



Cryptocurrency, Financial Crime and the Case for On-Chain Enforcement

A Technology Policy Paper

Submitted to the UK Government International Summit on Financial Crime
iSanctuary, Cambridge, United Kingdom

Executive Summary

Fraud is the United Kingdom's most prevalent crime. It accounts for an estimated 41% of all crime recorded in the Crime Survey for England and Wales, yet has historically received less than 1% of policing resources. Within that landscape, cryptocurrency has become the instrument of choice for sophisticated fraud operations: offering speed, pseudonymity, cross-border reach, and - critically - the ability to permanently realise criminal proceeds through the conversion of digital assets to fiat currency before any enforcement intervention is possible.

This paper sets out the scale of the problem, the structural characteristics of the blockchain environment that enable it, and the technical and legal frameworks through which REKTify™ - developed by iSanctuary - is already demonstrating that on-chain enforcement is operationally viable. REKTify™'s primary function is to achieve parity with the criminal: a criminal restraint order under sections 40-41 of POCA 2002, a civil freezing injunction, a Mareva order, or a sanctions notice can be deployed on-chain as an immutable, court-sanctioned token within seconds of being granted - matching precisely the speed at which criminals can move digital assets. This creates, for the first time, a real-time enforcement mechanism that operates on the same timescale as the threat. The paper also identifies the policy pathway through which the UK Government could establish the world's first nationally standardised on-chain legal enforcement and fraud marker system, embedding that capability within existing legal frameworks and funding mechanisms, with the potential to drive a substantial increase in the value of criminal assets seized and recovered each year.

Part I: The Scale of Cryptocurrency-Enabled Fraud in the United Kingdom

The United Kingdom is one of the world's largest cryptocurrency economies. The FCA's most recent consumer research indicates that approximately 8% of UK adults hold cryptoassets, representing roughly 4.2 million people. The UK ranks twelfth globally in the Chainalysis Crypto Adoption Index and is the largest cryptocurrency economy in Central, Northern and Western

Europe. This position of prominence brings significant economic opportunity but also commensurate exposure to financial crime.

Reported Losses

The headline figures are stark. Over the two financial years 2023 and 2024, fraud cost the UK economy an estimated £14.4 billion. Within that broader landscape, investment fraud - the category most closely associated with cryptocurrency scams - has escalated significantly.

£306m	Lost to cryptocurrency scams in 2023 alone - a 41% increase on the prior year (Action Fraud)
£649m	Total investment fraud losses reported in 2024, of which cryptocurrency and unspecified trading accounted for 75% of all commodity types cited (Action Fraud / City of London Police)
66%	Proportion of all UK investment fraud reports in 2024 linked to cryptocurrency - up 16 percentage points on 2023 (City of London Police)
41%	Share of all crime in England and Wales represented by fraud (Crime Survey for England and Wales, year ending September 2024)
14%	Estimated proportion of fraud cases reported to authorities - meaning actual losses are a substantial multiple of recorded figures (NCA / CSEW)

The Reporting Gap

The figures above represent only what is reported. The National Crime Agency and the Crime Survey for England and Wales consistently observe that fraud is profoundly under-reported, with an estimated 86% of cases never reaching Action Fraud or the police. Victims are frequently embarrassed, do not recognise that a crime has occurred, or have been manipulated into believing they have made a bad investment rather than been defrauded. For cryptocurrency fraud specifically, the complexity and unfamiliarity of the technology creates additional barriers to reporting. The true scale of losses is therefore considerably greater than published statistics suggest.

Part II: How Cryptocurrency Provides Cover for Fraudsters

Pseudonymity and the Anonymity Illusion

A common misconception is that cryptocurrency transactions are anonymous. In fact, every transaction on a public blockchain is permanently and immutably recorded. Wallet addresses, transaction values, and timestamps are all visible to anyone with access to a blockchain explorer. The more accurate description is pseudonymity: transactions are tied to alphanumeric addresses rather than named individuals, and the linkage between an address and its real-world controller is not visible on-chain.

This pseudonymity serves fraudsters in a number of ways. It removes the immediate accountability that attaches to a named bank account. It allows the rapid creation of new addresses at no cost and with no identity verification, enabling funds to be dispersed across hundreds of wallets within seconds. And it exploits the unfamiliarity of investigative tools and legal processes that were designed for traditional financial systems.

