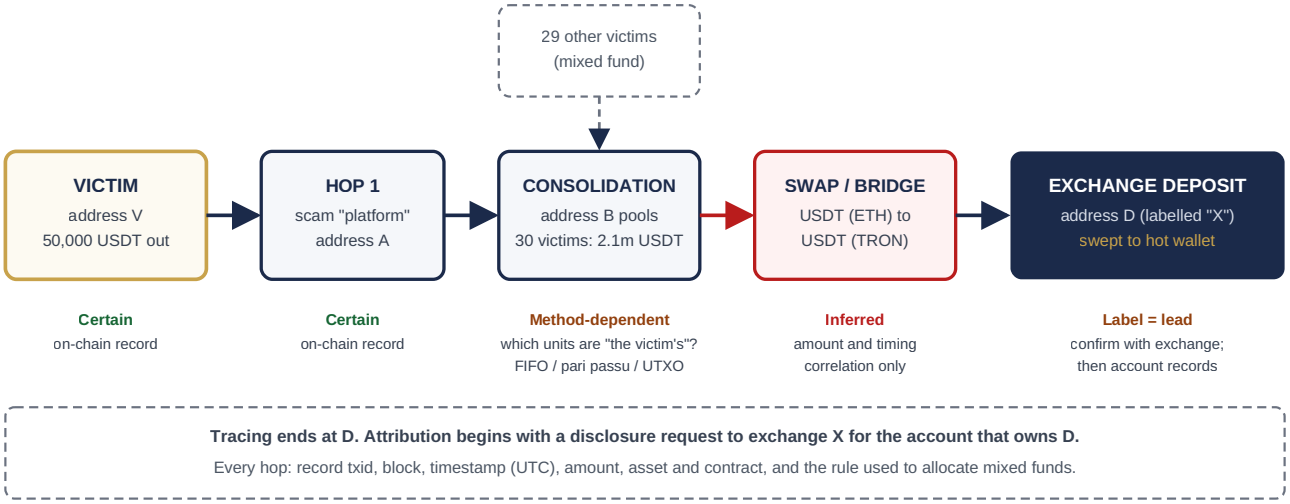
11 Tracing cryptocurrency transactions

Tracing follows value from address to address through the public record until it reaches somewhere identifiable, usually a regulated exchange. It is a technical exercise with a legal overlay: the English courts now require the method to be stated, justified by reference to the ledger model, applied consistently and fair as between competing victims.

11.1 Tools and techniques

Technique	What it does	Reliability and caveats
Block explorers	Public websites (mempool.space, blockchain.com, Etherscan, Tronscan, Solscan) that render ledger data by address, transaction or block.	**Established fact** The underlying data is verifiable against a node. The rendering, labels and "internal transactions" are the explorer's interpretation.
Transaction hashes and address histories	Start from a known hash or address; list every input and output.	Complete for the chain in question; blind to off-chain steps.
Block and timestamp data	Orders events; correlates with off-chain records.	Block time is approximate; convert everything to UTC.
Input and output analysis (UTXO)	Follows specific outputs through spends; the method endorsed for Bitcoin in Smithers [2026] EWHC 1907 (Comm).	Slower than balance-based methods but preserves identity of the traced units.
Change-address analysis	Infers which output returned to the payer.	**Uncertain** Inference. Published research (Möser and Narayanan, 2022) found individual change heuristics correct only 10 to 30% of the time in isolation; combined models do far better but remain probabilistic.
Cluster analysis and wallet-ownership heuristics	Groups addresses believed to be controlled by one entity, chiefly by the common-input-ownership heuristic (inputs spent together share a controller) and change inference.	**Uncertain** Defeated by CoinJoin and PayJoin by design; one wrong link can merge unrelated entities ("cluster collapse"). A US court admitted Chainalysis clustering in US v Sterlingov (2024) with corroboration; an English court rejected an analyst's tracing in D'Aloia (2024) for inconsistency.
Token-transfer records and smart-contract events	Reads Transfer and other events emitted by contracts.	Essential for stablecoins and NFTs; a log proves what the contract said, which is only value movement if the contract is genuine.
Exchange attribution labels	Marks addresses as belonging to a named service.	Lead, not proof. Record provider, version and date; corroborate with the service.
Cross-chain tracing	Correlates bridge, swap and exchange legs across chains by amount, time and destination.	Inference across the hop unless the bridge is deterministic; state it as such.
Graph analysis	Visualises flows between addresses and clusters; identifies consolidation points.	A picture is demonstrative, not source evidence. The underlying transaction list must be exhibited.
Commercial analytics platforms	Chainalysis Reactor, TRM Labs, Elliptic, Crystal Intelligence, Merkle Science, and open tools such as Breadcrumbs, combining all of the above with proprietary intelligence.	Powerful and widely used by law enforcement and exchanges. Methodology and error rates are partly undisclosed; different platforms produce different results for the same flow (D'Aloia). Obtain the platform's methodology documentation before relying on its output in court.

Figure 8 Tracing from a victim's wallet to an exchange



A typical investment-fraud flow. The strength of the evidence falls at the consolidation point and again at the cross-chain swap.

Shows: where a trace is factual, where it depends on an allocation method, and where it is inference. **Limitation:** real flows have many more hops, feints and dead ends; a trace that reaches an exchange is typical of investment frauds but not of professional laundering, which favours mixers, privacy coins and OTC cash-outs.

> **Text alternative:** Five boxes left to right: Victim address V sends 50,000 USDT; Hop 1, the scam platform's address A; Consolidation address B which pools 2.1 million USDT from 30 victims (a dashed box above shows 29 other victims feeding in); Swap or bridge converting USDT on Ethereum to USDT on TRON (red arrow); Exchange deposit address D labelled as exchange X and swept to a hot wallet. Beneath each box a certainty rating: certain (on-chain) for V and A; method-dependent at B (which units are the victim's: FIFO, pari passu or UTXO); inferred at the swap (amount and timing correlation only); label equals lead at D (confirm with the exchange, then obtain account records). A footer states that tracing ends at D and attribution begins with a disclosure request, and that every hop should record txid, block, UTC timestamp, amount, asset and contract, and the allocation rule.

11.2 Tracing is not attribution

Tracing shows the movement of assets between addresses. Attribution seeks to identify the person or entity controlling those addresses. They are separate analytical steps with separate evidence, separate standards of proof and separate failure modes, and a report should present them separately. A trace can be complete and correct while attribution is entirely open; an attribution can be solid (an exchange confirms the account holder) while the trace to that account is contested.

11.3 Where traced funds end up

Funds are commonly traced to: centralised exchanges (the best outcome: records and freezes); payment processors and merchant services (merchant KYC); stablecoin issuers (freeze and, for direct customers, redemption records); gambling platforms (KYC'd accounts, often offshore); mixers (trail ends or becomes probabilistic); bridges and cross-chain swap services (trail continues on another chain by inference); decentralised exchanges (trail continues on chain in a different token); OTC brokers (trail ends at the broker's account); and other services such as staking providers, NFT marketplaces or custodians. Tracing becomes materially harder through privacy-enhancing systems, nested services, chain swaps, layer-2 networks or long chains of one-use addresses; the report should say at which hop confidence declined and why.

11.4 Allocation methods for mixed funds

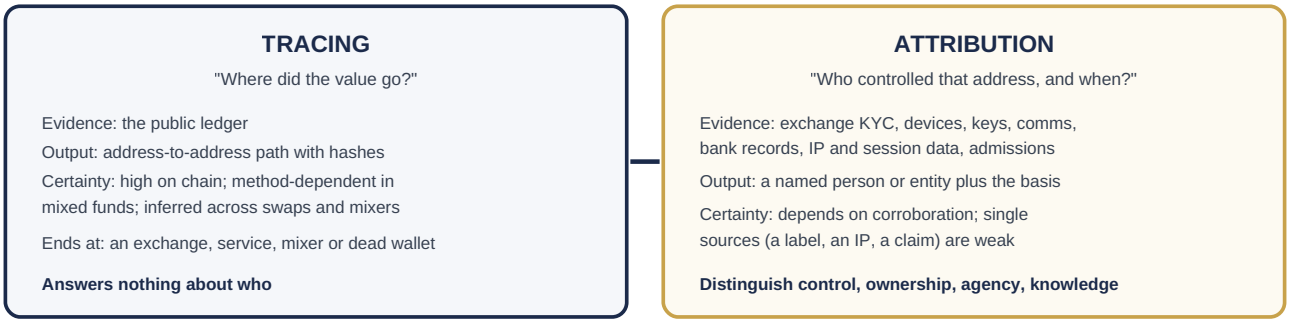
When the victim's assets are pooled with others' (as at address B in Figure 8), some rule must decide which outgoing units are "the victim's". English law does not mandate one rule. In D'Aloia the court held that first-in-first-out (Clayton's Case) is a rebuttable default and that pari passu, the rolling charge, and any other method that is "methodologically sound and properly evidenced" and treats all innocent claimants comparably are available. The court rejected the claimant's analysis because it purported to be FIFO but was not, changed during the case, and selectively matched outflows in a way that favoured the claimant over other victims. In Smithers [2026] EWHC 207 (Comm) the use of last-in-first-out across all assets for speed, without telling the legal team, created a risk of

freezing innocent addresses; in Smithers [2026] EWHC 1907 (Comm) the UTXO method was endorsed for Bitcoin because each output keeps its identity; in Wilden v Person Unknown [2026] EWHC 1355 (KB) LIFO was accepted where the report gave a transaction-by-transaction account with every hash. **Common practice** The reconcilable position is: match the method to the ledger model (UTXO for Bitcoin-family assets; an allocation rule for account-model and token assets), state it in the report before the analysis, apply it uniformly, reconcile the arithmetic at every hop, and disclose its limitations candidly, especially on a without-notice application.

12 Establishing attribution

Attribution is built, not found. It combines blockchain evidence with off-chain evidence from exchanges, devices, banks, communications and witnesses until the inference that a particular person controlled a particular address at a particular time is strong enough for the purpose in hand: a without-notice freezing order, summary judgment, a criminal charge, or a finding at trial.

Figure 9 **Tracing and attribution are two different questions**



Keep the two findings in separate sections of every report and every pleading.

Shows: the different evidence bases, outputs and certainty of the two exercises. **Limitation:** in practice they interact: an attribution (an exchange confirms the account) can validate a contested trace, and a trace can generate the attribution lead.

> **Text alternative:** Two panels. Tracing asks where the value went; evidence is the public ledger; output is an address-to-address path with hashes; certainty is high on chain, method-dependent in mixed funds and inferred across swaps and mixers; it ends at an exchange, service, mixer or dead wallet; it answers nothing about who. Attribution asks who controlled the address and when; evidence is exchange KYC, devices, keys, communications, bank records, IP and session data and admissions; output is a named person or entity plus the basis; certainty depends on corroboration and single sources are weak; it must distinguish control, ownership, agency and knowledge.

12.1 Sources of attribution evidence

Source	What it can establish	Weight and weaknesses
Exchange KYC and registration records	Name, date of birth, address, identity document, selfie, email, phone, registration date and IP.	Strong, but documents may be stolen, synthetic or those of a mule; check liveness data and consistency with device and bank records.
Bank accounts and payment records	Who funded the exchange account; who received the cash-out.	Strong, subject to mule accounts.
IP addresses and login history	Location and consistency of access; links between accounts.	Weak alone: VPNs, shared networks, carrier-grade NAT, mobile IPs. Useful in combination and for negative inference.
Device identifiers and browser data	Same device used across accounts; app installation; wallet artefacts.	Moderate; device sharing and spoofing exist.
Private keys, seed phrases, wallet backups	Ability to control the address.	Very strong as to control at the time found; says nothing about who else had a copy.
Digital-signature evidence (signed message)	The person could sign for the address at the time of signing.	Very strong as to control at that moment; obtain the message text, signature and verification method.
Cryptocurrency tax records and accounting software	Self-declared holdings and addresses (HMRC returns, Koinly-type exports).	Strong admissions where they exist.
Communications and social media	Addresses quoted, screenshots, boasts, instructions.	Variable; authenticate the source; an address in a message may be someone else's (a payment request).
Statements acknowledging control	Admissions in correspondence, interviews, witness statements.	Strong, subject to context and reliability.

Source	What it can establish	Weight and weaknesses
Seized computers, phones and hardware wallets	Wallet software, address lists, transaction history, key material, exchange apps.	Strong as to the device; who used the device at the material time is a separate question.
Witness testimony and business records	Who ran the treasury; who had the hardware wallet; who authorised transfers.	As for any documentary or oral evidence.
Law-enforcement returns and legal process	Production from exchanges, Telegram, telecoms, banks.	Strong; check collateral-use restrictions (section 13.5, 14.2).
Expert blockchain analysis	Clusters, patterns, links between a known address and a verified exchange account.	Inference with error rates; must be disclosed and validated (section 18).

12.2 The risks of single-source attribution

Relying solely on	Why it fails
An analytics provider's address label	Labels are heuristic, undated in many interfaces, sometimes wrong, and identify a service rather than a customer.
A wallet address appearing in a message	It may be the recipient's address, a payment request, a forwarded message, or planted.
A transaction originating from a device	Shows the device signed; not who was using it, whether it was compromised, or whether the key was also elsewhere.
A common IP address	VPNs, offices, households, mobile carriers and public Wi-Fi all share IPs; timing matters.
A public claim of ownership	People claim addresses they do not control (and deny addresses they do); check with a signed message.
A heuristic cluster	Common-input-ownership is broken by CoinJoin and by exchanges batching customer withdrawals; one bad link merges strangers.

12.3 Control, ownership, authorisation, agency and knowledge

These are distinct and a report should say which is being asserted.

- **Possession** is not available for digital assets in English law (they are not things in possession); the functional equivalent is **control**: the ability to exclude others and to effect dealings, typically by holding the key (UKJT Control report, March 2026).
- **Authorisation**: who directed the transaction. A person may direct a transaction without personally holding the key, by instructing an exchange, a custodian, a broker, an employee or a nominee. Conversely the key holder may have acted without authority (a rogue employee, a compromised delegation).
- **Beneficial ownership**: for whom the asset is held. An exchange controls the hot wallet but customers own the balances; a nominee controls a wallet for a principal; a trustee holds for beneficiaries (Sachs v Snape [2026] EWHC 1059 (Comm)).
- **Agency**: OTC brokers, custodians, MSPs and treasury staff routinely control addresses for others. The exchange's KYC identifies the agent, not the principal.
- **Knowledge**: whether the recipient knew of the fraud, which decides constructive trust, knowing receipt and bona fide purchaser questions (D'Aloia's findings about Bitkub's notice; Piroozzadeh on Binance's position as purchaser without notice).

> **DRAFTING THE ATTRIBUTION FINDING**
>
> A well-drafted finding reads: "Address D was assigned by exchange X to account 4471902, opened on [date] in the name of [name] with identity document [type/number redacted], funded from [bank] account ending 1234 in the same name, and accessed from device [ID] and IP ranges consistent with [location] on [n] occasions including within 10 minutes of each of the three withdrawals to address W. On that evidence the analyst's opinion is that [name] controlled account 4471902 at the material times. Whether [name] acted for another person is not determinable from these records." It does not read: "Address D belongs to [name]."

13 The legal framework in England and Wales

This section sets out the law that governs crypto asset claims, disclosure and enforcement in England and Wales as at September 2026. It separates settled propositions from live uncertainty, and it flags where Scotland, Northern Ireland, arbitration, tribunals and the criminal courts differ (section 13.9).

13.1 Crypto assets as property

Established fact The **Property (Digital Assets etc) Act 2025** (2025 c. 29) received Royal Assent and came into force on 2 December 2025. Its single operative provision, section 1, provides that "a thing (including a thing that is digital or electronic in nature) is not prevented from being the object of personal property rights merely because it is neither (a) a thing in possession, nor (b) a thing in action". It extends to England and Wales and Northern Ireland only. It implements the Law Commission's Digital Assets report (Law Com No 412, June 2023) and its supplemental report and draft Bill (July 2024). The Act is deliberately permissive and minimal: it removes the objection derived from Colonial Bank v Whinney (1885) that property must be one of two kinds. It does not define "digital asset", declare that any particular asset is property, or say what rights attach. Those remain matters of common law.

