TRM Academy

Misuse of Technology in Financial Crimes - Cryptocurrency

Quiz time!

Please navigate to the following link and follow the instructions outlined. The participant with the most right answers wins a prize!

- https://forms.gle/6f2z8Rzj9vBs8FCo8

Open source tools exercise

Please navigate to the following link and follow the instructions outlined. At the end I will ask different people to provide answers to the questions:

OSINT Exercise:

- https://docs.google.com/forms/d/e/1FAIpQLScL3gk-aHjSKrOoSqgESq8xDPCCPvihKKYUMsOIGFVXu1DyOg/viewform?usp=sharing

Blockchain intelligence

Definition

- Blockchain data:
  - transactional volume
  - alphanumeric account details for senders and receivers
  - times/dates for transactions
  - processes completed in transactions
  - fee information
  - data regarding confirmation of transactions

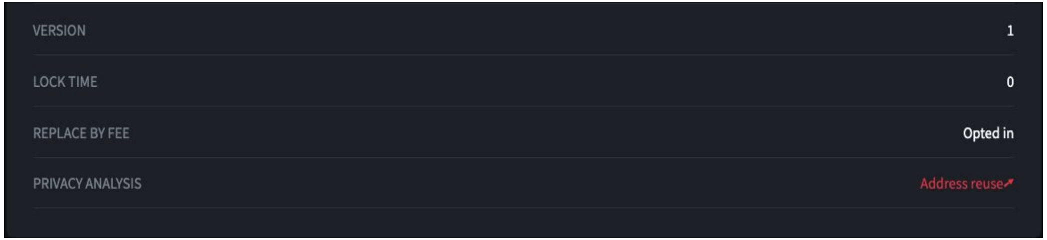
- Use cases:
  - Financial trading research
  - Understanding of blockchain economics
  - Identifying user behaviours and trends
  - Tracing the origin and destination of transactions
  - Risk management

Definition cont.

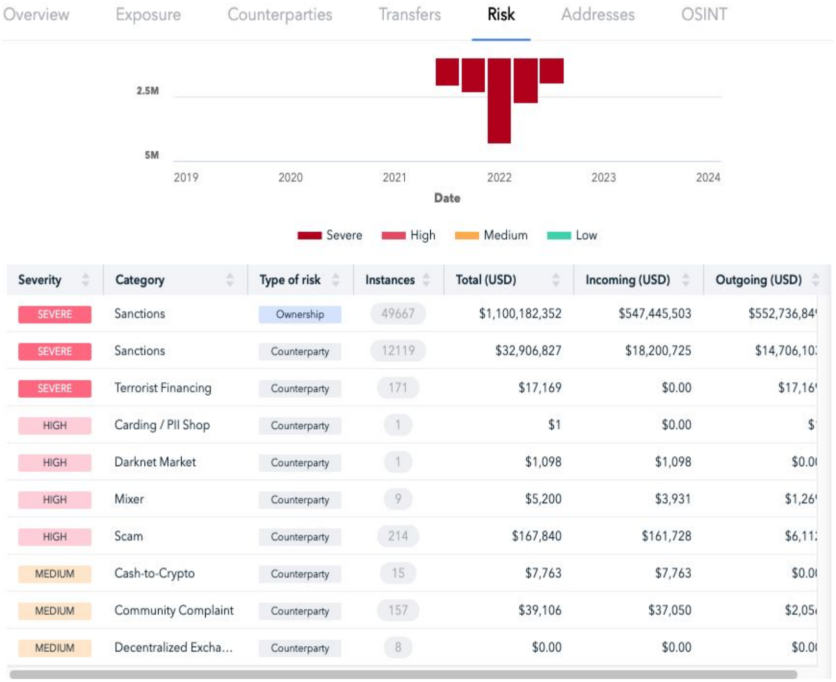
- Off chain insights:
  - Sanction processes
  - Social media/messaging sites (OSINT)
  - Closed source intelligence (often covert)
  - Network intelligence
  - Human sources

- Analysis process:
  - Break down large scale financial dataset into actionable intelligence
  - Done using data science tools including Artificial Intelligence elements
  - Objectives from a law enforcement perspective are graphing out money laundering activity, identifying key infrastructure and attributing to end users.

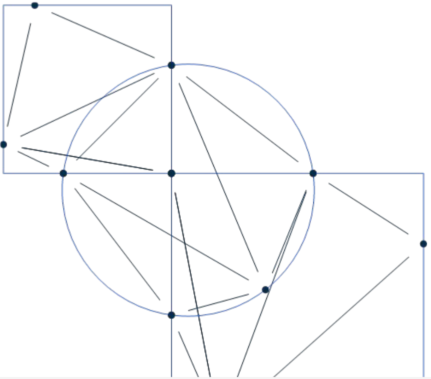
Turning data into actionable intelligence

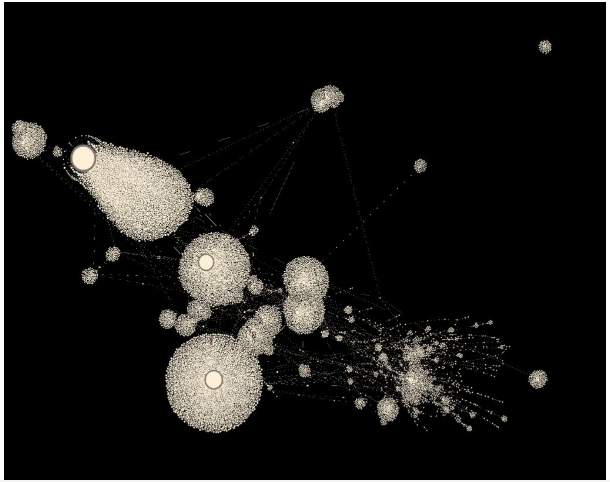


VERSION	1
LOCK TIME	0
REPLACE BY FEE	Opted in
PRIVACY ANALYSIS	Address reuse↗



Severity	Category	Type of risk	Instances	Total (USD)	Incoming (USD)	Outgoing (USD)
SEVERE	Sanctions	Ownership	49667	$1,100,182,352	$547,445,503	$552,736,84
SEVERE	Sanctions	Counterparty	12119	$32,906,827	$18,200,725	$14,706,10
SEVERE	Terrorist Financing	Counterparty	171	$17,169	$0.00	$17,16
HIGH	Carding / PII Shop	Counterparty	1	$1	$0.00	$
HIGH	Darknet Market	Counterparty	1	$1,098	$1,098	$0.0
HIGH	Mixer	Counterparty	9	$5,200	$3,931	$1,26
HIGH	Scam	Counterparty	214	$167,840	$161,728	$6,11
MEDIUM	Cash-to-Crypto	Counterparty	15	$7,763	$7,763	$0.0
MEDIUM	Community Complaint	Counterparty	157	$39,106	$37,050	$2,05
MEDIUM	Decentralized Excha...	Counterparty	8	$0.00	$0.00	$0.0

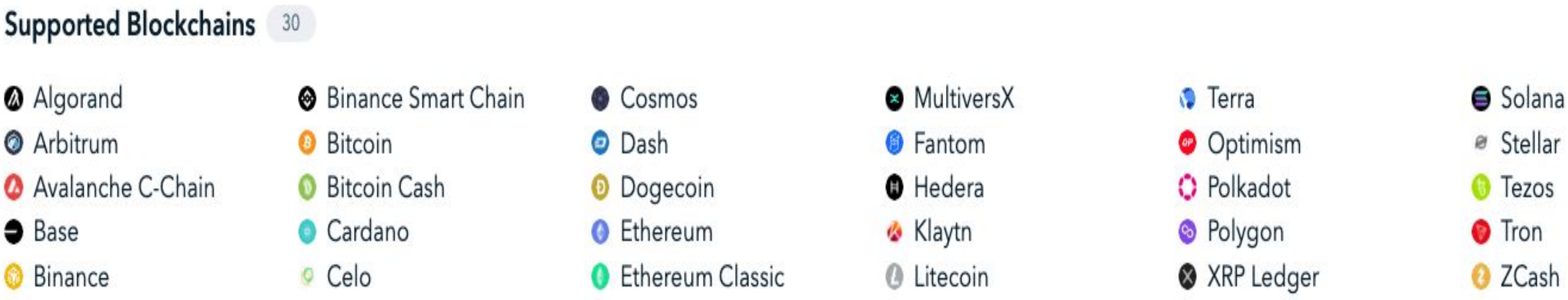




What assets are we referring to?

There are thousands of assets tied to blockchain technology. Many have specific use cases or features which set them apart from others. Examples of this include stablecoins, privacy coins and governance tokens. Some provide challenges to the blockchain analysis process whilst others can complement it.

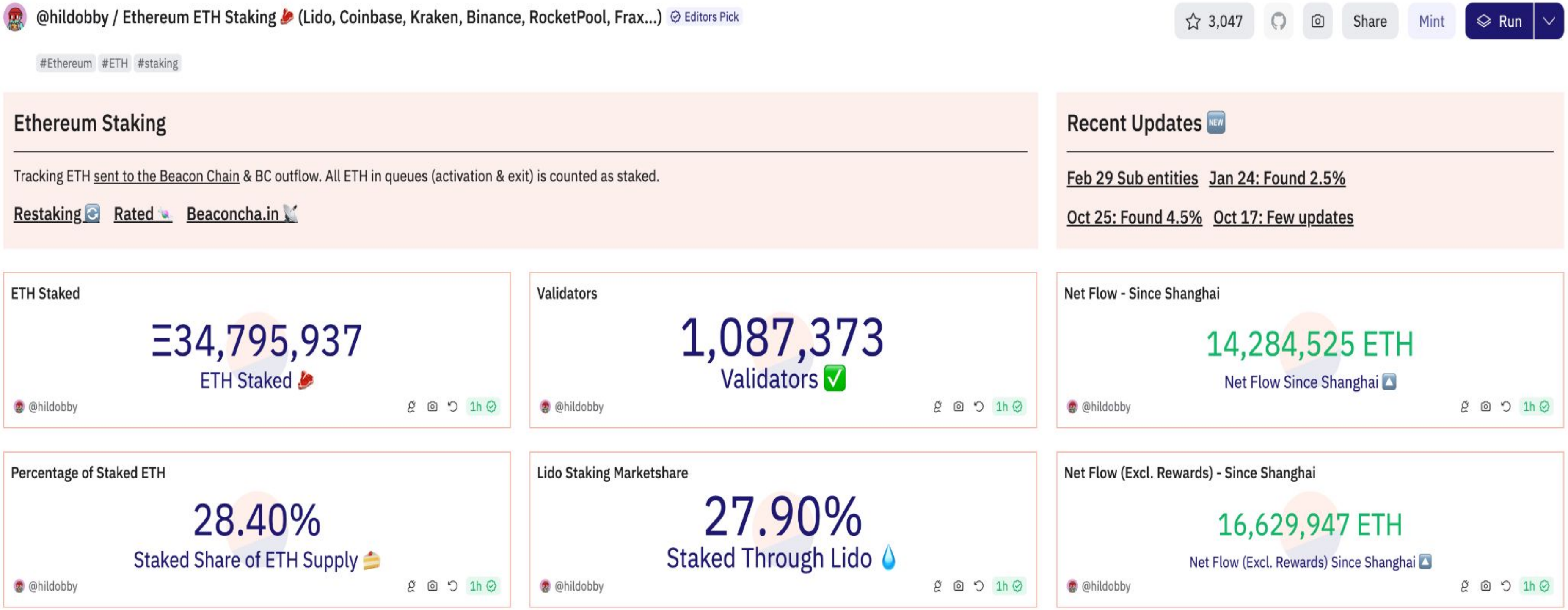
Using TRM as an example we concentrate on the assets seen to be most prevalent in money laundering investigations. The table below provides an outline of these:



Supported Blockchains 30

- Algorand
- Arbitrum
- Avalanche C-Chain
- Base
- Binance
- Binance Smart Chain
- Bitcoin
- Bitcoin Cash
- Cardano
- Celo
- Cosmos
- Dash
- Dogecoin
- Ethereum
- Ethereum Classic
- MultiversX
- Fantom
- Hedera
- Klaytn
- Litecoin
- Terra
- Optimism
- Polkadot
- Polygon
- XRP Ledger
- Solana
- Stellar
- Tezos
- Tron
- ZCash

Example: Financial analysis



@hildobby / Ethereum ETH Staking 🥩 (Lido, Coinbase, Kraken, Binance, RocketPool, Frax...) Editors Pick

#Ethereum #ETH #staking

Ethereum Staking

Tracking ETH sent to the Beacon Chain & BC outflow. All ETH in queues (activation & exit) is counted as staked.

Restaking 🔄 Rated ☄️ Beaconcha.in 📡

Recent Updates 🆕

Feb 29 Sub entities Jan 24: Found 2.5%

Oct 25: Found 4.5% Oct 17: Few updates

ETH Staked

Ξ34,795,937

ETH Staked 🥩

@hildobby 1h

Validators

1,087,373

Validators ✅

@hildobby 1h

Net Flow - Since Shanghai

14,284,525 ETH

Net Flow Since Shanghai 🔼

@hildobby 1h

Percentage of Staked ETH

28.40%

Staked Share of ETH Supply 🍰

@hildobby 1h

Lido Staking Marketshare

27.90%

Staked Through Lido 💧

@hildobby 1h

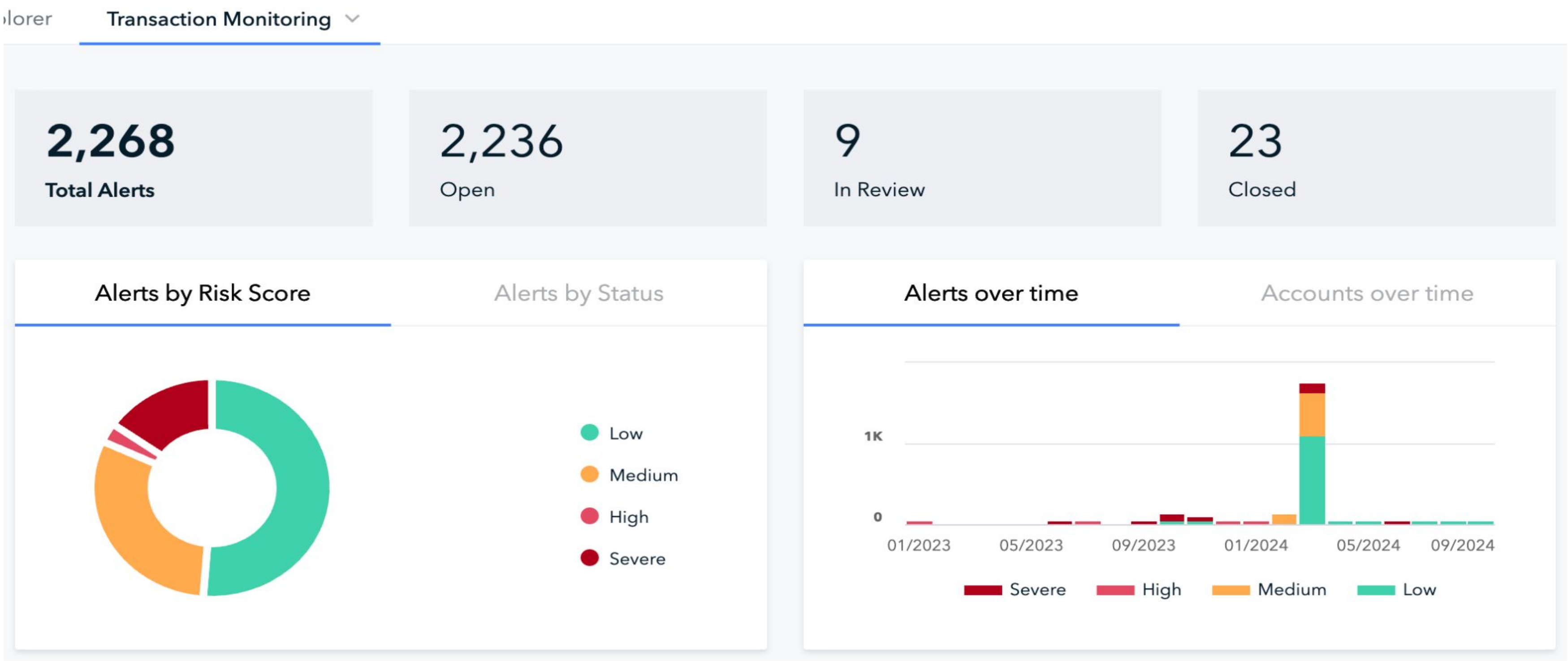
Net Flow (Excl. Rewards) - Since Shanghai

