COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Cryptocurrency and Blockchain Tracing

Following the Money on a Public Ledger, and Naming the Person Behind the Address

Cryptocurrency confounds the intuition that digital money is hard to trace. In fact most of it runs on public blockchains, permanent, open ledgers that record every transaction forever, so the movement of funds is more visible than in the banking system, not less. The difficulty is not seeing the transactions but two other things: the ledger records addresses, not names, so the flow must be tied to a person; and the on-chain record can be complicated deliberately by mixers, exchanges, chain-hopping and privacy techniques designed to break the trail. For a lawyer in fraud, asset recovery, divorce, insolvency or enforcement, this makes crypto both an unusually traceable asset and one that demands specialist analysis to follow and, crucially, to attribute. This guide sets out for UK lawyers how blockchains record value, how funds are traced across the ledger, how an address is linked to a real person through exchanges and off-chain evidence, and how tracing supports freezing, disclosure and recovery, with the honest limits of attribution kept firmly in view.

⏱ Estimated reading time: 25 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Cryptocurrency work combines on-chain tracing, following funds across public ledgers through mixers, bridges and exchanges, with the device and off-chain forensics that attribute an address to a person: wallet artefacts, exchange records, and the seed phrases and keys that prove control. The analysis supports freezing and proprietary injunctions, disclosure and asset recovery, and is reported under CPR Part 35 and CrimPR Part 19 with attribution stated at honest confidence.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ON-CHAIN TRACING & ATTRIBUTION | WALLET & EXCHANGE FORENSICS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: most cryptocurrency runs on public ledgers that record every transaction permanently, so funds are highly traceable, and the real work is attribution, tying an address to a person through exchanges, devices and off-chain evidence, and doing so at honest confidence despite mixers and other obfuscation.

How it records value (§3): a blockchain is a permanent public ledger of transactions between addresses, controlled by private keys held in wallets, so ownership means control of keys, and the transaction record is open to all. **Tracing (§4):** funds are followed address to address across the ledger with specialist analytics, through exchanges, bridges and services, building a picture of where value went. **Attribution (§5):** the ledger names addresses, not people, so linking an address to a person relies on exchange know-your-customer records, wallet artefacts on seized devices, seed phrases and keys, and behavioural clustering. **Obfuscation and limits (§6):** mixers, privacy coins and chain-hopping complicate the trail, and attribution is expressed at honest confidence, strong where an exchange or device ties it down, weaker where it rests on inference. **Deployment (§7):** freezing and proprietary injunctions, disclosure orders against exchanges, and tracing for asset recovery and enforcement.

- **The ledger is public and permanent:** most crypto transactions are visible forever, making funds highly traceable.
- **Ownership is control of keys:** a wallet holds the private keys; whoever controls them controls the funds.
- **Addresses are not names:** the ledger records addresses, so attribution to a person is the central task.
- **Exchanges and devices attribute:** know-your-customer records, wallet artefacts and seed phrases tie an address to a person.
- **State confidence honestly:** mixers and privacy tools complicate the trail; attribution is graded, not asserted.