The common law had already reached the same destination. AA v Persons Unknown [2019] EWHC 3556 (Comm) (Bryan J) held bitcoin to be property, adopting the UK Jurisdiction Taskforce's 2019 Legal Statement and the National Provincial Bank v Ainsworth indicia. Osbourne v Persons Unknown [2022] EWHC 1021 (Comm) extended the analysis to NFTs. D'Aloia v Persons Unknown [2024] EWHC 2342 (Ch) (Richard Farnhill, sitting as a Deputy High Court Judge) is the fullest reasoned analysis: USDT is property of a distinct kind, rivalrous, neither a thing in possession nor a thing in action, with the property right attaching to the token itself rather than to the right to control it. Uncertain Boonyaem v Persons Unknown [2023] EWHC 3180 (Comm) had suggested that USDT, because of Tether's redemption promise, is more naturally a thing in action; the two decisions are in tension and the point may matter to remedies. Wang v Darby [2021] EWHC 3054 (Comm) is the counterweight: that crypto is property does not make every holding a trust, and fungible crypto swapped under a commercial arrangement gave rise to no trust.

13.2 Causes of action

Claim	Position
Conversion	Jurisdiction-specific **Not available** for cryptoassets: Yuen v Li [2026] EWHC 532 (KB) (Cotter J, 10 March 2026), holding the court bound by OBG Ltd v Allan [2007] UKHL 21 and that the 2025 Act did not extend the tort. Do not plead it.
Proprietary claim / constructive trust	Property obtained by fraud is held on constructive trust from receipt (Westdeutsche; applied in Daburn v Persons Unknown [2025] EWHC 356 (Comm) and Murry v Persons Unknown [2025] EWHC 1664 (Comm)). Recipients are liable unless bona fide purchasers for value without notice. The workhorse claim against persons unknown and exchanges.
Equitable proprietary restitution	Survives Yuen v Li, citing Armstrong DLW GmbH v Winnington Networks [2012] EWHC 10 (Ch).
Unjust enrichment	Available, but "at the expense of" can fail where value passed through sequential hops rather than directly (D'Aloia).
Deceit, unlawful means conspiracy	Standard personal claims against the fraudsters (Daburn; Mooij v Persons Unknown [2024] EWHC 814 (Comm)).
Breach of confidence	Private keys and seed phrases as confidential information (Fetch.AI v Persons Unknown [2021] EWHC 2254 (Comm)); a route through PD6B gateway (21).
Breach of trust / fiduciary duty	Against managers and custodians who held crypto for the claimant (Sachs v Snape [2026] EWHC 1059 (Comm): delivery up ordered). Uncertain Whether software developers owe duties to owners was held arguable in Tulip Trading v Bitcoin Association [2023] EWCA Civ 83 but never tried.
Knowing receipt / dishonest assistance	Against exchanges and intermediaries with the requisite knowledge. In D'Aloia the exchange's bona fide purchase, ministerial receipt and change of position defences all failed because it had notice (an account declaring modest income withdrew THB 33 million in three days); knowing receipt was, however, not pleaded.

13.3 Following, tracing and remedies

D'Aloia distinguished **following** (tracking the same asset) from **tracing** (identifying substitute assets), held that following is available in principle for USDT if its identity is preserved, and that common law tracing fails through a mixed fund whereas equitable tracing survives it. Wilden v Person Unknown [2026] EWHC 1355 (KB) applied this: following as well as tracing is available "if the evidence shows that the identity of the crypto asset is preserved despite mixing". Smithers v Persons Unknown [2026] EWHC 1907 (Comm) (Bright J, 24 July 2026) then tied remedy to ledger architecture: Bitcoin outputs remain discrete and identifiable until spent, so the original asset can be identified and recovered in specie; account-model and token assets (USDC, ETH) lose individual identity on transfer, so the remedy tends to be compensatory. Piroozzadeh v Persons Unknown [2023] EWHC 1024 (Ch) illustrates the practical limit: deposits swept into an exchange's unsegregated hot wallet handling hundreds of transactions an hour make tracing "essentially futile", and the exchange takes as purchaser for value absent knowledge. Jones v Persons Unknown (No 2) [2025] EWHC 1823 (Comm) is the warning about collateral damage: an exchange that replenished a customer's wallet from another customer's account after a delivery-up order left that innocent third party without a remedy.

13.4 Interim remedies, persons unknown and service

Proprietary injunction v worldwide freezing order. A proprietary injunction requires a good arguable case that the claimant retains a proprietary interest in identified assets; the balance of convenience usually favours the claimant. A worldwide freezing order requires a good arguable case on the merits and a real risk of dissipation, with a cross-undertaking in damages. Both are routinely granted without notice against persons unknown and served on exchanges (LMN, Fetch.AI, Daburn, Murry, Smithers, Wilden). **Chabra** relief (TSB v Chabra [1992] 1 WLR 231) reaches a non-cause-of-action defendant holding assets for the wrongdoer. The practically decisive step is service on the exchange, which then freezes the account to avoid assisting a breach. Smithers [2026] EWHC 207 (Comm) shows the price of a fast tracing method: potentially frozen innocent addresses, protected only by the cross-undertaking.

Persons unknown. Define categories precisely (those who obtained the assets by fraud; those who received them with knowledge; innocent recipients) so that a person served can tell whether they fall within one. Uncertain Whether summary judgment can be entered against truly unidentified fraudsters is contested at first instance: Boonyaem refused (applying Cameron v Liverpool Victoria [2019] UKSC 6); Mooij declined to follow Boonyaem and gave judgment once alternative service had been effected. Murry shows the full arc: persons unknown converted into named defendants once exchange disclosure identified them.

Service. Alternative service under CPR 6.15 (and 6.27 for service out) by email, exchange messaging and blockchain-native methods is established: NFT airdrop as one method (D'Aloia [2022] EWHC 1723 (Ch)); NFT as the sole method (Osbourne v Persons Unknown [2023] EWHC 39 (KB)); NFT links together with OP_RETURN messages embedded in on-chain transfers to the receiving addresses (Smithers [2026] EWHC 1907 (Comm)). Daburn shows the limit: where emails bounced and message delivery was unconfirmed, proceedings were stayed against that category.

Service out and situs. The gateways most used are PD6B para 3.1(15) (constructive trustee), (16) (restitution), (9) (tort), (21) (confidence) and, for information orders against exchanges, (25) (disclosure to identify a defendant or locate the claimant's property), used in LMN v Bitflyer and Wilden. Uncertain The situs of a cryptoasset has been treated as the domicile of its owner (Ion Science v Persons Unknown, Butcher J, 21 December 2020, unreported), refined towards residence and central management in Tulip Trading; Lavender J in Osbourne [2023] EWHC 39 (KB) doubted whether that situs persists after transfer to unknown parties. The Law Commission's June 2025 consultation paper on digital assets in private international law provisionally proposes abandoning a mechanical lex situs for decentralised systems and creating a free-standing information order for fraud victims; no final report had been published by September 2026.

13.5 Disclosure: pre-action, third-party and in proceedings

Norwich Pharmacal orders identify the wrongdoer; **Bankers Trust** orders locate and preserve the claimant's traceable assets. Against foreign exchanges the gateway authority is LMN v Bitflyer Holdings [2022] EWHC 2954 (Comm) (Butcher J), which restated the five-part Bankers Trust test and imposed safeguards that should be built into every draft order: an undertaking limiting collateral use; undertakings as to the respondent's expenses and in damages; a carve-out where compliance would breach local law; confidentiality; and compliance dates that preserve a Part 11 challenge. Stanford Asset Holdings v AfrAsia Bank [2023] UKPC 35 confirms the jurisdiction but counsels that orders against foreign institutions whose compliance might breach local law be made only in exceptional circumstances. Wilden (2026) is the latest successful application, with indemnity costs against an exchange that ignored the proceedings. Smithers [2026] EWHC 207 (Comm) at [15] confirms that permission to share identities with law enforcement will be given and that exchanges become "more receptive" once enforcement agencies are involved.

CPR Part 31 and PD57AD. Under CPR 31.4 a "document" is "anything in which information of any description is recorded"; PD57AD para 2.5 to 2.6 expressly includes electronic documents, text messages, social media, deleted data, metadata and embedded data. Wallet files, exchange exports, chain-analytics reports, device images and chat exports are all documents. The live question is **control** (CPR 31.8; PD57AD para 1.9): a customer's contractual right to obtain statements and exports from an exchange is normally a right to inspect and take copies, so those records are disclosable by the customer (see Guide 6 in this series). **CPR 31.17** permits non-party disclosure against a UK exchange or bank once proceedings are on foot where the documents are likely to support or adversely affect a case and disclosure is necessary. **CPR 31.22** restricts collateral use: material obtained under a disclosure or Bankers Trust order cannot be handed to police, a foreign regulator or a parallel proceeding without permission or an express carve-out; draft the carve-out in. PD57AD's preservation duty (para 4) must extend to seed phrases, hardware wallets, exchange account access (accounts get closed and logs purged) and mobile devices. Uncertain PD57AD is under review: the Disclosure Review Working Group (Butcher J) reported in July 2026 that 64% of surveyed practitioners considered the reforms unsuccessful and that it would propose simplification, with consultation expected late 2026 or early 2027. The current text applies until amended.

13.6 Regulation and sanctions

- **MLR 2017 registration.** Jurisdiction-specific Cryptoasset exchange providers and custodian wallet providers carrying on business in the UK must be registered with the FCA (MLR 2017 regs 14A, 56 to 60); the FCA register is public and should be checked in every case. Registration is an AML status, not authorisation, and gives no FOS or FSCS protection.
- **The FSMA regime from 2027.** The Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 (SI 2026/102, made 4 February 2026) create eleven regulated activities (including operating a trading platform, issuing a qualifying stablecoin, safeguarding, dealing, arranging and staking) commencing 25 October 2027. The FCA published five policy statements on 30 June 2026 (PS26/9 to PS26/13). The authorisation gateway opens on 30 September 2026 and closes on 28 February 2027; MLR registrations do not convert automatically.
- **Financial promotions.** Since 8 October 2023 crypto promotions to UK consumers fall within s.21 FSMA, with risk warnings, a 24-hour cooling-off period and a ban on incentives; breach is a criminal offence. The FCA began High Court proceedings against HTX in February 2026 over unlawful promotions.
- **Travel Rule.** MLR 2017 regs 64A to 64G (in force 1 September 2023): originator and beneficiary information on cryptoasset transfers, with enhanced data at €1,000 or more; extends to self-hosted wallets; JMLSG Part II Sector 22 Annex 22-I gives approved guidance. FATF's seventh targeted update (July 2026) reported 83% of surveyed jurisdictions had Travel Rule legislation but that practical implementation lagged.
- **Sanctions.** UK sanctions apply to crypto dealings as to any other; OFSI's July 2025 Cryptoassets Threat Assessment found over 7% of suspected breach reports since 2022 involved crypto firms and identified eight evasion typologies. On 26 May 2026 the UK designated cryptoasset exchanges (including HTX and entities linked to Garantex, Grinex and the A7 network) under the Russia regulations for the first time. Uncertain The US delisted the Tornado Cash smart contracts on 21 March 2025 after Van Loon v Department of the Treasury (5th Cir. 2024); that has no effect on UK obligations, mixer use remains a red flag, and the developer

prosecutions continued (Roman Storm convicted on one count in August 2025 with a retrial of the hung counts reported as adjourned to 2027). Check the UK Consolidated List directly.

13.7 Criminal powers and disclosure

Jurisdiction-specific The **Economic Crime and Corporate Transparency Act 2023** (Schedules 8 and 9) inserted into Part 5 of the Proceeds of Crime Act 2002: Chapter 3C (search, seizure and detention of cryptoassets and "cryptoasset-related items" such as hardware wallets and seed phrases, ss.303Z20 to 303Z35); Chapter 3D (crypto wallet freezing orders, ss.303Z36 to 303Z40, available without notice in the magistrates' court on reasonable grounds to suspect, for up to two years extendable to three, against wallets administered by a UK-connected cryptoasset service provider); Chapter 3E (forfeiture, including conversion to cash and destruction where realisation is not in the public interest); and Chapter 3F. The provisions commenced in England and Wales on 26 April 2024. The statutory **Code of Practice under s.303Z25** (Recovery of Cryptoassets: search powers) came into force the same day (SI 2024/551), with Home Office Circulars 004/2024 (confiscation) and 005/2024 (forfeiture). Powers include seizure without prior arrest, "recreating" a wallet and transferring assets to a law-enforcement-controlled wallet, sale pending forfeiture, and release to victims. Procedure is in the Magistrates' Courts (Detention, Freezing and Forfeiture of Cryptoassets) Rules 2024 (SI 2024/1043). Practitioners should also check whether any POCA amendments in the Crime and Policing Act 2026 (2026 c. 20, Royal Assent 29 April 2026) have been commenced.

Disclosure. CPIA 1996 ss.3 and 7A and the Code of Practice, with the Attorney General's Guidelines on Disclosure 2024 (effective 29 May 2024, strengthened for digital material), govern unused material. Blockchain analytics outputs, analyst working notes, tool configurations and version, exchange returns, seed phrases and wallet extractions are all potentially disclosable, and reasonable lines of enquiry include exculpatory attribution evidence (alternative controllers of an address; CoinJoin participation; compromised delegations). Seed phrases and keys in unused material must be handled under restricted access (section 15.5). RIPA 2000 s.49 notices can compel disclosure of keys and passwords; the BIP-39 passphrase problem (section 4.3) limits their reach. SARs: virtual assets accounted for only 1.67% of SAR Portal submissions in 2024 to 2025, the smallest reporting sector, despite the scale of illicit flows.

13.8 Data protection

Jurisdiction-specific UK GDPR and the Data Protection Act 2018 apply as amended by the **Data (Use and Access) Act 2025**, whose main data-protection provisions commenced on 5 February 2026. Two changes matter here: the new "recognised legitimate interests" basis covers disclosure for the prevention and detection of crime and to public bodies without a balancing test; and international transfers are tested against a "not materially lower" standard of protection. The ICO's guidance on distributed ledger technologies (published August 2025, expressly under review following the 2025 Act) treats wallet addresses and public keys as capable of being personal data where they can be linked to an individual, acknowledges uncertainty about controllership on permissionless networks, and accepts that erasure may be achievable only by putting data "beyond use" (for example destroying the off-chain link between an address and an identity). Practically: minimise the addresses and transaction histories you collect and disclose; redact extended public keys (an xpub reveals a subject's entire wallet history); restrict KYC bundles to those who need them; and record the lawful basis for each transfer of personal data to a foreign exchange or provider.

13.9 Where the rules differ

Forum	Key differences from the England and Wales civil position
Scotland	The 2025 Act does not extend to Scotland; Scots property law is separate and the position of cryptoassets is less developed. Interim relief is by interdict and arrestment, not freezing injunction; the recovery of documents is under commission and diligence (s.1 Administration of Justice (Scotland) Act 1972) rather than CPR Part 31. POCA cryptoasset powers apply with a separate Scottish code of practice for constables. ECCTA commencement dates in Scotland differed from England and Wales.
Northern Ireland	The 2025 Act extends to Northern Ireland. Civil procedure follows the Rules of the Court of Judicature (NI), with discovery rather than disclosure and no PD57AD. POCA cryptoasset provisions commenced on NI-specific dates in 2024.

