Navigating the Rapids

The Current State of the English Law of Crypto-assets

Recent Case Law, Legislative Developments & Practical Implications

Presented by David Bowman (Weightmans) and Steve Sandford (CyXcel)

Law correct as of 24 September 2025

Meet Your Speakers

David Bowman
Legal Director
Weightmans
david.bowman@weightmans.com

Steve Sandford
Partner, Digital Forensics and Incident Response
CyXcel
steves@cyxcel.com

Introduction

"Cryptoassets are cryptographically secured digital representations of value or contractual rights that use some type of distributed ledger technology (DLT) and can be transferred, stored or traded electronically"

– Financial Conduct Authority (FCA)

Fast Facts

- In the first half 2025 the volume of stablecoin transaction alone accounted for $4.6 trillion across over a billion transactions (Visa/Allium)
- In late 2024 the FCA reported that 12% of all UK adults owned cryptocurrency with the average value held of £1,842.
- In the first year of regulating the promotion of cryptocurrencies (Oct 2023-24) the FCA issued 1702 alerts and removed 900 scam cryptocurrency websites and a further 50 fake apps.
- Globally business to business trading of cryptocurrency has increased from $100m per month in early 2023 to over $3billion a month in 2025.
- Major eCommerce businesses such as Amazon and Walmart are reportedly investing in developing their own cryptocurrencies to improve transaction profitability by cutting out payment fees by banks and credit card companies. Total control of currency.

Basic Glossary

Stable Coin: A cryptocurrency that aims to maintain a fixed value by reference to another currency, commodity or financial instrument ("pegging"). Examples: Tether (1 USD), USDC (1 USD), EURC (1 Euro), Pax Gold (1 oz AU).

Private Key: The encrypted password (extremely long series of alphanumeric characters) which allows the transfer of ownership of cryptocurrency tokens.

Public key: Your public address to send and receive cryptocurrency transactions. Key to identification and half of the cryptography that is essential to blockchain digital assets.

On-chain: The status of a transaction that has been properly recorded on the distributed public ledger.

Wallet: A digital storage location for keeping personal encryption keys secure.

Exchange: A website or app that allows users to buy or sell crypto-currency assets i.e. a service which facilitates the sale of tokens and the registration of transactions on the blockchain

Whitepaper: A technical document or prospectus released alongside the cryptocurrency / exchange which explains how the system works.

Legal Status of Crypto-assets

UK Jurisdiction Task Force Legal Statement (2019):

- “crypto assets have all the indicia of property”
- “the novel or distinctive features possessed by some cryptocurrencies – intangibility, cryptographic authentication, use of a distributed transaction ledger, decentralisation, rule by consensus – do not disqualify them from being property”
- “but a private key is not in itself to be treated as property because it is information”.

AA v Persons Unknown (2019): an application for a proprietary injunction and claims in restitution and/or constructive trust.

- "it is fallacious to proceed on the basis that the English law of property recognises no forms of property other than choses in possession and choses in action."
- “Essentially, and for the reasons identified in that [UKJTF] legal statement, I consider that a crypto asset such as Bitcoin are property. They meet the four criteria set out in Lord Wilberforce's classic definition of property in National Provincial Bank v Ainsworth [1965] 1 AC 1175 as being definable, identifiable by third parties, capable in their nature of assumption by third parties, and having some degree of permanence…”

Legal Status of Crypto-assets

Law Commission's Digital Assets Consultation Paper (2022):

"We conclude that the flexibility of common law allows for the recognition of a distinct category of personal property that can better recognise, accommodate and protect the unique features of certain digital assets (including crypto-tokens and cryptoassets). We recommend legislation to confirm the existence of this category and remove any uncertainty.

