CASE STUDY

One Hop From a $6bn Fraud

How Hoptrail identified and protected a client from exposure to the world's largest cryptocurrency seizure.

- During a crypto source of wealth engagement in 2025, Hoptrail uncovered evidence linking a prospect's Bitcoin wallet ecosystem to addresses attributed to the so-called Lantian Gerui fraud, a $6 billion money laundering scheme prosecuted in the UK.
- The connection was established by matching on-chain transaction data against publicly available records from law enforcement, court documents, mainstream media, and social media.
- This case study illustrates why in-depth EDD and ecosystem analysis are essential for complex crypto-native clients, and why institutions relying on automated transaction monitoring may face material blind spots in their anti-money laundering frameworks.

LANTIAN GERUI FRAUD

The Lantian Gerui Fraud was a Ponzi scheme orchestrated by Chinese national Zhimin Qian between 2014 and 2017. Qian carried out the fraud through her company, Tianjin Lantian Gerui Electronic Technology Co., Ltd, which marketed itself as a fintech and cryptocurrency venture, promising investors annualised returns of up to 300% by claiming to use their funds for Bitcoin mining and investments in advanced health technologies. The scheme targeted over 128,000 individuals across China.

The fraud collapsed in July 2017 following a Chinese government investigation into illegal fundraising, which suspended all Initial Coin Offerings and shut down domestic crypto trading platforms. Before the investigation intensified, Qian converted the illicit proceeds – estimated at RMB 43 billion ($6.1 billion) – into Bitcoin and fled China to the UK using a fake passport.

In 2018, UK Metropolitan Police raided Qian's London residence, seizing devices containing approximately BTC 61,000, then worth hundreds of millions. By the time of formal confiscation in 2021, assets were valued in the billions of pounds.

Following the arrest of an accomplice in 2021, Qian was arrested in April 2024 in York and pleaded guilty in September 2025 to money-laundering offences related to the criminal proceeds.[1] On 11 November 2025, she was sentenced to 11 years and eight months in prison.

KEY EVENTS

- **2018:** *Metropolitan Police Raid*
  UK Metropolitan Police raided Zhimin Qian's London residence. Officers seized encrypted devices later found to contain approximately BTC 61,000.

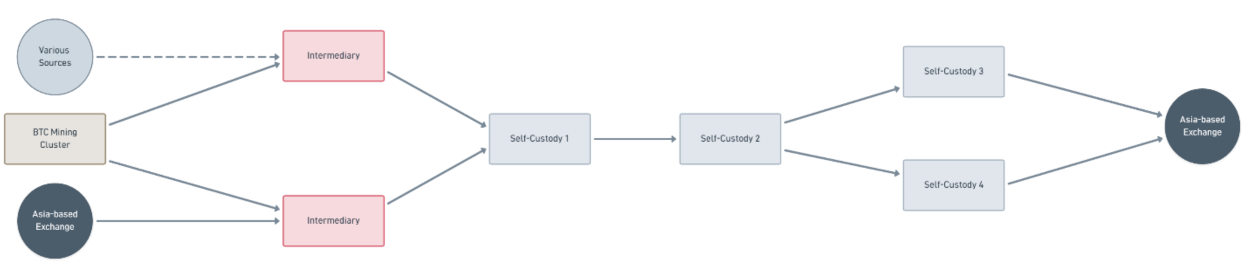
- **May 2021:** *Investigators Gain Access*
  Investigators began accessing the seized devices. On approximately 30 May 2021, around BTC 4,500 was siphoned from one of the seized wallets by unknown persons in the early hours. Qian's accomplice Jian Wen was arrested on money laundering charges.

- **June – September 2021:** *Formal Seizure & Transfer to Coinbase*
  Police formally transferred the seized Bitcoin to UK Government wallets at Coinbase.