Speed: The Critical Asymmetry

In conventional banking, a suspicious payment can be intercepted because settlement takes time. Bank transfers in the UK process through Faster Payments within seconds, but the underlying systems and correspondent banking relationships still provide intervention windows that do not exist in the same way on a blockchain.

On a public blockchain, a transaction achieves finality - the point at which it cannot be reversed - within minutes or even seconds, depending on the network. From the point at which a victim is deceived into sending cryptocurrency to a fraudster's wallet, the funds can be: broken into smaller amounts and dispersed across multiple wallets; passed through "mixers" or "tumblers" designed to obscure the transaction trail; converted through decentralised exchanges that do not hold customer data; and ultimately off-ramped through a centralised exchange into fiat currency. This entire process can be completed in under an hour. Law enforcement notification, asset tracing, and court application timescales are measured in days and weeks. The asymmetry is fundamental and is exploited by design.

The Off-Ramp: Where Criminal Proceeds Are Realised

Despite the apparent anonymity of the on-chain environment, every criminal who holds cryptocurrency must eventually convert it to usable money. It is important to be precise about the legal stages involved. Assets that are held or transferred on-chain and represent the proceeds of unlawful conduct already constitute criminal enrichment - they are property obtained through unlawful conduct within the meaning of the Proceeds of Crime Act 2002 (POCA). The "off-ramp" - the point at which digital assets are sent to a centralised exchange and converted into fiat currency - constitutes "conversion" as specifically defined under POCA 2002. That act of conversion is legally distinct and significant: it completes the laundering cycle, triggers additional money laundering offences, and enables criminal proceeds to enter the mainstream economy in a form that is far harder to trace or recover. It is by interdicting funds at or before this point that enforcement intervention is most effective.

The off-ramp is predominantly controlled by centralised exchanges (CEXs): regulated Virtual Asset Service Providers subject to Know Your Customer, Customer Due Diligence, and transaction monitoring obligations. These entities represent the chokepoint at which enforcement intervention

is most viable. However, their effectiveness depends entirely on the speed and quality of information they receive. Under current arrangements, that information arrives slowly, in formats that are difficult to act upon, and without the verification or legal authority necessary to compel immediate action.

Common Fraud Typologies

The City of London Police, the NCA, and Action Fraud data together illuminate the primary fraud typologies in which cryptocurrency plays a central role:

- Investment fraud and advance fee schemes that promise guaranteed returns from cryptocurrency trading, often promoted through AI-generated celebrity endorsements on social media platforms. In 2024, over £10 million was lost to fraudsters impersonating Martin Lewis, Elon Musk, and Jeremy Clarkson alone.
- Romance fraud, in which fraudsters cultivate relationships over weeks or months before directing victims to invest in fraudulent cryptocurrency platforms under their supposed guidance.
- Authorised push payment (APP) fraud, in which victims are deceived into sending cryptocurrency directly to fraudster-controlled wallets, facilitated by impersonation of banks, law enforcement, or government agencies.
- Ransomware and cyber-enabled extortion, where cryptocurrency is demanded as the exclusive payment mechanism, exploiting its irreversibility and cross-border reach.
- Rug pulls and fraudulent token issuance, in which operators create cryptocurrency projects, attract investment, and then withdraw all liquidity, leaving investors with worthless assets.

The International Dimension

Official estimates suggest that 75% of UK fraud has hallmarks of overseas involvement, and the NCA identifies the cyber-enabled nature of fraud and the cross-jurisdictional movement of proceeds as among the most significant operational challenges. Cryptocurrency amplifies this problem: funds can be sent from a UK victim to a server farm in Southeast Asia, through a mixer in Eastern Europe, and off-ramped through an exchange registered in a jurisdiction with minimal AML controls, all within the time it takes an investigator to identify the initial wallet address.

The UK Government's 2023 Fraud Strategy explicitly reconceptualised fraud as a global threat requiring a global response. The Home Office's 2026–2029 fraud strategy identifies cryptocurrency as a priority area, with specific commitments to enhance the NCA's capacity to trace crypto-linked fraud and support the Serious Fraud Office in digital asset investigations. The strategic direction is clear. The operational tools to deliver on it are not yet adequate.