"In July 2024 we published a short supplemental report and draft Bill aimed at implementing this recommendation. The draft Bill confirms the existence of a "third category" of personal property rights, capable of accommodating certain digital assets including crypto-tokens. The supplemental report explains the basis of the draft Bill, detailing the unique features of digital assets that mean they fall outside of the two traditional categories of personal property ("things in action" and "things in possession"). The supplemental report also highlights that the draft Bill leaves it to the courts to develop this "third category" of personal property by delineating its boundaries and the rights that attach to "third category" things."

Property (Digital Assets etc.) Bill

"1. Objects of personal property rights

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."

Case Law

1. D’Aloia v Persons Unknown and Others [2022] EWHC 1723 (Ch)
2. Ion Science Ltd v Persons Unknown [2020] Commercial Court (Unreported)
3. Tulip Trading Ltd v Bitcoin Association for BSV & Others [2023] EWCA Civ 83
4. Piroozzadeh v Persons Unknown and Others [2023] EWHC 1024 (Ch)
5. Mooij v Persons Unknown [2021] EWHC (Unreported)
6. Joseph Keen Shing Law v Persons Unknown and Huobi Global Ltd [2023] Commercial Court (Unreported)
7. Jones v Persons Unknown [2025] EWHC 1823 (Comm)

1. D’Aloia v Persons Unknown and Others [2022] EWHC 1723 (Ch)

Summary: Mr. Fabrizio D’Aloia, an Italian engineer and founder of Microgame, was defrauded of significant amounts of cryptocurrency, including Tether (USDT) and USD Coin (USDC) (both “stable coins”), through a sophisticated scam involving fraudulent online platforms.

Key Issues: The court considered whether it could grant a proprietary injunction and permit service of proceedings via unconventional means, such as through tokens imprinted in blockchain transactions to the wallets holding the misappropriated assets (“air dropping”).

Court's Decision: The High Court granted a proprietary injunction against persons unknown and allowed for service of court documents via non-fungible tokens (NFTs) airdropped into the digital wallets where the stolen assets were held. The court reaffirmed that crypto-assets are property under English law and can be the subject of legal remedies, but again this was a first instance decision that only binds the lower courts.

Implications: This case is significant as one of the first fully heard cases involving crypto-assets, moving beyond earlier cases that primarily addressed interim remedies. It demonstrates the common law’s adaptability in using innovative methods to address the challenges posed by the anonymous and decentralised nature of blockchain technology. For businesses, it underscores the importance of prompt legal action and the potential

2. Ion Science Ltd v Persons Unknown [2020] Commercial Court (Unreported)

Summary: Ion Science Ltd and its director were victims of an initial coin offering (ICO) fraud, losing approximately £577,002 worth of Bitcoin and Ethereum. They were misled into investing in what they believed was a legitimate cryptocurrency venture.

Key Issues: The claimants sought a proprietary injunction and a worldwide freezing order against unknown defendants. They also applied for Bankers Trust orders against cryptocurrency exchanges to obtain information aiding in the identification and recovery of the assets.

Court's Decision: The Commercial Court granted the proprietary injunction, worldwide freezing order, and disclosure orders. The court recognised that crypto-assets are property and that it had jurisdiction to grant such orders against persons unknown and to serve them out of the jurisdiction.

Implications: The case highlights practical legal strategies for businesses victimised by crypto fraud. It emphasises the court's willingness to support victims through interim remedies and cross-border cooperation. For businesses, it again illustrates the importance of swift action and the potential to leverage court orders in asset recovery efforts. The targeting of crypto-currency exchanges for remedies arising out of fraud is a developing area of interest for litigators.

3. Tulip Trading Ltd v Bitcoin Association for BSV & Others [2023] EWCA Civ 83

Summary: Tulip Trading Ltd, a Seychelles company associated with serial crypto-asset litigant Dr. Craig Wright, claimed loss of access to approximately 111,000 Bitcoin (valued in 2021 at over $4 billion but substantially higher at today's prices) due to a hack. The company argued that the developers of the Bitcoin network owed fiduciary and tortious duties to assist in regaining control over the assets.