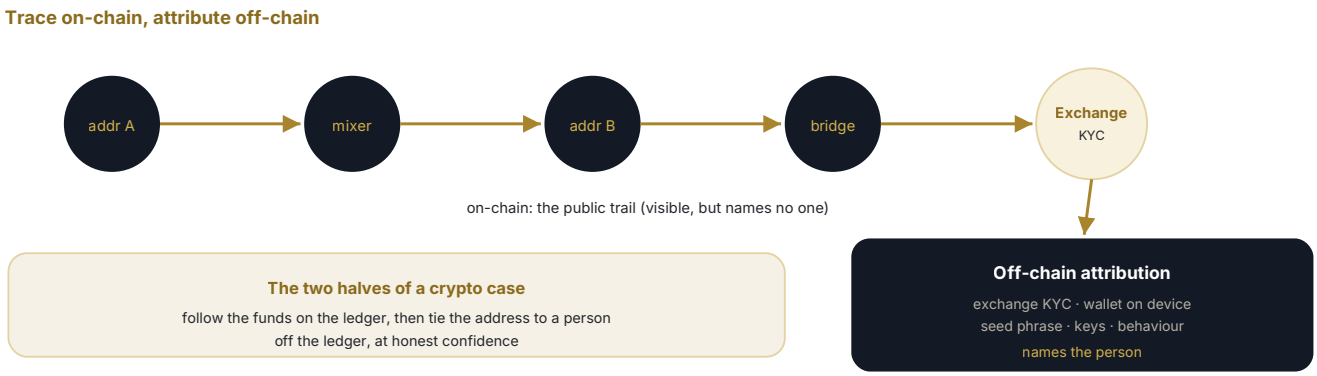

Figure 1 - a crypto case has two halves: on-chain tracing follows the visible funds through mixers, bridges and exchanges; off-chain attribution ties the address to a real person.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: visible money, hidden owners

People assume cryptocurrency is anonymous and untraceable, the money of the shadows. The truth is almost the opposite. Most cryptocurrencies, including the large ones, run on public blockchains: open, permanent ledgers that record every single transaction, forever, for anyone to see. Unlike a bank, which shows its records only to those with legal authority, a public blockchain shows everything to everyone, always. So the movement of funds is, in principle, more transparent than in the traditional financial system, not less: every transfer between addresses is there, timestamped and immutable, and a specialist can follow value across the ledger from one address to the next.

The real difficulty lies elsewhere, in two distinct places. First, the ledger records addresses, long strings of characters, not names. Seeing that funds moved from one address to another does not, by itself, tell you who controls either address. Bridging that gap, attribution, is the heart of crypto forensics, and it depends not on the blockchain alone but on off-chain evidence: the know-your-customer records that exchanges hold when someone cashes in or out, the wallet software and keys found on a seized device, a seed phrase written in a notebook, and patterns of behaviour that cluster addresses together. Second, the trail can be deliberately obscured. Mixers pool and shuffle funds to break the link between source and destination; bridges hop value between different blockchains; privacy coins conceal amounts and parties. None of this makes tracing impossible, but it makes it harder and demands that conclusions be stated at honest confidence rather than as false certainty. For the lawyer, the upshot is powerful: crypto is often more recoverable than clients fear and more traceable than opponents hope, provided the on-chain tracing is paired with disciplined off-chain attribution. This guide sets out how.

§ 0 3 · HOW IT RECORDS VALUE

How blockchains and wallets record value

- **The public ledger:** a blockchain is a shared, append-only record of transactions, replicated across many computers and effectively immutable, so every transfer between addresses is permanent and publicly visible: the transparency that makes tracing possible (§2).
- **Addresses and keys:** value sits at addresses controlled by private keys, so ownership is not registered in a name but proved by control of the key: whoever holds the key controls the funds, which makes keys and seed phrases central evidence (§5).
- **Wallets:** software or hardware that stores and uses the keys, from phone and desktop apps to hardware devices and exchange-hosted accounts, each leaving artefacts on devices and in accounts (guides 4, 5): the practical locus of control.
- **Exchanges and custodians:** services that convert crypto to and from traditional money and hold funds for users, and which, being regulated, collect know-your-customer identity records, the single richest attribution source (§5): the on-ramp and off-ramp where anonymity usually breaks.
- **Tokens, chains and contracts:** many currencies, tokens and smart-contract platforms, and bridges that move value between them, so a trail may cross several chains and services, requiring analysis that spans them (§4): the multi-chain reality.

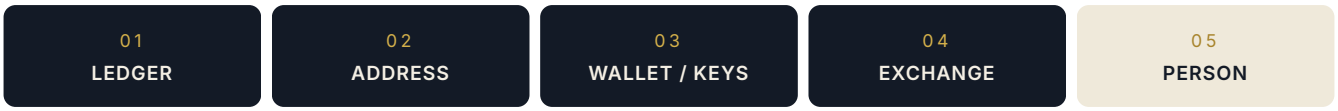

Figure 2 - from the public ledger to the person: the chain runs address to wallet to exchange, and it is the exchange and the device that finally supply the name.