Forum	Key differences from the England and Wales civil position
Arbitration	Tribunals have no power to bind exchanges or grant Norwich Pharmacal relief; interim relief against third parties must come from the court under s.44 Arbitration Act 1996. Document production follows the IBA Rules or institutional rules; tribunals commonly limit production to narrow, specific requests. 28 USC 1782 is generally unavailable for private commercial arbitrations after ZF Automotive (US Sup Ct, 2022).
Employment and other tribunals	Disclosure is by order under the tribunal's rules, typically narrower than PD57AD; no freezing jurisdiction; third-party orders are possible but rare. Crypto disputes there usually concern remuneration paid in tokens.
Criminal proceedings	Seizure, detention, freezing and forfeiture under POCA Part 5 Chapters 3C to 3F rather than civil injunctions; disclosure under CPIA 1996 and the AG Guidelines; expert evidence under CrimPR Part 19 with the Forensic Science Regulator's statutory Code of Practice (version 2, in force 2 October 2025) applying to forensic science activities in the criminal justice system; hearsay under Criminal Justice Act 2003 ss.114 to 117.
Insolvency	Office-holders use Insolvency Act 1986 ss.234 to 236 (delivery up, examination, production) alongside the civil remedies; cryptoassets form part of the estate (Van Rooyen [2026] EWHC 1286 (Ch)); the UKJT's 2024 Legal Statement on digital assets and insolvency is persuasive.

14 Cross-border evidence, the United States and other jurisdictions

Most exchanges, issuers and messaging platforms encountered in an English crypto case are incorporated abroad, hold their data abroad, and respond to foreign process on their own terms. This section maps the routes available to a lawyer in England and Wales, with particular attention to the United States, where many of the largest providers and the most productive evidence-gathering tools are located.

14.1 Choosing the route

Route	Who can use it	What it yields	Limits
English Bankers Trust / Norwich Pharmacal order served abroad	Civil claimants	Account holder identity, account records, destination of assets, from exchanges willing to comply (LMN v Bitflyer; Wilden)	No direct enforcement abroad; Stanford v AfrAsia caution; compliance often voluntary in practice; local-law carve-outs
Voluntary disclosure by exchange	Anyone with a credible request, usually via counsel	Variable; some exchanges (Gate.io in Murry) disclose account ownership voluntarily on receipt of an English order or a well-evidenced request	Discretionary; most exchanges require legal process from the jurisdiction of incorporation
28 USC 1782 application in a US federal district court	Any "interested person" in a foreign proceeding (including contemplated proceedings)	Subpoena-backed production from US-resident providers (Coinbase, Kraken, Circle, Gemini, Tether-related US entities, analytics vendors): KYC, IP logs, device data, bank links, internal records; can reach documents held abroad by US persons	Target must reside or be found in the district; Intel v AMD discretionary factors; generally unavailable for private arbitration (ZF Automotive, 2022); cost
Letter of request (Hague Evidence Convention 1970) issued under CPR 34.13	Civil litigants with proceedings on foot	Evidence from a witness or documents in a Convention state, executed by that state's courts	Slow (months); executing state applies its own limits; no US-style discovery in most civil-law states
Mutual legal assistance (Crime (International Co-operation) Act 2003; treaties)	Prosecutors and law enforcement only	Coercive measures abroad: production orders, search and seizure, freezing	Use limitation: evidence obtained by MLA may not be used for any other purpose without the requested state's consent; slow; not available to civil parties
UK-US Data Access Agreement (CLOUD Act) via Crime (Overseas Production Orders) Act 2019	UK law enforcement only	Direct production from US providers of content, stored data, traffic data and subscriber information for serious crime (maximum sentence three years or more)	Cannot target US persons or persons in the US; specific accounts only; no onward sharing without permission; in force since 3 October 2022; not available to civil litigants
Exchange law-enforcement portals (Binance, Coinbase, Kraken and others; many via the Kodex platform)	Law enforcement and, for some platforms, regulators	Structured request and response; preservation requests; emergency disclosures	Private parties are refused; portal credential compromise reported in 2025, so treat the response chain of custody carefully
Foreign proceedings in the exchange's home jurisdiction	Civil claimants	Local disclosure and freezing (Singapore, Hong Kong, Cayman, BVI, Seychelles, Lithuania and others are common)	Cost; local counsel; timing

14.2 The United States: what English lawyers need to know when instructing US counsel

Jurisdiction-specific US practice is the origin of much of the language in international crypto investigations (subpoenas, warrants, letters rogatory) and of many of the largest exchanges' compliance processes. The instruments are as follows.

- **Civil subpoenas (Federal Rule of Civil Procedure 45)** compel documents or testimony from non-parties in US litigation. Available to a foreign litigant only through a 1782 application (above) or by joining US proceedings.
- **Grand jury subpoenas and administrative subpoenas** are criminal or regulatory tools issued without judicial approval by prosecutors and agencies (DOJ, IRS-CI, FinCEN, SEC, CFTC). Exchanges receive thousands a year: Coinbase reported 12,716 government requests in the year to 30 September 2025, about 53% from outside the US, with UK requests up 16% year on year.
- **Stored Communications Act orders (18 USC 2703(d))** and **search warrants** obtain non-content and content data from providers; **seizure warrants** (18 USC 981, 21 USC 853) are used to seize cryptoassets at exchanges and issuers, and are commonly the trigger for a Tether freeze.
- **Letters rogatory** is the traditional term for court-to-court requests; for Hague Convention states the letter of request procedure applies; the US also executes non-Convention letters rogatory through 28 USC 1781 and the State Department.
- **Preservation letters** under 18 USC 2703(f) require providers to preserve records for 90 days (renewable) pending process; private parties send contractual or common-law preservation notices with no compulsory effect.
- **Admissibility** is governed by the Federal Rules of Evidence: Rule 702 and the Daubert standard for expert methodology (United States v Sterlingov (D.D.C., 29 February 2024) admitted Chainalysis Reactor clustering with corroboration, the court noting the absence of a documented error rate was not fatal); Rules 803(6) and 902(11) to (14) for business records and certified electronic records.

PRACTICAL SEQUENCING FOR AN ENGLISH CLAIMANT WITH A US-RESIDENT EXCHANGE IN THE CHAIN

(1) Obtain the English proprietary injunction and Bankers Trust order without notice and serve on the exchange by its published legal-process channel and email; most US exchanges will freeze the account on receipt even if they contest jurisdiction. (2) In parallel, instruct US counsel to file a 1782 application in the district where the exchange is found, exhibiting the English order and the tracing report. (3) Ask the English court in advance for permission to use material obtained under the Bankers Trust order in the 1782 proceedings and with law enforcement (CPR 31.22; Smithers [2026] EWHC 207 (Comm) at [15]). (4) Report to Action Fraud and the NCA so that the law-enforcement routes (DAA, MLA, exchange portals, issuer freezes) run alongside.

14.3 Other jurisdictions commonly encountered

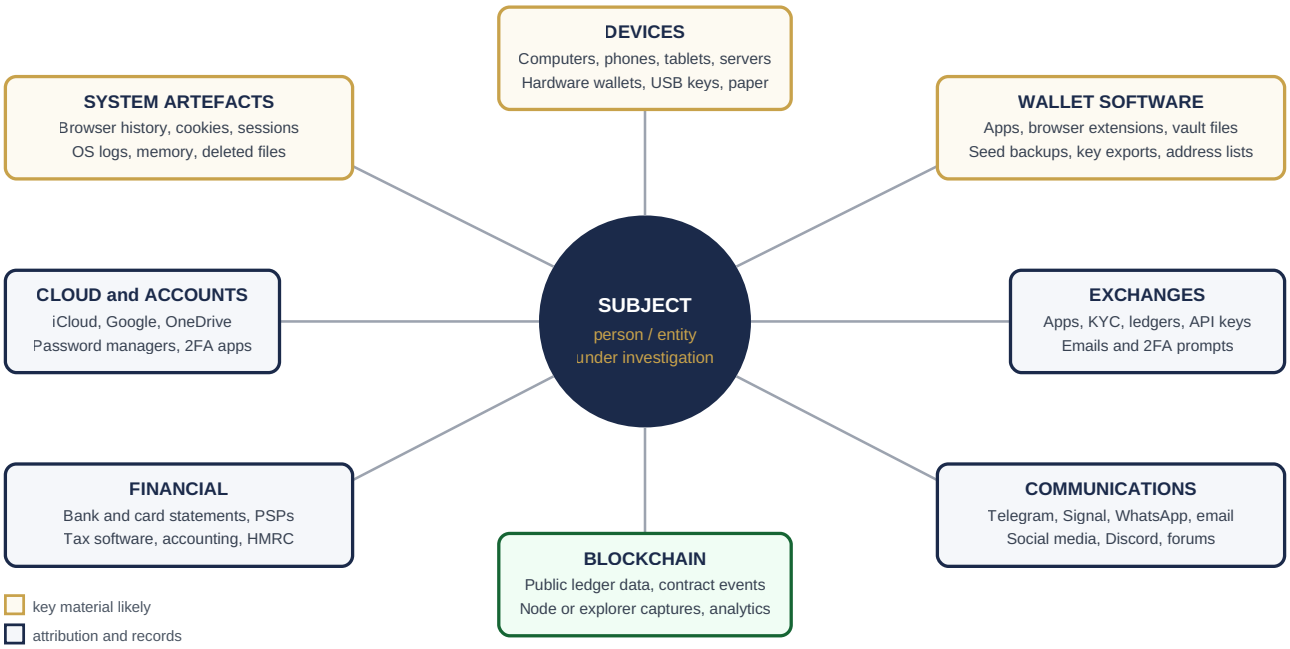
Jurisdiction	Why it arises	Notes
Singapore	Exchange holding companies; ByBit Fintech v Ho Kai Xin [2023] SGHC 199 held USDT to be property held on trust	Receptive to English orders; local proprietary injunctions and disclosure available
Hong Kong	Exchanges, OTC desks; active fraud-recovery jurisdiction	Mareva and Norwich Pharmacal relief available; SFC licensing regime for VA trading platforms
Cayman Islands, BVI, Seychelles	Incorporation of exchange groups (Binance Holdings, Bybit, HTX/Huobi entities)	Local disclosure proceedings possible; Seychelles entities have been persistently non-responsive (Wilden)
Lithuania and other EU states	EU-licensed exchange entities under MiCA	Hague Evidence Convention and EU-national procedures; GDPR governs disclosure; EDPB Guidelines 02/2025 on blockchain
Thailand, Philippines, Cambodia, Myanmar	Investment-fraud cash-out (D'Aloia's Bitkub; scam-compound operations)	Local exchanges respond to MLA and sometimes to English orders; enforcement of judgments is difficult

Jurisdiction	Why it arises	Notes
UAE	OTC desks, VARA-licensed exchanges, DIFC courts	DIFC and ADGM courts grant freezing and disclosure relief in crypto cases and are receptive to English judgments

15 Digital forensics and electronic disclosure

The blockchain is one evidence source among many. The attribution evidence, the key material, the communications and the exchange records all live on devices, in accounts and in third-party systems, and they are identified, preserved, collected, processed, reviewed, analysed and produced under the same disciplines as any other electronically stored information, with two additions: the extreme sensitivity of key material and the need to keep the public ledger and its interpretation separate.

Figure 10 Crypto evidence map: where the evidence lives



Eight families of evidence radiate from the subject. The gold-bordered families are where private keys and seed phrases are most likely to be found and must be handled under restricted access.

Shows: the breadth of sources beyond the ledger and the concentration of key material in devices, wallet software and system artefacts.
Limitation: corporate matters add treasury systems, custodian portals, MPC policy engines and identity providers (section 16).

> **Text alternative:** A hub labelled "Subject: person or entity under investigation" with eight spokes to: Devices (computers, phones, tablets, servers, hardware wallets, USB keys, paper); Wallet software (apps, browser extensions, vault files, seed backups, key exports, address lists); Exchanges (apps, KYC, ledgers, API keys, emails and 2FA prompts); Communications (Telegram, Signal, WhatsApp, email, social media, Discord, forums); Blockchain (public ledger data, contract events, node or explorer captures, analytics); Financial (bank and card statements, PSPs, tax software, accounting, HMRC); Cloud and accounts (iCloud, Google, OneDrive, password managers, 2FA apps); System artefacts (browser history, cookies, sessions, OS logs, memory, deleted files). Devices, wallet software and system artefacts are marked as places where key material is likely.

15.1 Potential evidence sources

Source	What to look for	Handling note
Computers, phones, tablets, servers	Wallet apps and their databases, browser profiles, screenshots, notes, photographs of seed cards, clipboard history, keychain entries.	Forensic image; capture volatile memory if the system is live and a wallet is unlocked.
Hardware wallets	Device itself; companion app data (Ledger Live, Trezor Suite) on the computer, which caches addresses and history.	Seize powered off; photograph; do not attempt PINs (wipe after repeated failures); bag separately from any written phrase.
Software wallets and browser extensions	Encrypted vault (MetaMask: LevelDB store under the browser profile's extension settings; recoverable by carving, including from deleted files), unencrypted address list and network settings, connected sites.	Vault without password yields addresses but not keys; modern vaults are not crackable on any realistic timescale.

Source	What to look for	Handling note
Seed phrases and private-key backups	Paper, metal plates, photographs, notes apps, password managers, cloud drives, emails to self, split across locations.	Highest sensitivity. Sealed exhibit, restricted access, logged handling.
Cryptocurrency and exchange applications	Cached balances, transaction history, deposit addresses, login tokens, push notifications, KYC uploads in the photo library.	Mobile extraction with app-level parsing; check for exchange emails and 2FA prompts corroborating activity.
Email accounts	Exchange registration and verification, withdrawal confirmations, deposit alerts, seed backups, invoices.	Collect from server with date range; withdrawal confirmation emails often quote the destination address and IP.
Telegram, Signal, WhatsApp and other messaging	OTC negotiations, addresses, payment instructions, screenshots, group membership.	Device extraction; Telegram cloud chats also on server; Signal and secret chats device-only.
Cloud storage	Seed photos, wallet backups, exported keys, spreadsheets of addresses.	Preservation letter and collection via API with hashes; note device-to-cloud sync as an alternative path.
Password managers and 2FA apps	Exchange credentials, seed phrases stored as notes, TOTP secrets proving account access.	Presence of a TOTP entry for an exchange is strong evidence of account use.
Web-browser history, cookies and session data	Explorer look-ups of specific addresses (a powerful attribution indicator), exchange sessions, DEX front-ends, mixer sites.	Parse with timestamps; a user who repeatedly looks up address X on an explorer has an interest in X.
Operating-system artefacts	Prefetch, jump lists, USB device history (hardware wallet connections), memory, hibernation files, deleted files.	USB history can prove a Ledger or Trezor was connected on a given date.
Tax and accounting software	Koinly, CoinTracker, Accointing exports; HMRC self-assessment; company ledgers.	Self-declared address lists are admissions.
Bank and payment-service records	Payments to and from exchanges and brokers; card purchases; faster-payments references.	Obtain through the client, CPR 31.17, or Bankers Trust.
Exchange records	Section 9.3.	Section 17.
Blockchain data	Transactions, logs, contract state at block; captured from a node or reputable explorer with hash of capture.	Record method, source, block and time of capture.
Social media and corporate systems	Public posts quoting addresses; corporate treasury, custodian portals, approval workflows, identity provider logs.	Corporate MPC and custody providers keep the approval trail that proves who authorised a transfer.

15.2 Preservation

Preservation in crypto matters has three layers. **The assets**: consider whether to move them to a secure wallet (in civil matters only with the client's authority or a court order; in criminal matters under Chapter 3C), or to freeze them at the exchange or issuer; moving assets creates a new transaction and must be logged. **The key material**: identify every copy of every seed and key, secure them, and record who has had access. **The records**: send preservation notices to exchanges, issuers, cloud providers and banks; suspend deletion on devices and accounts (PD57AD para 4); capture blockchain state at a stated block (exchange labels, contract state and explorer views change); export exchange account histories and API data before the account is frozen or closed and access is lost; and preserve the analyst's working files and tool versions (section 18.4).

