



Australian Government
Australian Taxation Office

Crypto Asset Trends and Investigative Techniques

OECD Tax Academy for Tax and
Financial Crime Investigation

Presented by Carla Walls and Ben Cuddy

November 2024

OFFICIAL | EXTERNAL

ATO Crypto Assets Directorate

What we do

- All source intelligence capability.
- Discover and target tax crime, evasion, and money laundering concerning crypto assets.
- Enable operational outcomes in collaboration with ATO and other domestic and international regulatory and law enforcement agencies.

Behaviours we examine

- Crypto asset-related tax evasion and fraud.
- Cybercrimes and related activities where crypto assets are utilised.
- Crypto asset enabled money laundering.
- Financial crimes involving crypto assets, including scams and fraud.

Crypto Asset Trends

- Continued growth in mainstream adoption both domestically and internationally driven by features such as:
 - low barriers to access
 - access to fast, low-cost international value transfers
 - increased personal control over assets and wealth
 - enhanced privacy
 - less regulated than traditional financial investments.
- Many legitimate use cases, however these features also make crypto assets vulnerable to criminal exploitation.



Obfuscation Techniques

- Layering funds through intermediary wallets
- Commingling illicit funds with funds from other sources
- Laundering through gambling services
- Use of mixers and tumblers
- Token swaps and cross-chain transactions
- Off-ramping - use of over-the-counter (OTC) service providers.

Not an exhaustive list!

Layering Funds Through Multiple Addresses

- Similar to traditional money laundering, in which funds are layered through multiple accounts or shell companies.
- Creates distance from, or obfuscates the source and/or destination of funds.
- Fees charged for each transaction – question whether fees paid make financial or commercial sense for legitimate operators?



Commingling With Other Funds

- Commingling funds from illicit sources with funds from other sources. This might include
 - Combining with legitimately sourced funds. For example, funds associated with investment, trading, or mining.
 - Combining with funds from other users. For example, via mixing services, moving funds through no-KYC exchanges.



Crypto asset gambling services

- Wide range of gambling services available:
 - Casino games
 - Sports betting
- High 'win' rates on most casino games.
- Disguise proceeds as gambling winnings, which may not be taxable, depending on the jurisdiction.



Token Swaps and Cross-Chain Transactions

Same chain token swaps

- Generally use decentralised finance (DeFi) platforms.
- Smart contracts facilitate exchange of one token for another on the same blockchain. For example, swapping ETH for USDT.
- High transparency, however complexity may slow down investigation.

Cross-chain transfers

- Asset from one blockchain (e.g. BTC) is sent to another blockchain.
- Various mechanisms –
 - Instant exchangers
 - Cross-chain bridges
 - Peer to peer, e.g. Bisq network
- Often transparent, however more complex than same-chain token swaps.

Use of OTC Services For Off-Ramping

Over-the-counter (OTC) services are crypto brokers that facilitate large trades between parties directly, bypassing public order books.

- Minimum trades usually USD 50,000 or equivalent.
- High liquidity and large trade volumes
- Genuine commercial services catering to institutional and high net worth traders
- Underground operators – operate on Telegram or other messaging services; usually no KYC and may advertise off-ramping of illicit proceeds.
 - Both commercial and underground services may be exploited by illicit actors.

Use of No-KYC Exchanges

These exchanges offer services to customers with no, or minimal Know Your Customer requirements.

- Often located in jurisdictions with low or no anti-money laundering regulation for crypto asset service providers.
- May be used to:
 - anonymise off-ramping transactions
 - obfuscate on-chain funds tracing (by routing through exchange infrastructure).



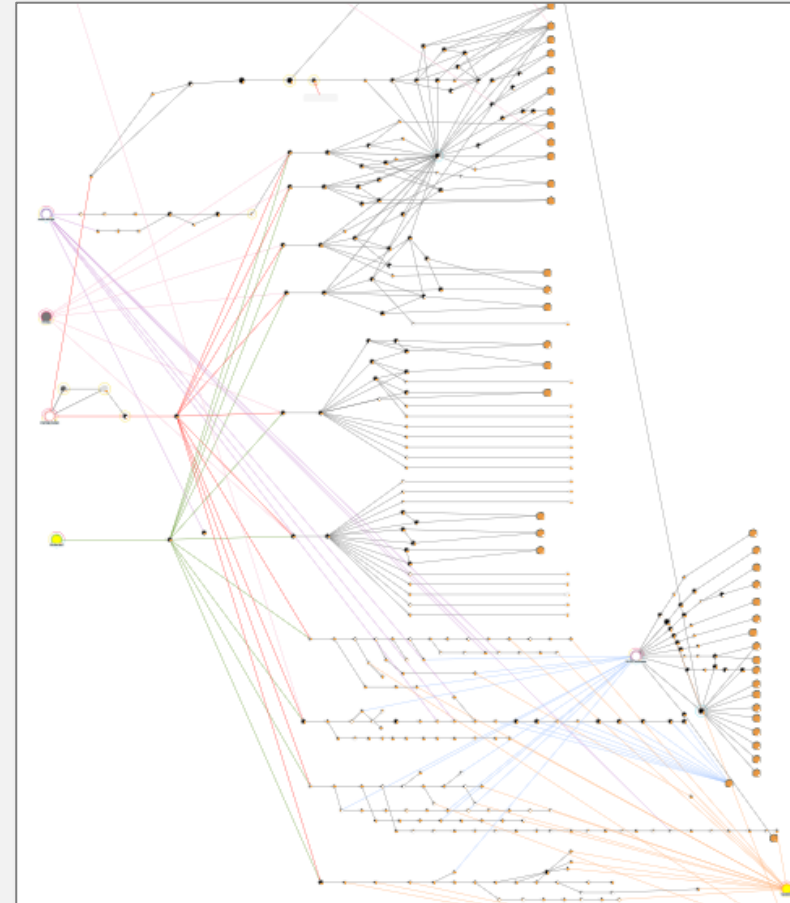
Case Study 1



Case Study: Transaction Dispersion

This case will look at a number of transaction dispersion techniques used by an individual in an attempt to legitimise and obfuscate the source of funds and their disposals.

