



Code of Ethics and Professional Conduct

Blockchain, Crypto & OSINT Investigators

1. Purpose

Blockchain, cryptocurrency and OSINT investigators may have access to powerful investigative techniques, specialist tools, sensitive data and methods capable of identifying individuals, organisations, financial activity and digital infrastructure.

With that capability comes responsibility.

This Code sets the minimum ethical and professional standards expected of investigators undertaking blockchain, crypto, digital asset or OSINT work.

It applies globally and should be read alongside all applicable laws, regulations and professional obligations within the investigator's jurisdiction.

2. Core Principles

Investigators must:

- Act lawfully, honestly and professionally.
- Maintain integrity, objectivity and independence.
- Have a legitimate and defensible purpose for investigative activity.
- Respect privacy and minimise unnecessary intrusion.
- Protect confidential and sensitive information.
- Preserve the integrity of evidence.
- Distinguish fact, inference, assumption and opinion.
- Communicate uncertainty and confidence accurately.
- Use investigative capabilities proportionately and responsibly.
- Avoid unnecessary harm.
- Remain accountable for their actions and conclusions.

Professional integrity takes precedence over technical skill.

The ability to perform an investigative technique does not automatically make its use lawful, necessary or ethical.

3. Lawful and Legitimate Investigations

Investigators must only undertake activity for lawful and legitimate purposes.

Investigators should be able to clearly explain:

- why an investigation is being conducted;
- what objective it seeks to achieve;
- who has requested or authorised it, where applicable; and
- why the methods being used are necessary and proportionate.

Investigators must not knowingly participate in or facilitate:

- unauthorised system access;
- hacking or malware deployment;
- credential theft;
- phishing or social engineering for unlawful purposes;
- stalking, harassment or intimidation;
- extortion or blackmail;
- unauthorised surveillance;
- unlawful interception of communications;
- impersonation of law enforcement;
- doxxing;
- fraud;
- theft or interference with digital assets; or
- any other unlawful or improper activity.

Where the legality of a proposed investigative technique is unclear, appropriate legal or professional advice should be sought before proceeding.

4. Integrity, Objectivity and Attribution

Investigators must follow the evidence rather than seek evidence to support a preferred conclusion.

Investigators must never:

- fabricate, manipulate or conceal evidence;
- deliberately misrepresent findings;
- exaggerate certainty;
- ignore material evidence that contradicts a hypothesis; or
- allow pressure from a client, employer, victim or other party to improperly influence a conclusion.

Attribution must be approached with particular caution.

Blockchain addresses, usernames, email addresses, telephone numbers, IP addresses, domains, social-media accounts and other digital identifiers must not be attributed to a person or organisation without a reasonable evidential basis.

Third-party labels, automated clustering, risk scores, AI outputs and investigative tool results should be treated as analytical inputs, not unquestionable facts.

Where possible, significant attribution should be independently corroborated.

Investigators must distinguish between:

- **Fact** — directly supported by evidence;
- **Inference** — a reasonable conclusion drawn from evidence;
- **Hypothesis** — a proposition requiring further investigation; and
- **Opinion** — professional judgement.

Where appropriate, confidence levels should be clearly stated.

5. Blockchain and Cryptocurrency Investigations

Blockchain investigators must recognise that transactional activity does not automatically establish ownership, identity, intent or criminal involvement.

Investigators should:

- validate material transactions;
- accurately record relevant wallet addresses and transaction hashes;
- distinguish direct relationships from inferred relationships;
- consider legitimate explanations for wallet behaviour;
- independently evaluate automated tracing or attribution;
- explain significant assumptions;
- understand the implications of exchanges, bridges, mixers, swap services, smart contracts, deposit addresses and nested services; and
- avoid presenting probabilistic clustering as established fact.

The movement of assets through an address does not, by itself, prove that the controller of that address committed or knowingly participated in criminal activity.

Investigators must never access, move, seize or control another person's cryptocurrency or digital assets without clear lawful authority.

Private keys, seed phrases and credentials must not be requested, retained or accessed unnecessarily.

6. OSINT, Privacy and Data Protection

Publicly accessible information is not automatically unrestricted information.

OSINT investigations must be necessary, proportionate and relevant to a legitimate investigative purpose.

Investigators must comply with applicable privacy and data-protection laws, including where relevant:

- UK GDPR;
- the Data Protection Act 2018;
- EU GDPR; and
- equivalent privacy legislation in other jurisdictions.

Investigators should collect only the personal information reasonably necessary for the investigation.