Key Issues: Whether the developers of a decentralised blockchain network owe fiduciary duties or duties of care to owners of crypto-assets on that network.

Court's Decision: The Court of Appeal overturned the High Court's dismissal of the case, allowing it to proceed to a full trial. The Court recognised that there is a serious issue to be tried regarding the existence of fiduciary duties between developers and users.

Implications: This case is closely watched as its outcome could significantly impact the responsibilities of blockchain developers. A ruling that developers owe fiduciary duties could alter the dynamics of blockchain governance and impose new obligations on those who maintain and update blockchain protocols. Such an outcome would likely push developers even further to keep their identities secret which will raise practical difficulties for any claimant. However, it is unclear whether the case will ever see the inside of a court room again – see Dr Wright's committal for contempt of court in other claims.

4. Piroozzadeh v Persons Unknown and Others [2023] EWHC 1024 (Ch)

Summary: Mr. Jahangir Piroozzadeh was defrauded of approximately 870,818 USDT through a murky cryptocurrency investment scheme which he was induced into by people he did not know (and presumably could not identify). He sought a freezing injunction against Binance Holdings Ltd (a well known exchange), alleging they held the stolen assets and were under a duty to prevent their dissipation.

Key Issues: The court examined whether it had jurisdiction over Binance, a foreign entity, and whether a freezing injunction was appropriate under the circumstances.

Court's Decision: The High Court discharged the freezing injunction against Binance. The court found that it lacked jurisdiction over the Cayman Islands-registered company and noted the challenges in establishing connections sufficient for English jurisdiction.

Implications: This case highlights jurisdictional hurdles in crypto-asset recovery, particularly when dealing with entities operating outside the UK, as many developers and exchanges are notionally based offshore. For businesses, it underscores the necessity of understanding the legal jurisdictions involved in cryptocurrency transactions and the importance of considering these factors when engaging with foreign exchanges. It is also a salutary lesson in not parting with valuable crypto-assets without doing your due diligence on the recipient.

5. Mooij v Persons Unknown [2021] EWHC (Unreported)

Summary: Mr. Mooij was deceived into transferring around 20.34 Bitcoins and € 330,000 to fraudulent entities posing as legitimate investment platforms. This was a summary judgment application against persons unknown.

Key Issues: The court considered whether the court could grant final relief against defendants who were not known to the Claimant. A common scenario in crypto-asset fraud.

Court's Decision: The High Court granted summary judgment and continued freezing orders against the unknown defendants as potential "newcomers" to litigation at the point in which they identify themselves to recover their illicit gains.

Implications: The case demonstrates the court's application of injunctive relief developed in other settings to the more novel crypto space. For businesses, it indicates that English courts are willing to accommodate the unique challenges of pursuing legal action against anonymous parties.

Point of interest: A summary judgment application regarding similar subject matter had failed in the case of Boonyaem v Persons Unknown and others [2023] EWHC 3180 (Comm) in part because the persons unknown might never become persons known.

6. Joseph Keen Shing Law v Persons Unknown and Huobi Global Ltd [2023] Commercial Court (Unreported)

Summary: Mr. Law was defrauded of significant cryptocurrency amounts and sought remedy, including freezing orders against unknown defendants and enforcement actions involving Huobi Global Ltd, a major cryptocurrency exchange.

Key Issues: The enforcement of judgments against assets held by foreign entities and the extent of cooperation required from cryptocurrency exchanges. Another important issue was whether an exchange could be required to liquidate crypto-assets into fiat currency to make the claimant whole.

Court's Decision: The court ordered Huobi to transfer the frozen assets into England and Wales to facilitate enforcement, highlighting the necessity of exchange compliance with court orders.

Implications: The case underscores the importance of cooperation from cryptocurrency exchanges in legal proceedings and the enforcement of judgments. For businesses, it emphasises the need to engage with reputable exchanges that are responsive to legal obligations and the potential complexities in recovering assets from foreign platforms. As one might expect there is a developing reputational risk to exchanges who are not cooperative with national authorities.