§ 0 4 · TRACING

Tracing funds across the ledger

- **Following the flow:** funds followed transaction by transaction from a starting address across the ledger, using specialist blockchain-analytics tools that map the movement of value and label known services: the visible trail reconstructed (§2).
- **Identifying services:** the trail passing through recognisable exchanges, mixers, bridges and other services, each a point where the funds either become attributable (an exchange) or are obscured (a mixer): the map annotated with what each hop is (§5, §6).
- **Clustering:** addresses grouped into common-control clusters from on-chain behaviour (shared inputs, change patterns), so a person's or entity's holdings can be gathered even across many addresses: the estate of addresses assembled (§5).
- **Cross-chain tracing:** value followed across bridges from one blockchain to another, so chain-hopping does not end the trail, though it complicates it and demands multi-chain analysis (§6): the trail continued across chains.
- **Timing and value:** the amounts and timestamps of transfers reconciled with off-chain events (a fraud, a transfer request, an exchange deposit), so the on-chain flow is tied to the real-world facts (guide 96's timeline discipline): the ledger married to the matter.

§ 0 5 · ATTRIBUTION

Attribution: linking an address to a person

- **Exchange know-your-customer records:** the strongest attribution, where funds reach a regulated exchange, its identity records (name, documents, bank account) tie the depositing address to a real person, obtained by disclosure order or lawful request (§7): the point where the address gets a name.
- **Wallet artefacts on devices:** wallet software, addresses, transaction history and, critically, private keys or seed phrases recovered from a seized or examined device, proving control of the funds by the device's owner (guides 4, 5): control shown on the person's own hardware.
- **Seed phrases and keys:** a recovered seed phrase or private key demonstrating the ability to control an address, powerful evidence of ownership, found on devices, in notes, in backups and in cloud storage (§8): the proof of control itself.
- **Behavioural and open-source links:** addresses linked to people through reused addresses posted publicly, forum and social activity, transaction patterns and open-source intelligence (guide 129): the softer links that corroborate.
- **Attribution graded honestly:** the confidence of attribution stated plainly, strong where an exchange record or a key on the person's device ties it down, weaker where it rests on clustering or inference alone (guide 100): the honesty that survives challenge (§6).

§ 0 6 · OBFUSCATION AND HONEST LIMITS

Obfuscation, honest limits and confidence

- **Mixers and tumblers:** services that pool many users' funds and redistribute them to break the link between source and destination, complicating but not always defeating tracing, since analytics and timing can sometimes see through them: an obstacle, honestly assessed, not an automatic dead end.
- **Chain-hopping and bridges:** value moved across blockchains to shed analytics coverage, followed by multi-chain tracing where the bridges are understood, with the trail's confidence noted at each hop (§4).
- **Privacy coins:** currencies designed to conceal amounts and parties, where on-chain tracing is genuinely limited, so attribution leans harder on off-chain evidence, exchanges, devices, keys (§5): the honest limit acknowledged.
- **Attribution is not the ledger's:** the core limit, that the blockchain proves a flow of value between addresses, not who controls them, so naming a person always depends on off-chain evidence and is stated at its true confidence (§5).
- **Volatility and reconciliation:** value expressed in the coin and, where relevant, converted at documented rates and times, since prices move sharply, and the tracing distinguishing the flow of coins from their fluctuating fiat value (guide 96).