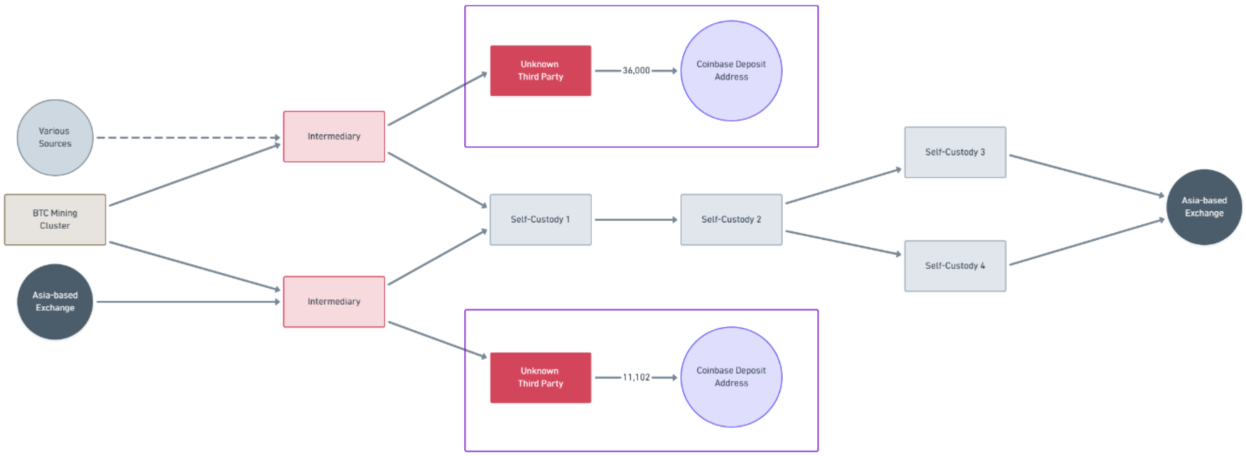
- **April 2024 –** *Zhimin Qian arrested in the UK*
  Qian arrested in York (UK), leading to a September 2025 guilty plea and November 2025 sentencing.

STEP 1: MAPPING THE WALLET ECOSYSTEM

The starting point for the investigation was a deposit wallet controlled by the prospect at an Asia-based trading venue. Hoptrail traced the sources of funds for the address, mapping wallets that fed into the venue. This exercise revealed a network of self-custody wallets that themselves received funds from various known and unknown sources, including crypto exchanges, mining pools, and the same Asia-based venue. Funds from these services were primarily channelled through two intermediary wallets (in red below).



The intermediary wallets were found to have received sizeable deposits in 2017, with one receiving more than BTC 9,000 ($11.45 million). These funds were then partly routed to the prospect's deposit address at the Asian exchange, but most were transferred to two unknown third-party wallets in mid-2017 (in dark red below).



These unidentified wallets were found to have collected extremely large sums of BTC in a matter of days in April 2017. In July 2021, their entire holdings were simultaneously withdrawn to two separate Coinbase deposit addresses. At the time, these assets were worth a combined $1.5 billion (£1.2 billion).

MAY 2021: CORROBORATING WITH OFF-CHAIN PUBLIC RECORD

Given the suspicious and abnormally large transfers in the subject's ecosystem – and the approximate four-year delay between deposits and withdrawals (to a venue not associated with the subject) – Hoptrail sought to corroborate blockchain evidence against multiple off-chain sources.

Research unearthed a series of articles referencing a sizeable BTC seizure by the UK's Metropolitan Police, beginning in mid-2021 – matching the approximate timeframe for the withdrawals to Coinbase.

- **July 2021:** The Guardian reported the seizure of £114 million in crypto-assets in June 2021, noting that police accessed the funds the month before.[1] The article confirmed the arrest of a 39-year-old woman, later identified at Qian's accomplice Jian Wen in UK court documents.[2]

- **January 2024:** Qian was named in press reports as an associate of Wen (operating under the pseudonym Yadi Zhang) – the first public mention of her in connection with the police seizures.[3]

[1] https://www.theguardian.com/technology/2021/jul/13/met-police-bitcoin-money-laundering-cryptocurrency
[2] https://www.judiciary.uk/wp-content/uploads/2024/05/Wen-Sentencing-Remarks.pdf
[3] https://www.serjeantsinn.com/wp-content/uploads/2024/01/Woman-accused-of-laundering-bitcoin-proceeds-of-5bn-fraud-in-London-trial-002.pdf

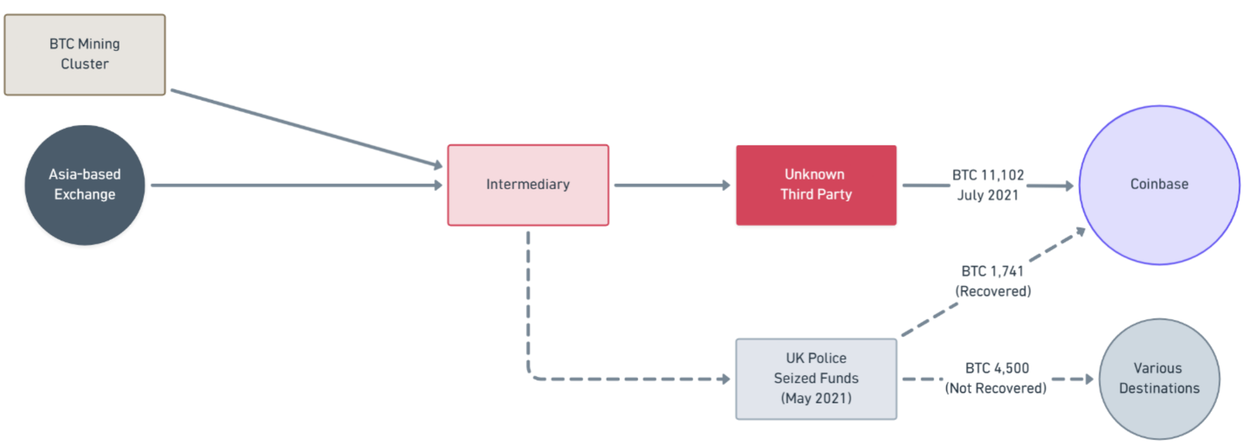
- **March 2024:** Financial Times confirmed UK law enforcement had seized BTC 61,000 and named Qian and Wen (whose age matched that of previous Guardian reporting).[4] The paper also reported that two wallets accessed by police in May 2021 held BTC valued at £1.2 billion, corresponding exactly to the values identified by Hoptrail.