Part III: How Technology Can Uncover and Disrupt Cryptocurrency Fraud

Blockchain Analytics: Necessary but Insufficient

Blockchain analytics platforms have transformed law enforcement's ability to trace cryptocurrency flows retrospectively. By clustering wallet addresses, identifying known exchange deposit

addresses, and flagging wallets previously associated with illicit activity, tools of this type can reconstruct a transaction trail across hundreds of hops and multiple chains. The NCA's Operation Elaborate, which dismantled the iSpooof fraud platform, demonstrated how blockchain analysis can be instrumental in taking down fraud infrastructure at scale.

However, analytics alone are a retrospective tool. They tell investigators where funds have been, not where they are going. They do not create any enforceable legal notice on the chain itself. They do not automatically alert centralised exchanges in real time. And they do not travel with the funds as they move: each new wallet requires a fresh analytical assessment. In a threat environment where funds move in minutes, a tool that operates on an hours or days timescale leaves a critical gap.

The REKTify™ Approach: On-Chain Legal Enforcement

REKTify™, developed by iSanctuary, addresses this gap through a fundamentally different mechanism. Rather than observing the blockchain from the outside, REKTify™ deploys directly onto it, placing an enforceable legal notice - in the form of a soulbound smart contract - on the target wallet within seconds of authorisation. This is the core proposition: for the first time, enforcement can operate at the same speed as the criminal. A restraint order under sections 40-41 of POCA 2002, a civil freezing injunction, a worldwide Mareva order, a police fraud marker, or a sanctions notice can each be placed on-chain as an immutable, court-sanctioned token within seconds of being granted. The notice cannot be moved or removed by the wallet holder. It travels with any funds as they move, applying a fresh marker at each subsequent wallet. And it generates automated, real-time alerts to investigators and, where appropriate, to centralised exchanges.

Core Technical Capabilities

- **On-chain notice:** Soulbound token deployment directly to target wallets, creating an irremovable on-chain legal marker that persists regardless of the wallet holder's actions. Only iSanctuary, as the issuing authority, can remove the marker.
- **Document attachment:** Court orders, freezing injunctions, police fraud references, and compliance certifications can be attached directly to the smart contract, enabling legally valid service of process on-chain.
- **Real-time alerting:** Continuous monitoring of flagged wallets, with automated alerts dispatched within seconds to investigators and exchanges when any transaction involving a marked wallet occurs.
- **Intelligence gathering:** Every interaction with a REKTify™ token generates intelligence, including IP addresses and geolocation data, supporting the identification of wallet controllers and the building of court-ready evidential packages.
- **Scale and persistence:** Notices can be placed across thousands of wallets simultaneously and track funds through multiple layers of obfuscation, with a new marker applied at each step.

Legal Validation

REKTify™ is not a theoretical proposition. It has been deployed in live litigation and has received judicial authorisation at the highest levels in two separate jurisdictions. In a landmark matter, the

High Court of Singapore granted authority to iSanctuary to place a worldwide freezing injunction - a Mareva order - on-chain via a smart contract, a legal first for that jurisdiction. The court accepted that on-chain service of process, with attached documentation, constituted legally valid service. Subsequently, the High Court of England and Wales granted an equivalent order, confirming that REKTify™'s methodology is recognised and enforceable within the domestic courts of the United Kingdom. Together, these orders establish a compelling cross-jurisdictional precedent for court-enforceable on-chain notice that is directly relevant to the UK policy framework under consideration.

In a further matter, REKTify™ traced over \$3 million in stolen cryptocurrency within six hours of the initial report, locating 95% of assets and placing centralised exchanges on immediate written notice. In 2023, the technology uncovered in excess of \$1 billion in unlawfully held cryptocurrency across multiple investigations.

Part IV: Policy Framework - Building a National On-Chain Fraud Marker System

The CIFAS Parallel

The United Kingdom already operates one of the world's most sophisticated shared fraud prevention systems in the traditional financial sector. CIFAS - the Credit Industry Fraud Avoidance System - allows banks, lenders, insurers, and other regulated institutions to place and share fraud markers against accounts and individuals. CIFAS markers trigger enhanced due diligence, transaction monitoring, and, where appropriate, account restriction. In 2024, CIFAS members reported preventing over £2.1 billion in fraud losses through shared National Fraud Database intelligence.