16,629,947 ETH

Net Flow (Excl. Rewards) Since Shanghai 🔼

@hildobby 1h

Example: Risk management



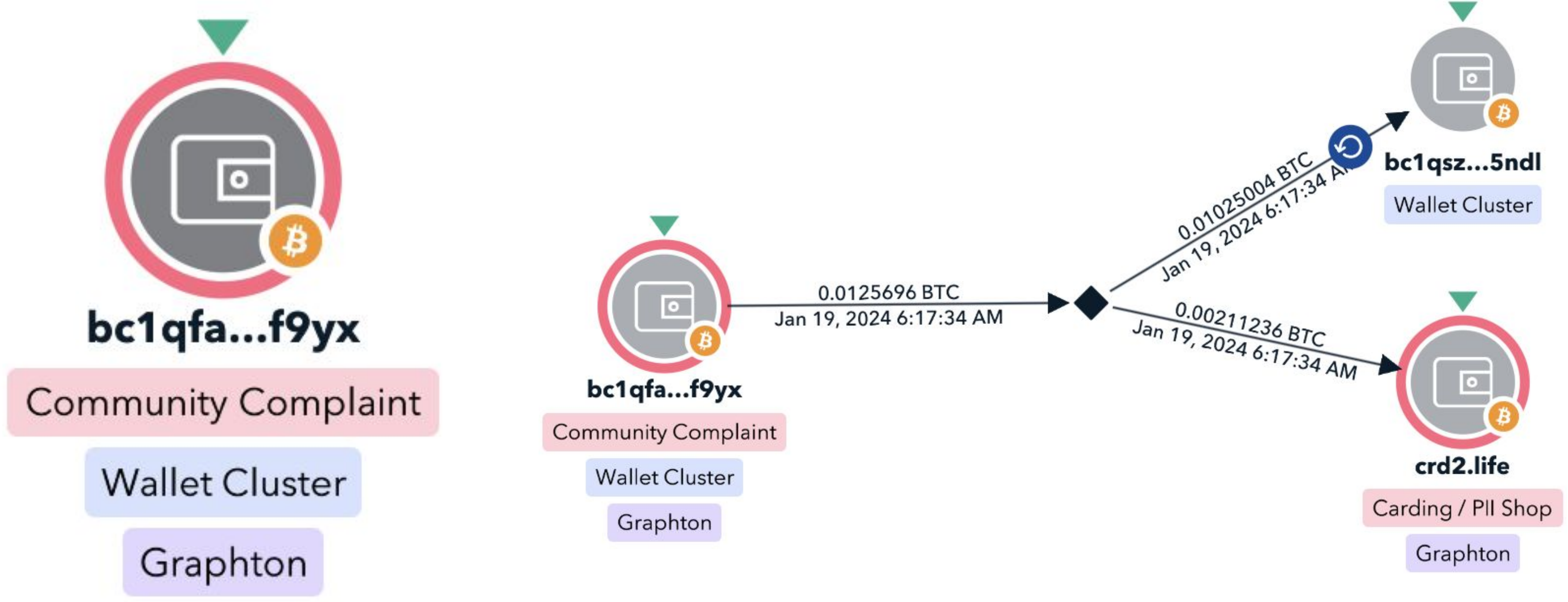
2,268
Total Alerts

2,236
Open

9
In Review

23
Closed

Example: Tracing money laundering



Strategy

Investigations involving cryptocurrencies/virtual assets can be resource intensive. To minimise the impact you need to carefully consider the parameters required to achieve the outcomes sought.

Points to consider:

- What are you trying to identify/prove? e.g. real world identity, total value of criminal proceeds…
- Is blockchain analysis the most efficient means of progressing the investigation?
- What value does it add and how much should it be prioritised?
- Is the analysis for intelligence or evidential purposes? How can you transition from one to the other?
- Are you looking at progressing matters utilising civil or criminal powers?
- Who is going to take responsibility for any legal process relevant to the analysis e.g. producing statements of evidence, giving testimony at court.

Judicial: Evidential Challenges

Clustering & Attribution

- It's not native blockchain data
- What clustering heuristic are you relying on?
- Who created the heuristic?
- Is it publicly available?
- If not have you asked originating source for insight?
- Has it been tested?
- Attribution by direct contact or heuristic?

Mixing Services

- Auto or manual de-mix?
- Can you share the process?
- What's the success rate?
- Any other corroborating data?

Smart Contracts

- Do you understand the coding language?
- What does the contract actually do?
- The dangers of relying too heavily on AI.

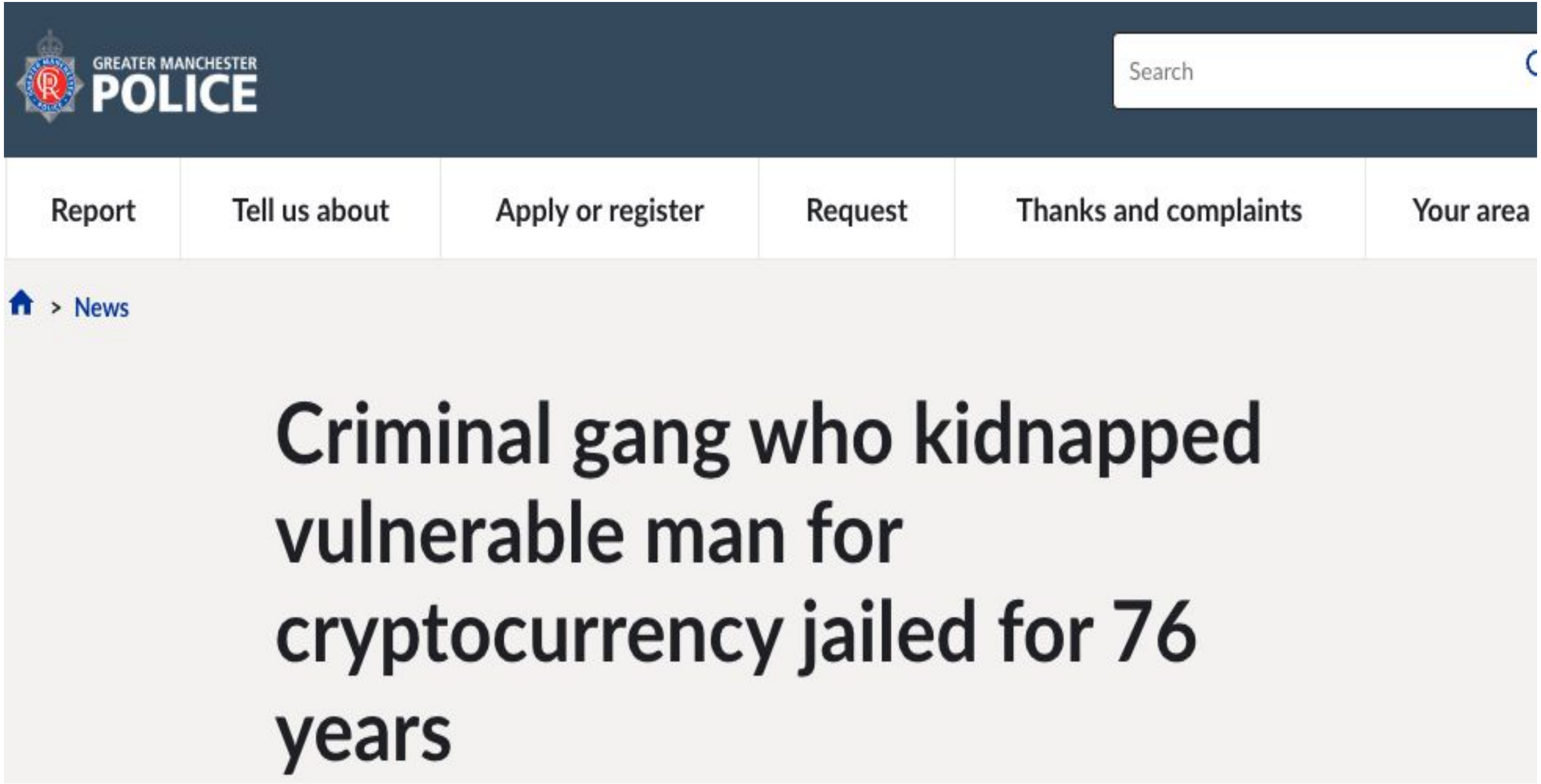
Cross Chain

- Natively different protocols
- Auto cross chain or manual?
- Data from source (bridge)?
- How was determination made?

Intel Only Products

- Consider parallel reconstruction
- Corroborate other data sources?
- Can they provide other investigation starting points?
- If not - strictly intel only
- Why? It's not native blockchain data!

Case study: Kidnap



Criminal gang who kidnapped vulnerable man for cryptocurrency jailed for 76 years

Excerpt from press release

“In December 2023 police received an anonymous call reporting concerns for welfare at a flat in Irlam. Upon attending, police gained entrance and identified a victim who said to the officer ‘can you take me with you?’. He explained that he’d been brought to this property against his will with a bag over his head. He spoke of the ordeal the offenders had subjected him to highlighting he’d been violently assaulted and tied up.

Officers searched the address and found a dressing gown strap which had been tied to the bed, along with electrical cables. He also had a burn mark on his hand, and bruises on his body from where he had been hit with a weapon. Detectives uncovered that the victim had acquired hundreds of thousands of pounds worth of cryptocurrency which the defendants, through use of violence, kidnap, and false imprisonment, sought to steal.”

Brief

- Provided exhibits and victim statement. Asked to complete analysis to answer the following questions:
    - A general overview of cryptocurrency and how transfers are made?
    - Who the wallets belong to?
    - What transfers have been made at what date and time?
    - How much were the transfers worth at the time?
    - Who have the transfers been made to?

- Tasked to provide the results in an MG11 and act as an expert witness in the case.
- Expert witness duty is to the court and not the requesting party (prosecution/defence):
    - *"I understand that my duty is to help the court to achieve the overriding objective by giving independent assistance by way of objective, unbiased opinion on matters within my expertise, both in preparing reports and giving oral evidence. I understand that this duty overrides any obligation to the party by whom I am engaged or the person who has paid or is liable to pay me. I confirm that I have complied with and will continue to comply with that duty."*

Outcomes

- Completed extensive analysis on the blockchain identifiers provided and created multiple exhibits documenting the findings.
- Provided a 31 page MG11 documenting the analysis completed and answers to the questions posed.
- Attended Crown Court and gave witness testimony in relation to statement completed and inferences made.
- Key points learnt:
  - Detail the settings used in the analysis tool as these can alter the appearance of transactions.
  - Highlight methodology for analysis, for example what accounting method used to follow funds?

Outcomes cont.

- Key points learnt:
    - Always consider alternative explanations for the analysis completed. Avoid using language that is too definite unless you are sure of the facts.
    - Clearly explain what inferences or details you are relying on within the analysis.
    - Use accessible and concise language to explain complex aspects.
    - If you have graphics in your statement make sure there is a key or written description for what they represent.
    - Utilise peer review to scrutinise evidence produced. As part of this process have them challenge the detail provided and consider what vulnerabilities are present in your analysis/statement.
    - Know your statement verbatim and practise explanations on technical aspects of evidence e.g. what is a Bitcoin? How does a transaction happen? What is the blockchain?

UTXO vs Account Based Blockchains

Analyzing the Blockchain

The two most common forms of blockchain you will encounter are:

UTXO - Unspent Transaction Output Blockchain

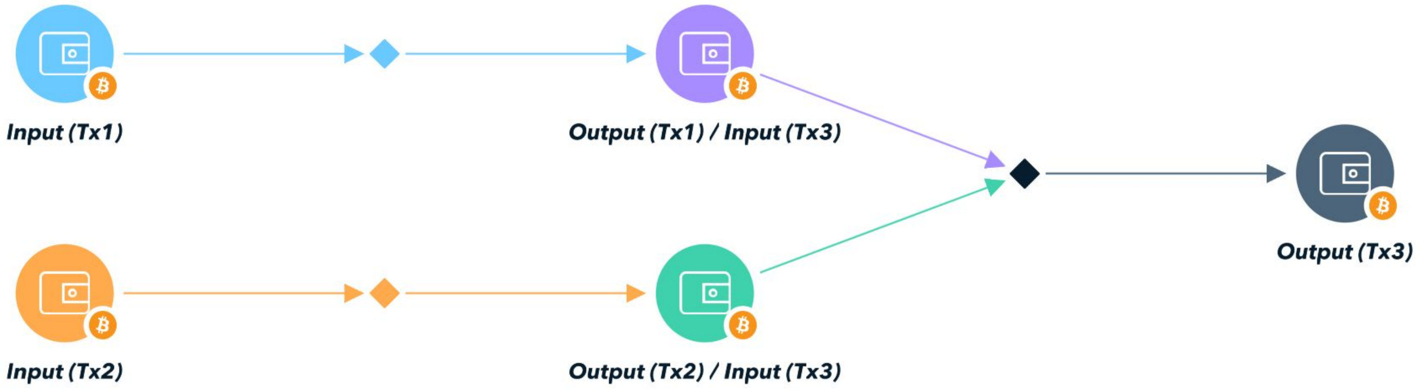
- For example Bitcoin and Litecoin
- Tracing Inputs and Outputs
- The full value of an address is spent in the transaction
- Think of this like handling cash, change is returned
- Multiple addresses in a wallet
- Fees taken from the input value

EVM / Account Based Blockchains

- For example, Ethereum, Polygon, Avalanche, TRON, Solana
- Single address making transactions similar to a credit or debit card
- Pay the exact amount (plus fees) with no change
- Fees (Gas) paid with the native asset of the blockchain

UTXO Inputs and Outputs

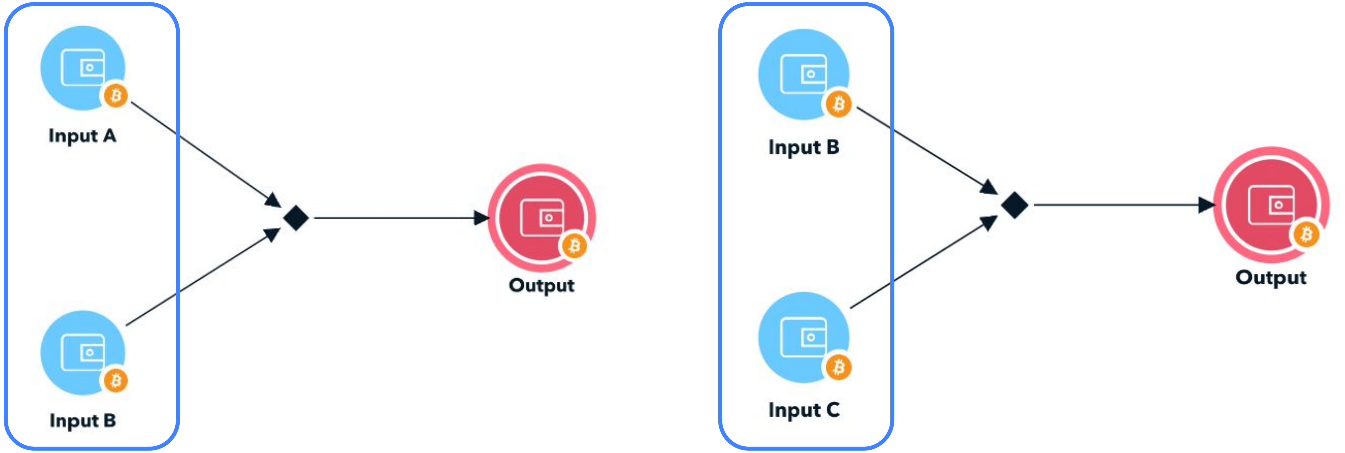
UTXO - Unspent Transaction Output. Outputs can be used as inputs in new transactions. UTXO Blockchains store a list of the unspent transaction outputs (think bank notes in a wallet).



Enough UTXOs to meet the payment amount and transaction fees. Must pay the whole of the UTXO, receive any change owed in the form of a single UTXO.

Clustering on UTXO

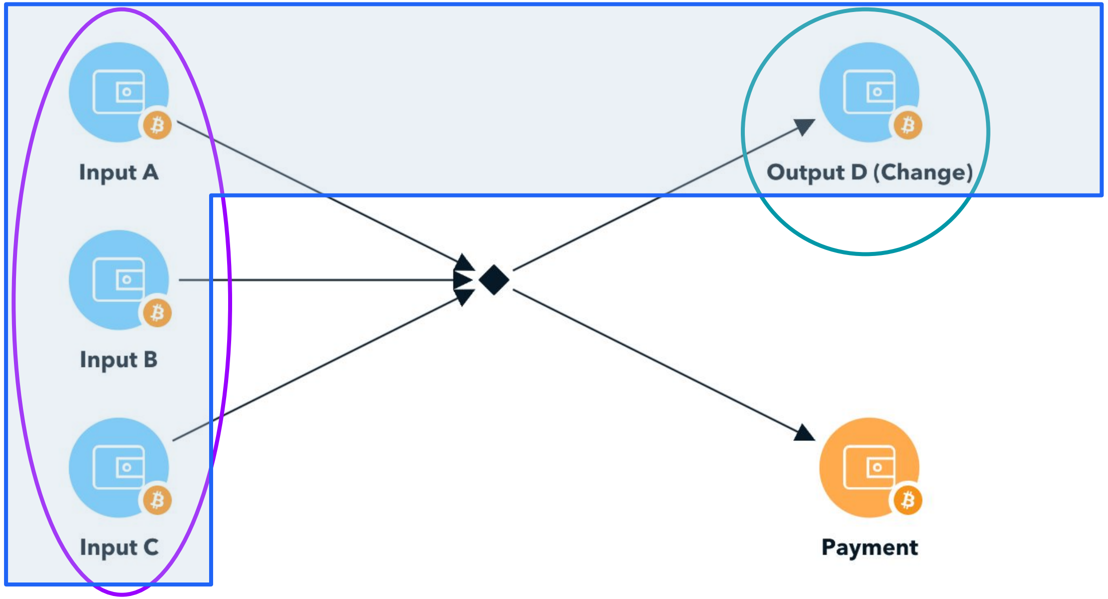
Using our understanding of UTXO blockchains, we can **infer** addresses in use by the same person or organisation and build a picture of activity conducted by this **cluster** of addresses.