- **April 2024:** Social media posts emerged strengthening link between the intermediary wallets and Qian and Wen.

STEP 3: UNAUTHORISED TRANSFERS

Part of the Financial Times reporting was an alleged unauthorised transfer on 30 May 2021 of around BTC 4,500 (£150 million) from a wallet seized by UK police.

Using the blockchain, Hoptrail isolated large BTC transfers in the early hours of 30 May 2021. This uncovered a withdrawal of $196 million at 4:33am from a wallet connected to one of the intermediary wallets. Tracing identified flows of BTC 1,741 back to Coinbase, pointing to a partial recovery by police of the siphoned funds but still leaving BTC 4,500 unaccounted for. Analysis found that no-KYC exchange platform TradeOgre was used to liquidate some of these proceeds.



[4] https://www.ft.com/content/0bc35bea-8a7d-4e0e-9406-64b480e03631?syn-25a6b1a6=1

WHAT HAPPENED NEXT?

Linkages between the subject and the Lantian Gerui fraud allowed Hoptrail to build a wider nexus, involving a complex network of wallets and transactions during the 2017 period. Further – and in some cases more direct – risk exposure was established, helping to demonstrate clear and obvious financial crime risks. In turn, this enabled the client to make a clear, informed onboarding decision regarding the prospect and to escalate the findings internally.

DATA MATCHING

Hoptrail utilised the following resources to match data points identified on the blockchain to draw a clear connection between the wallets under review and persons involved in the Lantian Gerui fraud:

Source	Data Point Matched
Law Enforcement	Seizure of ~BTC 61,000 from devices at Qian's London residence in 2018; access gained in 2021. Matched to on-chain transfer timing in July 2021.
Mainstream Media	Partial seizure reported at approximately £1.2 billion. Corroborated by Hoptrail's calculated value of $1.5 billion based on the BTC price at the time of the Coinbase transfer. Investigators began accessing wallets in or around late May 2021; approximately BTC 4,500 siphoned by unknown persons on 30 May 2021. This timeframe and amount were matched to specific on-chain transactions.
UK Court Documents	Age of Wen in sentencing remarks corroborated the age provided in 2021 reporting from the Guardian.
Social media	Independently identified a link between the intermediary wallet and the UK Government seizure address at Coinbase.

KEY TAKEAWAYS

The most significant insight from this investigation was not the connection itself, but how it was connected. Wallets attributed to Qian were not *sources* of funds flowing to the prospect's address. Instead, the wallets were co-participants in a shared ecosystem: they transacted through common intermediary addresses, shared counterparties, and operated within the same cluster of activity.

This distinction is key. Automated source of wealth screening works by tracing the direct origins of funds received by a wallet. If the flagged fraud addresses are not upstream sources – if they sit alongside the subject rather than behind them in the transaction graph – they will not appear in a standard SOW trace.

IMPLICATIONS FOR COMPLIANCE TEAMS

This case highlights a structural gap in automated AML tools when applied to complex, crypto-native clients. Transaction monitoring systems and automated SOW reports are essential components of any compliance framework, but they are designed to detect risk in direct fund flows. They are not designed to answer the broader question: *who else is operating in the same wallet ecosystem as my client?*

For institutions onboarding high-net-worth crypto-native clients - particularly those with complex, multi-year transaction histories - the lesson is clear: EDD-level analysis, of the kind applied by Hoptrail in this case, is critical in surfacing risks that exist beyond the direct transaction chain.

WORK WITH HOPTRAIL

Do you require in-depth analysis on complex crypto prospects?

Hoptrail's EDD reports are a combination of proprietary multi-hop on-chain tracing, entity attribution, and off-chain corroboration to surface risks that automated screening misses. Delivered in days, built to institutional standards, trusted by leading private banks and wealth managers.

Request an EDD report → hoptrail.io/contact
Learn more about EDD → hoptrail.io/products/edd-reports
Email the team → info@hoptrail.io