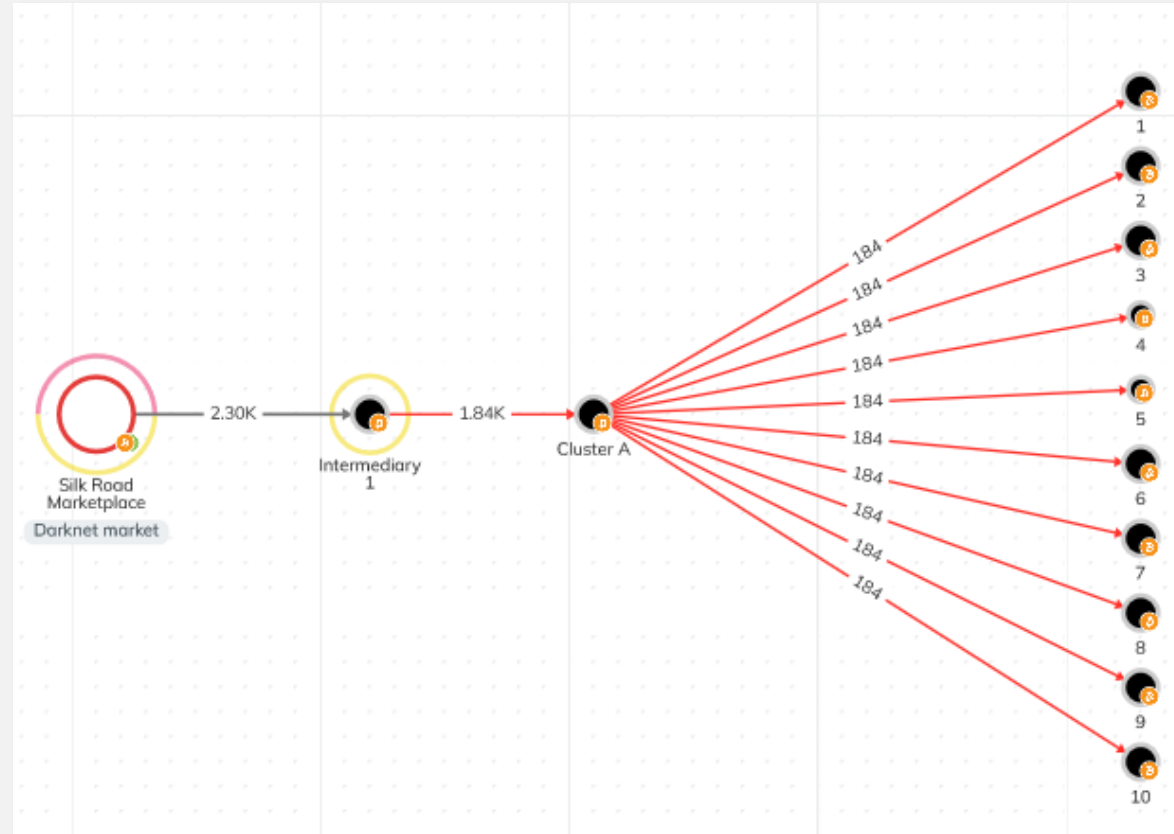
- This case resulted in an internal referral and led to over AUD 13.7 million in collections, after a successful audit and engagement of an Australian taxpayer.
- The crypto asset identification, analysis and intelligence provided the ATO insight into the individuals activity and provided assurance to the individuals claims upon engagement.



Source of Funds

In 2013, a BTC cluster assessed to be under the control of a Silk Road darknet vendor sent over 1800 BTC to an unidentified cluster (cluster A).

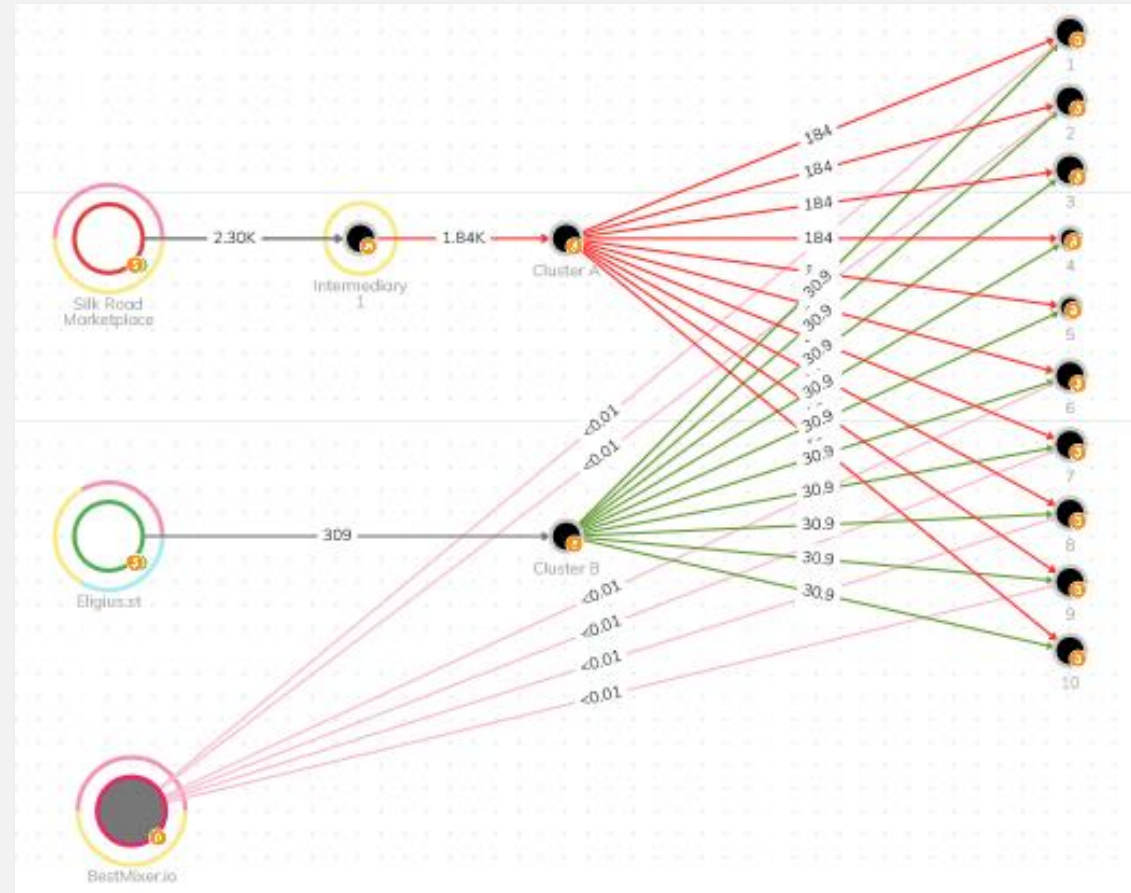
This cluster then sent the entire balance in equal amounts to 10 additional clusters.



Commingling

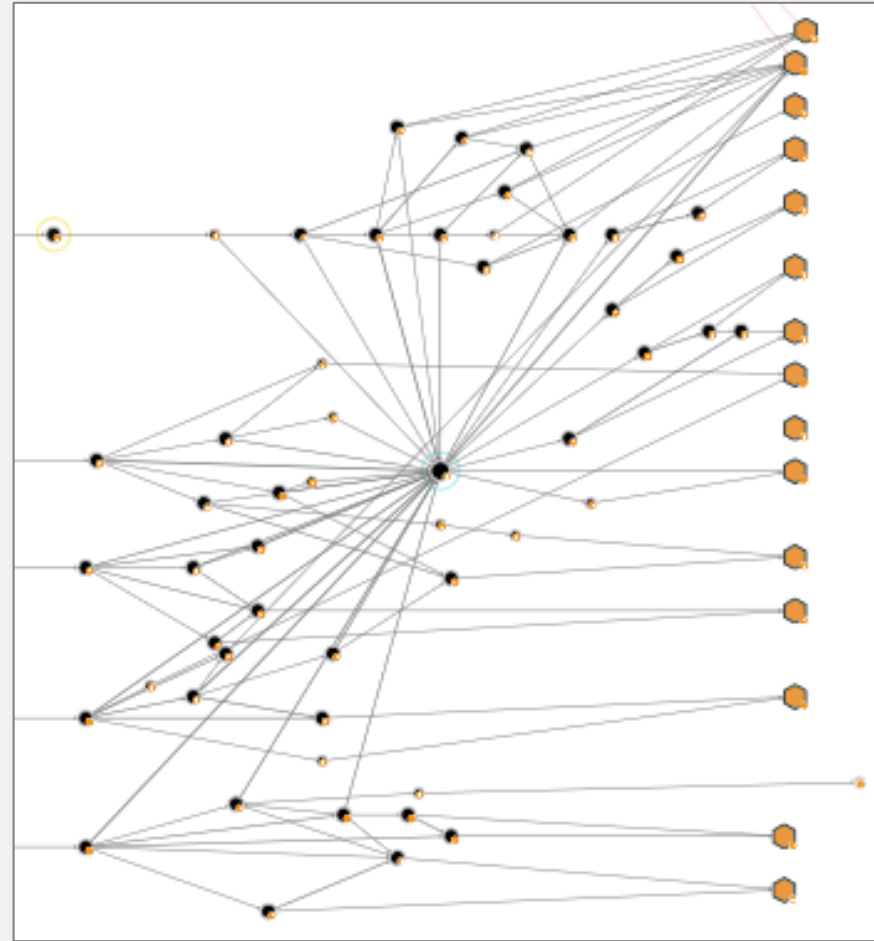
The entity co-mingled funds from various sources within each of the 10 secondary clusters.