§ 0 7 · DEPLOYMENT

Deployment: freezing, disclosure and recovery

- **Freezing and proprietary injunctions:** tracing supporting freezing orders and proprietary injunctions over identified crypto assets and against the exchanges holding them, so funds are secured before they move further (guide 98's asset-tracing context): the trail turned into a freeze.
- **Disclosure orders against exchanges:** orders (including against persons unknown, and third-party disclosure against exchanges) compelling the know-your-customer and account records that attribute an address, the mechanism that turns an on-chain trail into a named respondent (§5): the exchange compelled to name the holder.
- **Asset recovery and enforcement:** the traced and attributed funds pursued for recovery and enforcement, in fraud, insolvency and judgment enforcement, with the on-chain evidence supporting the claim (guide 20's proportionality applied to value at stake).
- **Concealed assets in divorce and insolvency:** tracing exposing crypto holdings hidden from disclosure in matrimonial and insolvency proceedings, from wallet artefacts, exchange records and the ledger, against a false statement of assets (guide 98).
- **Speed and preservation:** the practical urgency, that funds move in minutes and exchange records and device evidence must be preserved fast, so freezing and preservation are sought promptly and devices secured before wallets are wiped (guide 110's anti-forensic context): the race the mobility of crypto demands.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a crypto matter is never only the ledger, and attribution in particular lives off-chain, across devices, exchanges and the person's wider estate. The blockchain holds the permanent, public transaction trail. But the exchange holds the identity records and account history that name the holder; the person's devices hold the wallet software, addresses, transaction history and, decisively, the private keys or seed phrases that prove control; backups and cloud storage hold copies of wallets and seed phrases; notes and paper hold written-down seed phrases; and the counterparties, the other side of a trade, a co-signer, hold their own records. The discipline is to pair the on-chain trail with these off-chain sources, because the ledger shows the flow but the exchange and the device supply the name and the proof of control. When the trail runs through a mixer, an exchange deposit downstream may still attribute it; when the wallet app is deleted, a seed phrase in a cloud note or a notebook restores control; and when a person denies ownership, a private key on their own device is hard to explain away.

EVIDENCE	THE BLOCKCHAIN	EXCHANGE RECORDS	PERSON'S DEVICES	BACKUPS / CLOUD	NOTES / PAPER	DELETED / RECOVERABLE
Transaction flow	Y: permanent, public	Deposit/ withdrawal logs	Wallet history	Wallet backups	n/a	Immutable on-chain
Holder identity	Address only	Y: KYC records	Account logins	Account data	n/a	n/a
Control (keys)	n/a	Custodied by exchange	Y: keys / seed	Y: seed backups	Y: written seed	Recoverable (guide 4)
Address ownership	Clustering	Y: linked to account	Wallet addresses	Backup wallets	Noted addresses	Varies
Timing / value	Y: timestamps	Trade records	App timestamps	n/a	n/a	On-chain permanent

Fallback strategy in one line: pair the permanent on-chain trail with off-chain attribution; when the ledger only shows an address, the exchange names the holder and the device proves control through its keys.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE FRAUD TRACED THROUGH THE MIXER TO THE EXCHANGE

Funds stolen in an investment fraud were moved off in cryptocurrency, and the victim feared they were gone. The §4 tracing showed otherwise: the funds were followed across the public ledger from the receiving address, through a mixer that had been used in an attempt to break the trail, but §6 analytics and timing saw through enough of the mixing to continue the trace, to a deposit at a regulated exchange. That deposit was the §5 attribution point: a disclosure order against the exchange produced the know-your-customer records naming the account holder, and a §7 freezing order secured the funds before they could be withdrawn. What had looked like an untraceable disappearance was, on a public and permanent ledger, a followable trail ending at a named person. The lesson is §2's: crypto is often more traceable than victims fear, the ledger is permanent and public, mixers complicate rather than always defeat the trace, and the exchange at the end of the trail supplies the name that turns tracing into recovery.

EXAMPLE 2 · THE SEED PHRASE THAT PROVED CONTROL

A respondent in an asset-recovery matter denied owning a set of addresses holding substantial value. The §5 device forensics settled it: examination of his seized devices recovered a wallet application and, in a §8 cloud note he had saved and forgotten, the seed phrase that controlled the very addresses in issue (guide 4's recovery of deleted and stored data). Possession of the seed phrase demonstrated the ability to control the funds, powerful evidence of ownership that the on-chain data alone could not provide. The §6 attribution was, in consequence, strong rather than inferential: this was not clustering or probability but the key itself, on his own devices and in his own storage. The denial did not survive. The lesson is §5's: the blockchain shows a flow between addresses, but control of the keys proves ownership, and a seed phrase recovered from a person's own device or storage is among the most compelling attribution evidence there is.