15.3 Collection methodology

- **Devices:** forensic imaging (write-blocked, hashed), with live memory capture where a wallet may be unlocked; mobile devices by full-file-system extraction where lawful and proportionate. ISO/IEC 27037 and the NPCC/ACPO Good Practice Guide principles apply; the Forensic Science Regulator's Code (version 2) applies to criminal work.
- **Accounts and cloud:** API or export collection with logged credentials, date ranges and hashes; screenshots only as a last resort and always with the underlying data.

- **Blockchain:** capture raw transaction data from a synchronised node or a reputable explorer's API; record the source, block height, block hash and time; hash the capture file. For layer 2 and pruned data, capture from the network's own archive and record that it is not verifiable from the base chain.
- **Exchange and third-party productions:** receive in native format with a covering certificate; hash on receipt; record the request, the response and any gaps.
- **Analytics:** export the full transaction list underlying any graph; record platform, version, label date and the heuristics enabled.

15.4 Metadata and chain of custody

The metadata that matters: for blockchain captures, block height, block hash, capture time (UTC), source node or explorer, and tool version; for device artefacts, file system timestamps, application database timestamps and the time zone of the device; for exchange productions, the exchange's own timestamps and time zone (frequently UTC but not always), the identity of the responding officer and the date of production; for communications, message IDs, server timestamps and device timestamps (which differ). Chain of custody for crypto evidence must cover three things that ordinary digital evidence does not: the physical custody of key-bearing exhibits; the "cryptographic custody" of any wallet into which assets have been moved (who holds the destination key, where, under what dual control); and every on-chain act performed by the investigator (a sweep, a test deposit, a signed message), each logged with txid, block, fee, destination, authorising person, tool and version.

15.5 The special risks of private keys and seed phrases

A KEY IN A BUNDLE IS A KEY IN THE WORLD

Disclosure of a private key or seed phrase enables anyone who sees it to transfer the assets, irreversibly and untraceably to a person. Keys must never appear in an ordinary disclosure bundle, a witness statement, an exhibit served by email, an expert report, or a court document. Where the existence or content of a key is relevant, describe it (wallet type, number of words, where found, hash of the phrase) and produce the phrase itself only under a confidentiality regime with restricted access and, where necessary, an order for inspection at a controlled location. Store keys offline, encrypted, under dual control; never type a seed into an internet-connected device to "check" it; derive a watch-only view from the extended public key instead; log every access. In criminal proceedings the same applies to unused material: a seed phrase in the MG6C schedule must be handled as a restricted exhibit.

15.6 Relationships every report should keep straight

Pair	Point
Blockchain evidence and electronically stored information	The ledger is public, replicated and verifiable; ESI is private, held by a party or third party and disclosed under rules. The two must be correlated but are obtained, authenticated and challenged differently.
Publicly available records and data obtained through legal process	Public ledger data needs no permission and carries no collateral-use restriction; exchange records obtained under a Bankers Trust order or MLA carry use restrictions.
Native files and exported records	A wallet database and an exchange's CSV export of it are different documents; the native file has metadata and deleted content the export lacks.
Screenshots and authenticated source data	A screenshot of an explorer page proves that a page looked like that at some time on some device. The underlying transaction data proves the transaction. Always obtain the latter.
Transaction records and account records	A transaction is an on-chain event; an account record is the exchange's internal narrative. A deposit appears in both; an internal transfer in one only.
Metadata and substantive communications	Message timestamps, device IDs and IP addresses corroborate or undermine what the message says.
Forensic collection and expert interpretation	Collecting the vault file is a technical, repeatable act. Concluding that its owner controlled address X is opinion evidence subject to Part 35 and to challenge.

15.7 Privilege, confidentiality, data protection and proportionality

Privilege. Tracing reports commissioned by solicitors for litigation are prima facie privileged until deployed; once served in support of a without-notice application they are before the court. Analyst working notes and tool outputs underlying a served report are likely to be disclosable, and the duty of full and frank disclosure on a without-notice application overrides tactical reticence (Smithers). Communications with an exchange's compliance team are not privileged. In criminal work the prosecution's analytics material is unused material subject to CPIA scheduling.

Confidentiality. Exchange productions contain third parties' personal data (counterparties, other customers in a hot-wallet analysis); handle under the CPR 31.22 restriction and a confidentiality club where appropriate. An xpub or full address history is a complete financial biography and should be redacted from public documents.

UK GDPR and data minimisation. Collect only the addresses, date ranges and account fields that the issues require; record the lawful basis (contract, legitimate interests, the DUAA 2025 recognised legitimate interest for crime prevention, or legal obligation) for each collection and each transfer abroad; apply retention limits to KYC bundles and device images; consider a data protection impact assessment for large tracing projects touching many uninvolved addresses.

Proportionality. Under PD57AD para 6.4 and CPR 1.1, the cost of a full multi-chain tracing exercise and of device imaging must be weighed against the sums at stake and the prospects of recovery; a trace that ends at a mixer or a Seychelles exchange with no assets may not justify further spend. Stage the work: freeze first, trace to the first identifiable service, obtain its records, then decide whether to go further.

16 Source architecture and alternative evidence paths

Do not examine the wallet, the device or the exchange in isolation. Every crypto holding is embedded in a web of associated locations, and when the primary source is unavailable, damaged, encrypted, deleted or abroad, an equivalent or corroborating record usually exists somewhere else.

16.1 Associated evidence locations for a crypto matter

Location	What it holds in a crypto matter
Physical device	Wallet apps, browser extensions, vault files, exchange apps, photos of seeds, memory (if live).
Local storage	Browser profile directories, app databases, downloads (CSV exports, keystore JSON files), hibernation and page files.
Connected computers	Hardware-wallet companion apps caching addresses and history; USB connection logs; synced browser profiles.
Mobile applications	Wallet and exchange apps; Telegram, Signal, WhatsApp; authenticator apps holding exchange TOTP secrets; photo library.
Synchronised accounts	Browser sync (Chrome, Firefox, Edge) replicating extension data; iCloud Keychain and Google Password Manager holding exchange credentials.
Cloud platforms	iCloud, Google Drive, OneDrive, Dropbox: seed photos, wallet backups, keystore files, exported histories; cloud backups of the phone.
Backups	Time Machine, Windows File History, phone backups (iTunes/Finder, Google One), NAS; may hold earlier vault versions and deleted files.
Administrative consoles	Corporate custody and MPC platforms (approval workflows, policy engines, signer lists); exchange sub-account and API management; Safe multisig owner lists.
Identity providers	Microsoft Entra, Google Workspace, Okta: who logged in to the custody console and when; MFA events.
Network infrastructure	Firewall and proxy logs showing connections to exchange domains, explorer look-ups and wallet RPC endpoints; VPN logs.
Third-party service providers	Exchanges, issuers, custodians, analytics vendors, payment processors, banks, telecoms, Telegram, cloud providers.
Counterpart devices	The other party to a Telegram negotiation or a transfer holds the same messages and often the same addresses; the recipient's exchange holds the deposit record.
The public ledger	Always available, always verifiable; the fixed point against which every other source is checked.

16.2 Alternative Evidence Paths

Evidence	Local device	Cloud	Backup	Logs	Counterpart device	Deleted / recoverable
Seed phrase / private key	**Y (vault, photos, notes)**	Sometimes (drive, notes sync)	Sometimes (device backup)	n/a	n/a	Varies (carving of vault files and photos often succeeds)
Wallet address list	**Y (unencrypted app state)**	**Y (exchange withdrawal records, tax software)**	**Y**	Limited (explorer look-ups in proxy logs)	Possibly (addresses quoted in chats)	Varies
Transaction history	**Y (app cache)**	**Y (public ledger, exchange ledger)**	**Y**	**Y (ledger is the log)**	**Y (recipient's records)**	n/a (ledger is permanent; L2 blobs pruned)
Exchange account identity	Limited (app login, emails)	**Y (exchange KYC file)**	Sometimes (email backups)	**Y (exchange IP and session logs)**	n/a	Varies (retention 5 years plus under MLR 2017 reg 40)

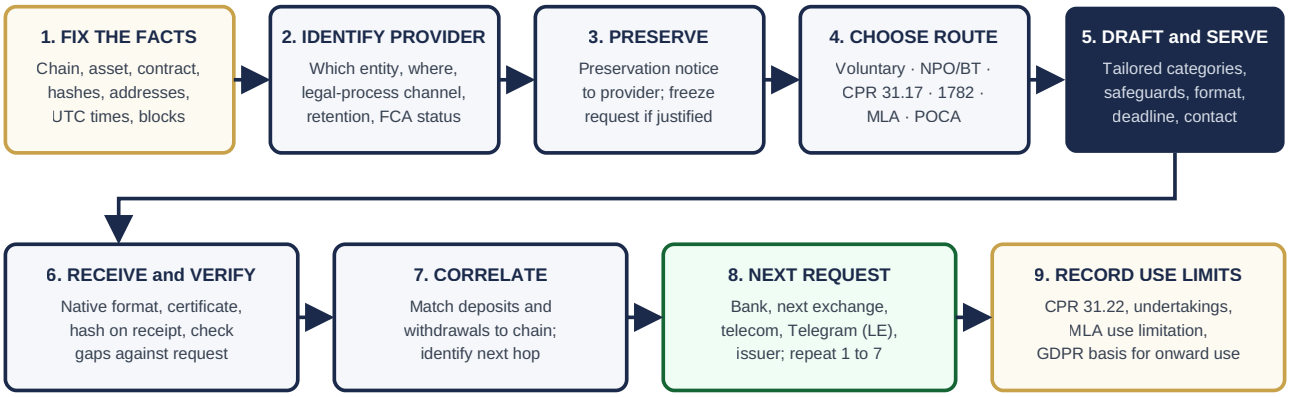
Evidence	Local device	Cloud	Backup	Logs	Counterpart device	Deleted / recoverable
OTC / Telegram negotiation	**Y (Telegram database)**	**Y (cloud chats on Telegram servers; criminal process only)**	Sometimes	Limited (IP and phone number to authorities)	**Y (broker's device)**	Varies (deleted messages sometimes recoverable from device cache)
Authorisation of a corporate transfer	Limited	**Y (custody console, MPC policy logs)**	n/a	**Y (identity provider, approval workflow)**	Possibly (co-signer's device)	Varies
Fiat leg (bank / card)	Limited (banking app)	**Y (bank records)**	n/a	**Y (bank and PSP logs)**	**Y (counterparty's bank)**	n/a
Hardware wallet use	**Y (companion app, USB history)**	Sometimes (Ledger account sync)	**Y (system backups)**	**Y (OS device logs)**	n/a	Varies

Fallback strategy. When the primary source is unavailable (device lost or wiped), damaged, encrypted (a vault without a password), deleted or inaccessible (an exchange abroad that will not respond), pursue in order: the public ledger for movement; the exchange or issuer at the other end of each transfer for identity; cloud and backup copies of the device for key material and address lists; counterpart devices and accounts for communications; and identity-provider and network logs for who acted when.

17 Disclosure requests and legal process

A crypto disclosure request succeeds or fails on precision. The provider's compliance team must be able to find the account from the identifiers supplied, must be told exactly which categories of record are sought, and must not be asked for records it does not keep. This section gives the drafting method, the identifiers, the categories, and model wording.

Figure 11 **Model disclosure-request workflow**



Requests iterate: each production identifies the next provider. Preservation should precede every formal step.

Shows: the order of operations and the point at which use restrictions attach. **Limitation:** in urgent cases steps 3 to 5 collapse into a single without-notice application with the exchange served the same day.

> **Text alternative:** Nine numbered steps in two rows. 1 Fix the facts (chain, asset, contract, hashes, addresses, UTC times, blocks). 2 Identify the provider (which entity, where, legal-process channel, retention, FCA status). 3 Preserve (preservation notice; freeze request if justified). 4 Choose the route (voluntary, Norwich Pharmacal or Bankers Trust, CPR 31.17, 1782, MLA, POCA). 5 Draft and serve (tailored categories, safeguards, format, deadline, contact). 6 Receive and verify (native format, certificate, hash on receipt, check gaps). 7 Correlate (match deposits and withdrawals to the chain; identify the next hop). 8 Next request (bank, next exchange, telecom, Telegram via law enforcement, issuer; repeat). 9 Record use limits (CPR 31.22, undertakings, MLA use limitation, GDPR basis).

17.1 Identifiers to include, where known

Identifier	Why the provider needs it
Blockchain and asset standard	"USDT" alone cannot be searched; "USDT (TRC-20) on TRON" can.
Wallet addresses	Exact, case-preserved (Ethereum addresses are case-insensitive but checksummed; Bitcoin bech32 is lower case; TRON begins with T). State whether each is believed to be a deposit address, a withdrawal destination or a hot wallet.
Transaction hashes	The fastest key into an exchange's deposit and withdrawal tables.
Token contract addresses	Distinguishes genuine USDT from counterfeit tokens and one chain's deployment from another.
Dates, times and time zone	Always UTC with the block number; ask the provider to state its own time zone.
Block numbers	Unambiguous even when clocks disagree.
Exchange account identifiers	User ID, UID, account number, email on file, if known from the client or earlier productions.
Email addresses, telephone numbers, usernames	Alternative keys into the account.
IP addresses	With date and time; providers can search login logs.
Payment methods	Bank account numbers, card last-four digits, PSP references.
Related entities and aliases	Known associates, corporate vehicles, Telegram handles.
Requested categories of records	Section 17.2. Numbered, so the response can be checked against the request.

17.2 Categories of record commonly sought from a centralised exchange

Category	Typical content	Note
KYC and customer identification	Identity documents, selfie or liveness, proof of address, date of birth, nationality, PEP and sanctions screening results.	Ask for the document images, not just the extracted fields.
Account-opening documents	Registration date, email, phone, terms accepted, referral codes.	
Account ownership and beneficial ownership	Corporate accounts: directors, UBOs, authorised users, sub-accounts.	
Deposit and withdrawal records	On-chain deposits (address, txid, asset, amount, time, confirmations) and withdrawals (destination address, txid, requesting user, IP, 2FA method).	Withdrawal requests carry the richest attribution data.
Internal ledger entries	All balance movements including internal transfers, fees, staking rewards, conversions.	Ask for the complete ledger, not a filtered "transaction history".
Trading and conversion history	Orders, fills, pairs, prices, times, OTC trades.	
Wallet addresses associated with the account	All deposit addresses ever assigned (per asset and chain) and all withdrawal addresses used, with whitelist records.	Deposit addresses for every asset, not only the one traced.
Transaction hashes	For every on-chain deposit and withdrawal.	
IP logs, device and session information, login history	Registration IP; every login with IP, timestamp, user agent, device ID, geolocation if recorded; API key creation and use.	Specify the date range.
Communications	Support tickets, chats, emails, in-app messages.	
Fraud or compliance alerts and internal investigation records	Transaction-monitoring alerts, risk scores, EDD reviews, decisions to lift blocks.	Central to notice arguments (D'Aloia).
Suspicious activity reports	Whether a SAR or DAML was filed.	**Jurisdiction-specific** Tipping-off (POCA s.333A) prevents disclosure of a UK SAR; ask only whether the account was restricted and when.
Account restrictions, freezes and closures	Dates, reasons, who requested, what balance was held at freeze.	
Linked bank accounts and payment instruments	Account numbers, names, card details, PSP references, fiat deposit and withdrawal history.	The bridge to the banking system.
Tax documentation	Tax residency self-certifications, CARF/DAC8 reporting data, 1099 equivalents.	UK CARF reporting by cryptoasset service providers begins for 2026 data.
Counterparties and related accounts	Accounts sharing device, IP, bank account or identity document; internal-transfer counterparties.	Ask expressly; exchanges can run these links quickly.