For example, each of the 10 clusters also received transfers from Mining pool Eligius.St, and many also received transfers from mixing service BestMixer.io.



Manual Obfuscation

Bitcoin was transferred through hundreds of intermediate addresses, splitting and consolidating amounts at different stages, before ultimately sending to an Australian exchange for conversion to fiat.

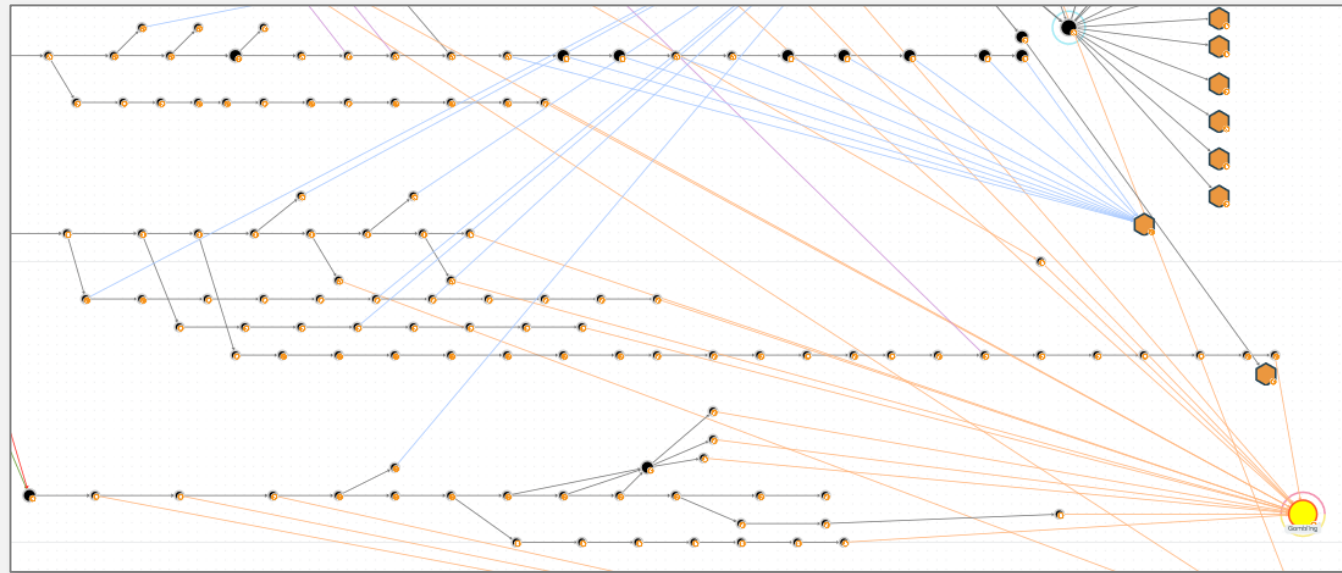


Peelchains

A common BTC transaction pattern, involving a long series of small transactions, with larger 'change' sent to a new address each time.

Often used as a layering technique to obfuscate funds flows, but may have legitimate uses.

Embedded feature in some wallet software and exchange payout mechanisms.



Mixers

- Mixers or 'tumblers' are software applications that typically pool incoming funds from multiple users, and 'mix' them, before re-distributing the funds proportionally to the senders, minus a small fee.
- This creates a disconnect between the user's deposit and withdrawal. Mixing is often used to cover up the movement of funds obtained from theft, darknet markets, or other illicit sources.



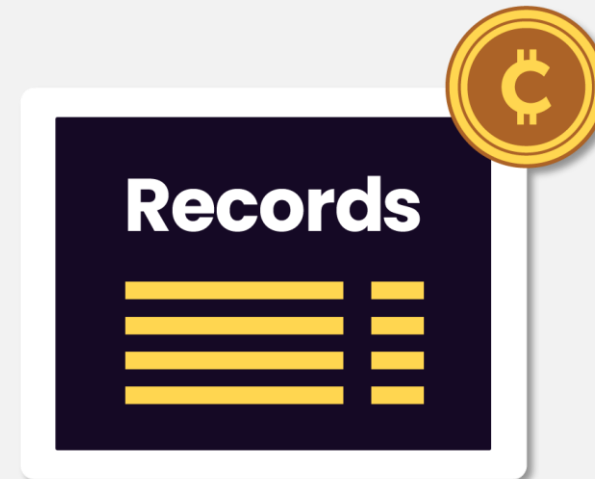
Gambling Services



- Crypto gambling services include both licensed and unlicensed casinos and poker rooms.
- Regulation may be limited, and enforceable only in certain jurisdictions.
- May be used to obfuscate funds flows, and 'legitimise' the source of funds.

No-KYC Exchanges

- No- or limited- KYC exchanges exist in various jurisdictions.
- Users do not provide identifying information, however blockchain analysis allows investigators to see sending and receiving transactions to/from these exchanges.
- In conjunction with other information and analysis, this can be used to assist in tracing funds flows to the source or destination.
- However, this should be done with caution.



Summary and Case Results

Following the flow of funds was significantly complicated by the use of multiple obfuscation techniques, over an extended period of time.

However, careful analysis and understanding of complex techniques assisted in identifying the source and destination of most funds.

Resulted in referral to client engagement for review of income tax lodgments.