EXAMPLE 3 · THE HIDDEN HOLDINGS IN THE DIVORCE

In financial-remedy proceedings, one party's asset disclosure omitted any cryptocurrency, but the other suspected substantial hidden holdings. The §7 and §8 approach uncovered them: examination of devices revealed wallet apps and exchange account artefacts, exchange disclosure produced trading and holding records, and on-chain tracing (§4) followed the funds and clustered the addresses under common control, together establishing holdings the disclosure had concealed. The §6 value was reconciled at documented rates and dates given crypto's volatility. The concealment, measured against the sworn statement of assets, became evidence in itself. The lesson is §7's: cryptocurrency is a common vehicle for concealing assets in divorce and insolvency, but the combination of device artefacts, exchange records and the permanent public ledger routinely exposes holdings a party has tried to keep off the disclosure, and the omission itself carries weight.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Assuming crypto is untraceable:** the fundamental error, treating a public-ledger asset as gone when it is often highly traceable (Example 1, §2).
- **Confusing tracing with attribution:** a followed trail mistaken for a named owner, when attribution needs off-chain evidence (§5).
- **Delay:** funds moved and exchange or device evidence lost before freezing and preservation are sought (§7).
- **Ignoring the devices:** the on-chain trail pursued while the wallets, keys and seed phrases on the person's devices, the proof of control, are overlooked (Example 2, §5).
- **Overstating attribution:** a clustering inference presented as certainty rather than at honest confidence (§6).
- **Stopping at a mixer or bridge:** the trace abandoned at an obfuscation point that analytics might have seen through (Example 1, §6).
- **Mishandling value:** volatile crypto value not reconciled at documented rates and dates (§6).
- **Missing hidden holdings:** a bare disclosure accepted without testing devices and exchanges for concealed crypto (Example 3).

Technical limitations

- **The ledger names no one:** attribution always depends on off-chain evidence; the blockchain proves flow, not ownership: the core limit (§5).
- **Privacy coins resist tracing:** some currencies genuinely conceal parties and amounts, shifting the burden to off-chain evidence (§6).
- **Mixers and bridges add uncertainty:** obfuscation lowers confidence and sometimes breaks the trail: honestly assessed, not assumed defeated or defeated (§6).
- **Control can be lost or shared:** keys may be held by several people or a custodian, so control is established, not assumed from an address (§5).
- **Speed outpaces process:** funds move in minutes while orders take time, so preservation and freezing must be sought urgently (§7).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- What addresses, wallets, exchanges and transactions are known, so tracing has a starting point and freezing can be considered urgently?
- What devices, backups, cloud accounts and written notes might hold wallet software, keys or seed phrases proving control?
- What is the real-world event (the fraud, the transfer, the concealment) that the on-chain flow should be tied to?

Ask your opponent (or an exchange)

- Please preserve and disclose all account, identity (know-your-customer) and transaction records for the accounts and addresses at Schedule 1, and freeze the identified assets pending order.
- Please disclose all cryptocurrency wallets, addresses, exchange accounts and holdings, and preserve the devices, backups and notes that hold wallet software, keys or seed phrases.
- Please confirm the identity linked to the depositing address and the destination of the traced funds.

Ask your eDiscovery / forensic provider

- Where do the funds go on-chain, and does the trail reach an exchange that can attribute them?
- What device, exchange and key evidence attributes the addresses to a person, and at what confidence?
- What must be preserved or frozen now, before funds move or evidence is lost?