17.3 Other providers

Provider	What they hold	Route and caveats
Self-hosted wallet software providers	Usually no account; some hold telemetry, IP logs from RPC or swap features, app-store purchase records, cloud backup metadata.	Ask what exists before drafting; expect little.
Payment processors and on-ramps (MoonPay, Ramp, Banxa, PayPal)	KYC for fiat-to-crypto purchases, card details, destination addresses.	Often more productive than the exchange for retail fraudsters buying crypto.
Stablecoin issuers	Blacklist and freeze records, mint and redemption records for direct customers, law-enforcement request logs.	Tether responds to law-enforcement requests and to court orders; Circle acts on regulatory or court order. Civil requests via counsel are considered case by case.

Provider	What they hold	Route and caveats
OTC brokers	Their own exchange accounts, bank records, Telegram history.	A defendant or Norwich Pharmacal respondent in their own right; expect non-cooperation.
Messaging platforms	Telegram: IP and phone number to authorities on a valid order in a criminal case; WhatsApp and Signal: minimal metadata.	Criminal process only; civil route is the counterpart device.
Cloud providers	Backups, files, account access logs.	Preservation notice then NPO / 1782 / MLA depending on provider location.
Telecoms	Subscriber details for a phone number used for exchange 2FA or Telegram.	Lawful process; UK communications data is obtainable by authorities under the Investigatory Powers Act 2016, not by civil parties save via NPO in narrow cases.
Banks	The fiat legs.	Bankers Trust, CPR 31.17, or the client's own records.
Blockchain-analytics providers	Methodology documentation, label provenance and dating, cluster membership at a date.	Necessary where their output is relied on and challenged; obtain through the instructing party's licence or by third-party disclosure.

17.4 Drafting principles

- **Tailor to the provider's actual records.** Check the provider's published law-enforcement or legal-process guidelines, which usually list the data categories it holds and its retention periods. Do not assume all providers keep IP logs, device fingerprints or internal alerts.
- **Jurisdiction and service.** Identify the correct legal entity (exchange groups have dozens); serve at its legal-process address and the email its terms specify; for foreign entities, obtain permission to serve out under PD6B para 3.1(25) for information orders.
- **Retention periods.** UK MLR 2017 reg 40 requires five years' retention of CDD and transaction records; other jurisdictions differ; session logs are often held for months only. Send preservation notices immediately.
- **Authentication.** Ask for a certificate or witness statement from a records custodian identifying the systems from which the records were extracted, the extraction date and time zone, and confirming they are business records (Civil Evidence Act 1995 s.9; CJA 2003 s.117 in criminal proceedings).
- **Confidentiality and non-disclosure to the account holder.** Ask for a gagging provision (in the order, not merely the letter) for a defined period; exchanges will otherwise notify customers.
- **Privilege.** Providers' internal legal advice is not sought; compliance alerts and investigation notes are.
- **Proportionality and relevance.** Limit date ranges to the tracing window plus a margin; limit to accounts connected to the identified addresses and their linked accounts; avoid "all documents relating to".
- **Data protection.** State the lawful basis and the use restriction; ask for personal data of third parties to be provided under the confidentiality regime.
- **Format.** Native or structured export (CSV, JSON) with a data dictionary; images of KYC documents; logs with UTC timestamps.

17.5 Model wording

A. PRESERVATION NOTICE TO AN EXCHANGE (CIVIL)

We act for [client] in relation to the misappropriation of [asset and amount] from wallet address [address] on [date, UTC]. Our tracing evidence indicates that [amount] of those assets were transferred by transaction [hash] on the [network] blockchain at block [number] to address [address], which we understand to be a deposit address administered by [exchange entity] ("the Deposit Address"). We ask that you immediately preserve, and refrain from deleting, altering or overwriting, all records relating to the customer account(s) to which the Deposit Address is or was assigned, including without limitation KYC and onboarding records, the complete account ledger, deposit and withdrawal records with transaction hashes and destination addresses, all deposit and withdrawal addresses associated with the account(s) for every asset, login and session logs with IP addresses and device identifiers from [date] to date, communications with the account holder, compliance alerts and restriction records, and linked bank accounts and payment instruments. We further ask that you consider placing a hold on the assets standing to the credit of the account(s) pending an application to the High Court of England and Wales, notice of which will be given to you. Please confirm within [48 hours] that preservation is in place and identify the legal entity and address for service of court process. This letter is not to be disclosed to the account holder.

B. SCHEDULE TO A BANKERS TRUST ORDER (CATEGORIES OF DOCUMENTS)

The Respondent shall, within [7] days of service, disclose to the Applicant's solicitors by way of witness statement or certificate of a records custodian, together with copies of the underlying records in native electronic form: (1) the name, date of birth, residential address, nationality, identity document(s) and all contact details held in respect of each customer account to which any of the addresses listed in Schedule 2 has been assigned or from which any of the transactions listed in Schedule 3 was made; (2) the complete ledger of each such account from [date] to the date of this Order, including all deposits, withdrawals, trades, conversions, fees and internal transfers, identifying for each the asset, amount, date and time (with time zone), transaction hash where applicable, and counterparty account where applicable; (3) all cryptoasset addresses assigned to or used by each such account for the receipt or withdrawal of any asset; (4) the current balance of each such account by asset; (5) all IP addresses, device identifiers and user-agent strings recorded on registration and on each login, deposit and withdrawal from [date] to the date of this Order; (6) details of all bank accounts, cards and payment instruments linked to each such account; (7) records of any restriction, freeze or closure applied to each such account and the reasons; and (8) the identity of any other account held with the Respondent that shares an identity document, telephone number, email address, device identifier, bank account or payment instrument with any such account. Nothing in this Order requires the Respondent to disclose the fact or content of any report made under Part 7 of the Proceeds of Crime Act 2002 or equivalent legislation.

C. SAFEGUARDS TO BE INCLUDED IN THE ORDER (AFTER LMN V BITFLYER)

The Applicant undertakes (a) not to use any information obtained pursuant to this Order for any purpose other than the identification of the persons responsible for, and the location and recovery of, the assets described in Schedule 1, and in particular not to commence any substantive claim against the Respondent without the permission of the Court, save that the Applicant may provide such information to [the National Crime Agency, the City of London Police and any other law enforcement or regulatory authority in any jurisdiction] for the purpose of the investigation and prosecution of the wrongdoing described in the Applicant's evidence; (b) to pay the Respondent's reasonable costs of compliance; and (c) to comply with any order the Court may make as to damages if the Court finds that this Order has caused loss to the Respondent or to any third party. The Respondent shall not be required to do anything that would breach the law of the jurisdiction in which the relevant records are held, provided that it identifies the provision relied on within [7] days. The Respondent shall not disclose the existence of this Order to the holder of any account referred to in it until [date] or further order.

D. INSTRUCTION TO A BLOCKCHAIN-TRACING EXPERT (CPR PART 35)

You are instructed to trace the movement of [asset and amount] transferred from address [address] by transaction(s) [hash(es)] on [date, UTC] and to report on the addresses and services at which those assets, or their traceable proceeds, were held as at [date/block]. Your report must (1) identify the ledger model of each chain traversed and the tracing method applied to each (UTXO-based for Bitcoin-family chains; a stated allocation rule for account-based and token assets), and explain why that method is appropriate; (2) apply the stated method consistently and set out every hop in a schedule identifying transaction hash, block, timestamp (UTC), asset, contract address where applicable, amount in and out, and the allocation applied at any point of mixing, so that the arithmetic can be reconciled at each hop; (3) treat all persons whose funds were commingled with the traced assets comparably, and state expressly where the method disadvantages or advantages our client relative to others; (4) distinguish findings drawn from ledger data from inferences drawn from heuristics, attribution labels, timing or amount correlation, cross-chain swaps or mixers, stating the source, version and date of any commercial analytics used and the confidence attached to each inference; (5) identify every limitation, including any step taken for speed rather than completeness; and (6) not express any conclusion as to the identity of the person controlling any address save by reference to specific off-chain evidence identified in the report. You are reminded of your overriding duty to the Court under CPR 35.3 and that this report may be relied on at a without-notice hearing where the duty of full and frank disclosure applies.

18 Evidentiary and procedural issues

Blockchain evidence is unusually easy to verify and unusually easy to misdescribe. The courts have not doubted its admissibility; they have scrutinised how it was interpreted, whether the method was disclosed, and whether the arithmetic worked.

18.1 Authentication

Identifying and verifying a transaction. A transaction is identified by its hash. Anyone with the hash can retrieve the transaction from any full node or explorer and confirm its contents, its block and its position; the block header chain then proves that the transaction has been part of the canonical ledger since that block. The most robust authentication is a capture from a synchronised node run by the party or its expert, with the raw transaction data, block hash and capture time exhibited and hashed. Explorer output is acceptable in practice if the source, URL, date and time of capture are recorded and the underlying data is exhibited or reproducible; a screenshot alone is weak.

Explorer output as evidence. Treat an explorer page as a rendering by a third-party website of public data. Its transaction fields can be re-verified from the chain; its labels, "internal transactions" and fiat-value conversions are the site's own computations and need separate support. Where an explorer's label is relied on, obtain the labelling basis or, better, confirmation from the labelled entity.

Business records. Exchange productions are business records; in civil proceedings hearsay is admissible under the Civil Evidence Act 1995 with weight assessed under s.4, and s.9 allows documents forming part of the records of a business to be received on a certificate. In criminal proceedings s.117 Criminal Justice Act 2003 governs business documents and s.114 the residual discretion. Blockchain data itself is arguably not hearsay at all (it is machine-generated output of a deterministic process) but the safer course is to prove it by a witness who explains the capture.

18.2 Expert evidence

CPR Part 35 applies: expert evidence is restricted to what is reasonably required (r.35.1); the expert's duty is to the court (r.35.3); permission is needed (r.35.4); the report must comply with PD35 and state the substance of instructions. In criminal proceedings CrimPR Part 19 and, for forensic science activities, the Forensic Science Regulator's Code of Practice (version 2, in force 2 October 2025) apply; whether crypto tracing is a defined forensic science activity under the Code should be checked against the current annexes. The English cases establish the following expectations.

Expectation	Source
State the method in the report before the analysis and do not change it without a supplemental report.	D'Aloia [2024] EWHC 2342 (Ch): the analyst said FIFO, did not apply it, and shifted method; a method first articulated in solicitors' correspondence was worthless.
Evidence the tool: produce the platform's methodology documentation, version and the heuristics enabled.	D'Aloia: no documentation from Crystal or TRM was produced; outputs from the two were irreconcilable.
Reconcile the arithmetic at every hop; the judge may check it unprompted.	D'Aloia: "it is also open to me to identify where, numerically, the figures do not add up".
Treat competing victims comparably; do not match outflows selectively.	D'Aloia: selective matching that favoured the claimant was not a tracing method.
Match the method to the ledger: UTXO for Bitcoin; allocation rules for account and token assets.	Smithers [2026] EWHC 1907 (Comm).

Expectation	Source
Disclose limitations, including any step taken for speed, to the legal team and the court, especially without notice.	Smithers [2026] EWHC 207 (Comm): LIFO used for urgency without warning; risk of false-positive freezes.
A transaction-by-transaction schedule with every hash will carry a method the court might otherwise doubt.	Wilden [2026] EWHC 1355 (KB): LIFO accepted on granular evidence.
Separate tracing from attribution; base any attribution opinion on identified off-chain evidence.	General; see section 12.

Uncertain No English authority directs a single joint expert on crypto tracing, and on without-notice applications the tracing material is typically served as a witness statement exhibiting an analyst's report rather than as Part 35 evidence, yet the court acts on it to freeze third-party assets. Instructing solicitors should apply Part 35 discipline to that material regardless of its formal status.

18.3 Reliability of blockchain-analytics tools

The platforms are widely used by law enforcement, exchanges and regulators and are often right. Their limits are documented. Peer-reviewed work found individual change heuristics correct only 10 to 30% of the time in isolation and demonstrated "cluster collapse", where naive merging combined 184 million clusters into one super-cluster of 224 million addresses (Möser and Narayanan, 2022); a 2022 digital-forensics paper reported simulated error rates for clustering heuristics of the order of 57 to 93% under its model. In United States v Sterlingov (D.D.C. 2024) the court admitted Chainalysis Reactor evidence on the basis of corroboration by manual tracing and other vendors, distinguishing the widely accepted co-spend heuristic from proprietary behavioural heuristics; the defendant was sentenced to twelve and a half years. In England, D'Aloia excluded the weight of an analyst's output for opacity and inconsistency. The correct position for a report is that analytics output is expert-assisted inference whose reliability depends on the heuristic used, the corroboration available and the candour with which limitations are stated. Vendor accuracy claims ("95%") should be treated as marketing unless the denominator is explained.

18.4 Preservation of the evidence and of the analysis

Preserve both the original evidence and the analytical steps used to interpret it. That means: the raw captures (transaction data, block hashes, exchange exports) with hashes; the analytics platform's exported case file or graph data as at the date of the report, since labels and clusters change; the tool version; the analyst's working notes and the list of heuristics applied; and every intermediate schedule. Volatile sources (exchange session logs, mempool observations, layer-2 blob data, explorer labels) should be captured at the time and dated. If a second analyst or the opponent cannot reproduce the trace from the preserved material, the report is exposed.

18.5 Time, timestamps and confirmation status

- Block timestamps are set by the block producer and are approximate; they record when the block was assembled, not when the user signed or when the funds were "sent" in any commercial sense. Bitcoin permits about two hours of tolerance; Ethereum slots are fixed at 12-second intervals so timestamps are reliable to within a slot.
- Explorers display local time by default; exchange logs use their own clock and zone; device artefacts use the device's zone. State every time in UTC with its source.
- Confirmation status is a property of the moment of capture. Record block height and hash at capture and, for Ethereum, whether the block was finalised.
- Reorganisations: a transaction observed in a block that is later orphaned will disappear from the canonical chain and may reappear in a later block with the same hash or be replaced. Deep reorganisations are rare on major chains but have occurred.

- Duplicate and incomplete records: exchanges may record one on-chain deposit as several ledger entries; explorers may show a token transfer both as a transaction and as a log; D'Aloia's expert schedules contained duplicated transactions. De-duplicate by hash and log index and say so.

18.6 Demonstrative and source evidence

A flow diagram, a graph from an analytics platform or a summary table is demonstrative: it helps the court understand the source evidence but is not itself proof. The source evidence is the transaction list, the exchange production and the device artefacts. Every demonstrative should be traceable to an exhibited schedule with hashes, and the report should say which is which.