7. Jones v Persons Unknown [2025] EWHC 1823 (Comm)

Summary: The respondent was defrauded into investing in cryptocurrency, purchasing 89.6 Bitcoin through a fake online account controlled by fraudsters. After discovering the scam, he hired legal and investigative help, which traced the stolen Bitcoin to a wallet (the "T wallet") controlled by D4. The respondent obtained a court judgment against the fraudsters and D4, ordering them to return the 89.6 Bitcoin. None of the Defendants appeared. D4 complied, returning the Bitcoin along with interest and legal costs. The cryptocurrency exchange who held the wallet applied to set aside the judgment in November 2024.

Key Issues: D4 satisfied the respondent's judgment by transferring Bitcoin from a different wallet (the "R wallet"). It then reimbursed itself from the T wallet, which did not contain the respondent's stolen Bitcoin but held mixed funds, including Bitcoin belonging to the applicant's customers. Did the cryptocurrency exchange have the right to set aside the judgment that had caused this loss to it?

Court's Decision: Application refused. The test to be satisfied was that the exchange was directly affected by the original judgment.

- The applicant was only indirectly affected. D4 had satisfied the judgment using Bitcoin from the R wallet, and later reimbursed itself from the T wallet, which included Bitcoin belonging to the applicant or its customers.
- These actions were choices made by D4, not direct consequences of the court order. D4 did not need to use Bitcoin belonging to the applicant to comply with the judgment. Therefore, the applicant's claim was against D4 under contract, not against the judgment itself.
- Even if the applicant had been directly affected, the court noted: The applicant had no proprietary interest in the Bitcoin. It had not shown any actual loss to itself. The judgment did not order transfer of Bitcoin belonging to the applicant. There was significant delay in bringing the application. The delay caused prejudice to the respondent, especially due to D4 being struck off.

Implications: This application shows the risks to an exchange of meddling in litigation between victim and fraudsters (even those who are unknown).

Observations

- The law of England and Wales recognises ownership of crypto asset (token) as personal property.
- The Courts are prepared to extend the injunctive relief to defend that personal property.
- There are practical difficulties in giving effect to that relief, but the Courts are innovating relatively quickly.
- All the cases cited are at first instance. There is very little appellate court treatment of the law and nothing from the Supreme Court. However, the rug is not likely to be pulled from under the sector.
- An increasing number of cases are going to be dealt with by arbitration, especially those directed at exchanges. Look out for strange jurisdiction and governing law clauses.
- NB: Part 4 The Economic Crime and Corporate Transparency Act 2023 specifically provides for the extension of the civil recovery of crypto-assets by law enforcement authorities as from 7 November 2024.

In Brief: Regulatory Developments

Crypto Investigations Introduction

Basic Glossary

Blockchain: A digital ledger that records transactions in linked blocks, shared across many computers.

Block: A group of transactions bundled together and added to the blockchain.

Node: A computer that keeps a copy of the blockchain and helps validate transactions.

Decentralised: No single person or company controls the system; it's managed by many users.

Hash: A unique code that identifies a block and links it to the previous one.

Ledger: The record of all transactions on the blockchain.

Token: A digital asset built on a blockchain, often used in apps or games.

Bridge: A tool or protocol that allows you to move cryptocurrencies or tokens from one blockchain to another.

Mixer (or Tumbler): A service that mixes different users' cryptocurrencies together to make transactions harder to trace.

Cryptocurrencies and Criminal Exploitation

Decentralised Digital Transactions

Cryptocurrencies enable fast, borderless transactions without central authority oversight, transforming the financial landscape.

Criminal Exploitation Risks

Digital currencies are exploited for theft, fraud, money laundering, and ransomware due to their pseudonymous nature.