Input addresses usually have the same private key (controlling entity able to spend the funds).
In this case addresses A, B, and C are clustered together.

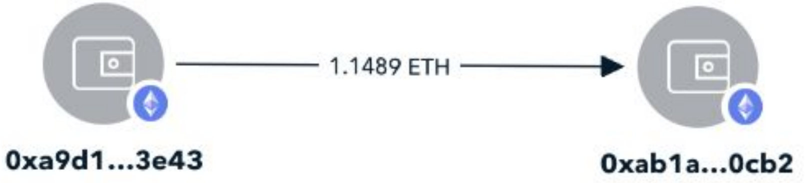
Clustering on UTXO

In this payment transaction, addresses A, B, C, and D would be clustered together. In transactions where we are grouping the input addresses, we can refer to this as a **co-spend transaction**. Further to this is the presence of a **change address** that can be grouped with the input addresses.

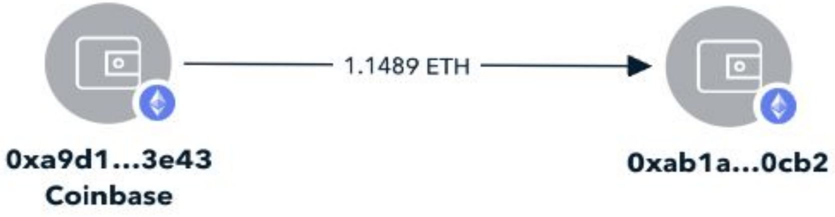


Account Based - Tokens and Gas fees

On account based chains you will be tracing not only the native asset, for example Ether on Ethereum, but tokens like USDT Tether and NFTs (Digital artwork etc.). Hundreds and thousands of digital assets on a single blockchain.

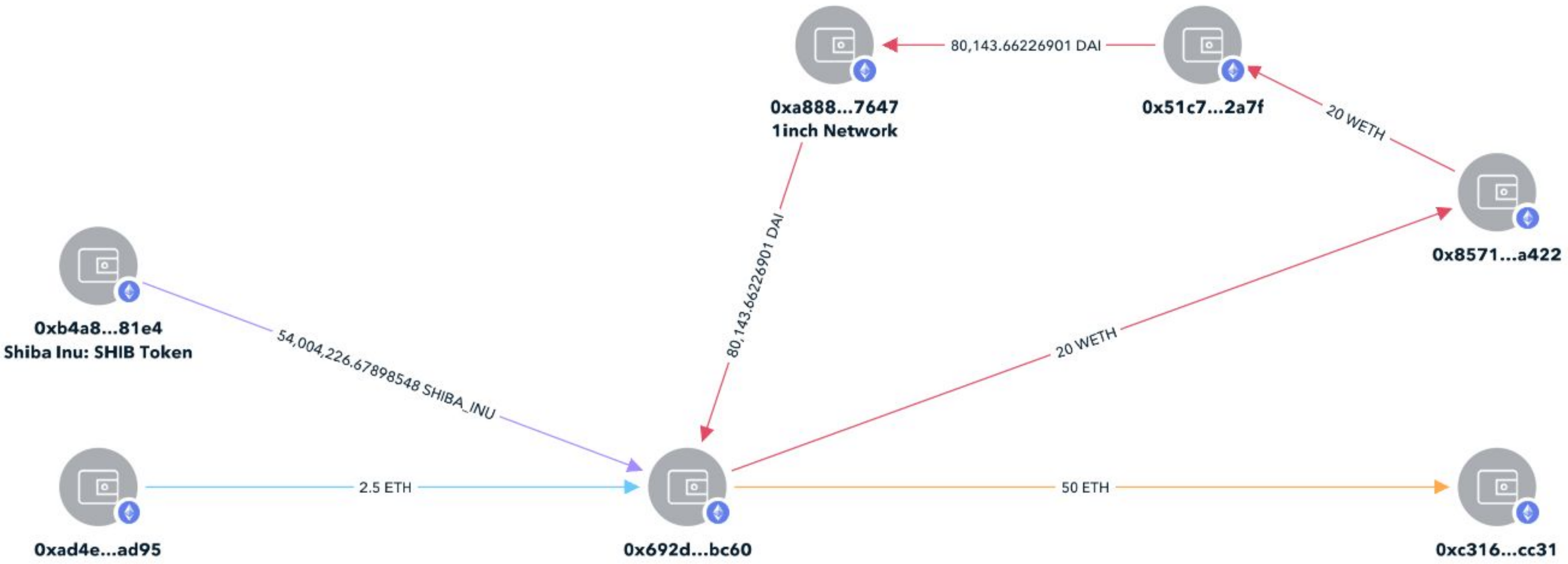


For every transaction of a token the user must pay the Gas (fee) with the blockchains native asset, in this case Ether (ETH). This has implications for the investigator to identify where the native asset funding comes from, for example a compliant exchange.



Account Based - Tokens and Gas fees

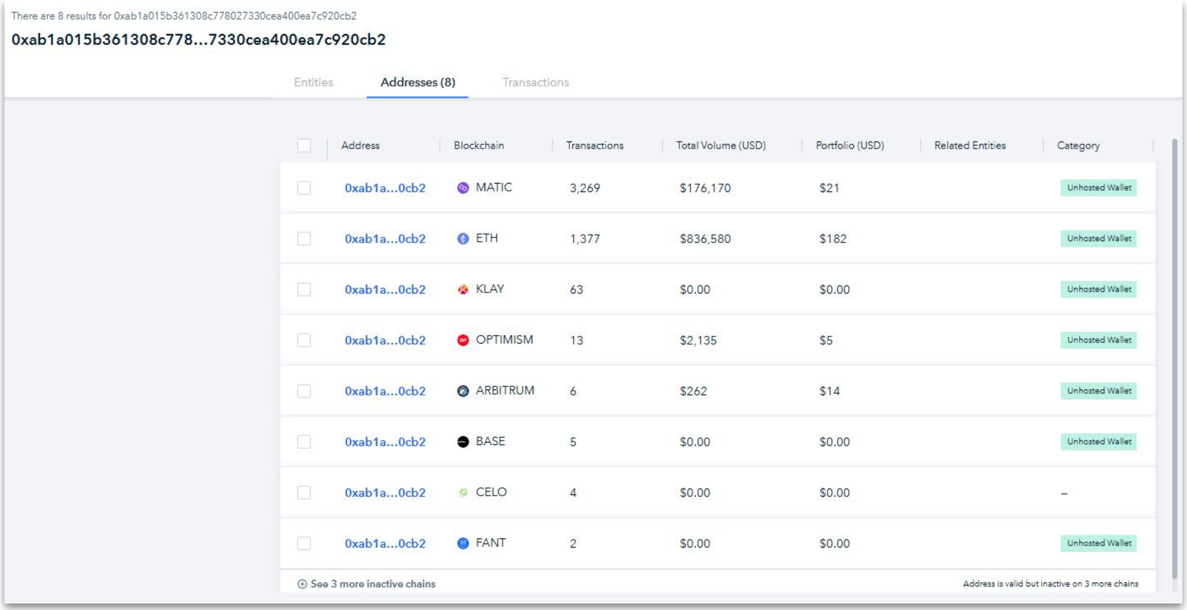
Here we see an address sending and receiving ETH, as well as using 1inch decentralized service to swap assets



Account Based

On account based chains the same address can be active across multiple blockchains and controlled by the same private key (i.e. same owner across all valid chains).

Therefore, an investigator should use the search function in TRM to identify all active chains, or similarly open source tools like DeBank, Etherscan, and Blockscan.



There are 8 results for 0xab1a015b361308c778027330cea400ea7c920cb2

0xab1a015b361308c778...7330cea400ea7c920cb2

□	Address	Blockchain	Transactions	Total Volume (USD)	Portfolio (USD)	Related Entities	Category
□	0xab1a...0cb2	MATIC	3,269	$176,170	$21		Unhosted Wallet
□	0xab1a...0cb2	ETH	1,377	$836,580	$182		Unhosted Wallet
□	0xab1a...0cb2	KLAY	63	$0.00	$0.00		Unhosted Wallet
□	0xab1a...0cb2	OPTIMISM	13	$2,135	$5		Unhosted Wallet
□	0xab1a...0cb2	ARBITRUM	6	$262	$14		Unhosted Wallet
□	0xab1a...0cb2	BASE	5	$0.00	$0.00		Unhosted Wallet
□	0xab1a...0cb2	CELO	4	$0.00	$0.00		–
□	0xab1a...0cb2	FANT	2	$0.00	$0.00		Unhosted Wallet

⊕ See 3 more inactive chains

Address is valid but inactive on 3 more chains

Criminality and case studies

What we are seeing:

- Malicious smart contracts: Need to interpret them if directly linked to criminality
- Use of USDT on TRON: Understand Fee/Gas funding (including Bandwidth/Energy)
- Use of specialist money laundering networks: Understanding fingerprint of such entities.
- Use of fraudulent cryptocurrency projects: Collaborating with partners to progress effectively.
- Solana and memecoins: Identifying and accessing materials to learn new tracing skills.
- Continued use of regulated off-ramps, gambling entities, nested services, OTC brokers, exchanges with limited KYC/AML, USDT on Tron, international networks using shell companies: Extensive knowledge of money laundering methodologies.

What's on the horizon:

Threat actors increasingly leveraged AI to defraud victims. TRM saw fraudsters use AI in multiple ways in 2024. Financial groomers and other scammers use large language models (LLMs) to:

- More easily create personas customized to the area in which their targeted victim resides, and to have more realistic conversations
- Create live voice and video deepfakes of famous individuals (or of victims relatives or CEOs) to trick victims to invest money, pay an invoice, or make a hostage payment
- Send a higher quantity of (and better quality of) phishing messages
- Create pornographic images of individuals in order to extort them
- Create fake personas to bypass Know Your Customer (KYC) requirements

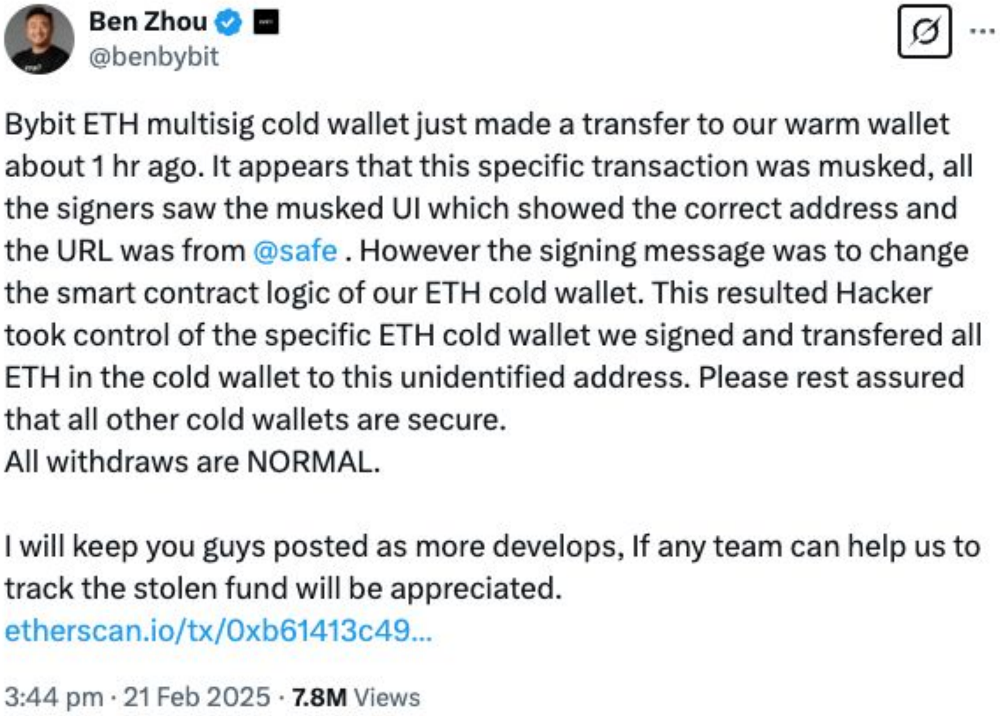
TRM believes criminals of all kinds will heavily expand their use of AI in 2025

Bybit Hack

What happened

The initial breach occurred at 14:16 GMT (09:16 EST), when an unauthorised entity executed a malicious contract siphoning a significant amount of cryptocurrency from a Bybit cold wallet. The total stolen assets included:

- 401,346 ETH (~$1.139 billion).
- 90,375 Lido stETH (~$256 million).
- 15,000 cmETH (~$42.5 million; Note: these funds were successfully rescued by the issuing project)
- 8,000 mETH (~$22.6 million)

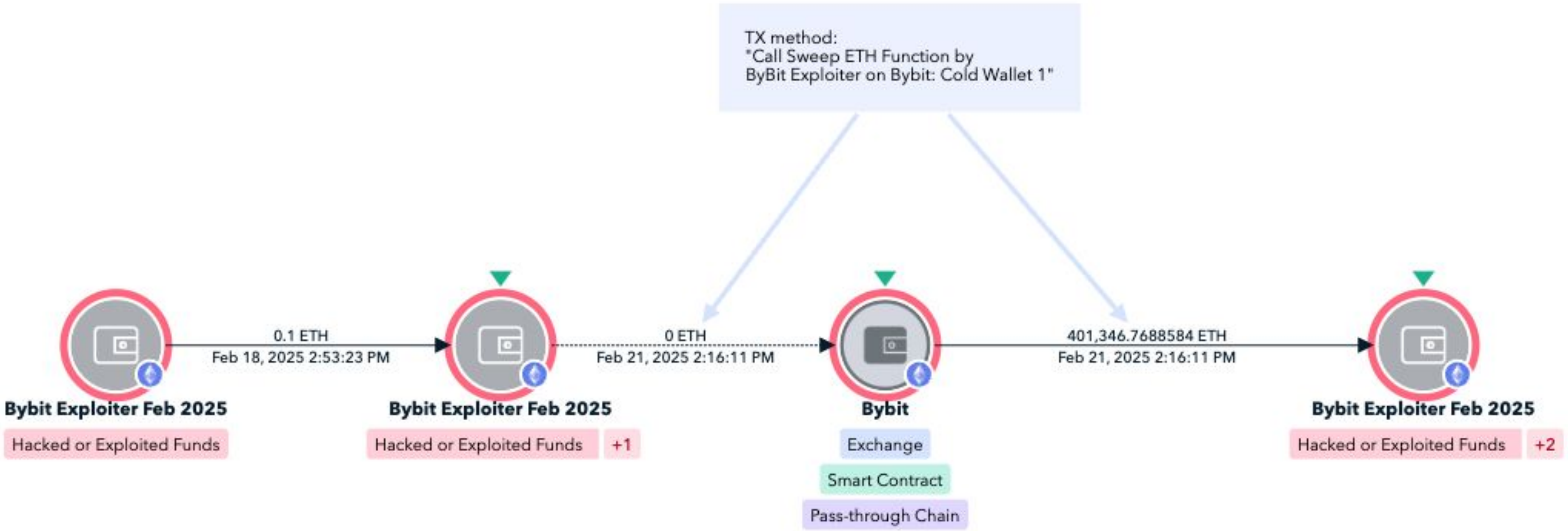


Ben Zhou
@benbybit

Bybit ETH multisig cold wallet just made a transfer to our warm wallet about 1 hr ago. It appears that this specific transaction was musked, all the signers saw the musked UI which showed the correct address and the URL was from @safe . However the signing message was to change the smart contract logic of our ETH cold wallet. This resulted Hacker took control of the specific ETH cold wallet we signed and transfered all ETH in the cold wallet to this unidentified address. Please rest assured that all other cold wallets are secure.
All withdraws are NORMAL.

I will keep you guys posted as more develops, If any team can help us to track the stolen fund will be appreciated.
etherscan.io/tx/0xb61413c49...