Results:

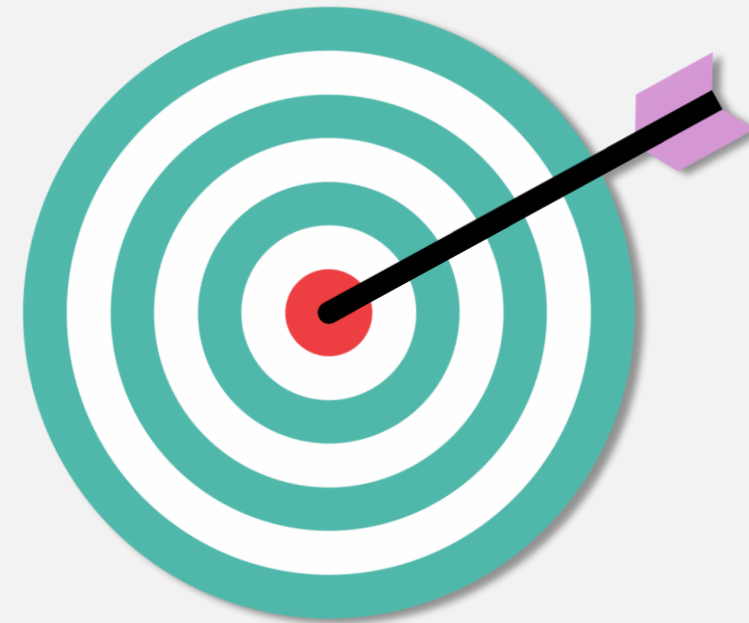
- Intelligence report supported audit team to evaluate the accuracy and validity of the taxpayer's reporting and statements the source of their income.
- Audit activity resulted in the collection of AUD 13.7 million in unpaid taxes and penalties.

Questions



Proactive Discovery and Targeting Approach

- A systematic approach to discovering the highest risk tax crime, evasion, and money laundering activities concerning crypto assets.
- Leverages multiple open and closed sources of data and information to understand risk populations and identify targets for further analysis and treatment opportunities.



Open Source Information and Intelligence Resources

- Open source blockchain explorers
- Crypto news and blogs
- Marketplace listings
- DeFi aggregators and Application Programming Interfaces (APIs)
- Social media



Third Party Data Sources

ATO crypto data matching program

- Our crypto asset data-matching program has been in place since April 2019.
- The ATO obtains data relating to transactions and account information from Australian crypto asset service providers (CASPs).
- The data obtained is used to identify the buyers and sellers of crypto-assets and quantify the related transactions.



Referrals From Domestic and International Partners

- Intelligence received from domestic and international partners – regulatory and law enforcement agencies.
- Key partnerships are facilitated via:
 - The Joint Chiefs of Global Tax Enforcement Alliance (J5)
 - The Australian Serious Financial Crime Taskforce
- We also collaborate globally with traditional and non-traditional partners, both private and public, on intelligence-led operations, expertise sharing, capacity development, policy, and law reform.



Case Study 2



Case Study: Proactive Targeting

- Tasked with identifying emerging risks associated with Non-Fungible Token (NFT) boom in 2021-2022.
- Identified potential for significant tax evasion relating to NFT creation, sale, and trade.
- This case study examines the techniques we used to detect, analyse, and ultimately treat tax risks associated with one of Australia's most significant NFT creators.

Identifying NFTs on the Blockchain

- Identify NFT token contract addresses.
- Publicly available through:
 - NFT marketplaces
 - Market aggregators
 - Blockchain explorers.

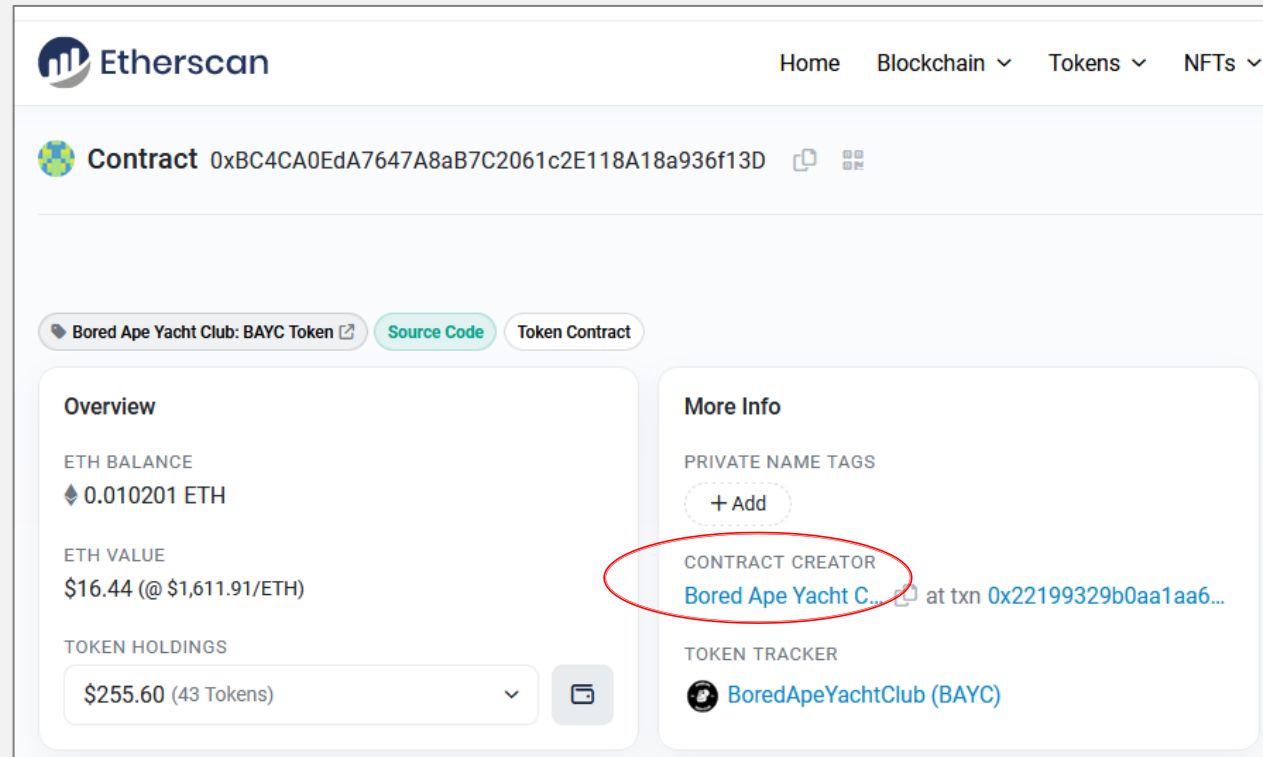
The image displays two screenshots illustrating how to identify NFT token contract addresses.

The top screenshot shows the Rarible website for the Bored Ape Yacht Club (BAYC) collection. The URL is <https://rarible.com/boredapeyachtclub/items>. The collection is titled "Bored Ape Yacht Club" and was created by 0x00000...0000. A sidebar on the right lists statistics: Floor (28.49 ETH), Volume (1.5M ETH), Items (10K), and Owners (5.8K). The Blockchain is identified as Ethereum, and the Address is 0xbc4...f13d.

The bottom screenshot shows the Etherscan website for the Bored Ape Yacht Club (BAYC) token contract. The contract address is 0xBC4CA0EdA7647A8aB7C2061c2E118A18a936f13D, which is circled in red. The page includes an Overview section with ETH Balance (0.010201 ETH), ETH Value (\$34.02), and Token Holdings (\$420.58). The More Info section lists the Contract Creator as Bored Ape Yacht Club and the Token Tracker as BoredApeYachtClub (BAYC).