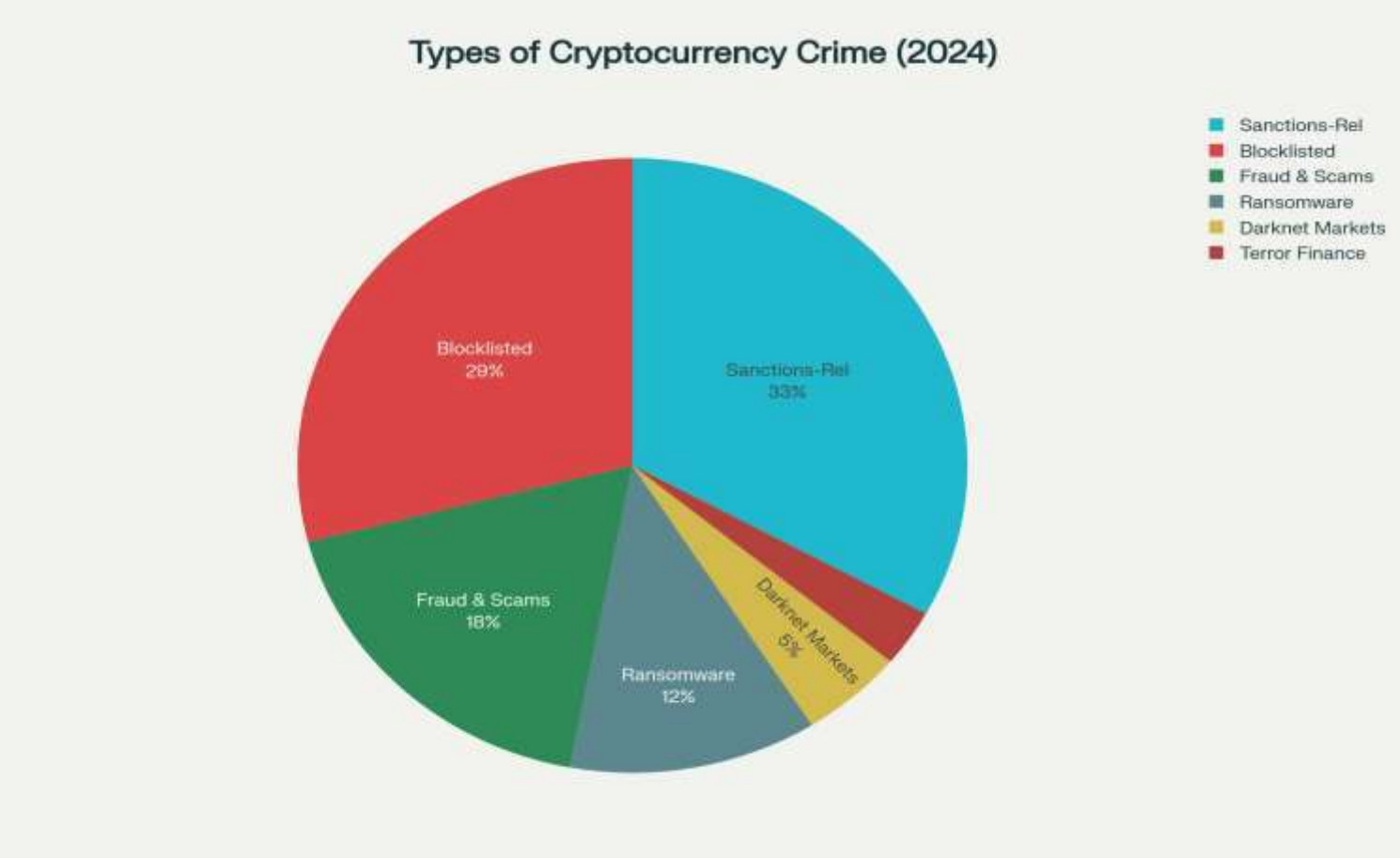
Challenges for Law Enforcement

The lack of central control complicates tracking and reversing illicit crypto transactions, challenging enforcement agencies.