REKTify™ applies the same principle to the blockchain. A marker affixed to a wallet acts as a transparent, universally visible signal to all centralised exchanges and digital asset service providers that the wallet is associated with a court order, police fraud reference, or other legal concern. As a CIFAS marker prompts a bank to apply enhanced scrutiny and potential account restriction, a REKTify™ marker prompts a VASP to temporarily freeze inbound funds and conduct focused, targeted analysis before permitting any withdrawal or conversion.

Account Freezing Orders and the Digital Analogue

Account Freezing Orders (AFOs), introduced under the Criminal Finances Act 2017 as amendments to POCA, allow enforcement agencies to freeze bank accounts suspected of containing the proceeds of crime without requiring a criminal conviction. They are among the UK's most powerful tools for rapid asset denial. Under sections 40-41 of POCA 2002, the Crown Court also has the power to make criminal restraint orders - prohibiting any person from dealing with realisable property where there are reasonable grounds to suspect they have benefited from criminal conduct. REKTify™ creates, for the first time, a direct on-chain mechanism for both of these instruments: a criminal restraint order, a civil freezing order, or an AFO can be deployed as an immutable soulbound token on a target wallet within seconds, providing the enforcement parity with criminal activity that has until now been structurally impossible.

Where a REKTify™ marker has been deployed to a wallet and a VASP has, in response, suspended the relevant funds, the legal and operational framework for a digital freezing order already exists in practice. A standardised policy process - akin to the AFO framework - applied to frozen digital assets would enable swift, structured forfeiture proceedings; direct compensation to identifiable victims from recovered funds; and, where victims are unidentifiable, redistribution of recovered assets under the Asset Recovery Incentivisation Scheme (ARIS).

ARIS currently redistributes recovered criminal assets to law enforcement, the Crown Prosecution Service, the National Crime Agency, and the Home Office. In the financial year ending March 2024, £98.1 million in ARIS funding was distributed to agencies. The integration of recovered digital assets into this pipeline would materially increase the funds available to combat serious and organised crime. Crucially, where REKTify™ is deployed as a fraud marker - identifying and flagging illicit assets before they are converted - the operational cost of deployment can readily be offset against the value of assets frozen and recovered. This makes the technology genuinely cost-neutral for government and law enforcement from the outset, and self-funding at scale as recovery volumes increase.

A further and significant legal consequence flows from REKTify™'s on-chain deployment. Where a criminal restraint order or civil freezing injunction has been served via a REKTify™ token on a self-custody wallet, and the subject of that order refuses to surrender the private keys to their wallet and then moves or dissipates the funds, they commit additional criminal offences. Breach of a restraint order under section 41 of POCA 2002 constitutes contempt of the Crown Court. Beyond that, as confirmed in *R v Kenny*, breach of a restraint order can also give rise to a charge of perverting the course of justice - a serious criminal offence. The on-chain notice means that the subject cannot credibly claim ignorance of the order. Where funds are subsequently moved from a marked wallet, REKTify™'s real-time alerting and intelligence-gathering capabilities provide immediate, timestamped evidence of that breach, strengthening the case for further criminal proceedings.

Sanctions Enforcement and the Prevention of Terrorist Financing

An increasingly significant application of REKTify™ lies in the enforcement of financial sanctions. Sanctions authorities including OFAC, the UK Office of Financial Sanctions Implementation (OFSI), and equivalent bodies across allied jurisdictions regularly identify cryptocurrency wallet addresses as sanctioned, whether on grounds of terrorist financing, corruption, proliferation, or other designated activity. At present, that designation data is collected by blockchain analytics tools and may be identified through transaction monitoring by regulated entities - but the sanctions notice itself has no on-chain presence. It exists only in external databases and the compliance systems of those who subscribe to them.

REKTify™ offers the ability to place an official, verified sanctions notice directly on the wallet as an immutable on-chain token. This has significant practical and legal consequences. First, it provides a universally visible warning to all participants in the blockchain ecosystem - not only regulated VASPs - that the wallet is subject to sanctions. This is particularly important in the context of terrorist financing, where criminal actors frequently exploit the anonymity of cryptocurrency platforms and social media to solicit funds from members of the public who believe they are contributing to a legitimate cause. A prominent example is fundraising campaigns on platforms

such as Telegram that purport to collect donations for humanitarian purposes - such as aid for civilian hospitals in conflict zones - when the wallet receiving those funds is in fact controlled by a proscribed organisation. A REKTify™ sanctions notice on such a wallet provides a visible, verifiable warning that can prevent innocent third parties from sending funds in good faith.

