Cryptocurrency And Blockchain Tracing

Cryptocurrency tracing involves following transactions on public ledgers and attributing addresses to individuals. This guide covers the process from tracing funds across the ledger to identifying owners, addressing obfuscation, and detailing deployment strategies for freezing and recovery. It also includes common mistakes and expert advice.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
https://e-discovery.uk/library/cryptocurrency-and-blockchain-tracing

CRYPTOCURRENCY & BLOCKCHAIN · A GUIDE FOR UK LAWYERS Cryptocurrency and Blockchain Tracing Following the Money on a Public Ledger, and Naming the Person Behind the Address COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM WALLET & EXCHANGE FORENSICS CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide

§ 01 · 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. KYC

§ 02 · FIRST PRINCIPLES The problem in plain English: visible money, hidden owners

§ 03 · HOWITRECORDSVALUE How blockchains and wallets record value LEDGER ADDRESS WALLET / KEYS EXCHANGE PERSON

§ 04 · TRACING Tracing funds across the ledger

§ 05 · ATTRIBUTION Attribution: linking an address to a person

§ 06 · OBFUSCATIONANDHONESTLIMITS Obfuscation, honest limits and confidence

§ 07 · DEPLOYMENT Deployment: freezing, disclosure and recovery

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE THE EXCHANGE PER S ON'S BACKUPS / NOTES / DELETED / BLOCKCHAIN RECORDS DEVICES CLOUD PAPER RECOVERABLE

§ 09 · IN THE WILD Worked examples EXAMPLE1 ·

THEFRAUDTRACEDTHROUGHTHEMIXERTOTHEEXCHANGE EXAMPLE2 · THESEEDPHRASETHATPROVEDCONTROL EXAMPLE3 · THEHIDDENHOLDINGSINTHEDIVORCE

§ 10 · WHEREITGOESWRONG Common mistakes and technical limitations Common mistakes Technical limitations

§ 11 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client Ask your opponent (or an exchange) Ask your e Discovery / forensic provider SUGGESTED WORDING · INSTRUCTIONFORACRYPTOCURRENCYTR AC INGAND AT TRIBUTION

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The crypto-tracing checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions Isn't cryptocurrency untraceable? If we can trace the funds, do we know who owns them? What is a seed phrase, and why does it matter so much? The funds went through a mixer. Is the trail dead? Can crypto be frozen and recovered? Could someone be hiding cryptocurrency in our matter?

§ 14 · REFERENCE Glossary Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab Speak to a forensic examiner, not a salesperson. INSTRUCTTHELAB NEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

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 there for e 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 some time s 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.