3:44 pm · 21 Feb 2025 · 7.8M Views



TX method:
"Call Sweep ETH Function by
ByBit Exploiter on Bybit: Cold Wallet 1"

Bybit Exploiter Feb 2025

Hacked or Exploited Funds

0.1 ETH
Feb 18, 2025 2:53:23 PM

Bybit Exploiter Feb 2025

Hacked or Exploited Funds +1

0 ETH
Feb 21, 2025 2:16:11 PM

Bybit

Exchange

Smart Contract

Pass-through Chain

401,346.7688584 ETH
Feb 21, 2025 2:16:11 PM

Bybit Exploiter Feb 2025

Hacked or Exploited Funds +2

Key Money Laundering Typologies

- **Rapid Multi-Channel Fund Movement:**
  - **Speed and Volume:** Within 48 hours, initial laundering of approximately USD 160 million was observed, which later increased to over USD 400 million by February 26, 2025. This rapid movement suggests either an expansion of their laundering infrastructure or the involvement of sophisticated underground networks capable of handling high-volume transactions.

- **Use of Intermediary Wallets and Cross-Chain Bridges:**
  - **Multiple Intermediaries:** Stolen funds are routed through several intermediary wallets.
  - **Cross-Chain Conversions:** Portions of the Ethereum assets were moved through networks on Binance Smart Chain and Solana. Cross-chain bridges are used to convert funds into different cryptocurrencies, notably converting a major share directly into Bitcoin.

Key Money Laundering Typologies

- **Decentralized Exchanges (DEXs) and Automated Transactions:**
  - **DEXs for Conversion:** The use of decentralized exchanges facilitated rapid conversion of cryptocurrencies with minimal oversight, helping to obscure the origins of funds.

- **Abandonment of Traditional Mixers:**
  - **Shift from Traditional Mixers:** Traditional cryptocurrency mixers (e.g., Tornado Cash) have been a mainstay for laundering illicit funds. However, given the enormous volume of this hack, these services became impractical, pushing the hackers to adopt more automated and multi-layered laundering methods.

Investigative Tactics Utilised

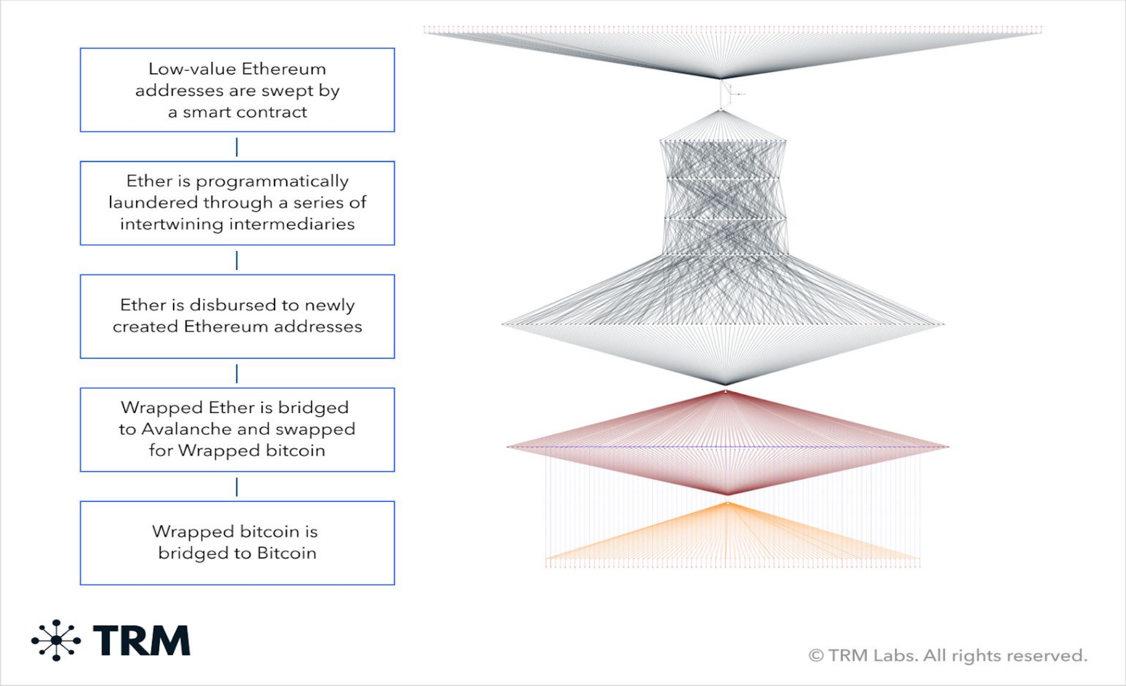
- **On call incident response team:** On being made aware of the compromise the on call team begin extensive blockchain analysis to identify relevant addresses/transactions. As part of this they worked through multiple intermediary transactions and followed funds through cross chain swap bridges. Much of this work was resource intensive as the rapid movement of funds may not always have allowed for our signatures to catch up. As such there will have been manual aspects of interrogating transaction data to follow from one protocol to another.

  Further to the above the team utilised their extensive experience of DPRK methodologies to identify patterns and signatures which benefited the analysis process. Essentially this meant building out behavioural patterns which provided for an inference that activity was linked to the offenders. This could be the repeat of a transaction process previously seen, utilising network intelligence or identifying unique transaction details.

Investigative Tactics Utilized

- **Address Tagging within TRM Forensics:** The work of the incident response team identified the compromised Bybit addresses and the infrastructure used by the offenders. As a result of these efforts we were able to rapidly tag compromised addresses as “Hacked” or “Stolen Funds” and create a dedicated tracking entity called "Bybit Exploiter Feb 2025". This allowed for all investigators utilising TRM Forensics to monitor asset movements in real time.

- **Enhanced Data Sharing:** To effectively progress the investigation into the compromise it was necessary to share data as close to real-time as possible. The entities involved in this data sharing were both private industry players, and public sector law enforcement entities.



Low-value Ethereum addresses are swept by a smart contract

Ether is programmatically laundered through a series of intertwining intermediaries

Ether is disbursed to newly created Ethereum addresses

Wrapped Ether is bridged to Avalanche and swapped for Wrapped bitcoin

Wrapped bitcoin is bridged to Bitcoin

- As of the 27/02/2025 most of the converted Bitcoin remains largely stationary, suggesting that the hackers are preparing for large-scale liquidation or further obfuscation through over-the-counter (OTC) networks.
- This hypothesis is based on previous experience of North Korea's "flood the zone" technique. This involves overwhelming compliance teams and blockchain analysts with rapid, high-frequency transactions, further complicating efforts to trace the money trail.

Complex money laundering

Insight: South East Asia

- According to recent reports, South East Asia (SEA) has experienced a rapid growth in it’s illicit digital economy. Existing illicit infrastructure such as casinos and connected junkets have been supplemented by online counterparts and peer to peer cryptocurrency exchanges run through communication applications.

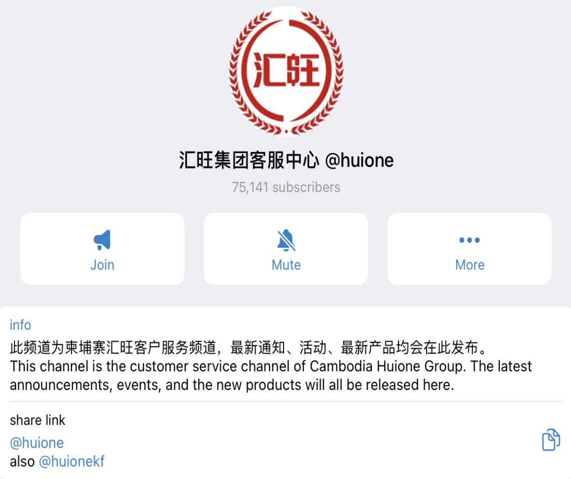
- Aspects of this growth has been seen to coincide with the large scale movement of organised crime groups into offending such as “pig butchering”. Cryptocurrency plays a significant role in such criminality, as a result sophisticated and increasingly digitised money laundering systems are necessary.

- Another factor contributing to the growth is the continued expansion of the synthetic drug trade within SEA which generates significant illicit revenue streams.

- Organised Crime Groups (with transnational links) have exploited “Special Economic Zones”, unstable political landscapes and readily available money laundering infrastructure to setup highly profitable endeavours.

- It is also alleged that these OCG’s proactively utilise human trafficking/slavery to perpetrate the criminality.

Huione Pay and similar services



汇旺集团客服中心 @huione

75,141 subscribers

info

此频道为柬埔寨汇旺客户服务频道，最新通知、活动、最新产品均会在此发布。
This channel is the customer service channel of Cambodia Huione Group. The latest announcements, events, and the new products will all be released here.

share link

@huione
also @huionekf

- Huione Guarantee is part of Huione Group, a Cambodian online marketplace with links to Cambodia’s ruling Hun family.

- The platform offers deposit and escrow services for peer-to-peer transactions in USDT stablecoin over Telegram. It has an associated app called Huione Pay.

- The Huione ecosystem is made up of a network of thousands of instant messaging app channels, each run by a different merchant. Huione Guarantee operates the platform and acts as a guarantor or escrow provider for all transactions, helping to prevent fraud.

- The merchants use the channels to offer a multitude of service including online gambling, high-risk exchange services, and advertisement for third-party offerings

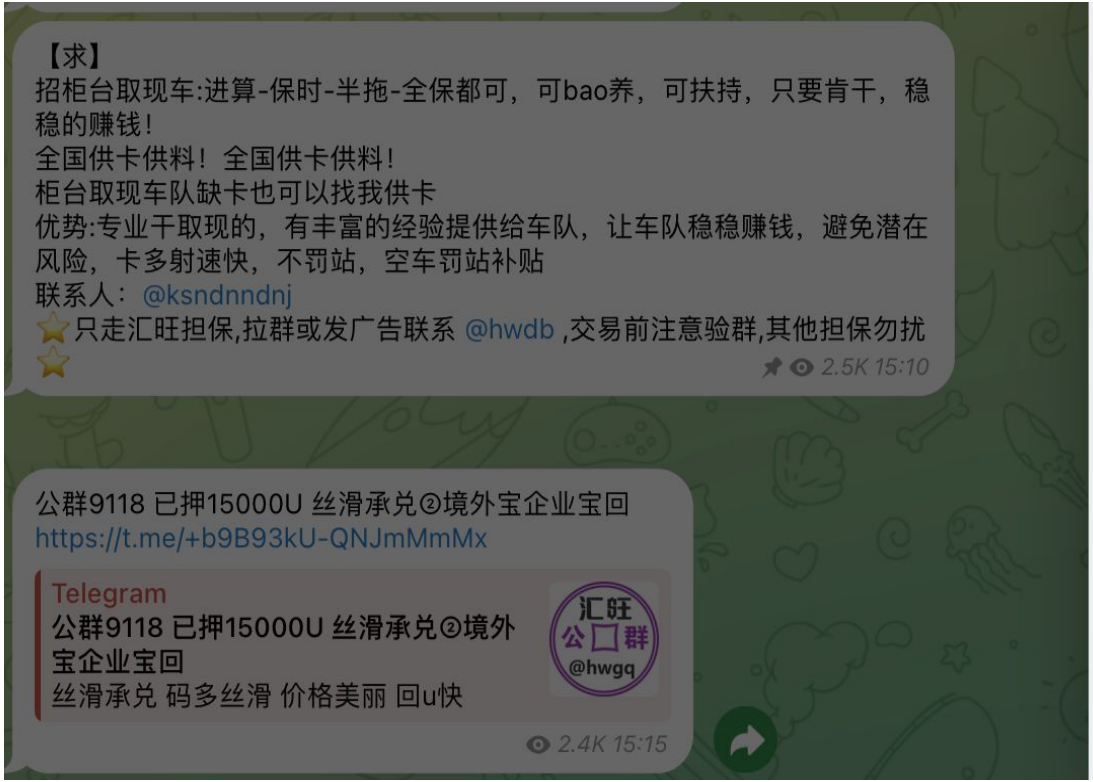
Huione Pay and similar services

- The service does not govern what can be offered on the platform and as a result it has become an attractive service to criminality. The escrow aspect adds trust to transactions and the lack of scrutiny provides a fertile environment for money laundering.

- This can be seen when reviewing the content within merchant channels. Many of the entities behind the channels make thinly veiled offers of criminal services such as money laundering, digital face altering programs and electric shackles for binding “runaway dogs,” a reference to scam center workers who try to escape.

- Investigators should consider the potential implications for any blockchain analysis being completed which features Huione. The mechanisms of Huione allow for pig butchering/scam entities to deposit criminal proceeds into channels linked to professional money laundering entities (PMLE). Subsequent movements of funds will be linked to the processes employed by the PMLE and not directly the predicate offenders. The investigation strategy needs to carefully consider who is being targeted and what the objectives are.

Advertisement



【求】
招柜台取现车:进算-保时-半拖-全保都可，可bao养，可扶持，只要肯干，稳稳的赚钱！
全国供卡供料！全国供卡供料！
柜台取现车队缺卡也可以找我供卡
优势:专业干取现的，有丰富的经验提供给车队，让车队稳稳赚钱，避免潜在风险，卡多射速快，不罚站，空车罚站补贴
联系人：@ksndnndnj
⭐只走汇旺担保,拉群或发广告联系 @hwdb ,交易前注意验群,其他担保勿扰⭐

2.5K 15:10

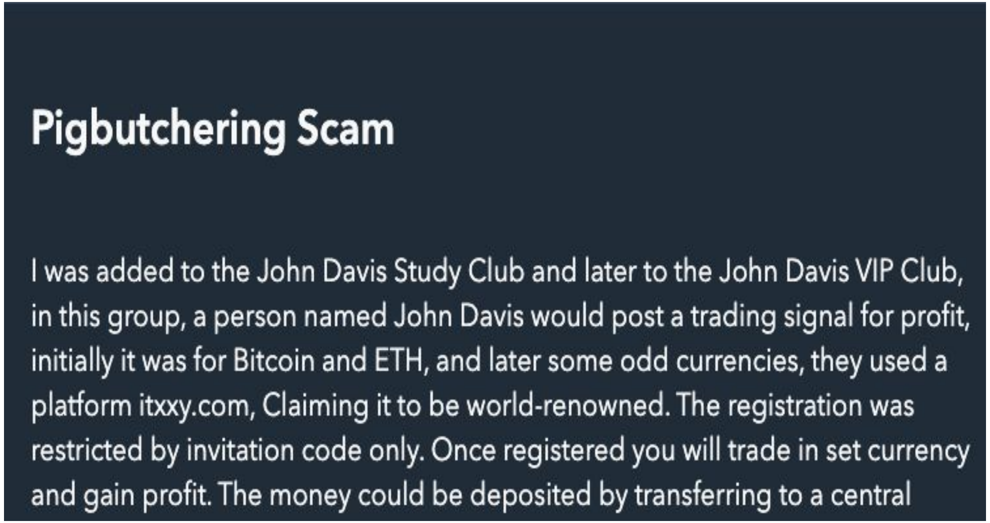
公群9118 已押15000U 丝滑承兑②境外宝企业宝回
https://t.me/+b9B93kU-QNJmMmMx

Telegram
公群9118 已押15000U 丝滑承兑②境外宝企业宝回
丝滑承兑 码多丝滑 价格美丽 回u快

2.4K 15:15

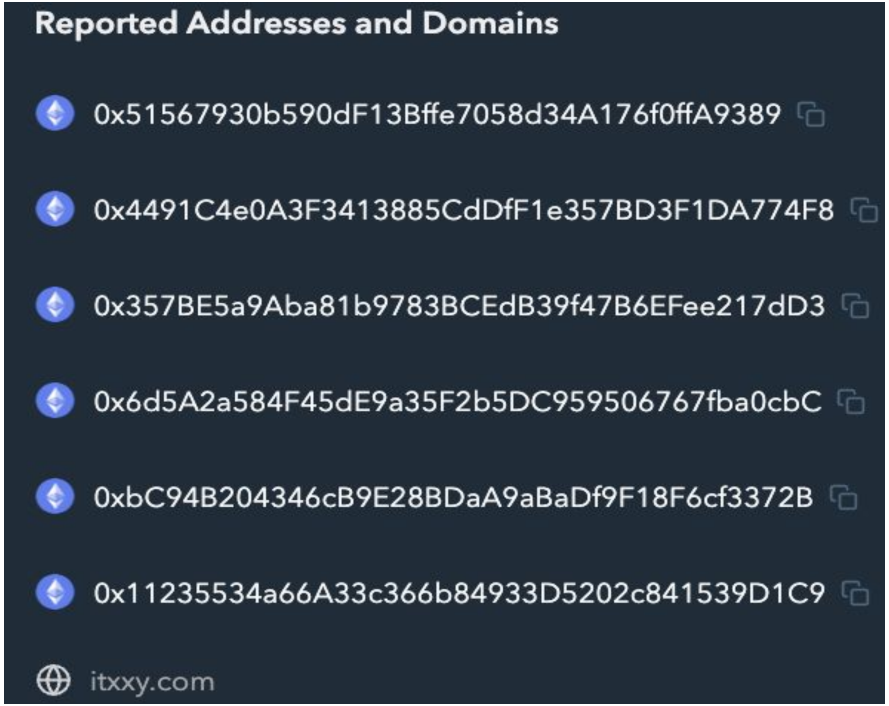
【Want】
Recruiting cash withdrawal vehicles: calculated, insured, semi-trailer, fully insured, can be maintained, supported, as long as you are willing to work, you can make money steadily!
Card supply and materials nationwide! Card supply and materials nationwide!
If the cash withdrawal fleet at the counter is short of cards, you can also find me to supply cards
Advantages: Professional cash withdrawal, with rich experience to provide to the fleet, so that the fleet can make money steadily and avoid potential risks, more cards, faster shooting speed, no penalty, empty vehicle penalty subsidy
Contact: @ksndnndnj
⭐Only use Huiwang guarantee, contact @hwdb for group or advertisement, please check the group before trading, other guarantees do not disturb⭐

Example



Pigbutchering Scam

I was added to the John Davis Study Club and later to the John Davis VIP Club, in this group, a person named John Davis would post a trading signal for profit, initially it was for Bitcoin and ETH, and later some odd currencies, they used a platform itxxy.com, Claiming it to be world-renowned. The registration was restricted by invitation code only. Once registered you will trade in set currency and gain profit. The money could be deposited by transferring to a central



Reported Addresses and Domains

0x51567930b590dF13Bffe7058d34A176f0ffA9389

0x4491C4e0A3F3413885CdDfF1e357BD3F1DA774F8

0x357BE5a9Aba81b9783BCEdB39f47B6EFee217dD3

0x6d5A2a584F45dE9a35F2b5DC959506767fba0cbC

0xbC94B204346cB9E28BDaA9aBaDf9F18F6cf3372B

0x11235534a66A33c366b84933D5202c841539D1C9

itxxy.com

Open source tools pros and cons

- Valuable for corroborating information from software providers.
- Can provide additional insights not available in paid for software.
- Highlight a solid understanding of the concepts.