SUGGESTED WORDING · INSTRUCTION FOR A CRYPTOCURRENCY TRACING AND ATTRIBUTION

> "We instruct you to trace and attribute the cryptocurrency at Schedule 1. Please: (1) trace the funds across the relevant blockchains from the identified address(es), through any mixers, bridges and services, identifying exchanges and other attributable points and clustering addresses under common control, and reconcile the flow, amounts and timing with the real-world events at Schedule 2; (2) attribute the addresses to a person or entity using off-chain evidence, exchange know-your-customer records (by disclosure order or lawful request), wallet artefacts, private keys and seed phrases recovered from devices, backups, cloud storage and notes, and open-source links, and state the confidence of each attribution honestly; (3) identify the assets and holders against whom freezing, proprietary and disclosure relief may be sought, and advise on urgency given the speed at which funds move; (4) preserve the device, wallet and exchange evidence and the integrity of the analysis; and (5) express value at documented rates and dates given volatility, and confine on-chain conclusions to flow rather than ownership, which rests on the off-chain evidence."

§ 12 · QUICK CONTROL

Checklist and red flags · When to involve a digital forensic expert

The crypto-tracing checklist

- ☐ Starting addresses, wallets and exchanges identified
- ☐ Funds traced across chains, through mixers and bridges
- ☐ Exchanges and attributable points on the trail identified
- ☐ Addresses clustered under common control
- ☐ Exchange know-your-customer records sought by order
- ☐ Devices examined for wallets, keys and seed phrases
- ☐ Attribution graded at honest confidence, not overstated
- ☐ Freezing and preservation sought urgently
- ☐ Value reconciled at documented rates and dates
- ☐ On-chain flow distinguished from off-chain ownership

Red flags

- Crypto assumed untraceable and written off: Example 1.
- A traced trail treated as a named owner without attribution: §5.
- Devices and seed phrases ignored in favour of the ledger alone: Example 2.
- A disclosure omitting crypto accepted without testing: Example 3.
- Delay while funds move and records lapse.
- Clustering inference presented as certainty.
- A trace abandoned at a mixer without attempting to see through it.

When to involve a digital forensic expert

Early and urgently, because crypto moves in minutes and both the on-chain trace and the off-chain evidence are time-sensitive: the expert traces the funds across the ledger and through mixers and bridges, identifies the exchanges and attributable points, and clusters the addresses, so a supposedly lost asset is followed to a nameable end (Example 1, §4); at attribution, where exchange records, device artefacts and recovered seed phrases tie the addresses to a person at honest confidence, distinguishing flow from ownership (Example 2, §5); at the freezing and disclosure stage, supporting proprietary injunctions and orders against exchanges before funds move (§7); in divorce and insolvency, exposing concealed holdings against a false disclosure (Example 3); and at deployment, presenting the tracing and attribution under CPR Part 35 or CrimPR Part 19. Through **cflab.uk** and **e-discovery.uk**, cryptocurrency work joins the two halves of every crypto case, following the visible funds on the permanent ledger and naming the person behind the address off it, so that an asset thought untraceable is, more often than not, both traced and recovered.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Isn't cryptocurrency untraceable?

Usually the opposite (§2, Example 1). Most crypto runs on public blockchains, permanent, open ledgers that record every transaction forever, so funds are often more traceable than money in the banking system. The difficulty is not seeing the transactions but tying an address to a person, and dealing with deliberate obfuscation like mixers. A specialist can frequently follow the funds and, through exchanges and devices, name the holder.

If we can trace the funds, do we know who owns them?

Not from the ledger alone (§5). The blockchain records addresses, not names, so tracing shows the flow of value, not who controls it. Attribution comes from off-chain evidence: exchange know-your-customer records where funds are cashed in or out, wallet software and keys on a person's devices, recovered seed phrases, and behavioural links. Tracing and attribution are two different tasks, and naming the owner depends on the second.

What is a seed phrase, and why does it matter so much?

A seed phrase is the master secret that controls a wallet's keys and therefore its funds (§3). Because ownership of crypto is control of keys, possession of the seed phrase is powerful evidence of ownership, and one recovered from a person's own device, cloud note or notebook (Example 2) can prove control of addresses they deny owning. It is among the most compelling attribution evidence, which is why devices, backups and notes are examined, not just the ledger.