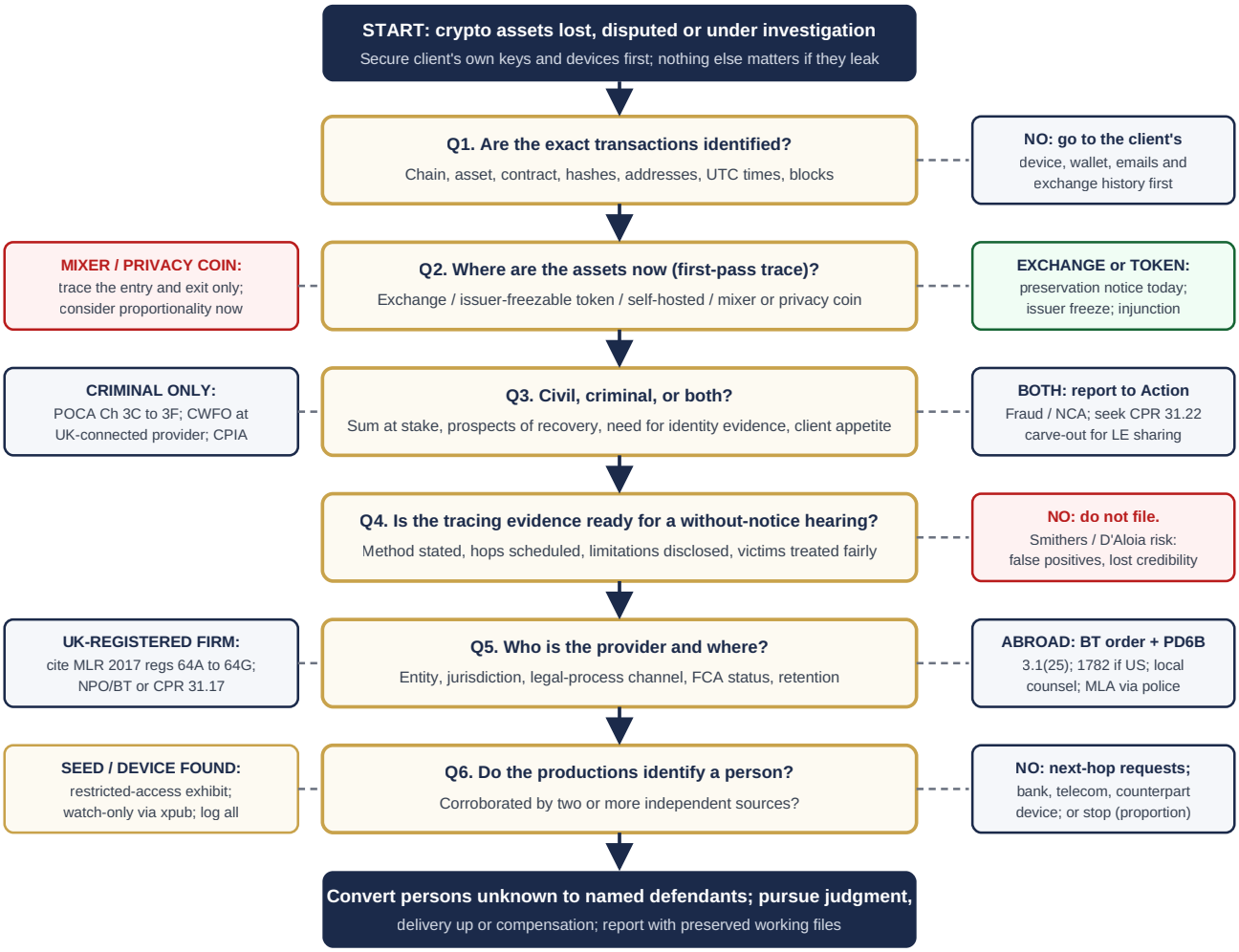
18.7 Recommended investigative workflow

Step	Activity	Output
1	Initial identification	Victim or subject addresses, transactions, chains and assets confirmed from the client's own records and devices; block-referenced capture.
2	Immediate preservation and freeze	Preservation notices; issuer freeze request where justified; without-notice application prepared with candid limitations.
3	First-pass trace	Trace to the first identifiable service per chain using the ledger-appropriate method; schedule of hops; confidence at each hop.
4	Exchange and provider disclosure	Orders and requests served; productions received, hashed and correlated to the chain.
5	Device and account forensics	Imaging, extraction, artefact analysis; key material secured; address lists and communications recovered.
6	Attribution analysis	Evidence-and-attribution matrix (section 23.3) completed for each address and person; gaps identified.
7	Iteration	Further requests to next-hop providers, banks, telecoms; persons unknown converted to named defendants where evidence allows.
8	Reporting	Part 35-compliant report separating source evidence, method, tracing findings, attribution opinion and limitations; preserved working files; demonstratives cross-referenced to schedules.

19 Investigative workflow and decision tree

The decision tree below is the sequence a litigation team should run in the first 72 hours of a crypto matter. It is designed to be worked through with the client and the forensic provider on the first call.

Figure 12 **First-72-hours decision tree for a crypto recovery or investigation**



Work down the centre; the side boxes are the branches most often taken.

Shows: the order in which the questions should be asked and the branch each answer opens. **Limitation:** a simplification; regulatory, insolvency and family matters have their own additional branches.

> **Text alternative:** Start: secure the client's own keys and devices first. Q1 Are the exact transactions identified (chain, asset, contract, hashes, addresses, UTC times, blocks)? If no, go to the client's device, wallet, emails and exchange history first. Q2 Where are the assets now? If at an exchange or in a freezable token: preservation notice today, issuer freeze, injunction. If in a mixer or privacy coin: trace entry and exit only and consider proportionality now. Q3 Civil, criminal or both? If both: report to Action Fraud and the NCA and seek a CPR 31.22 carve-out for sharing with law enforcement. If criminal only: POCA Chapters 3C to 3F, crypto wallet freezing order at a UK-connected provider, CPIA disclosure. Q4 Is the tracing evidence ready for a without-notice hearing (method stated, hops scheduled, limitations disclosed, victims treated fairly)? If no, do not file. Q5 Who is the provider and where? If abroad: Bankers Trust order with PD6B 3.1(25), 1782 if in the US, local counsel, MLA via police. If a UK-registered firm: cite MLR 2017 regs 64A to 64G and use a Norwich Pharmacal or Bankers Trust order or CPR 31.17. If a seed or device is found: restricted-access exhibit, watch-only view via xpub, log everything. Q6 Do the productions identify a person, corroborated by two or more independent sources? If no: next-hop requests to bank, telecom or counterpart device, or stop on proportionality grounds. End: convert persons unknown to named defendants, pursue judgment, delivery up or compensation, and report with preserved working files.

20 Worked examples

Eight hypothetical scenarios. All names, addresses, hashes and figures are invented; any resemblance to real persons or matters is coincidental. Each example ends with the evidential lesson.

EXAMPLE 1 **A simple transfer between two self-hosted wallets**

Ms Okonkwo sends 0.5 BTC from her Electrum wallet to a hardware wallet she has just set up. On chain: one input from address bc1q…a1 (her Electrum receive address), two outputs (0.5 BTC to bc1p…t9, a Taproot address, and 0.0198 BTC change to bc1q…c4), fee 0.0002 BTC, block 964,880. Nothing on the ledger indicates that both wallets are hers. Attribution evidence: the Electrum wallet file on her laptop listing bc1q…a1 and bc1q…c4; Trezor Suite on the same laptop listing bc1p…t9; USB device history showing a Trezor connected at 14:02 UTC on the day; and a signed message from bc1p…t9. **Lesson:** a self-hosted-to-self-hosted transfer looks identical to a payment to a stranger; only device evidence shows it was internal.

EXAMPLE 2 **A token transfer on Ethereum requiring ETH for gas**

A fraudster's wallet 0x9b…2e receives 40,000 USDT from a victim. The wallet has no ETH, so the USDT cannot move. Eleven minutes later 0.02 ETH arrives at 0x9b…2e from an address labelled as a Kraken hot wallet; four minutes after that the USDT is sent onward. The Kraken withdrawal is the attribution lead: a Bankers Trust order against Kraken's UK entity yields the account that withdrew 0.02 ETH to 0x9b…2e at that time, its KYC and its login IPs. **Lesson:** the gas-funding transaction is often the weakest point in a launderer's operational security, because a small amount of ETH has to come from somewhere, and that somewhere is frequently a KYC'd account.

EXAMPLE 3 **Funds transferred to an exchange and then moved internally**

Rothwell Capital Partners LLP traces 3.2 million USDT from a fake "yield platform" through three hops to deposit address TQx…7h at a large exchange. The exchange's production shows: the deposit was credited to account UID 55120987 (KYC: a 24-year-old in Bangkok with declared monthly income of THB 20,000); within 30 minutes the balance was transferred by internal transfer to UID 55121004 and then to UID 55121022; UID 55121022 converted to BTC and withdrew to bc1q…m2, a self-hosted address, six hours later. None of the internal transfers touched the chain. The three accounts share a device fingerprint and a registration IP. **Lesson:** without the internal ledger, the trace would have stopped at TQx…7h and the wrong person (a mule) would have been the sole defendant. The shared device fingerprint supports a single-operator inference; it does not identify the operator.

EXAMPLE 4 **A stablecoin transaction across multiple addresses and chains**

500,000 USDT (ERC-20) is split into five transfers of 100,000 to five fresh Ethereum addresses, each of which bridges to TRON through a cross-chain swap service, arriving as USDT (TRC-20) in amounts of 99,700 to 99,850 over the following hour. The Ethereum legs are certain; the TRON legs are matched by amount, timing and the swap service's known deposit and payout addresses. The expert's schedule marks the five bridge crossings as "inferred: amount and timing correlation via [service]" and assigns lower confidence to them. Tether is asked to blacklist the five TRON destination addresses; it does so within 48 hours on receipt of the police reference number and the English injunction. **Lesson:** name the network and contract at every hop; state the cross-chain links as inference; use the issuer's freeze in parallel with the court's order, not instead of it.

EXAMPLE 5 **Use of an OTC broker**

A darknet vendor cashes out 2 BTC through "@LondonSwapz", found in a Telegram group. The broker sends 2 BTC from a self-hosted wallet to his personal account at a UK-registered exchange, sells it, and withdraws £[sum] to his personal bank account; the customer collects cash in a car park. On chain: vendor cluster → broker's self-hosted wallet → exchange deposit address. The exchange's records identify the broker (in his own name). The Telegram export from the broker's seized phone identifies the customer's handle and numeric user ID; the exchange's records show 140 similar deposits in six months; the bank statements show matching cash withdrawals. **Lesson:** the exchange identifies the broker, not the customer; the customer is identified from the broker's device and, in a criminal case, from Telegram on a valid order.

EXAMPLE 6 **Attribution through exchange KYC records**

In a shareholder dispute at Marlow & Finch Ltd, 180 ETH leaves the company's Safe multisig treasury to address 0x4c…f1. The company's Safe transaction log shows the transfer was proposed and executed by the two signer keys held by the finance director and the CEO. 0x4c…f1 later sends 180 ETH to a Coinbase deposit address. A 1782 application in the Northern District of California obtains Coinbase's file: the account is in the finance director's name, opened three years earlier, funded from his personal UK bank account, and accessed from an IP range matching the company's office at the time of the deposit. He had claimed 0x4c…f1 was a supplier's address. **Lesson:** the Safe signer log proves authorisation; the Coinbase KYC proves the beneficiary; the IP evidence corroborates; together they answer control, authorisation and beneficial ownership separately.

EXAMPLE 7 **A transaction linked to a device but not proving sole control**

Police seize a laptop from a shared flat. Forensic examination finds a MetaMask vault whose unencrypted state lists address 0x77…b3, from which £600,000 of stolen tokens were dispersed. The vault cannot be decrypted. The laptop's Windows account was shared by three flatmates; browser history shows the MetaMask extension used at times when the suspect was, on cell-site evidence, elsewhere; the seed phrase was found photographed in a cloud account belonging to a flatmate. **Lesson:** the device links the address to the household; it does not show who used it at the material time or who else held the seed. Charging on the device evidence alone invites a successful "someone else had the key" defence.

EXAMPLE 8 **A tracing analysis that ends without conclusive attribution**

A pension-scheme member loses 41 BTC to a romance fraud. The trace is clean for six hops, then the funds enter a series of equal-value CoinJoin transactions over three days, exit to twelve fresh addresses, and move to a Seychelles-incorporated exchange that does not respond to English orders and has no UK or US presence. An analytics label attributes two of the twelve exit addresses to the same "entity" on a behavioural heuristic. The expert reports that the movement to the CoinJoin is certain; that allocation of exits is probabilistic and does not meet a standard on which freezing relief could fairly be sought against the twelve; and that the exchange label is unverified. Counsel advises reporting to law enforcement, registering the loss with the exchange in case of a future freeze, and not spending further on tracing. **Lesson:** a candid negative conclusion is a legitimate and valuable expert output; pressing on with weak inference would risk innocent third parties and the client's costs.

21 Common mistakes and technical limitations

Most failures in crypto evidence are not failures of technology. They are failures to say what was assumed.

21.1 Common mistakes

Mistake	Consequence	Avoid by
Treating an analytics label as proof of ownership	Wrong defendant; freezing innocent accounts; credibility loss	Corroborate with the labelled entity; describe as unverified until confirmed
Conflating tracing with attribution	Pleadings assert identity the evidence does not support	Separate sections and separate findings
Not stating the tracing method, or changing it	D'Aloia: claim fails against the exchange	Method in the instruction and in the report; supplemental report for any change
Using a fast method without disclosing the trade-off	Smithers: false-positive freezes; full-and-frank-disclosure risk	Candid limitations section; UTXO for Bitcoin
Mixing chains or mis-scaling decimals	Schedule of loss wrong by orders of magnitude	Name chain, contract and decimals for every figure
Ignoring failed transactions and gas-funding transfers	Lost attribution leads and evidence of intent	Include all transactions from and to the address
Relying on screenshots	Unauthenticated; challengeable	Capture raw data with block hash and time; keep screenshots as illustration only
Putting a seed phrase or key in a bundle, report or email	Assets can be taken by anyone who sees it	Restricted-access exhibit; describe, do not reproduce
Typing a found seed into a wallet to "check the balance"	Exposure of the key; possible allegation of tampering; alteration of evidence	Watch-only via xpub in an isolated environment; log the act
Assuming an empty wallet is empty	Missed assets under other derivation paths or a passphrase	Scan all standard paths (44', 49', 84', 86') and record gap limits; note passphrase possibility
Pleading conversion	Struck out (Yuen v Li)	Proprietary claim, constructive trust, restitution, deceit, conspiracy
Serving on the wrong exchange entity, or not at all	No freeze; jurisdiction challenge; Daburn stay	Identify the entity from the terms of service; serve by every permitted channel; prove receipt
Forgetting collateral-use restrictions	Contempt risk when material is passed to police or used abroad	Build the carve-out into the order (section 17.5 C)
Letting exchange accounts close before export	Loss of the client's own history and API data	Export everything on day one
Treating Tether's freeze as the remedy	Freeze lifted; no proprietary finding; litigation risk	Court order plus freeze
Time-zone errors	Sequence of events wrong; alibi evidence mis-read	UTC and block numbers everywhere

21.2 Technical limitations to state in any report

- Heuristic clustering has published error rates and is defeated by CoinJoin, PayJoin, exchange batching and address reuse patterns.
- Cross-chain swaps, instant exchangers and mixers break the cryptographic link; continuation is inference.
- Privacy coins hide sender, amount and recipient; Monero's planned replacement of ring signatures (FCMP++) had not activated by September 2026 and claims of reliable Monero tracing should be treated with caution.
- Layer-2 data may not be recoverable from the base chain after the pruning window; Lightning payments leave no public record at all.

- Explorer "internal transactions" and labels are derived, not stored; they vary by explorer and change over time.
- Unconfirmed transactions are replaceable; mempool observations are not consensus data and are not retained.
- Post-EIP-7702 an Ethereum EOA may execute code; post-ERC-4337 the transaction sender may be a bundler; the payer of gas may not be the actor.
- MPC wallets have no seed phrase to seize; one device is insufficient to move funds.
- A modern browser-wallet vault cannot be decrypted without the password; the address list usually can be recovered.
- Exchange records depend on the exchange's data quality: duplicates, time-zone inconsistencies and incomplete address lists are common.

22 Question banks: client, opponent and provider

The questions below are intended to be asked in the first meetings and in correspondence. Their purpose is to fix the facts before any tracing or application is undertaken.

22.1 Questions for the client

1. Which assets, on which blockchains, in what amounts? Do you have the transaction hashes?
2. Which addresses do you control, and how (which wallets, which devices, which seed phrases, who else has access)?
3. Where is every copy of every seed phrase and private key now? Has anyone else ever seen them?
4. Which exchange accounts do you hold, in which names and entities, and have you exported the full history and API data?
5. How did the assets leave your control: an instruction you gave, a compromised device, a phishing link, a "platform" you deposited into, an employee?
6. Has anything been moved, sold, converted or "recovered" since the loss? By whom?
7. Have you contacted the exchange, the issuer, the police or a "recovery service"? What did you send them?
8. What communications exist with the counterparty (Telegram, WhatsApp, email, platform chat)? On which devices?
9. Which devices were used for the wallet and the exchange accounts? Are they still available and unchanged?
10. Did you use a hardware wallet? Where is it? Has anyone attempted the PIN?
11. What do your tax or accounting records say about your holdings and addresses?
12. Is any of the crypto held for or with anyone else (partner, company, clients, joint venture)?
13. Have you signed any message from any address, or can you now?
14. What is the realistic value at stake and what budget is proportionate?