- Usually only provide basic functionality or require technical skillset to implement.
- Often have limited "off-chain" intelligence insights.
- Difficult to know what information the site is logging and who has access to that.
- Challenging to find analysis software.

Links to OSINT Tool repositories

- Bellingcat: https://bellingcat.gitbook.io/toolkit
- https://start.me/p/wMzpnL/cryptocurrency-investigations

Crypto 101

Terminology

FIAT Currency

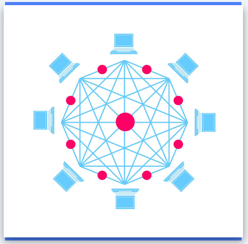
- Minted by a Central Bank
- Means "by decree"
- Fits into an envelope neatly

Terminology

FIAT Currency

- Minted by a Central Bank
- Means “by decree”
- Fits into an envelope neatly

DLT



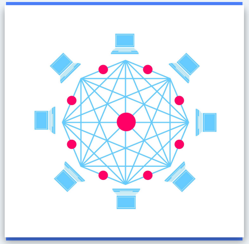
- Distributed Ledger Technology
- System used to sync ledger

Terminology

FIAT Currency

- Minted by a Central Bank
- Means “by decree”
- Fits into an envelope neatly

DLT



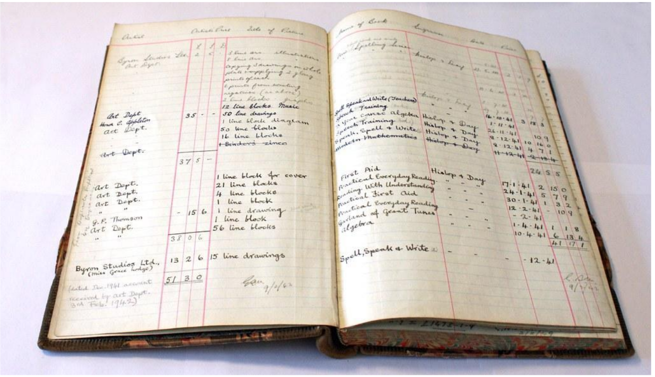
- Distributed Ledger Technology
- System used to sync ledger

Cryptocurrency

- AKA: Digital Asset
- AKA: Virtual Asset
- Not necessarily NFTs

BRIEF HISTORY

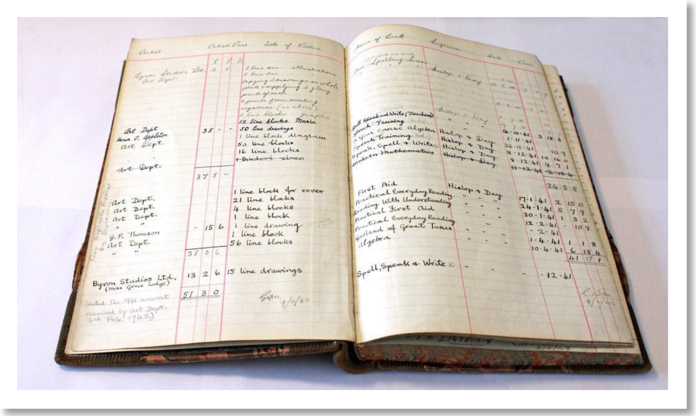
Ledgers & Databases



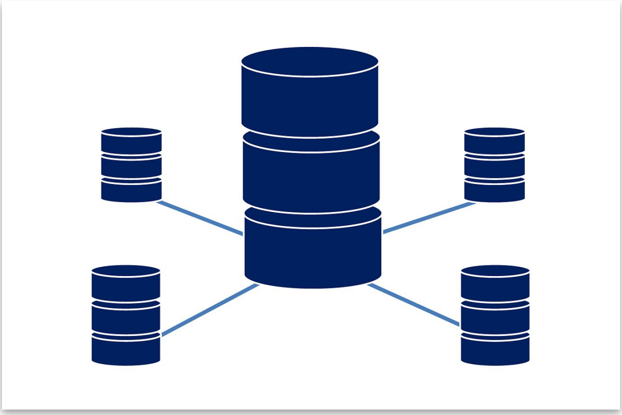
Ledger as a record of accounts
~15th Century

BRIEF HISTORY

Ledgers & Databases

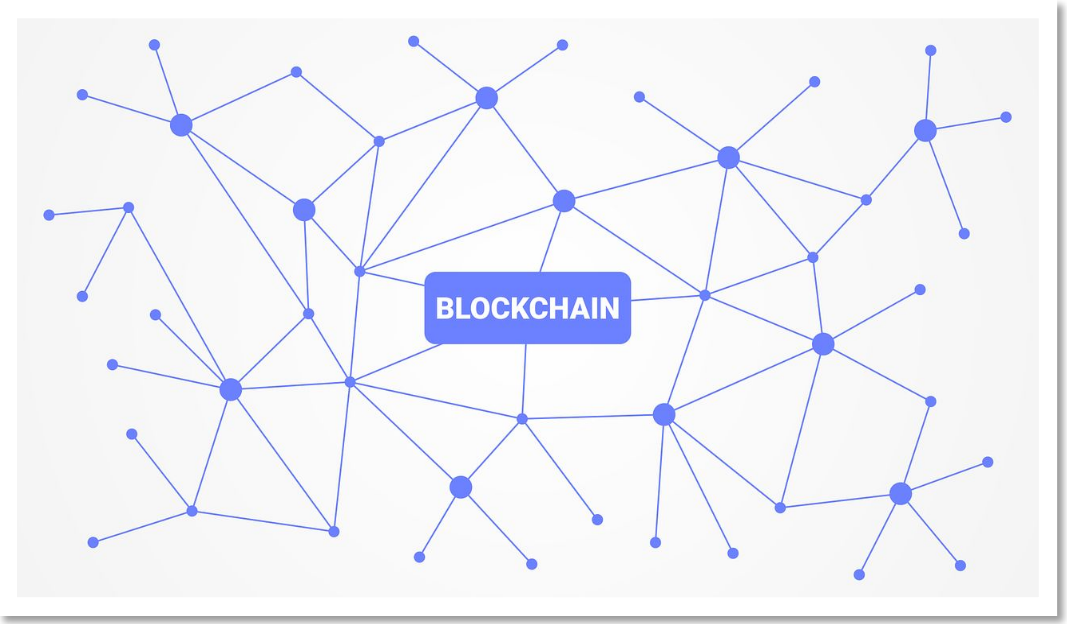


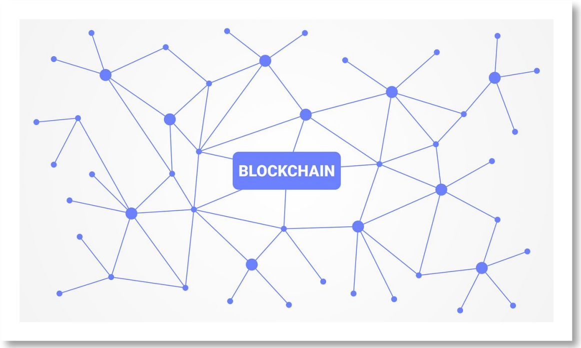
Ledger as a record of accounts
~15th Century



Relational databases
1970s

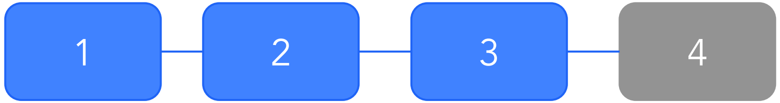
Blockchain is a time-stamped data progression tied to a decentralized database





≠

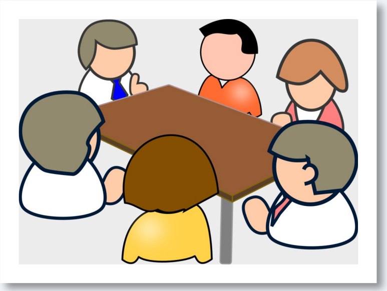
Blockchain helps to order cryptocurrency transactions and maintain consensus across decentralized ledgers.



"...a chain of blocks with each block being made up of a number of transactions clustered into a block by mining. Once a block has been mined it is essentially locked, and nothing can be added or changed. Each transaction in the block is then said to have a 'confirmation.'"

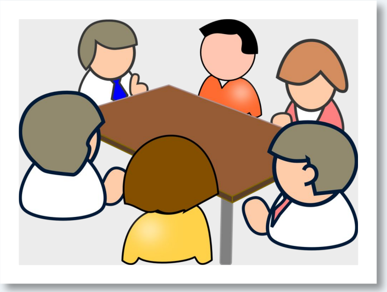
NICK FURNEAUX
Investigating
Cryptocurrencies 2017

Types of Blockchain



Public

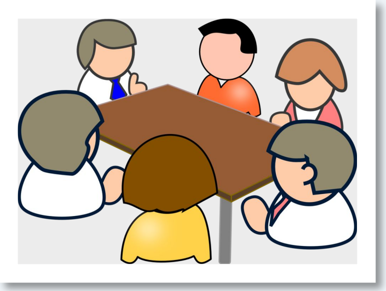
Types of Blockchain



Public

Private

Types of Blockchain

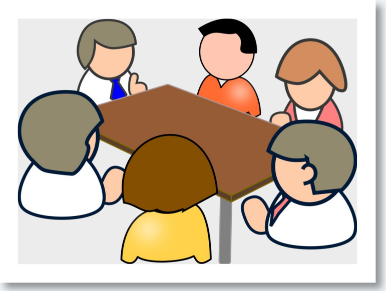


Public

Private

Consortium

Types of Blockchain



Public

Private

Consortium

Hybrid

On-Chain vs Off-Chain

On-Chain

All transaction data exists on its blockchain

Token can exist beyond any specific application (eternal)

Off-Chain

Data held off-chain

Transactions can be made P2P but not settled until sync with the blockchain

How does the blockchain affect investigations?

Difficulties

- Hard to understand
- Difficult to interpret
- Risk of 51% attack
- Barrier to entry

Training

Forensic tools

Graphic Browsers

Lowering the Barrier

Advantages

- Transparency
- Ability to trace
- Programmatic
- Lends itself to analysis
- Easier than cash

- No statute of limitation
- Open-source data
- Digital Chain-of-Evidence
- Easy to seize
- Great tools available

Where are you likely to see crypto in crime?

Cybercrime

- Ransomware
- Programmatic money laundering
- Darknet markets
- Business email compromise
- Crypto-market manipulation
- Exchange hacks
- Defi exploits

Traditional crime

- Money Laundering
- Terrorist Financing
- Fraud
- ICO scams
- Ponzi schemes
- Romance scams
- Money mules
- Extortion
- Investment fraud
- Credit card theft

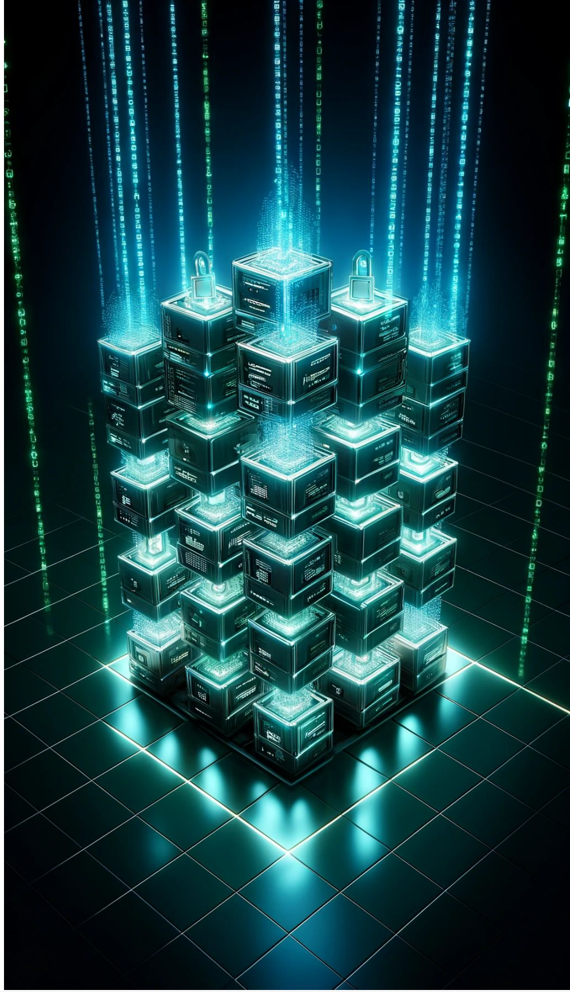
What is Cryptocurrency

- Simplest terms - Digital Money stored on public, decentralised (mostly) ledgers, known as Blockchains

- Blockchain cryptography is super secure! What happens on the blockchain…

- Chain of Blocks - Immutable, tamper proof record of all transactions

- Different chain, different cryptocurrency
  - Bitcoin = BTC, Ethereum = ETH, Tron = TRX
  - USDT -> Multiple Chains



What is Cryptocurrency

- Blocks are filled with transactions

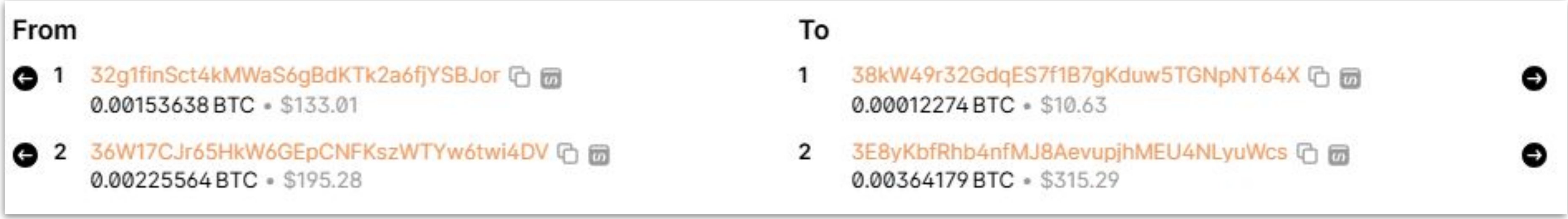
- Transactions are used to send crypto from one address to another.
  - Viewable to anyone - Pseudo Anonymous
  - TX hash is unique to each TX
    - e559008afee5b6ceb0407e503c8993d2c205ad972cbbd18af6f426b8bc2c0a25 (BTC)
    - 0xe0927e7540ce65beb12aa8c9263707906714e627d1b2d558c9082af46c9a0508 (ETH)

- Transactions need to be validated, which costs money. TX Fees are paid by the sender

- Use of transactions vary - crypto, contracts, messages - But will always have three elements
  - Input, Output and Hash