Need for Global Cooperation

Mitigating crypto-related crimes requires robust investigative frameworks and international collaboration.

The Evolving Landscape of Cryptocurrency Crime



Cross-Chain Crime and Obfuscation Techniques

- Modern cryptocurrency criminals employ increasingly sophisticated **obfuscation methods** to evade detection.
- This **chain-hopping** behaviour creates significant challenges for investigators who must trace funds across multiple blockchain ecosystems with varying technical architectures and investigative tools.
- **North Korea** alone accounts for approximately **12%** of cross-chain criminal activity.
- These actors demonstrate remarkable sophistication in using **bridges**, **mixers**, and decentralised finance protocols to obscure transaction trails.

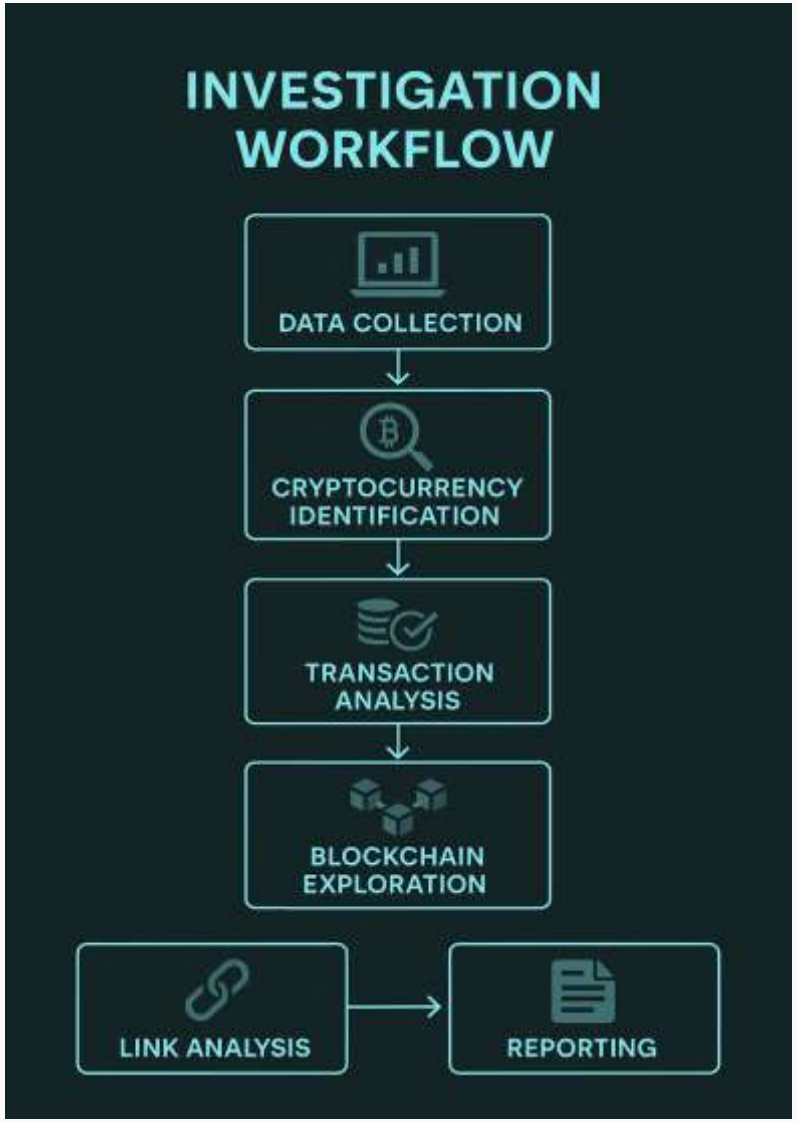
Foundational Investigation Methodologies

Blockchain Analysis and Transaction Tracing
The foundation of cryptocurrency investigation lies in blockchain analysis

Address & Cluster Analysis
Address clustering involves grouping cryptocurrency addresses that likely belong to the same entity based on transaction patterns, timing, and behavioural indicators.