22.2 Questions for the opponent (or persons unknown once identified)

1. Identify every address you controlled between [dates], and how each was controlled.
2. Identify every exchange, custodian and broker account you held or used, and every account used on your behalf.
3. State whether you hold, or have held, the seed phrase or private key for address [X], and who else has.
4. Explain the source of the ETH (or other native asset) used to fund gas at address [X] on [date].
5. Explain each internal transfer from account [UID] to account [UID] on [date].
6. Identify the person on whose instructions each transfer from address [X] was made.
7. State whether any funds received at address [X] were received as a purchaser for value, and produce the contract, the price and the payment.
8. Produce your Telegram, WhatsApp and email communications with [handle] between [dates].
9. Confirm the devices used to access address [X] and preserve them.
10. Explain the transactions on [date] that were reverted (failed) at address [X].

22.3 Questions for the forensic or eDisclosure provider

1. Which chains and asset standards can you trace, and with which tools (name, version, licence)?
2. What tracing method will you apply to each chain and why? Will it be stated in the report before the analysis?
3. How do you treat mixed funds, and how will you show fairness between competing victims?
4. How do you distinguish ledger facts from heuristic inference and from labels in your schedules?
5. Can you provide the analytics platform's methodology documentation and the date and provenance of each label relied on?
6. How will you capture and preserve the raw data (node or explorer, block hash, time, hashes of captures)?

7. How will you handle seed phrases and keys found on devices: storage, access control, logging, watch-only derivation?
8. What is your approach to encrypted wallet vaults and to live memory capture?
9. Have you given evidence in an English court on crypto tracing, and have your reports been the subject of adverse comment?
10. Are you accredited or aligned to ISO 17025, and do you work to ISO/IEC 27037 and 27042 and the FSR Code (for criminal work)?
11. What are the data-protection arrangements for exchange productions and third-party personal data?
12. What are the limitations you expect in this matter, and at what hop do you expect confidence to fall?
13. Will you preserve working files and intermediate schedules so that another analyst can reproduce the trace?
14. What is the cost to trace to the first identifiable service per chain, and the cost of each further stage?

23 Checklists and the evidence-and-attribution matrix

Two checklists and one matrix. The first checklist governs obtaining records; the second governs reviewing blockchain evidence served by the other side or produced by your own expert. The matrix is the working document for attribution.

23.1 Checklist: counsel seeking crypto-related records

- ☐ Chain, asset standard and token contract identified for every transaction.
- ☐ Transaction hashes, addresses, block numbers and UTC times listed in a schedule.
- ☐ Correct provider legal entity and its legal-process channel identified; FCA register checked.
- ☐ Provider's published data categories and retention periods reviewed; request tailored.
- ☐ Preservation notice sent and acknowledged.
- ☐ Issuer freeze request considered for stablecoins (in parallel with court relief).
- ☐ Route chosen: voluntary, NPO/BT, CPR 31.17, 1782, letter of request, MLA/POCA.
- ☐ Permission to serve out under PD6B 3.1(25) sought for foreign information orders.
- ☐ LMN v Bitflyer safeguards drafted: collateral use, costs, damages, local-law carve-out, confidentiality, gagging period.
- ☐ Carve-out for sharing with law enforcement and foreign proceedings included.
- ☐ Travel Rule records (MLR 2017 regs 64A to 64G) requested from UK firms.
- ☐ Linked-account and shared-identifier search requested.
- ☐ Native format, data dictionary and custodian certificate requested.
- ☐ Lawful basis and use restriction stated for personal data; confidentiality regime in place.
- ☐ Client's own exchange history and API data exported before any account is frozen.
- ☐ Diary for follow-up, next-hop requests and undertakings compliance.

23.2 Checklist: counsel reviewing blockchain evidence

- ☐ Is the raw transaction data exhibited, with block hash and capture time, or only screenshots?
- ☐ Is the tracing method stated before the analysis, and is it appropriate to the ledger model?
- ☐ Was the method applied consistently? Does the arithmetic reconcile at every hop?
- ☐ How are mixed funds allocated, and are other victims treated comparably?
- ☐ Are labels dated and sourced? Have they been corroborated by the labelled entity?
- ☐ Are inferences (change, clustering, cross-chain, mixer exits) marked as such with stated confidence?
- ☐ Are failed transactions and gas-funding transfers included?
- ☐ Are the chain, contract and decimals correct for every figure?
- ☐ Are all times in UTC with sources; is the block number given?
- ☐ Does the report separate tracing from attribution; is every attribution tied to identified off-chain evidence?
- ☐ Does the report distinguish control from ownership, authorisation, agency and knowledge?
- ☐ Are tool names, versions and heuristics disclosed; is the platform's methodology documentation available?
- ☐ Were any steps taken for speed, and were they disclosed to the court?
- ☐ Are working files preserved so that the analysis can be reproduced?
- ☐ Does the report comply with CPR 35 / PD35 (or CrimPR 19), including the statement of truth and the substance of instructions?
- ☐ Does the report contain any key material that should not be there?

23.3 Model evidence-and-attribution matrix

Complete one row per address (or exchange account) of interest. Score each column as Direct (D), Corroborating (C), Absent (A) or Contradicting (X), and record the source and date. Role asserted means control, authorisation, beneficial ownership or agency. An attribution should not be pleaded as established unless at least one D and one independent C are present and no X is unexplained.

Address / account	Ledger facts (hashes, hops)	Exchange KYC	Bank / fiat leg	Device or key evidence	Signed msg / admission	IP / session	Comms citing address	Analytics label	Candidate person	Role asserted	Overall
0x4c…f1	D (schedule 3, hops 1 to 4)	D (Coinbase, 1782 return, 12 May)	C (personal a/c ending 9921)	A	A	C (office IP range)	X (said to be a supplier; none found)	C ("Coinbase" deposit)	Finance director	Control; beneficial owner	Made out, subject to the X
TQx…7h	D	D (mule account, THB)	A	A	A	C (shared device with 2 other UIDs)	A	C	Unknown operator of 3 UIDs	Control as agent for unknown principal	Operator known; principal not
bc1q…m2	D	A (self-hosted)	A	A	A	A	A	A	None	n/a	Not attributed

24 Red flags

Indicators that a crypto matter needs urgent or specialist attention, grouped by the moment at which they usually appear.

24.1 On first instruction

- The client cannot say which chain or asset was involved, or has only a screenshot of a "platform dashboard": the platform may never have held real assets.
- The client has already "verified" a found seed phrase by typing it into a wallet, or has shared it with a "recovery service".
- A recovery firm has promised guaranteed recovery for an upfront fee: a common secondary fraud.
- Assets are in a stablecoin at an exchange: freeze opportunity measured in hours.
- A hardware wallet has been found and someone has been trying PINs.
- The suspect device is live and a wallet may be unlocked: memory capture before shutdown.

24.2 In the tracing evidence

- The method is not stated, or the report says FIFO but the schedule does not follow it.
- The schedule does not reconcile hop by hop; duplicates; timestamps in different zones.
- Labels without dates or provenance; two platforms disagree.
- A cluster including an exchange hot wallet or a known CoinJoin coordinator: probable cluster collapse.
- Cross-chain or mixer links stated as fact.
- "The address belongs to X" with no off-chain source.
- Amounts that are exactly round after a supposed swap or bridge: probably the wrong leg.

24.3 In the opponent's or provider's conduct

- An exchange that does not engage with English process (indemnity costs in Wilden); nested exchanges; entities incorporated in non-responsive jurisdictions.
- An account whose activity is inconsistent with declared income or occupation (notice; D'Aloia).
- Automatic compliance blocks lifted without documented inquiry.
- Withdrawals immediately after each deposit; use of fresh addresses per withdrawal; VPN-only logins.
- Exposure to designated addresses or to exchanges designated by the UK in May 2026.
- A witness who denies control of an address but whose device shows repeated explorer look-ups of it.

25 When to involve a digital forensic expert

Many crypto matters can be triaged by a well-informed litigation team with a block explorer. The following situations call for a digital forensic and tracing specialist from the outset.

Situation	Why a specialist is needed
Any without-notice application relying on tracing	The evidence must satisfy Part 35-style discipline and full and frank disclosure; Smithers and D'Aloia show the cost of getting it wrong.
Mixed funds, multiple victims, pooled exchange wallets	Allocation method, fairness between victims and reconciliation require expertise and defensible tooling.
Cross-chain movement, bridges, swap services, layer 2	Correlation across chains and recovery of pruned or off-chain data.
Bitcoin tracing for in-specie recovery	UTXO-level analysis endorsed in Smithers [2026] EWHC 1907 (Comm).
Seized or disputed devices, hardware wallets, seed phrases	Imaging, memory capture, vault recovery, safe watch-only derivation, restricted handling, chain of custody.
Corporate treasury, multisig, MPC and custody disputes	Reconstructing who authorised what from console logs, policy engines and identity providers.
Challenging the other side's analytics evidence	Heuristic error rates, label provenance, method consistency, reproduction of the trace.
Ethereum accounts with delegation (EIP-7702) or account abstraction	Determining the actor behind a transaction whose sender is a bundler or whose EOA runs code.
Privacy coins, mixers and CoinJoin	Establishing what can and cannot be said, so that the report is candid and the client's budget is protected.
Criminal proceedings	FSR Code compliance, CPIA scheduling of analytics material, defence review of prosecution attribution.
Insolvency and estate matters with lost or disputed keys	Systematic recovery of key material from devices, backups and cloud; derivation-path scanning; valuation at date.

26 Practical recommendations

Twelve recommendations for preserving, analysing, tracing, attributing and presenting crypto-asset evidence.

1. **Secure the client's own keys and devices before doing anything else**, and treat every seed phrase encountered as a restricted-access exhibit.
2. **Fix the facts in a schedule on day one**: chain, asset, contract, hashes, addresses, UTC times, blocks.
3. **Preserve and freeze in parallel**: preservation notices, issuer freeze requests, and a without-notice application with candid limitations.
4. **Match the tracing method to the ledger** and state it before the analysis; UTXO for Bitcoin, a stated allocation rule for account and token assets; never change it silently.
5. **Trace to the first identifiable service, then obtain its records** before spending further on chain analysis.
6. **Treat labels and clusters as leads**; corroborate every attribution with at least two independent off-chain sources and record them in a matrix.
7. **Keep tracing and attribution in separate sections** of every report, pleading and witness statement, and separate control from ownership, authorisation, agency and knowledge.
8. **Draft disclosure orders with the LMN v Bitflyer safeguards and a law-enforcement carve-out**, and cite the Travel Rule regulations against UK firms.
9. **Use the US routes where a US provider is in the chain**: 1782 for civil claimants, the Data Access Agreement and exchange portals for law enforcement.
10. **Capture raw data, not screenshots**, with block hash and time; preserve working files so the trace can be reproduced.
11. **Date-stamp every technical and legal statement**: block heights, delegation status, labels, sanctions listings, regulatory perimeters and the state of PD57AD reform all move.
12. **Know when to stop.** A candid report that the trail ends at a mixer or a non-responsive exchange, with a recommendation to report to law enforcement and register the loss, is often the best advice a client can receive.

27 Glossary

Account abstraction (ERC-4337)
Ethereum standard under which smart-contract wallets submit "UserOperations" through bundlers to an EntryPoint contract; the on-chain sender is the bundler.

Address
Public identifier derived from a public key or script to which value is assigned on a ledger.

Attribution
Identifying the person or entity that controlled an address or account at a time.

Bankers Trust order
Court order requiring a third party (bank, exchange) to disclose information to locate and preserve the claimant's traceable assets.

BIP-32 / 39 / 44
Bitcoin standards for hierarchical deterministic wallets, mnemonic seed phrases and derivation paths respectively.

Block
A batch of transactions committed to the ledger together with a reference to the previous block.

Blockchain
A distributed ledger arranged as a chain of blocks.

Bridge
A mechanism locking an asset on one chain and issuing an equivalent on another.

Change output
In the UTXO model, the output returning surplus input value to the payer.

Clustering
Grouping addresses believed to share a controller, by heuristic.

CoinJoin
A Bitcoin transaction combining many users' inputs and outputs to defeat clustering.

Cold wallet
Keys held offline (hardware device, paper, metal).

Confirmation
A block built on top of the block containing a transaction.

Consensus mechanism
The rule by which nodes agree on the next block (proof of work, proof of stake).

Crypto wallet freezing order (CWFO)
Magistrates' court order under POCA 2002 ss.303Z36 to 303Z40 freezing cryptoassets held with a UK-connected service provider.

Custodial wallet
A wallet whose keys are held by a service provider for the customer.

DeFi
Decentralised finance: financial services implemented as smart contracts without a custodian.

Derivation path
The route from a seed to a particular key in an HD wallet (e.g. m/84'/0'/0'/0/0).

DEX
Decentralised exchange: a smart contract swapping tokens from pooled liquidity.

Digital signature
Cryptographic proof, made with a private key, that a message was authorised by the key holder.

EIP-1559
Ethereum fee mechanism with a burned base fee and a priority fee.

EIP-7702
Ethereum change (May 2025) allowing an EOA to delegate to contract code.

EOA
Externally owned account: an Ethereum account controlled by a private key.

ERC-20 / ERC-721 / ERC-1155
Ethereum token standards: fungible, non-fungible and semi-fungible respectively.

Event log
Data emitted by a smart contract during execution; token transfers are recorded this way.

Exchange-hosted address
An address controlled by a centralised exchange.

Finality
The point past which a protocol treats a block as irreversible.

Following
Tracking the same asset from hand to hand (contrast tracing).

Gas
The unit of computational work on Ethereum, paid for in ETH.

Hash
A fixed-length fingerprint of data; a transaction ID is the hash of the transaction.

HD wallet
Hierarchical deterministic wallet generating unlimited keys from one seed.

Hot wallet
Keys held online for operational use; at an exchange, the pooled wallet serving withdrawals.

KYC
Know-your-customer: identity verification by a regulated service.

Layer 2
A network settling to a base chain in batches (rollups; Lightning).

Mempool
A node's set of unconfirmed transactions; not consensus data.

Miner / validator
The participant assembling and proposing blocks under proof of work / proof of stake.

Mixer
A service or contract pooling funds to obscure the link between deposits and withdrawals.

MPC
Multi-party computation: a signing arrangement in which the key never exists whole.

Multisig
A wallet requiring m of n keys to sign.

Node
A computer running the network software and holding a copy of the ledger.

Nonce
On account-model chains, the per-account transaction counter.

Norwich Pharmacal order
Court order requiring a third party mixed up in wrongdoing to identify the wrongdoer.

OP_RETURN
A Bitcoin output type carrying arbitrary data; used for service of proceedings in Smithers (2026).

OTC broker
A person or desk facilitating crypto transactions outside an exchange's order book.

Passphrase (BIP-39)
An optional extra word that produces a different wallet from the same seed phrase.

Peel chain
A sequence of transactions each paying out a small amount and passing the remainder to a new change address.

Private key
The secret number that authorises spending from an address.

Proprietary injunction
Injunction preserving specific assets in which the claimant claims a proprietary interest.

Public key
The shareable counterpart of a private key, used to verify signatures.

Replace-by-fee (RBF)
Replacing an unconfirmed Bitcoin transaction with a higher-fee version.

Reorganisation (reorg)
Abandonment of one chain branch in favour of another.

Seed phrase
12 to 24 words encoding the master secret of an HD wallet.

Self-hosted (unhosted) wallet
A wallet whose keys are held by the user.

Smart contract
Program code deployed on a blockchain and executed by the network.

Stablecoin
A token designed to hold a stable value against a reference asset.