What is Cryptocurrency

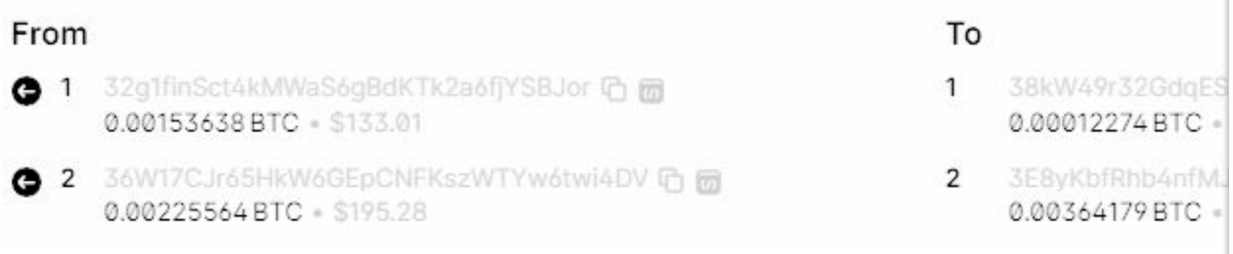
e559008afee5b6ceb0407e503c8993d2c205ad972cbbd18af6f426b8bc2c0a25



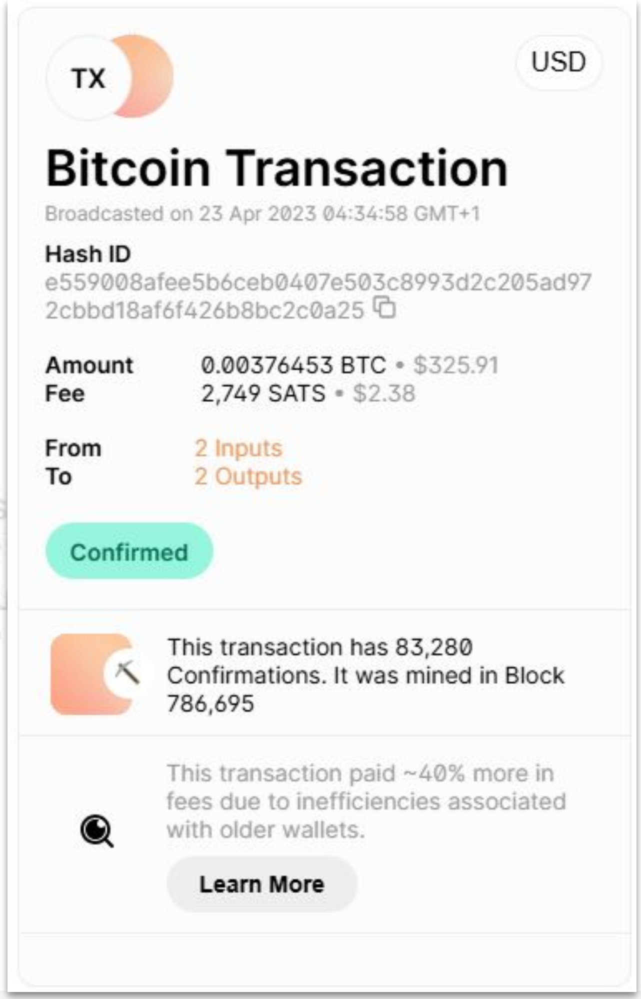
From		To	
1	32g1finSct4kMWaS6gBdKTk2a6fjYSBJor 0.00153638 BTC • $133.01	1	38kW49r32GdqES7f1B7gKduw5TGNpNT64X 0.00012274 BTC • $10.63
2	36W17CJr65HkW6GEpCNFKszWTYw6twi4DV 0.00225564 BTC • $195.28	2	3E8yKbfRhb4nfMJ8AevupjhMEU4NLyuWcs 0.00364179 BTC • $315.29

What is Cryptocurrency

e559008afee5b6ceb0407e503c8993d2c205ad972cbbd18af6f426b8bc2c0a25



From		To	
1	32g1finSct4kMWaS6gBdKTk2a6fjYSBJor 0.00153638 BTC • $133.01	1	38kW49r32GdqES 0.00012274 BTC •
2	36W17CJr65HkW6GEpCNFKszWTYw6twi4DV 0.00225564 BTC • $195.28	2	3E8yKbfRhb4nfMJ 0.00364179 BTC •



Bitcoin Transaction

Broadcasted on 23 Apr 2023 04:34:58 GMT+1

Hash ID
e559008afee5b6ceb0407e503c8993d2c205ad972cbbd18af6f426b8bc2c0a25

Amount 0.00376453 BTC • $325.91
Fee 2,749 SATS • $2.38

From 2 Inputs
To 2 Outputs

Confirmed

This transaction has 83,280 Confirmations. It was mined in Block 786,695

This transaction paid ~40% more in fees due to inefficiencies associated with older wallets.

What is Cryptocurrency

- Transactions contain Addresses
- Unique identifier used to receive and send cryptocurrency transactions
  - Bank account number
- Unique due to the way they are derived - Private/Public key relationship
- In order to send funds FROM an address, one must control the private key
  - Think bank account pin code/password
- Exposure of Private key can expose user to theft and loss of funds
- Addresses and Private keys are stored in a Wallet

What is Cryptocurrency

- A wallet is a collection of public and private keys

- A wallet allows a user to build and send transactions on the blockchain as well as accessing web 3.0 services like DeFi and NFTs

- Wallets generate addresses in a structured way from mnemonic seed words
  - More on those later

- Wallets can be:
  - Custodial or Non-Custodial
  - Hot or Cold
  - Digital or physical
    - Paper, Brain, Software, Hardware, Mobile etc

Seed Phrases

Seed Phrases

What are Seed Phrases and why are they important?

- A crypto wallet uses private keys to access the blockchain and its data
- A private key enables the wallet to calculate a balance of funds and build transactions
- The problem is that private keys are long strings are usually shown as long strings of hexadecimal such as:

  ```
  c25146ff39c432cd9406cac218cf5b82d74b799823736e128f85ed3b3e43c4e9
  ```

- This makes it difficult to copy accurately.

Seed Phrases

What are Seed Phrases and why are they important?

- The Bitcoin Improvement Proposal for seed words was published 2013-09-10.
- BIP39 - Mnemonic code for generating deterministic keys
- In simple terms, takes the private key, splits it and uses the values to index words from a specific wordlist.
- You can see example of wordlists here - https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt

Seed Phrases

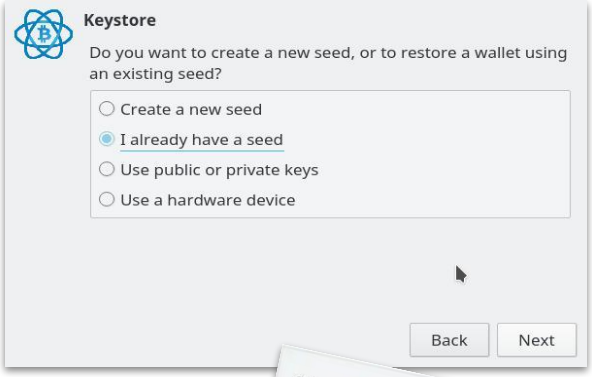
What are Seed Phrases and why are they important?

- IF YOU HAVE THE SEED WORDS YOU CAN TRANSACT ANY FUNDS CONTROLLED BY THE KEY
- ANYONE ELSE WITH THE SEED WORDS CAN POTENTIALLY TRANSACT THE FUNDS BEFORE YOU

Seed Phrases

How do I use a seed phrase to recreate a wallet?

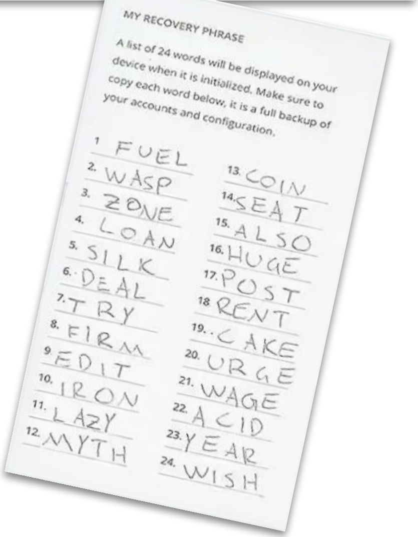
- Almost all wallets enable you to enter seed words to recreate an existing wallet



Keystore

Do you want to create a new seed, or to restore a wallet using an existing seed?

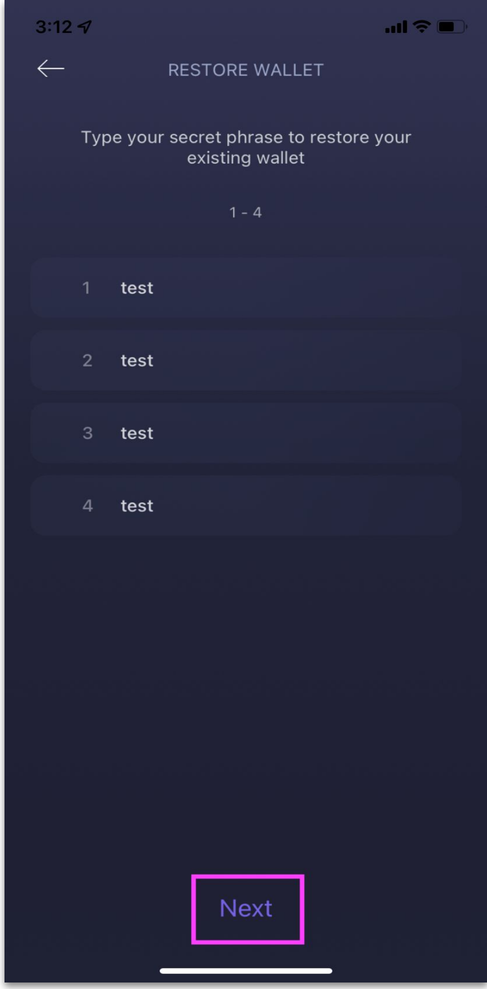
○ Create a new seed
● I already have a seed
○ Use public or private keys
○ Use a hardware device



MY RECOVERY PHRASE

A list of 24 words will be displayed on your device when it is initialized. Make sure to copy each word below, it is a full backup of your accounts and configuration.

1. FUEL
2. WASP
3. ZONE
4. LOAN
5. SILK
6. DEAL
7. TRY
8. FIRM
9. EDIT
10. IRON
11. LAZY
12. MYTH
13. COIN
14. SEAT
15. ALSO
16. HUGE
17. POST
18. RENT
19. CAKE
20. URGE
21. WAGE
22. ACID
23. YEAR
24. WISH



3:12

RESTORE WALLET

Type your secret phrase to restore your existing wallet

1 - 4

1 test

2 test

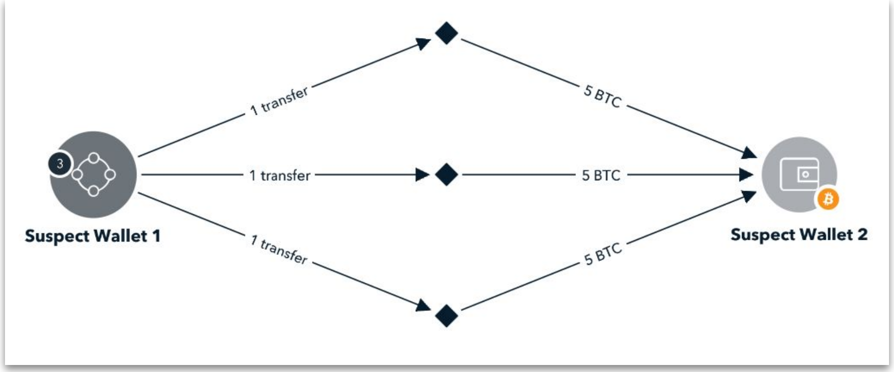
3 test

4 test

Seed Phrases

What are the potential risks associated with seizing seed phrases?

- Another person having access to the seed words!
- Incomplete list
- Switched words
- Split list
- Not finding the correct derivation path



DeFi explainer

Intro to Decentralized Finance

- Decentralized Finance (DeFi) aims to provide financial services without the use of intermediaries
- Allows for peer-to-peer transactions and for users to access services services normally controlled by institutions
  - Trading, Lending, Borrowing, etc.
- The main goals for the DeFi ecosystem are to provide users with:
  - Accessibility
  - Inclusivity
  - Transparency
  - Innovation

How DeFi Apps Work

Built on Blockchains

Apps like Uniswap are built on blockchain technology like Ethereum.

They operate without a central authority

Users trade, lend, and borrow assets on a peer-to-peer basis

Liquidity Pools

A reserve of two tokens (e.g. ETH and DAI) that users trade between

Price is determined by the pool's relative balance

Liquidity providers add an equal value of two tokens to the pool and receive liquidity tokens representing their share of the pool.

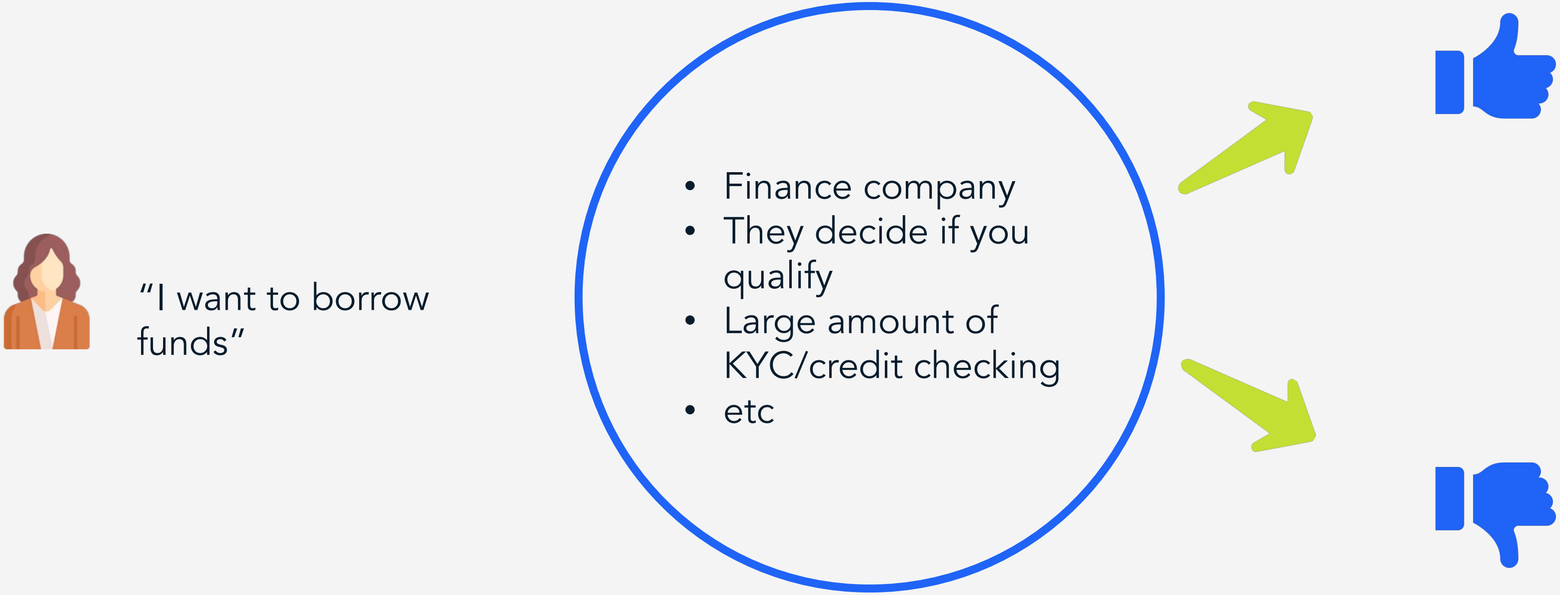
Trading

When a user trades on Uniswap the trade is routed through smart contracts

The smart contract calculates the price based on the pools current balances

The more a user trades against a pool the more the price changes = Slippage

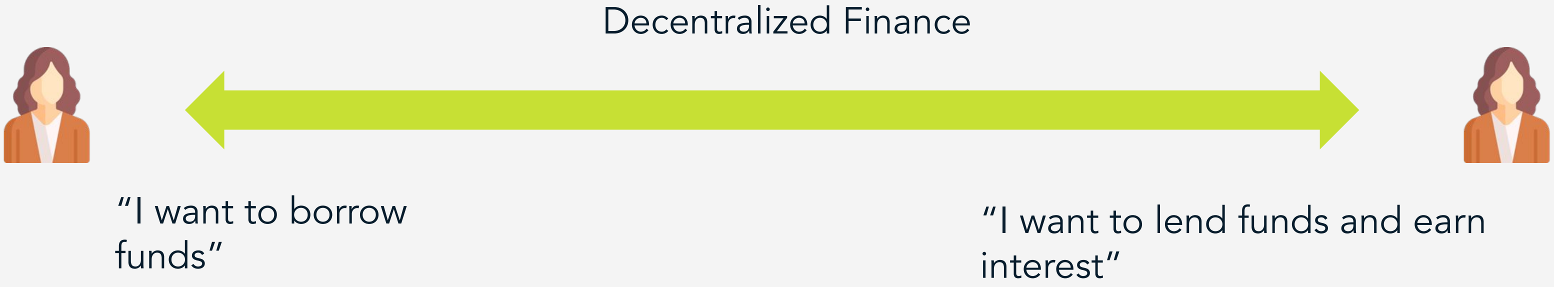
DeFi – Decentralized Finance



"I want to borrow funds"