The funds went through a mixer. Is the trail dead?

Not necessarily (§6, Example 1). Mixers pool and shuffle funds to break the link between source and destination, and they complicate tracing, but analytics and timing can sometimes see through enough of the mixing to continue the trace, and the funds often surface again at an attributable exchange. A mixer lowers confidence and may in some cases defeat the trace, but it is an obstacle to be assessed honestly, not an automatic dead end.

Can crypto be frozen and recovered?

Often yes (§7, Example 1). Tracing supports freezing orders and proprietary injunctions over identified assets and against the exchanges holding them, and disclosure orders (including against persons unknown and third-party exchanges) compel the records that name the holder. Because funds move fast, freezing and preservation are sought urgently. Traced and attributed crypto is frequently recoverable, which is why acting quickly matters so much.

Could someone be hiding cryptocurrency in our matter?

It is common in divorce and insolvency (Example 3, §7). Crypto is used to conceal assets from disclosure, but device artefacts (wallet apps, exchange accounts), exchange records and the permanent public ledger together routinely expose holdings a party has left off their statement of assets. The concealment itself, measured against a sworn disclosure, then becomes evidence. If hidden crypto is suspected, the devices and exchanges are tested rather than the bare disclosure accepted.

§ 14 · REFERENCE

Glossary

Blockchain
A permanent, public, shared ledger of transactions.

Address
A ledger identifier holding funds; not a name.

Private key
The secret that controls an address's funds.

Seed phrase
The master secret that recovers a wallet's keys.

Wallet
Software or hardware storing and using keys.

Exchange
A service converting crypto to money, holding KYC records.

Mixer / tumbler
A service that shuffles funds to break the trail.

Bridge
A service moving value between blockchains.

Clustering
Grouping addresses under likely common control.

Attribution
Linking an address to a real person or entity.

Sources and authoritative references

The cryptocurrency and tracing disciplines in this guide draw on materials published by our laboratory and e-discovery practice, referenced here as sources:

- cflab.uk, digital forensics services (blockchain tracing, wallet and exchange forensics, attribution, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 04 · Collection and Phase 06 · Analysis (device, exchange and on-chain evidence as practised): e-discovery.uk/edrm/collection · e-discovery.uk/edrm/analysis
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- HM Treasury / FCA, cryptoasset regulation and anti-money-laundering framework (know-your-customer and exchange obligations): fca.org.uk, cryptoassets · UK Jurisdiction Taskforce, legal statement on cryptoassets: gov.uk
- Forensic Science Regulator, Code of Practice v2 (integrity and method): gov.uk, FSR Code · ISO/IEC 27037: iso.org, 27037
- CPR Part 25 (interim and freezing orders), PD 57AD and CPR Part 35: justice.gov.uk, Part 25 · justice.gov.uk, PD 57AD · justice.gov.uk, Part 35

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Cryptocurrency work at the laboratory joins the two halves that every crypto case requires. On-chain, the funds are traced across the public ledger from the identified addresses, through mixers and bridges that are assessed rather than treated as automatic dead ends, with services identified, addresses clustered under common control, and the flow reconciled with the real-world events and, given volatility, with documented values and dates (§4, §6). Off-chain, attribution ties the addresses to a person: exchange know-your-customer records obtained by disclosure order, wallet artefacts, private keys and seed phrases recovered from devices, backups, cloud storage and notes, and behavioural links, each stated at honest confidence, strong where a key on the person's device or an exchange record ties it down, weaker where it rests on inference (§5, Example 2). Because funds move in minutes, freezing, proprietary and disclosure relief and the preservation of device and exchange evidence are pursued urgently (§7). The same work exposes crypto concealed from disclosure in divorce and insolvency (Example 3). Reports run under CPR Part 35 or CrimPR Part 19. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the message for anyone who fears crypto has vanished is usually the encouraging one: on a permanent public ledger, it can more often than not be both traced and recovered.

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

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