Sweep
Moving all assets from a wallet to another, e.g. by law enforcement after seizure.

Token
An asset created by a smart contract on a host chain.

Tracing
Identifying substitute assets representing the claimant's value (contrast following); colloquially, following value across a ledger.

Transaction
A signed, broadcast instruction re-assigning value or calling a contract.

Travel Rule
Requirement to collect and transmit originator and beneficiary information on crypto transfers (MLR 2017 regs 64A to 64G).

UTXO
Unspent transaction output: Bitcoin's unit of value.

Wallet
Software or hardware managing keys and addresses; it does not contain coins.

Worldwide freezing order
Injunction restraining a defendant from dealing with assets anywhere, subject to exceptions.

xpub
Extended public key from which all non-hardened child addresses can be derived without any private key.

28 References and authorities

All online sources accessed 3 and 4 September 2026 unless stated. Neutral citations are given where they exist; Find Case Law (The National Archives) URLs are given for judgments because BAILII restricts automated access. Case names use the short forms adopted in the text.

Legislation and rules (UK)

1. Property (Digital Assets etc) Act 2025 (c. 29). legislation.gov.uk/ukpga/2025/29
2. Proceeds of Crime Act 2002, Part 5 Chapters 3C to 3F (ss.303Z20 to 303Z40) as inserted by the Economic Crime and Corporate Transparency Act 2023 (c. 56), Schs 8 and 9. legislation.gov.uk/ukpga/2002/29/part/5/chapter/3D; legislation.gov.uk/ukpga/2023/56/schedule/9
3. Code of Practice issued under s.303Z25 POCA 2002 (Recovery of Cryptoassets: search powers), in force 26 April 2024 (SI 2024/551). gov.uk POCA codes of practice; SI 2024/551
4. Home Office Circulars 004/2024 and 005/2024 (cryptoasset confiscation and forfeiture provisions). gov.uk Circular 005/2024
5. Magistrates' Courts (Detention, Freezing and Forfeiture of Cryptoassets) Rules 2024, SI 2024/1043. legislation.gov.uk/uksi/2024/1043
6. Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692, regs 14A, 40, 56 to 60 and 64A to 64G (Travel Rule, inserted by SI 2022/860, in force 1 September 2023). legislation.gov.uk/uksi/2022/860/regulation/5
7. Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026, SI 2026/102 (full commencement 25 October 2027). legislation.gov.uk/uksi/2026/102
8. Financial Services and Markets Act 2023 (c. 29). legislation.gov.uk/ukpga/2023/29
9. Data (Use and Access) Act 2025 (c. 18); main data-protection provisions commenced 5 February 2026. legislation.gov.uk/ukpga/2025/18
10. Crime (International Co-operation) Act 2003 (c. 32). legislation.gov.uk/ukpga/2003/32
11. Crime (Overseas Production Orders) Act 2019 and SI 2020/38 (designation of the UK-US Data Access Agreement). legislation.gov.uk/uksi/2020/38
12. Regulation of Investigatory Powers Act 2000, ss.49 and 53. legislation.gov.uk/ukpga/2000/23/section/49
13. Civil Procedure Rules Part 31; PD57AD; Part 35; PD6B; Part 34 (34.13, 34.16 to 34.21). CPR Part 31; PD57AD; CPR Part 35; PD6B
14. Criminal Procedure and Investigations Act 1996; Attorney General's Guidelines on Disclosure 2024 (effective 29 May 2024). gov.uk AG Guidelines
15. Forensic Science Regulator Code of Practice, version 2 (in force 2 October 2025); FSR-GUI-0001 Declarations Guidance (March 2026). gov.uk FSR Code
16. Civil Evidence Act 1995 ss.4 and 9; Criminal Justice Act 2003 ss.114 to 117.

Cases (England and Wales unless stated)

1. AA v Persons Unknown [2019] EWHC 3556 (Comm). bailii.org
2. Ion Science Ltd v Persons Unknown (Comm, Butcher J, 21 December 2020, unreported).
3. Fetch.AI Ltd v Persons Unknown [2021] EWHC 2254 (Comm). bailii.org
4. Wang v Darby [2021] EWHC 3054 (Comm).
5. Osbourne v Persons Unknown [2022] EWHC 1021 (Comm); Osbourne v Persons Unknown Category A [2023] EWHC 39 (KB). caselaw.nationalarchives.gov.uk/ewhc/kb/2023/39
6. D'Aloia v Persons Unknown [2022] EWHC 1723 (Ch); D'Aloia v Persons Unknown Category A [2024] EWHC 2342 (Ch). caselaw.nationalarchives.gov.uk/ewhc/ch/2024/2342
7. LMN v Bitflyer Holdings Inc [2022] EWHC 2954 (Comm). caselaw.nationalarchives.gov.uk/ewhc/comm/2022/2954
8. Jones v Persons Unknown [2022] EWHC 2543 (Comm); Jones v Persons Unknown (No 2) [2025] EWHC 1823 (Comm). caselaw.nationalarchives.gov.uk/ewhc/comm/2025/1823
9. Tulip Trading Ltd v van der Laan [2023] EWCA Civ 83. judiciary.uk
10. Piroozzadeh v Persons Unknown [2023] EWHC 1024 (Ch). caselaw.nationalarchives.gov.uk/ewhc/ch/2023/1024
11. Boonyaem v Persons Unknown Category A [2023] EWHC 3180 (Comm). caselaw.nationalarchives.gov.uk/ewhc/comm/2023/3180
12. Mooij v Persons Unknown [2024] EWHC 814 (Comm). caselaw.nationalarchives.gov.uk/ewhc/comm/2024/814
13. Daburn v Persons Unknown [2025] EWHC 356 (Comm). caselaw.nationalarchives.gov.uk/ewhc/comm/2025/356
14. Murry v Persons Unknown [2025] EWHC 1664 (Comm). caselaw.nationalarchives.gov.uk/ewhc/comm/2025/1664

15. Smithers v Persons Unknown [2026] EWHC 207 (Comm); Smithers v Persons Unknown [2026] EWHC 1907 (Comm). caselaw.nationalarchives.gov.uk/ewhc/comm/2026/207; caselaw.nationalarchives.gov.uk/ewhc/comm/2026/1907
16. Yuen v Li [2026] EWHC 532 (KB). caselaw.nationalarchives.gov.uk/ewhc/kb/2026/532
17. Wilden v Person Unknown and Huobi Global S.A. [2026] EWHC 1355 (KB). caselaw.nationalarchives.gov.uk/ewhc/kb/2026/1355
18. Sachs v Snape [2026] EWHC 1059 (Comm). caselaw.nationalarchives.gov.uk/ewhc/comm/2026/1059
19. Van Rooyen v Respondents Listed in the Schedule [2026] EWHC 1286 (Ch). caselaw.nationalarchives.gov.uk/ewhc/ch/2026/1286
20. Stanford Asset Holdings Ltd v AfrAsia Bank Ltd [2023] UKPC 35; Cameron v Liverpool Victoria Insurance Co Ltd [2019] UKSC 6; Wolverhampton City Council v London Gypsies and Travellers [2023] UKSC 47; OBG Ltd v Allan [2007] UKHL 21; TSB Private Bank International SA v Chabra [1992] 1 WLR 231; Bankers Trust Co v Shapira [1980] 1 WLR 1274; Norwich Pharmacal Co v Customs and Excise Commissioners [1974] AC 133.
21. ByBit Fintech Ltd v Ho Kai Xin [2023] SGHC 199 (Singapore). elitigation.sg
22. United States v Sterlingov, No. 21-cr-399 (RDM) (D.D.C., memorandum opinion 29 February 2024); Van Loon v Department of the Treasury, 122 F.4th 549 (5th Cir. 2024); ZF Automotive US Inc v Luxshare Ltd, 596 U.S. 619 (2022); Intel Corp v Advanced Micro Devices Inc, 542 U.S. 241 (2004).

Official publications, regulators and guidance

1. Law Commission, Digital Assets: Final Report (Law Com No 412, June 2023); Supplemental Report and Draft Bill (July 2024); Digital assets and electronic trade documents in private international law, Consultation Paper (June 2025). lawcom.gov.uk/project/digital-assets
2. UK Jurisdiction Taskforce, Legal Statement on Cryptoassets and Smart Contracts (2019); Legal Statement on Digital Assets and English Insolvency Law (2024); Report on Control of Digital Assets (27 March 2026). lawtechuk.io
3. FCA, Cryptoassets: AML/CTF regime (MLR registration); New regime for cryptoasset regulation (gateway opening 30 September 2026); Policy Statements PS26/9 to PS26/13 (30 June 2026); Financial promotions: marketing to UK consumers; Statement on Travel Rule expectations (17 August 2023). fca.org.uk cryptoassets AML/CTF; fca.org.uk new regime; fca.org.uk Travel Rule statement
4. JMLSG, Part II Sector 22 and Annex 22-I Cryptoasset Transfers (Travel Rule) (HM Treasury approved April 2025). jmlsg.org.uk
5. OFSI, Cryptoassets Threat Assessment (21 July 2025). gov.uk OFSI threat assessments
6. NCA UKFIU, SARs Annual Report 2025. nationalcrimeagency.gov.uk
7. Bank of England, Regulatory regime for sterling-denominated systemic stablecoins: consultation (November 2025) and policy statement with draft Code of Practice (June 2026). bankofengland.co.uk
8. ICO, Distributed ledger technologies guidance (August 2025, under review). ico.org.uk; EDPB Guidelines 02/2025 on processing of personal data through blockchain technologies. edpb.europa.eu
9. Home Office, Mutual Legal Assistance Guidelines; CPS, International prosecution guidance. cps.gov.uk
10. Judiciary of England and Wales, Disclosure Review Working Group: PD57AD survey summary (July 2026). judiciary.uk
11. HHJ Pelling KC, "Issues in Crypto Currency Claims", DIFC Courts seminar (13 November 2023). judiciary.uk
12. FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs (seventh update, July 2026); Recommendations 15 and 16. fatf-gafi.org
13. US Department of Justice / IRS-CI, press releases on Samourai Wallet sentencing (November 2025) and Terraform (Do Kwon) plea and sentence (2025). irs.gov
14. Coinbase, Transparency Report 2025. coinbase.com; Binance Law Enforcement Request System. binance.com

Technical standards and specifications

1. Bitcoin Improvement Proposals: BIP-32 (HD wallets), BIP-39 (mnemonics), BIP-44 (derivation), BIP-125 (opt-in RBF), BIP-173/350 (bech32/bech32m). github.com/bitcoin/bips
2. Bitcoin Core release notes 28.0, 30.0 (10 October 2025) and 31.0 (19 April 2026). bitcoincore.org/en/releases
3. Ethereum Improvement Proposals: EIP-20, EIP-721, EIP-1155, EIP-1559, EIP-4337, EIP-4844, EIP-7702. eips.ethereum.org; Ethereum roadmap pages for Dencun, Pectra and Fusaka. ethereum.org/en/roadmap
4. Tether, Transparency and supported chains; Update on transition plan for legacy blockchains (2025); Announcement of KPMG audit opinion (13 August 2026). tether.io/news
5. ISO/IEC 27037:2012 (identification, collection, acquisition and preservation of digital evidence); ISO/IEC 27041; ISO/IEC 27042; ISO/IEC 27043; ISO/IEC 27050 series (electronic discovery). iso.org
6. ACPO/NPCC Good Practice Guide for Digital Evidence, v5 (2012).
7. MetaMask, How to recover your Secret Recovery Phrase (vault location); MetaMask/browser-passworder. support.metamask.io

Academic and analytical sources

1. Meiklejohn S et al, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names", IMC 2013. cseweb.ucsd.edu
2. Möser M and Narayanan A, "Resurrecting Address Clustering in Bitcoin", Financial Cryptography 2022. arxiv.org/pdf/2107.05749
3. Gong Y, Chow K-P, Ting H-F and Yiu S-M, "Analyzing the Error Rates of Bitcoin Clustering Heuristics", Advances in Digital Forensics XVIII (2022). link.springer.com
4. Horsman G, "ACPO principles for digital evidence: time for an update?", Forensic Science International: Reports (2020).
5. Chainalysis, 2026 Crypto Crime Report; TRM Labs, 2026 Crypto Crime Report (both estimating 2025 illicit flows of roughly $154 to 158 billion). trmlabs.com
6. Clifford Chance, briefing on D'Aloia (October 2024); Freshfields, "Tracing cryptoassets in the English High Court: what Wilden means for recovery" (2026); Norton Rose Fulbright, "When blockchain analytics meet the Daubert test" (2024). cliffordchance.com
7. Financial Markets Law Committee, Digital Assets and Governing Law. fmlc.org

Items flagged in the text as uncertain (for example the status of the Crime and Policing Act 2026 amendments to POCA, the Glamsterdam upgrade, the retrial in US v Storm, and the ICO's revised DLT guidance) should be re-checked against the primary source before reliance.

29 Disclaimer, and how a specialist laboratory can assist

DISCLAIMER

This publication provides general information about cryptocurrency assets, their investigation, tracing, attribution and disclosure for a professional legal audience. It does not constitute legal advice, expert evidence, or advice on any particular matter, and it should not be relied on as such. The law, procedural rules, regulatory requirements and technology described change frequently; positions are stated as at 4 September 2026 and online sources were accessed on 3 and 4 September 2026. Readers should verify the current position and take advice from a suitably qualified lawyer, and where appropriate instruct a digital forensic or blockchain-tracing expert, before acting. Case names, addresses, hashes and figures in the worked examples are fictitious. Computer Forensics Lab Ltd accepts no liability for any loss arising from reliance on this publication.

How a specialist UK electronic disclosure and digital forensic laboratory can assist

A laboratory that combines digital forensics, electronic disclosure and blockchain tracing under one roof can support a legal team at each stage described in this guide, in civil, criminal, insolvency and regulatory matters:

- **Rapid triage and first-pass tracing** to the first identifiable service on each chain, with a ledger-appropriate method stated in advance and a candid limitations section suitable for a without-notice application.
- **Preservation and collection** of devices, hardware wallets, browser-wallet vaults, mobile applications, cloud accounts and exchange histories, with restricted-access handling of seed phrases and keys, watch-only derivation, and full chain of custody covering physical and cryptographic custody.
- **Exchange and provider disclosure support**: identifying the correct entity, drafting the technical schedules and identifiers for Bankers Trust, Norwich Pharmacal, CPR 31.17 and 1782 applications, and correlating productions to the chain.
- **Attribution analysis** built on the evidence-and-attribution matrix, distinguishing control from ownership, authorisation, agency and knowledge, and cross-checking analytics labels against primary records.
- **Expert evidence** under CPR Part 35 and CrimPR Part 19 from examiners with court experience, including review and challenge of the opposing side's blockchain-analytics evidence, reproduction of traces from preserved working files, and reports that separate source evidence, method, findings and opinion.
- **Corporate and custody matters**: reconstruction of who authorised transfers from multisig, MPC and custodian consoles, identity-provider and network logs, and internal investigations.
- **Electronic disclosure** of the surrounding ESI (email, chat, documents) on a hosted review platform integrated with the tracing schedules, within PD57AD, Part 31 and CPIA frameworks.

The lab operates an NPCC and ISO 17025 aligned practice and is registered with the ICO. Contact details follow.

SCAN TO SAVE
OUR CONTACT DETAILS

INSTRUCT THE LAB

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES
+44 (0)20 7164 6971

EMAIL
info@cflab.uk

E-DISCOVERY
e-discovery.uk

Cryptocurrency matters: first-pass tracing and preservation advice within one working day; restricted-access handling of seed phrases and hardware wallets; Part 35 and CrimPR 19 expert evidence; exchange disclosure schedules; review of opposing analytics evidence.

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom
cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace
CFL Electronic Evidence Series · Guide 7 · Cryptocurrency Assets: Investigation, Tracing, Attribution and Disclosure · September 2026 edition