- Finance company
- They decide if you qualify
- Large amount of KYC/credit checking
- etc

DeFi – Decentralized Finance



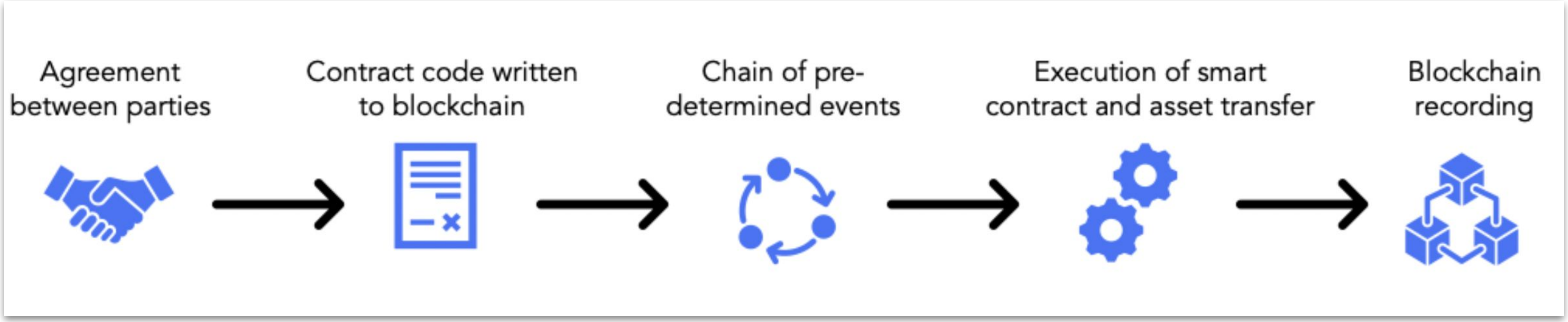
Decentralized Finance

“I want to borrow funds”

“I want to lend funds and earn interest”

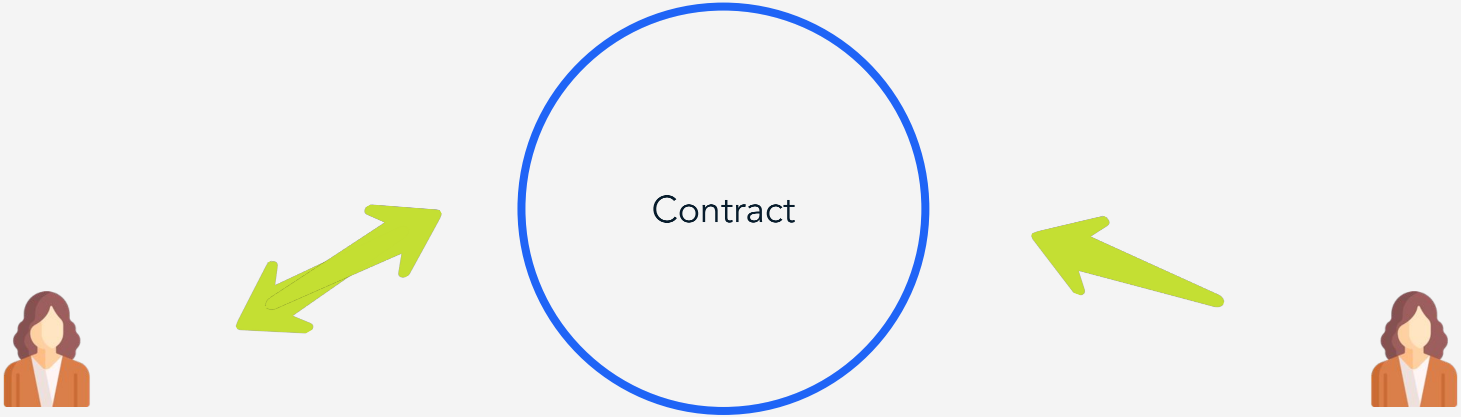
Smart Contracts

A self-executing contract written in code that exists on a blockchain; a mechanism for transferring value.



Agreement between parties → Contract code written to blockchain → Chain of pre-determined events → Execution of smart contract and asset transfer → Blockchain recording

DeFi – Decentralized Finance

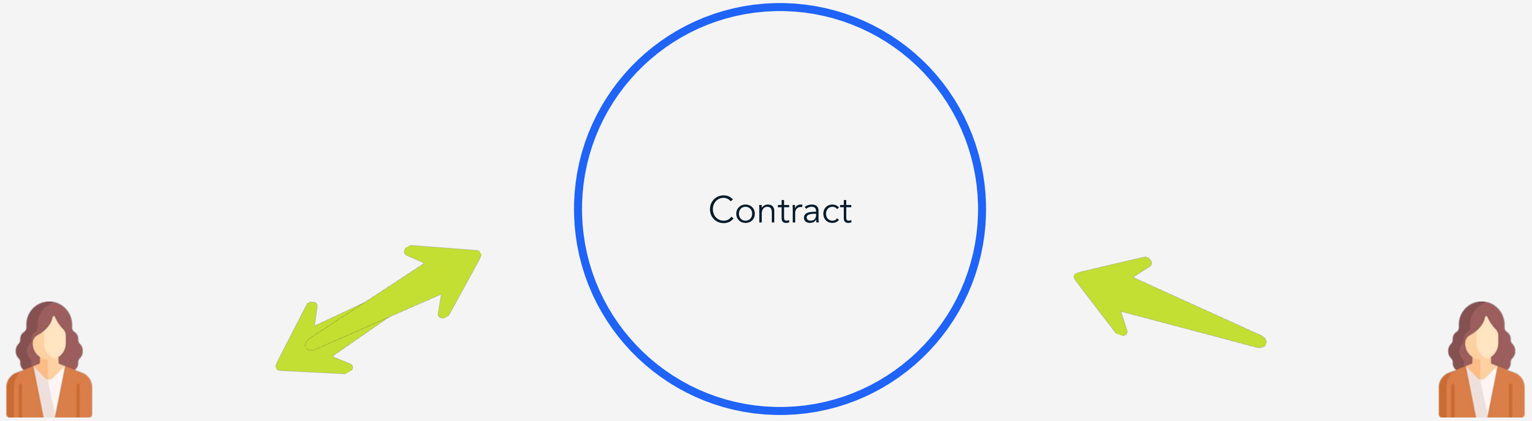


Contract

"I want to borrow funds"

"I want to 'lend' funds and earn interest"
(Yield farming/liquidity mining)

DeFi – Decentralized Finance



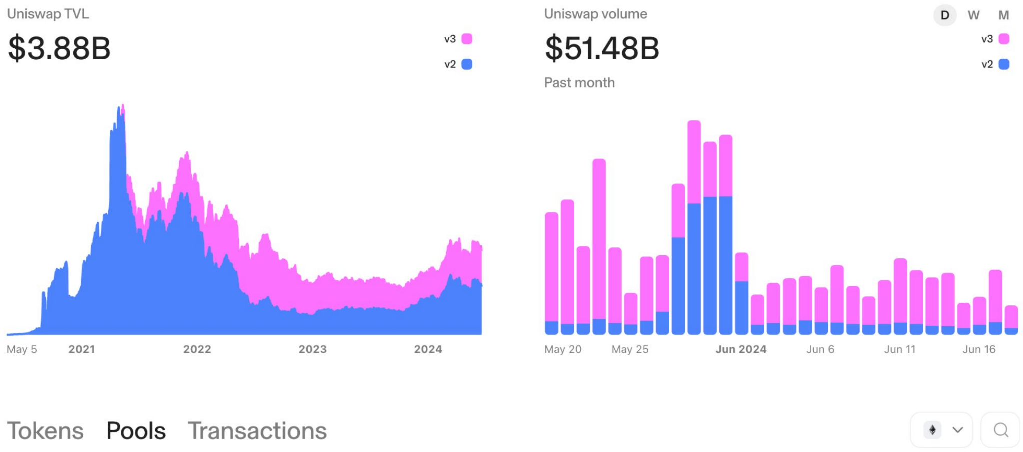
- Almost all based on the Ethereum platform or increasingly Binance Smart Chain
- To investigate we need to understand ERC-20 tokens and how to follow the chain

Understanding Liquidity Pools

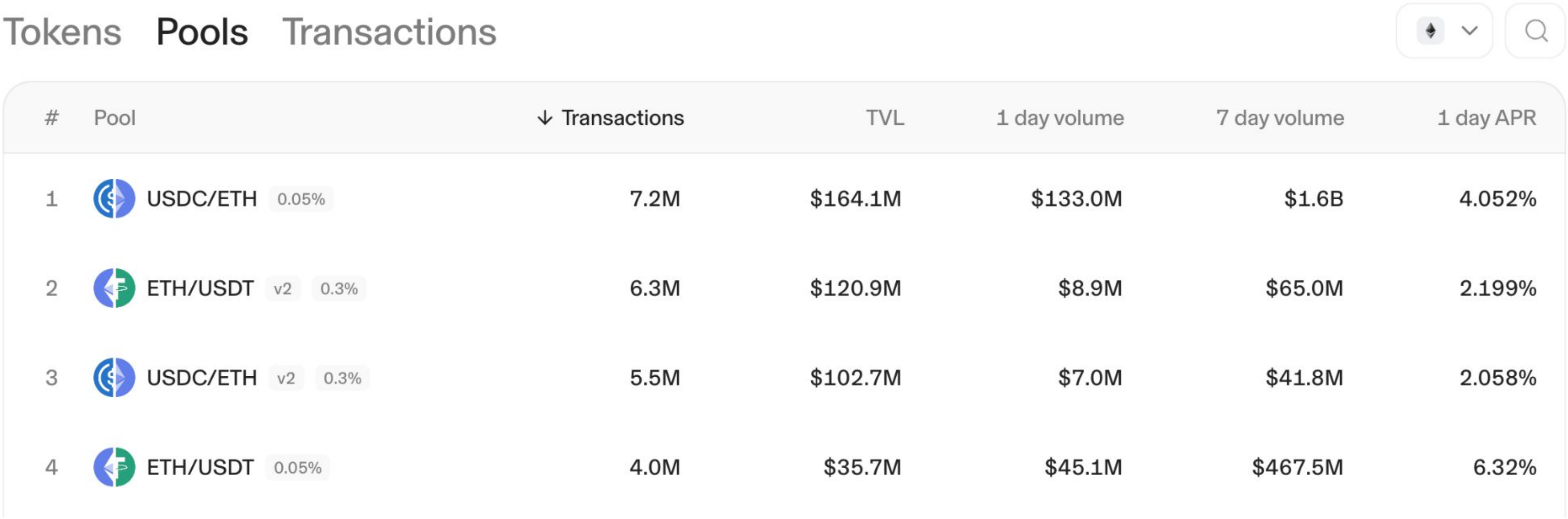
- Smart Contracts on decentralized platforms used to facilitate trading between two tokens
- The pools allow for users to conduct instantaneous trades at any time
- Prices are automatically rebalanced based on the available liquidity of a paired asset within the pool
- This is achieved through the use of an Automated Market Maker (AMM) rather than the traditional Order Book system

Understanding Liquidity Pools

- https://app.uniswap.org/explore/pools/ethereum



Understanding Liquidity Pools



#	Pool	↓ Transactions	TVL	1 day volume	7 day volume	1 day APR
1	USDC/ETH 0.05%	7.2M	$164.1M	$133.0M	$1.6B	4.052%
2	ETH/USDT v2 0.3%	6.3M	$120.9M	$8.9M	$65.0M	2.199%
3	USDC/ETH v2 0.3%	5.5M	$102.7M	$7.0M	$41.8M	2.058%
4	ETH/USDT 0.05%	4.0M	$35.7M	$45.1M	$467.5M	6.32%

Diving in the Deep End: Funding the Pools

- The pools are funded by individuals called Liquidity Providers
- Equal values of each asset in the trading pair will be deposited into the pools to enable users to trade
- This Liquidity Providers are incentivized to perform this service in return for rewards
- While potentially profitable this activity carries risk for the Liquidity Providers
  - Impermanent Loss
  - Smart Contract Vulnerability
  - Rug Pulls

Getting Your Hands Dirty: Yield Farming

- Yield Farming (Liquidity Mining) is the practice of receiving rewards in return for providing liquidity to DeFi protocols
- As a Liquidity Provider (LP) the user will be issued LP tokens which represent their share of the liquidity pool
  - These tokens can be transferred, traded,or staked
  - LPs can redeem the tokens to recoup the underlying assets in the pool, plus any accrued fees
  - Additional rewards can be generated as a percentage of fees associated with the transactions within the pool

The Essentials of Crypto Staking

- Staking is the process of locking up cryptocurrency as collateral to support a network
- Users that participate in staking receive awards in the form of additional tokens or potentially voting rights in the governance of the protocol
- Staking can also be used at the blockchain level where users stake their crypto in order to act as validators and verify transactions in blocks
    - Incentivizes good behavior among validators, which increases network security
- Many of the same risks as participating in Liquidity Pools with a few unique variables

MEV Bots

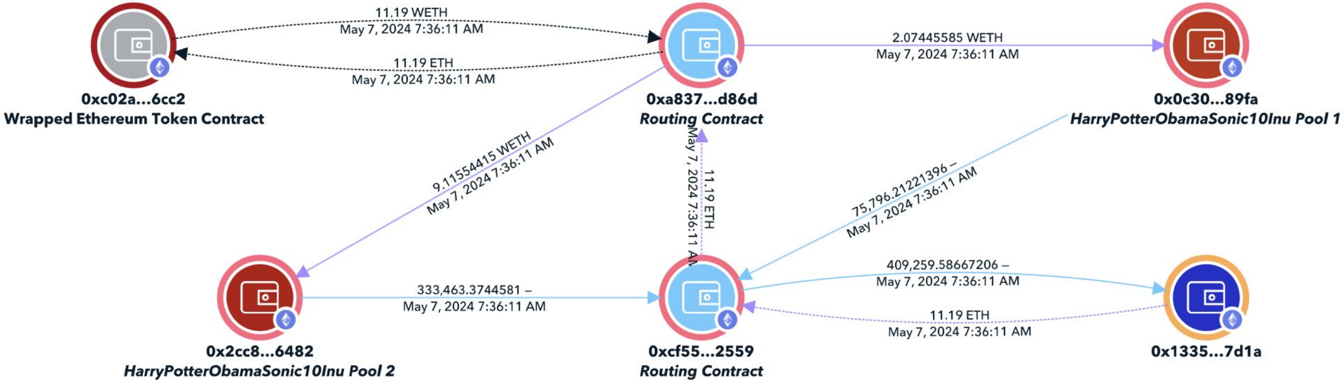
MEV (Miner Extractable Value) bots are automated programs used in blockchain networks to exploit the opportunities of rearranging, including, or excluding transactions within a block to maximize their profit. Here's a simple explanation of how they work and their impact:

How MEV Bots Work

1. Scanning the Mempool: MEV bots monitor the mempool, which is where pending transactions are held before they are confirmed in a block.
2. Identifying Profitable Opportunities: They look for opportunities to profit from these transactions. Common strategies include:
   - Arbitrage: Taking advantage of price differences for the same asset across different exchanges.
   - Front-Running: Detecting a large trade and executing a similar trade just before it to benefit from the price change caused by the large trade.
   - Sandwich Attacks: Placing one order before and one after a victim's transaction to manipulate the price and profit from the difference.
3. Submitting Transactions: Once a profitable opportunity is found, the bot submits its transactions with higher gas fees to incentivize miners to include them in the next block before the original transactions.