Transaction Flow Analysis
Tracing the movement of funds through multiple addresses and intermediary services.

Digital Forensics & Wallet Analysis
Extract wallet files and recover private keys from devices seized during investigations.



Open Source Intelligence (OSINT)

What Is OSINT?

- OSINT refers to gathering information from publicly available sources like:
  - Social media
  - Forums
  - News articles
  - Public records

How Blockchain Links to Real Identities

Although blockchain is **pseudonymous** (not truly anonymous), OSINT can help link wallet addresses to real people by:

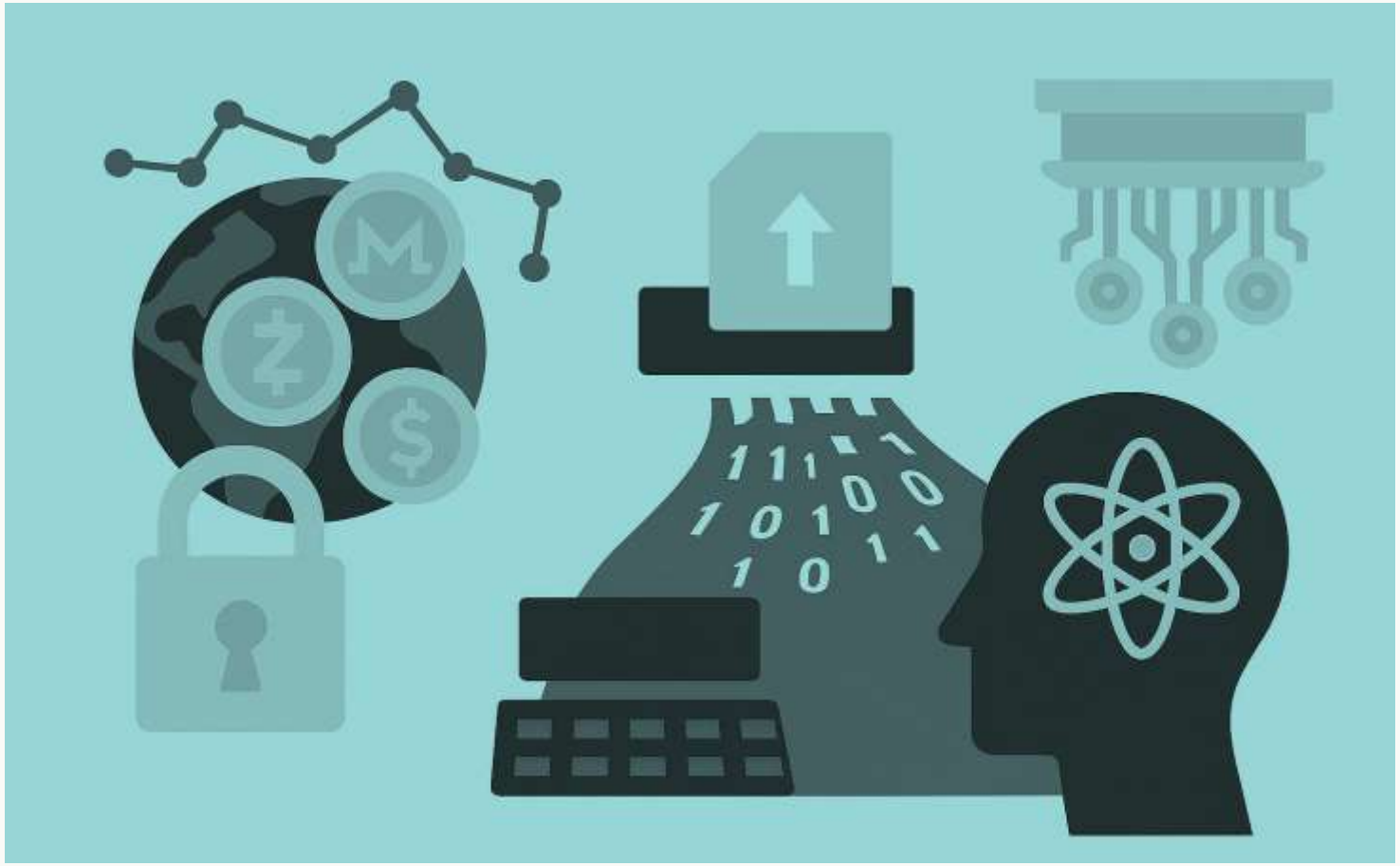
- **Transaction Patterns -** Repeated behaviours or timing can hint at identity.
- **Wallet Reuse -** Using the same wallet across platforms (e.g., Twitter, GitHub) can expose identity.
- **Metadata & IP Leaks -** Info from exchanges, forums, or leaked data can connect wallets to users.
- **Bridges & Mixers -** Bridges move assets between blockchains and may leave traces. Mixers try to hide traces, but patterns can still be analysed.