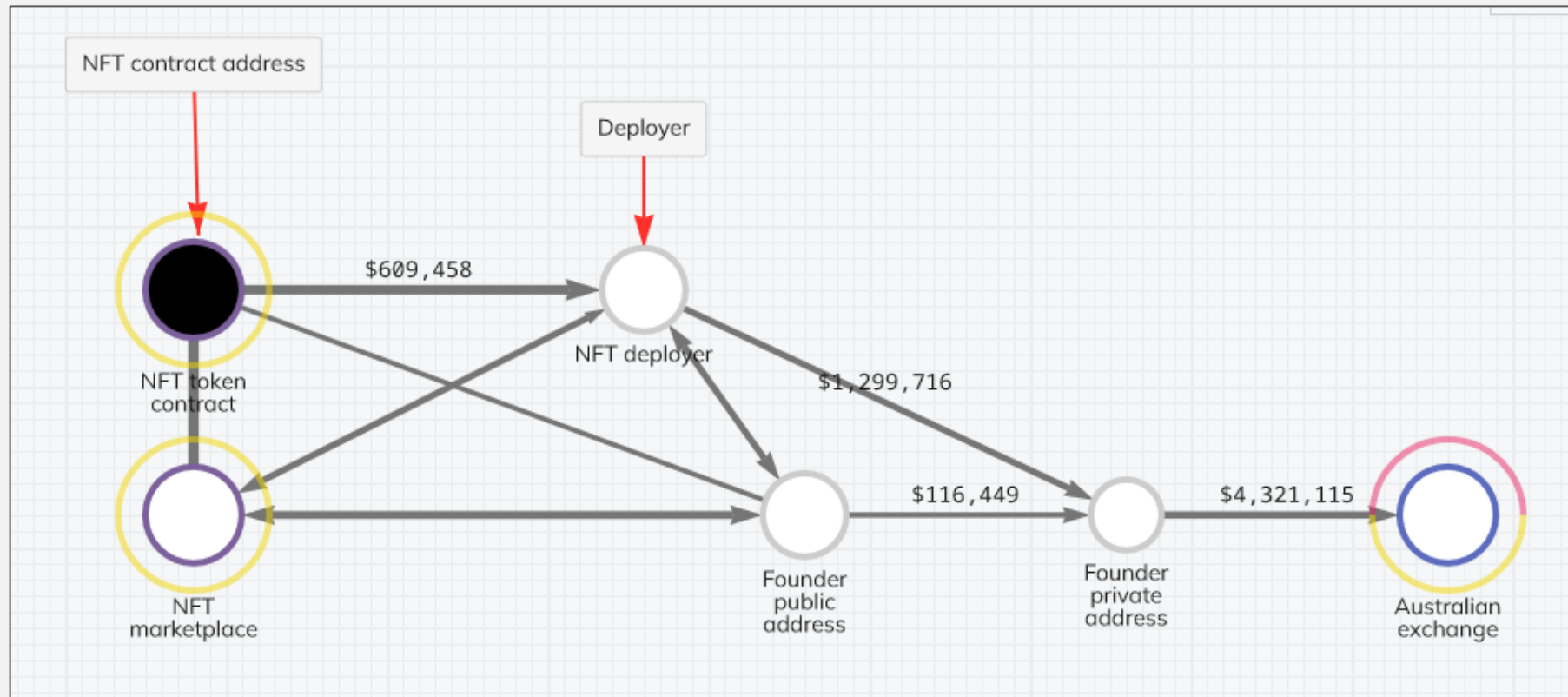
From Project to Creator

- Use a public blockchain explorer to:
 - Find the contract creator address.
 - Commence following funds flows to and from project addresses.



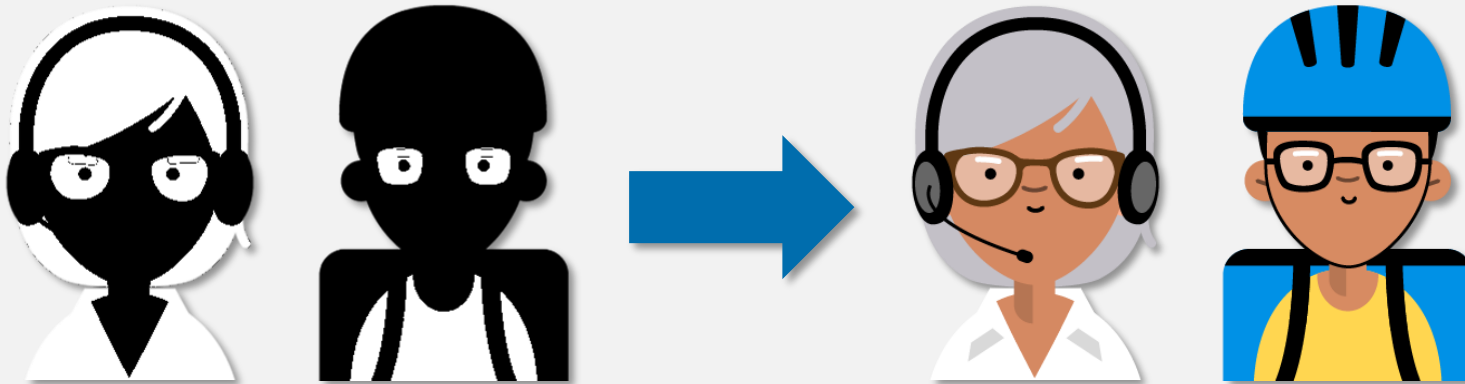
Identifying Creator Wallets

Tracing flow of funds to centralised Australian crypto asset service provider.



Attributing Creator Identities

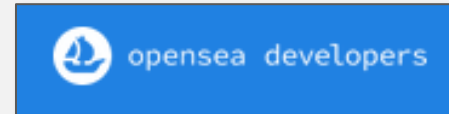
- Know-Your-Customer and transaction information held by exchange.
- Financial Intelligence Unit (FIU) reports linking exchange payments to Australian taxpayers.
- Use of common monikers across platforms linked to real-world identities.
- Branding linked to public intellectual property registrations.



Quantifying Economic Activity: OpenSea API

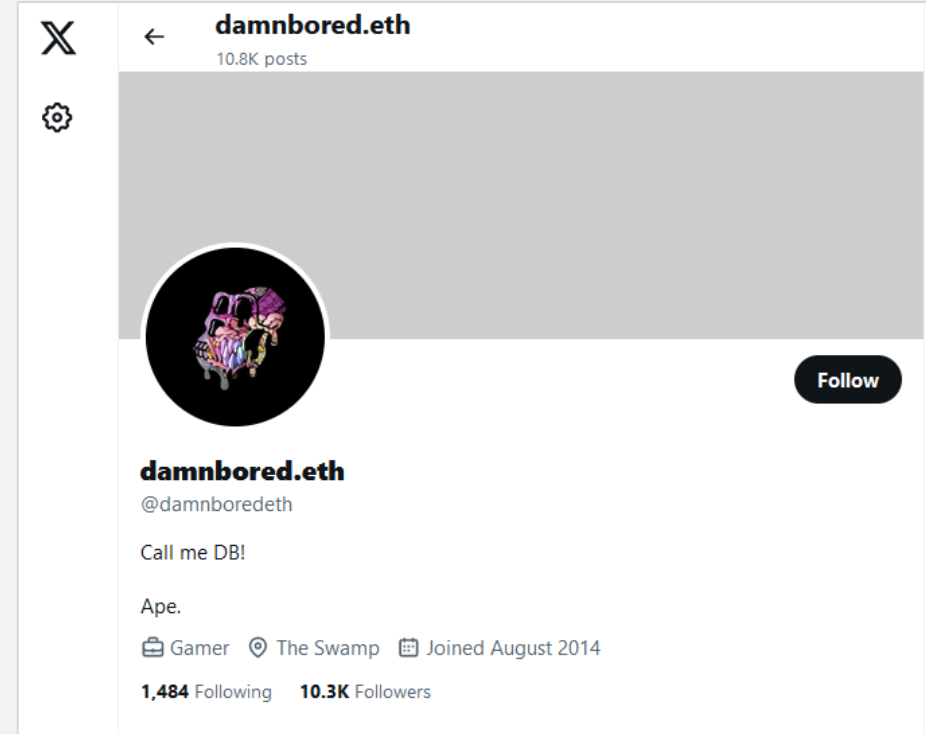
Access marketplace data to identify volume of activity and proceeds generated.