Second, where a person sends funds to a REKTify™-marked sanctions wallet, the on-chain notice substantially reduces the scope for a defence of ignorance. Under UK law, the knowledge or reasonable suspicion that property is the proceeds of crime or linked to terrorist financing is central to a number of offences under POCA 2002 and the Terrorism Act 2000. An immutable, publicly visible on-chain notice creates a strong inference that a sender had, or ought to have had, knowledge of the sanctions designation - materially increasing the prospects of prosecution and reducing the credibility of a claim that the transaction was inadvertent. In the context of counter-terrorist financing, where the ability to demonstrate knowledge is often the decisive evidential question, this is a meaningful addition to the enforcement toolkit.

Supporting VASPs to Meet Compliance Obligations

The UK's regulatory framework for Virtual Asset Service Providers is rapidly maturing. VASPs are subject to increasing obligations in respect of KYC, Customer Due Diligence, transaction monitoring, and Suspicious Activity Reporting. However, they currently lack a standardised, real-time mechanism to receive and act upon notifications of suspected criminal funds arriving on their platforms.

REKTify™ directly addresses this gap. By providing centralised exchanges with clear, verified, on-chain signals of criminal association - derived from court orders, police fraud references, or regulatory notices - the technology enables VASPs to discharge their compliance obligations more effectively and defensibly, while providing a clear audit trail supporting SAR filing obligations and demonstrating proactive compliance to regulators.

Part V: Recommendations

iSanctuary invites the UK Government to consider the following steps, which would position the United Kingdom as the first jurisdiction to deploy nationally standardised on-chain criminal restraint and civil freezing orders, establish a blockchain fraud marker system, and build a sanctions enforcement capability that operates at the speed of the criminal threat. Adoption has the potential to drive a substantial uplift in the value of digital criminal assets seized and recovered, at a cost that is offset by the proceeds of that recovery.

1. Formalise on-chain deployment of criminal restraint orders and civil freezing orders under POCA 2002 as a standard enforcement tool, working with the Crown Prosecution Service, the NCA, and the judiciary to establish a recognised process for REKTify™ deployment at the point an order is granted. This single step has the greatest potential to increase asset seizure volumes: by placing a restraint or freezing order on-chain within seconds, enforcement can for the first time operate at the speed of the criminal and prevent dissipation before it occurs.
2. Develop a standardised REKTify™ fraud marker framework for blockchain assets, analogous to the CIFAS National Fraud Database, for adoption across all UK-regulated

VASPs. This would create a shared, real-time intelligence layer for the blockchain environment that alerts exchanges to inbound criminal funds before off-ramping occurs, equivalent to the system that prevented over £2.1 billion in traditional fraud losses in 2024 alone.

3. Integrate REKTify™-recovered digital assets into the ARIS distribution framework under POCA, ensuring that illicit cryptocurrency is redirected to fund further enforcement activity and victim compensation. The operational cost of REKTify™ deployment is offset by recovered proceeds, making the model cost-neutral from the outset. Given the scale of unrecovered cryptocurrency fraud proceeds, the pipeline into ARIS has the potential to grow substantially beyond the £98.1 million distributed in the year to March 2024.
4. Work with OFSI and allied sanctions authorities to develop a programme for placing official sanctions notices on designated cryptocurrency wallets via REKTify™, providing an on-chain warning visible to all participants in the blockchain ecosystem and reducing the scope for innocent third parties to inadvertently send funds to sanctioned addresses, including those linked to terrorist financing.
5. Engage with iSanctuary to pilot a coordinated deployment programme in partnership with the City of London Police, the NCA, and a cohort of UK-regulated VASPs, with a view to generating the operational evidence base for national adoption and demonstrating, with measured data, the uplift in asset seizure and recovery that on-chain enforcement can deliver.



50–60 Station Road, Cambridge CB1 2JH, United Kingdom
+44 (0)20 3871 2529 • info@isanctuary.io • www.isanctuary.io

REKTify™ is a registered trademark of iSanctuary.