Particular care should be taken when collecting information relating to:

- family members and uninvolved third parties;
- children;
- home addresses;
- personal relationships;
- health;
- financial circumstances;
- private communications; and
- other highly sensitive personal information.

Before collecting, retaining, sharing or publishing personal information, investigators should consider:

- Is it relevant?
- Is it necessary?



- Is there a less intrusive way to achieve the same objective?
- Is the information reliable?
- Could an innocent person be harmed if it is wrong?
- Who genuinely needs access to it?
- How long does it need to be retained?

Investigators must not collect personal information simply because it is technically accessible.

7. Confidentiality and Information Security

Investigators must protect information obtained through professional work.

This includes:

- client and victim information;
- investigation files;
- wallet addresses linked to cases;
- personally identifiable information;
- evidence;
- credentials;
- investigative methodology;
- confidential intelligence; and
- commercially sensitive information.

Sensitive information must not be disclosed without legitimate authority or purpose.

Case information must not be published, shared on social media or used for marketing simply to demonstrate investigative capability.

Where real investigations are used for training or case studies, appropriate anonymisation should be applied unless identification is lawfully justified.

8. Evidence and Record Keeping

Investigators must preserve evidence accurately and maintain sufficient records to explain how significant conclusions were reached.

Where appropriate, investigators should retain:

- source information;
- URLs;
- screenshots;
- timestamps;
- transaction hashes;
- wallet addresses;
- investigative notes;
- tool outputs; and
- analytical reasoning.

Material evidence must never be fabricated or intentionally altered.

Where evidence has been redacted, summarised or modified for presentation, this should be made clear where relevant.



Errors should be acknowledged and corrected promptly.

9. Investigative Tools and Artificial Intelligence

Investigators remain responsible for their conclusions regardless of the software, platform or AI system used.

No investigative tool should be treated as infallible.

Investigators must reasonably understand the limitations of tools upon which they rely and independently verify significant findings.

AI may assist with:

- analysis;
- research;
- pattern identification;
- data processing; and
- reporting.

However, AI must not replace professional judgement.

Investigators must:

- verify material AI-generated findings;
 - protect confidential information;
 - avoid unnecessary disclosure of personal or sensitive case data to third-party systems;
 - remain alert to fabricated or inaccurate outputs; and
 - remain personally accountable for findings issued under their name.
-

10. Competence and Professional Conduct

Investigators must work within the limits of their competence, training and experience.

They must not knowingly misrepresent:

- qualifications;
- certifications;
- experience;
- investigative capability;
- access to tools;
- relationships with law enforcement;
- success rates; or
- ability to recover assets.

Investigators must not guarantee recovery of stolen cryptocurrency or other assets.

Tracing funds, identifying endpoints, obtaining preservation or freezing action and recovering assets are separate processes and must not be presented as equivalent.

Investigators must treat victims, witnesses, subjects and other parties professionally and with dignity.

An allegation does not establish guilt.



11. Conflicts of Interest

Investigators must identify and appropriately manage actual, potential or perceived conflicts of interest.

Financial incentives, personal relationships, commercial arrangements, referral fees or other interests must not improperly influence investigative conclusions.

Where a conflict prevents impartiality, the investigator should decline or withdraw from the work.

12. Responsible Use of Investigative Knowledge

Investigators may gain knowledge capable of:

- identifying individuals;
- tracing financial activity;
- discovering hidden relationships;
- locating digital infrastructure;
- analysing wallet behaviour;
- overcoming investigative obstacles; and
- identifying techniques used to conceal activity.

This knowledge must only be used for lawful and legitimate purposes.

Investigators must not knowingly use or share investigative knowledge to:

- facilitate criminal activity;
- enable fraud or theft;
- evade legitimate law-enforcement action;
- harass or target innocent individuals;
- compromise privacy without justification;
- conceal criminal proceeds; or
- cause unnecessary harm.

Investigators must recognise the dual-use nature of advanced investigative knowledge and exercise professional judgement before sharing sensitive methods.



Investigator Declaration

I confirm that I have read and understood this **Code of Ethics and Professional Conduct for Blockchain, Crypto & OSINT Investigators**.

I understand that access to advanced investigative techniques carries responsibilities beyond technical competence.

I agree to use investigative skills, knowledge and tools only for lawful, legitimate and ethical purposes.

I will act with integrity, maintain professional standards, protect sensitive information and avoid misuse of the capabilities I acquire.

I understand that serious misconduct, dishonesty or misuse of investigative techniques may make me unsuitable for advanced investigative training or professional investigative work.

Full Name: _____

Organisation: _____

Role: _____

Signature: _____

Date: _____