- NFT marketplaces commonly show sales data and secondary market sales from which royalties can be calculated.
- APIs may be available to link into marketplace data if looking at multiple projects.
- NFT and DeFi data aggregators often capture this information from across platforms.



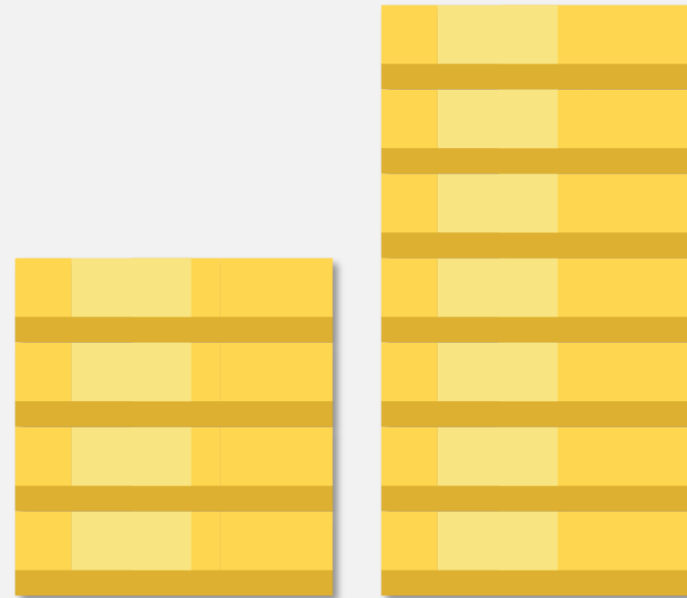
Ethereum Name Service: Attributing Payment Destinations

- Pivot to web search to examine monikers, for example, 'nftsmadembroke.eth'
- Monikers regularly utilised across platforms including social media.
- Multi-source attribution is possible.



Examining Other Crypto Asset Activity

- Etherscan also highlighted other token transfers associated with creator addresses:
 - Transfers of ERC-20 tokens.
 - NFT purchases and sales.
- NFTs and other tokens may be used to store wealth outside of the regulated financial system.



Identifying NFT Assets Held by Entities

ETH Price: \$1,547.74 (-4.27%) Gas: 11 Gwei

Search by Address / Txn Hash / Block / Token / Domain

Etherscan


Home Blockchain Tokens NFTs Resources Developers More Sign In

BoredApeYachtCl...
Bored Ape Yacht Club

Chat with Owner

Min Price (24H) 0.0000 ETH (\$0.00) Last Sale (Item) 0.66 ETH (\$1,021.51) Last Sale (Contract) 25 ETH (\$38,693.50)

Details

Owner: 0x7285e8f0186a0A41E73ceF7603AD7b80A2d...
Contract Address: 0xBC4CA0EdA7647A8aB7C2061c2E118A1...
Creator: Bored Ape Yacht Club: Deployer
Classification: Off-Chain (IPFS)
Token ID: 2017
Token Standard: ERC-721
Marketplaces: 
[Affiliate Disclosure](#)

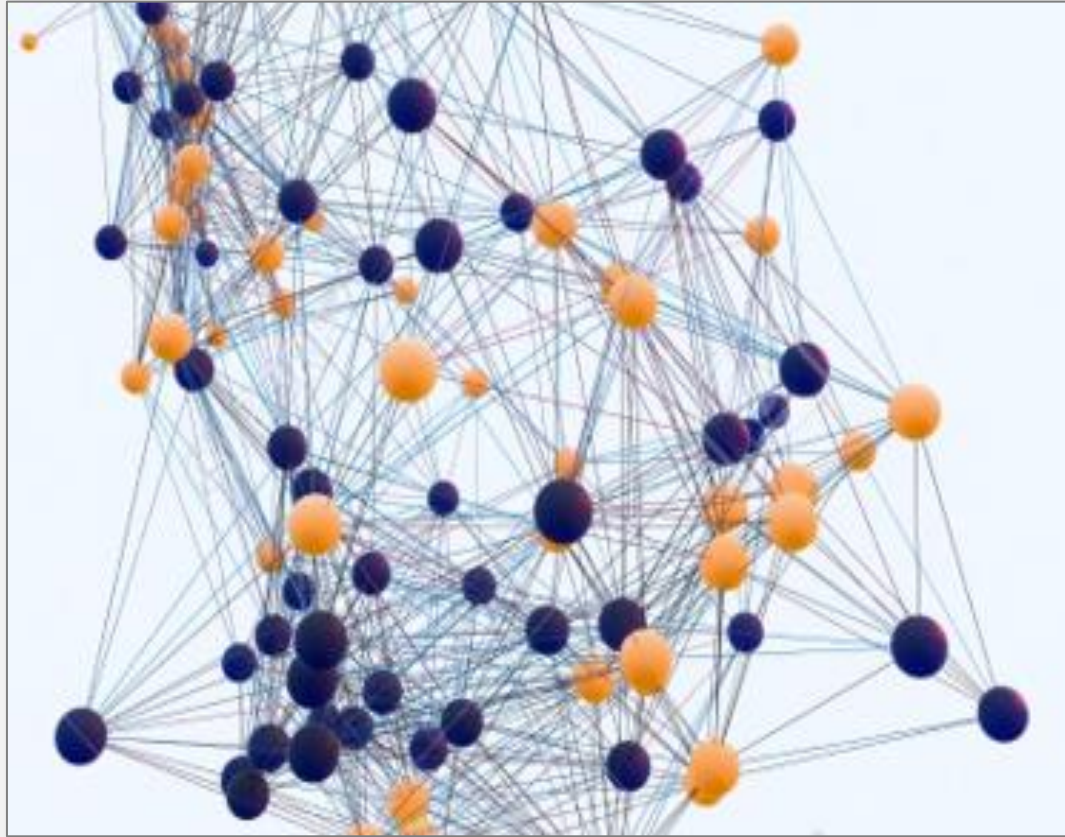
Properties (6)

- Etherscan shows purchases and sales of NFTs by the address holder.
- This includes value at time of sale, which can be used to calculate profits for tax purposes.