Advanced Investigations

- **Artificial Intelligence**
- **Mixer and Tumbler Analysis**
- **DeFI Protocol Investigation**
- **NFT Investigation Methods**

Technical Challenges

- **Privacy Coins**
- **Scaling Solutions**
- **Quantum computing**



Emerging Threats and Opportunities

Artificial Intelligence (AI)

- **Opportunity:**
  - AI tools can automate complex investigations and enhance analytics.
- **Challenge:**
  - Criminals may use AI for more sophisticated attacks and evasion.
- **Key Point:**
  - Investigators must keep pace with rapidly evolving AI capabilities.

DAOs & Advanced Smart Contracts

- **New Crime Categories:**
  - Decentralised Autonomous Organisations (DAOs) and complex smart contracts create new investigation challenges.
- **Expertise Needed:**
  - Understanding decentralised governance, automated protocols, and smart contract interactions is essential.

Asset Recovery

- **Exchange-based seizures** are the most common, involving cooperation with regulated cryptocurrency exchanges to freeze accounts and seize funds. These operations require proper legal process and coordination with exchange compliance teams.

- **Direct wallet seizures** occur when investigators obtain private keys through device seizures, court orders, or voluntary surrender. These seizures require specialised technical expertise to ensure proper handling of cryptographic materials and maintain chain of custody for legal proceedings.

- **Smart contract**-based freezing has emerged as a powerful tool for certain types of digital assets. Stablecoin issuers can freeze specific tokens through smart contract functions, effectively immobilising funds even when private keys remain unknown. This capability has proven particularly valuable in large-scale fraud investigations.

Case Studies

- The **IntelBroker** investigation showcased how blockchain analysis combined with traditional investigative methods can identify sophisticated cybercriminals operating across international boundaries
- The **Colonial Pipeline** ransomware case remains a landmark example of successful cryptocurrency recovery.
- The **Philippines kidnapping** case illustrated how blockchain analysis can support investigations of violent crimes involving cryptocurrency payments.

Key Takeaways

Multidisciplinary Collaboration

- Effective crypto investigations require **technology expertise**, **legal knowledge**, and **global cooperation**.
- Teams often include **analysts**, **law enforcement**, **legal advisors**, and **international partners**.

Success Factors

- **Advanced Tools:** Use of blockchain analytics, OSINT, and AI-powered platforms.
- **Training:** Ongoing education for investigators and stakeholders.
- **Partnerships:** Collaboration with industry, regulators, and global agencies.

Future Outlook

- **Adapting to AI:** Leveraging AI for faster, smarter investigations.
- **Privacy Tech:** Navigating new privacy tools and anonymisation methods.
- **Regulatory Changes:** Staying ahead of evolving laws and compliance requirements.

Thank You for Listening. Any Questions?

David Bowman
Legal Director
Weightmans
david.bowman@weightmans.com

Steve Sandford
Partner, Digital Forensics and Incident Response
CyXcel
steves@cyxcel.com