Txn Hash	Age	Action	Price	From	To
0x7e51e2d32d785e19...	198 days 11 hrs ago	Transfer		0x5d3f81...B914Fd7C	Blur.io: Marketplace 2
0x2ff0149aeb214c65e...	199 days 16 hrs ago	Sale	71.85 ETH (\$115,524.74)	0x2Efb79...842cF36D	0x5d3f81...B914Fd7C

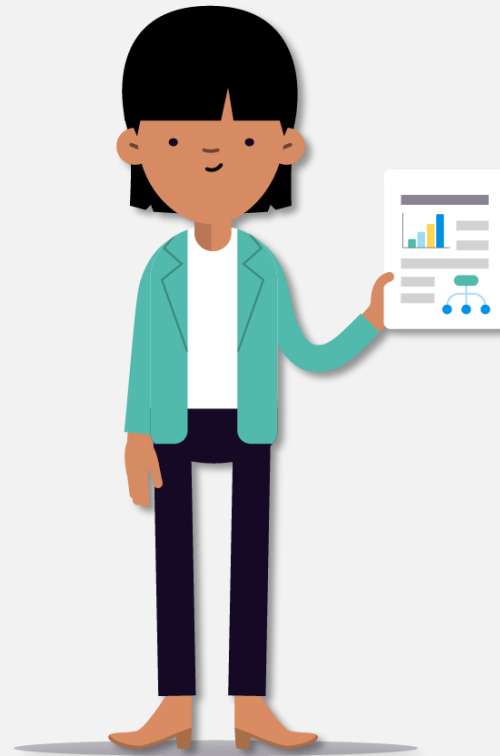
Evaluating Taxpayer Activities

- Multi-source income and assets evaluation
 - OSINT
 - Blockchain analysis
 - 'Closed' source data
 - FIU holdings
 - Company records
 - Tax reporting
 - Third party data



Intelligence Outcomes

- Global leaders in the NFT creator community identified
- Over AUD 11 million in proceeds in 2022 and 2023
- Creators cashed out proceeds in Australia
- In collaboration with international partners, conducted audit activity resulting profits brought to tax in Australia.
- To date, over AUD 1.27 million in liabilities raised, with further potential collection pending finalisation of audit.



Questions



Case Study 3



Case Study: Leveraging Open Source Tools

- Intelligence referral from international partners regarding multinational NFT scam network.
- In collaboration with partners, identified over USD 12 million in proceeds sent to Australian entities.
- Intelligence analysis undertaken to attribute Australian recipients, quantify associated scam proceeds, and evaluate role in rug pull network.
- Resulting intelligence brief provided to domestic and international law enforcement partners to progress criminal investigations.

Tracking Rug Pull Proceeds

- USD 120 million rug pull scam network
- Hyped NFT projects that failed to deliver.
- Project funds drained and traced to offshore founder.
- Portion of proceeds send to Australian Digital Currency Exchange address.



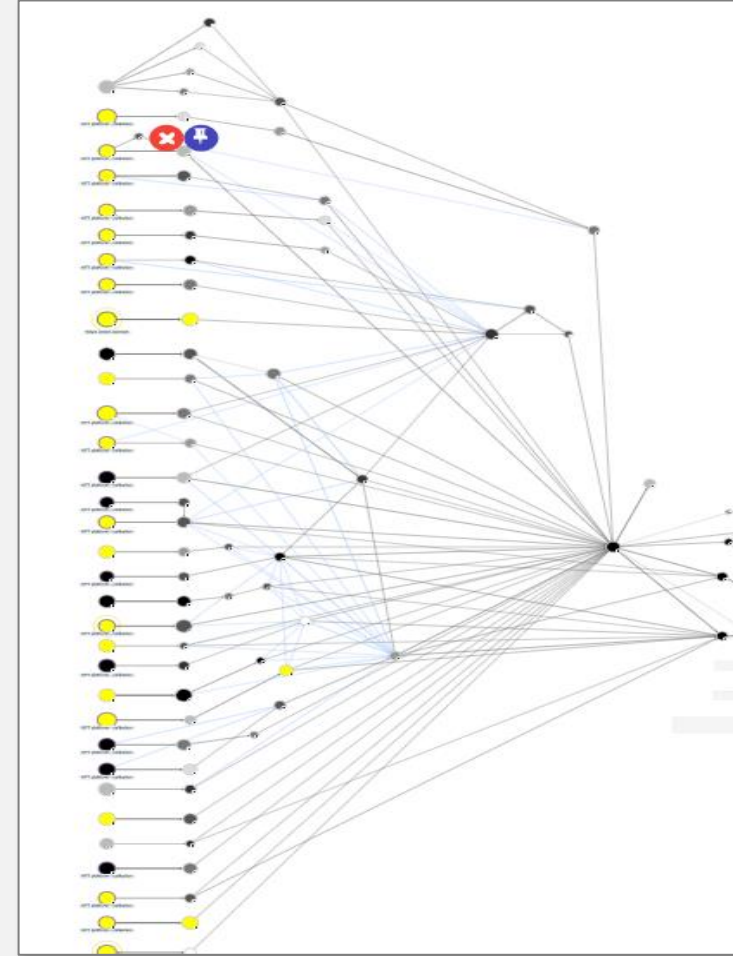
Australian Recipient: OSINT & ATO Holdings

- Australian crypto asset exchange account held by Australian company.
- E-commerce, online marketing, and NFT education activities.
- Crypto assets cashed out immediately on receipt.
- Proceeds transferred to another Australian e-commerce company.
- Fiat transfers to second Australian company from offshore founder of the alleged rug pull network.
- Second company also made payments to other digital marketing firms referencing 'NFTs'.



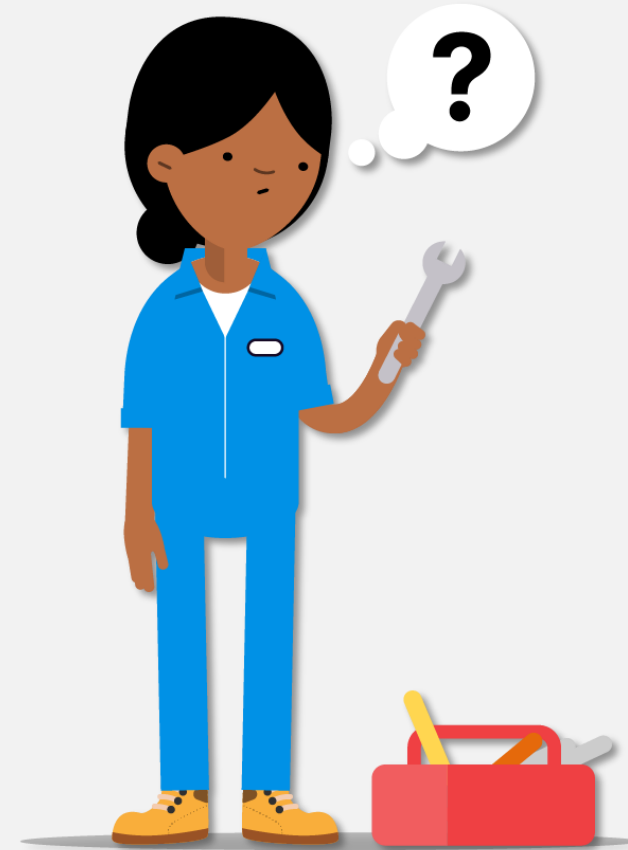
Blockchain Analysis

- Blockchain analysis identified total funds received >AUD 12 million
- Funds received over short period of time (November 2021 to June 2022)
- Over AUD 1.25 million from alleged 'rug pull' projects
- Remainder of funds sourced indirectly from a large number of digital currency exchanges.



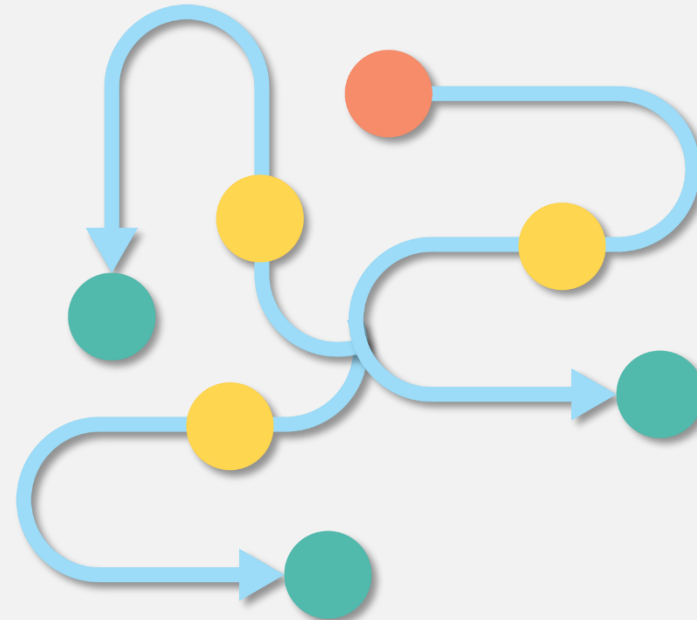
Intelligence Gaps

- Source of additional funds received by Company 1.
- Volume of funds received from scam projects.
- Role of Australian entities in alleged rug pull network.



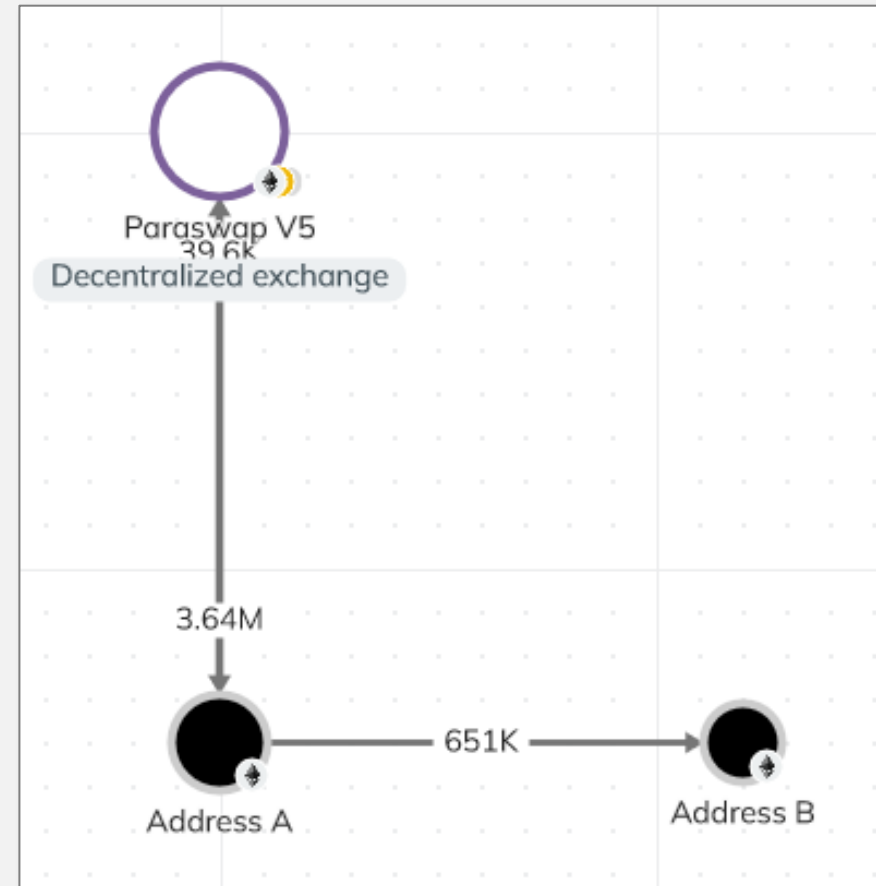
Analysing Indirect Transaction Routes

- Counterparty tracing to assess indirect transfer routes from exchanges.
- Identified linked smart contract addresses NOT identified by commercial tool.
- Same/similar transaction route to scam NFT proceeds.
- OSINT identified these as NFT projects.



Token Swap Transactions

- Other funds received indirect from decentralised swap protocols
- Examine token swap transactions to identify source
- Example: Address A sent 651,000 Tether to target address (Address B)
- Tether sourced from ParaSwap V5 (decentralised exchange).



Results of Blockchain and OSINT Analysis

Blockchain analysis

- Exposure to an additional 16 NFT projects (an additional AUD 1.5 million)

OSINT

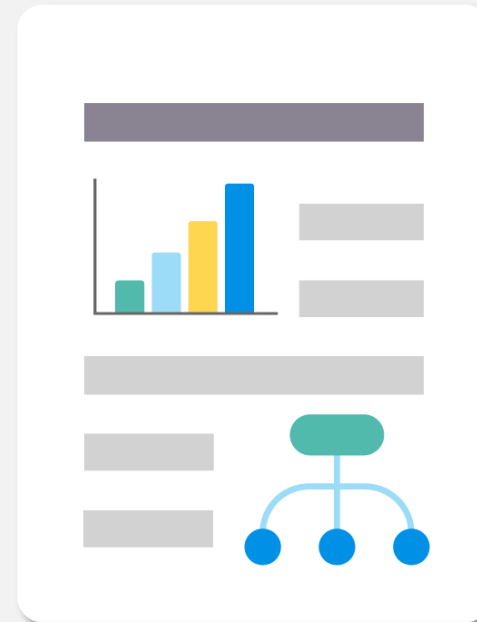
- Additional NFTs included six projects which were alleged to be rug pulls
- OSINT collection on monikers referenced in fiat transfers for Company 2 found OS links to Director of Company 1
- AND
- Matched social media accounts which promoted alleged scam NFTs

Assessed

- Transfers to Company 1 from NFT projects likely consideration for promotion of rug pull network's projects.

Overall Assessment

- Crypto asset transfers to Australian company likely represent consideration for marketing services provided to scam network
- Value of crypto assets received not in line with market rates for social media marketing – possible commission basis.
- Business income before and after scam period vastly less than that received from scam activity.
- Tax paid on income received – refer to law enforcement for consideration of proceeds.



Summary: Integrating OSINT and Blockchain Analysis

- Wide range of OSINT vectors for collection – including platforms, aggregators, project advertising, online communities.
- Extensive availability of open source blockchain data and tools.
- Opportunity for integration with closed source information
 - Digital Currency Exchange data
 - Tax and regulatory data
 - Financial reporting and intelligence
 - Telecommunications data
 - Partner agency intelligence holdings.

Questions