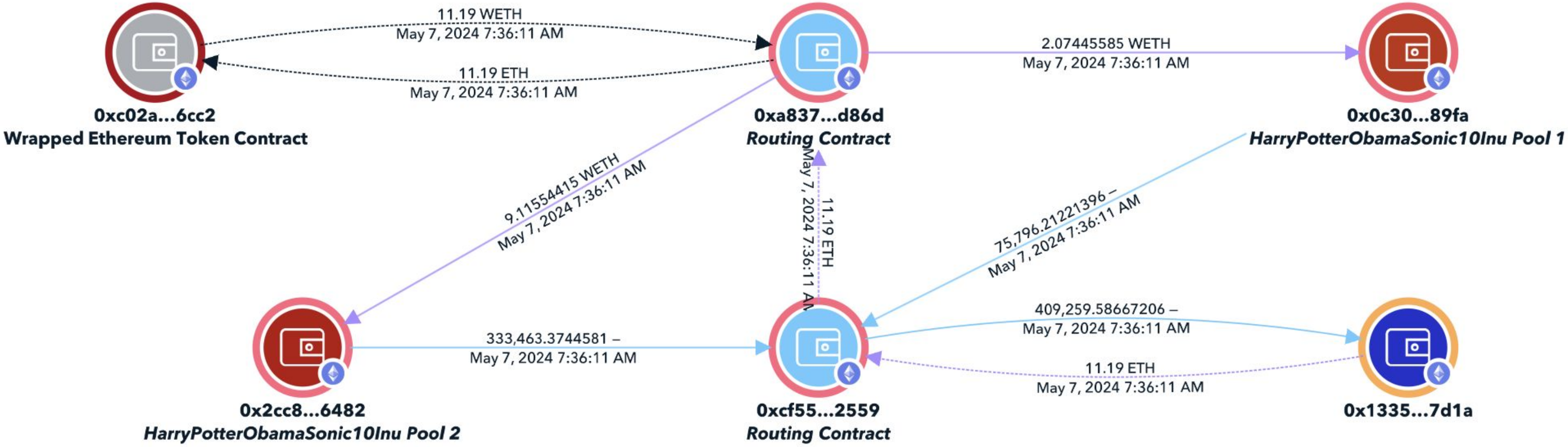
DeFi Examples

- UniSwap Regular Swap - C



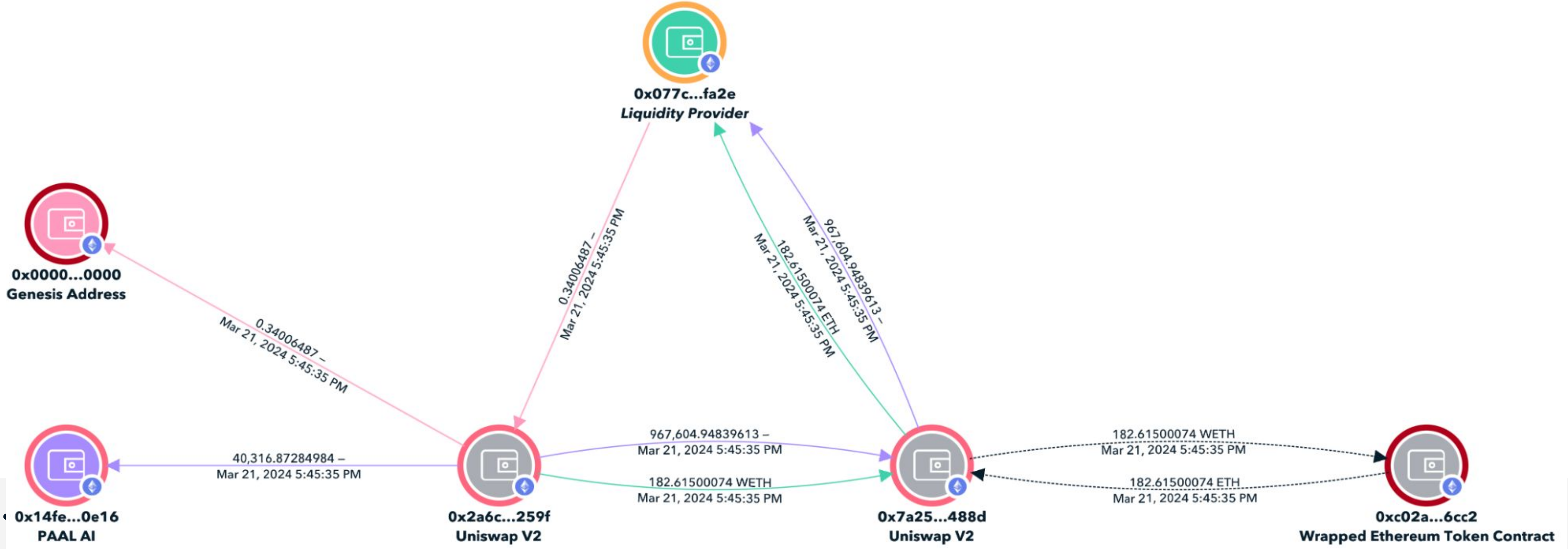
DeFi Examples

- Liquidity Pool Funding - 0xa0a968eb494a76da20c777d7055aca5d95c97d02e075a0fa379bfb37e55968b5



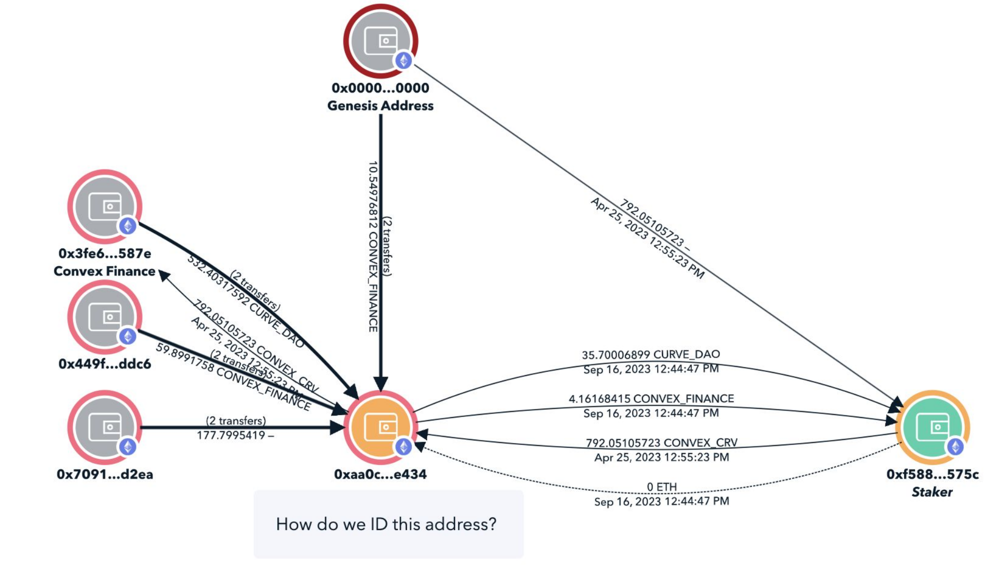
DeFi Examples

- Liquidity Pool Removal - 0xcfa555e7f37ca913bece3d6c2310312f7ad94f0f03c80dc3b0b6a8aeda52c24d


0x077c...fa2e
Liquidity Provider
0x0000...0000
Genesis Address
0x14fe...0e16
PAAL AI
0x2a6c...259f
Uniswap V2
0x7a25...488d
Uniswap V2
0xc02a...6cc2
Wrapped Ethereum Token Contract
0.34006487 – Mar 21, 2024 5:45:35 PM
0.34006487 – Mar 21, 2024 5:45:35 PM
182.61500074 ETH Mar 21, 2024 5:45:35 PM
967,604.94839613 – Mar 21, 2024 5:45:35 PM
40,316.87284984 – Mar 21, 2024 5:45:35 PM
967,604.94839613 – Mar 21, 2024 5:45:35 PM
182.61500074 WETH Mar 21, 2024 5:45:35 PM
182.61500074 WETH Mar 21, 2024 5:45:35 PM
182.61500074 ETH Mar 21, 2024 5:45:35 PM

DeFi Examples

- Staking Transaction - 0xefe057de9ea57492ca52b98ecf685fb36da71e256334794d5de9991b6664e687



How do we ID this address?

Stablecoins

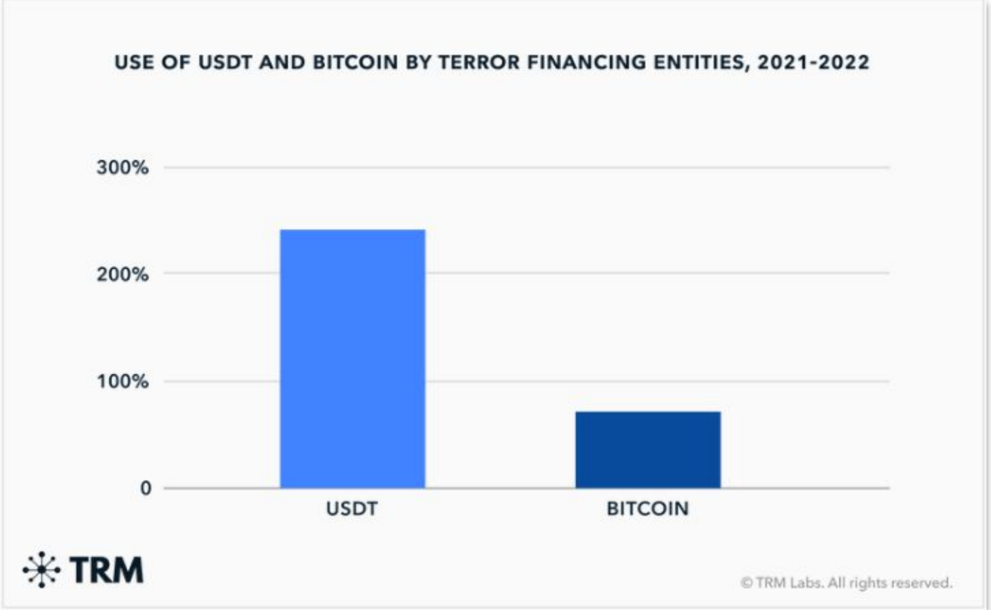
- Building block of decentralized finance
- One solution to crypto price volatility
- Most are pegged to the USD, but some are in other fiat currencies
- Tether (USDT) the most dominant stablecoin

Stablecoins

Significant increase in the use of the TRON blockchain among terrorist groups and associated fundraising campaigns

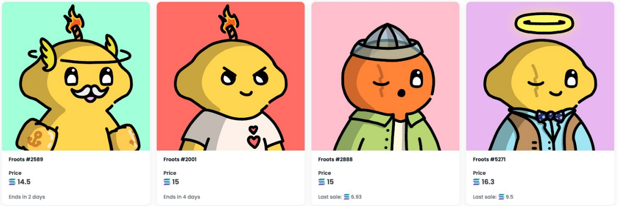
Majority of those actors collected donations in the stablecoin Tether (USDT).

Among the terror financing entities tracked by TRM Labs in 2022, there was a 240% year-on-year increase in the use of Tether - against a 78% rise in Bitcoin use.



What Are Non-Fungible Tokens?

- Unit of data stored on a blockchain, certifying a digital asset to be unique
- Often bought and sold with cryptocurrency
- Can be used to represent items such as photos, videos, audio, and other types of digital files



Froots #2589
Price
≡ 14.5
Ends in 2 days

Froots #2001
Price
≡ 15
Ends in 4 days

Froots #2888
Price
≡ 15
Last sale: ≡ 6.93

Froots #5271
Price
≡ 16.3
Last sale: ≡ 9.5

Froots NFT Collection on OpenSea.io

Fungible vs Non-Fungible

Fungible	Non-Fungible
Easily exchanged *Ex. $5 bill*	Not interchangeable *Ex. Concert ticket*

CeFi vs DeFi

coinbase

kraken

GEMINI

BINANCE.US

UNISWAP

SushiSwap

PancakeSwap

dYdX

VASPs

VASPs - Virtual Asset Service Providers

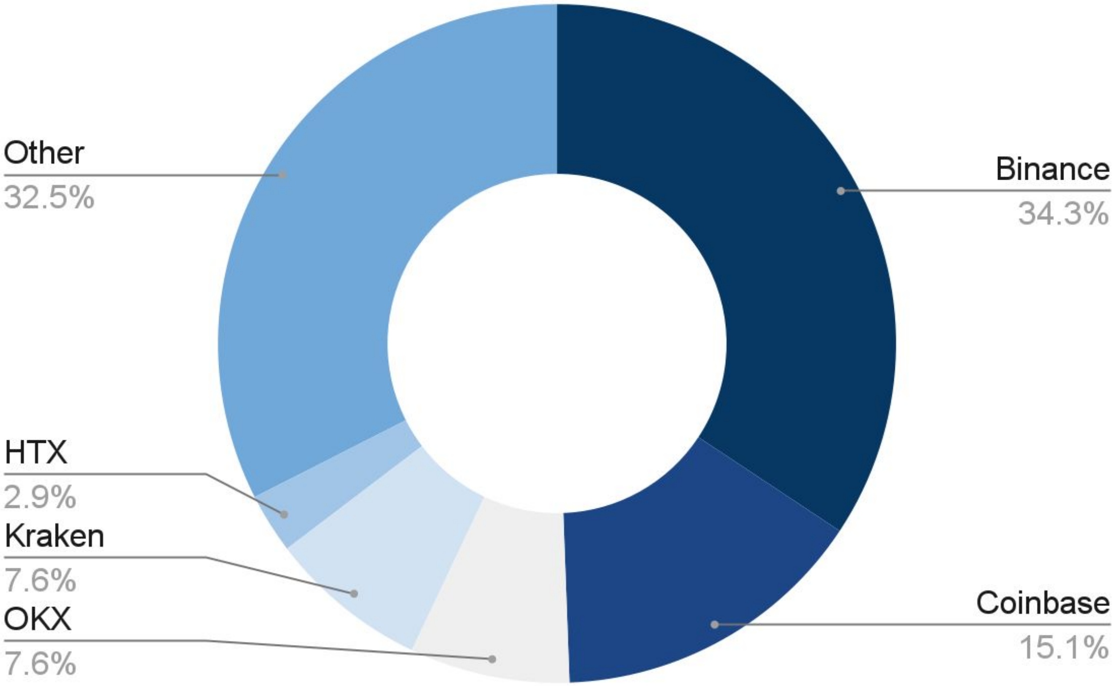
- VASPs Underpin the Cryptocurrency ecosystem - Serve as On/Off Ramps
- Buy/sell crypto - VASP will be involved somewhere
- Biggest part of the VASP ecosystem - <u>Exchanges</u>
    - Exchanges are MASSIVE part of the ecosystem
        - 4,000+, 100+ countries, $4 Trillion+
            - Volume higher than Germany's GDP

$4T of volume is heavily concentrated across top global exchanges

The top 5 exchanges accounted for ~70% of volume in 2023 and the top 20 exchanges accounted for ~90% of total exchange volume in 2023

Since 2020, 10 exchanges consistently have accounted for >75% of total exchange volume

Top 5 Exchanges by Total Crypto Volume[1]



[1] Data is for 1 Jan 2023 - 31 Dec 2023

Exchanges are key to understanding and combating illicit crypto activity

Exchanges can serve as:

- Partners in combating crime
- Targets of crime
- Facilitators of crime

Exchanges serve as partners for combating illicit activity

Exchanges that collect Know-Your-Customer (KYC) information can be a key source in criminal investigations globally, working with law enforcement officials to identify suspects with KYC and other forms of data

Exchanges may collect information about the person including nationality, first and last name, and date of birth

Customers might also be asked to provide the number of a government-issued ID, a photo of the ID, a selfie with the ID, or a combination of these to verify identify

Exchanges may ask for additional verification measures including proof of address, facial recognition, and a questionnaire with additional information

Exchanges can also facilitate illicit activity

What are High-Risk Exchanges?

A High-Risk Exchange (HRE) is one that can have a combination of characteristics that can enable illicit activity, including:

- Weak KYC & AML procedures
- Exploit accounts of other exchanges for trading without their knowledge (i.e., nested)
- Cash-to-crypto on-ramps and off-ramps
- Non-cooperation with international law enforcement

High-Risk Exchanges at a glance

High-Risk exchanges are known for large volumes of illicit activity

- > 1400 High-Risk Exchanges
- ~$25B Total Volume
- ~$80M in illicit activity

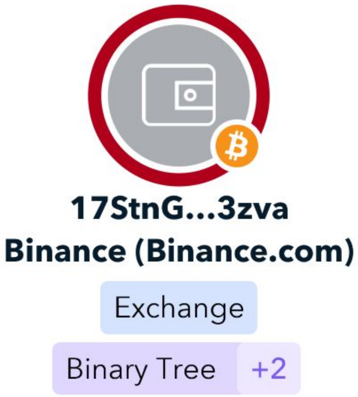
Nested Entities

Provides cryptocurrency services using the infrastructure of another exchange.

Typically will have:

- Lax KYC and AML processes
- Exploited by criminals

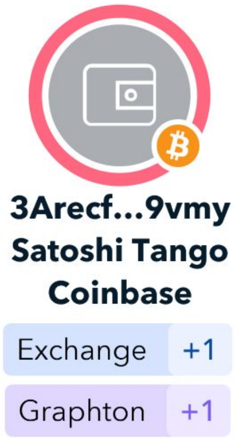
Implications for service legal requests on the host service, may direct you away from their service and the information you need is held by the nested service.



17StnG...3zva
Binance (Binance.com)

Exchange

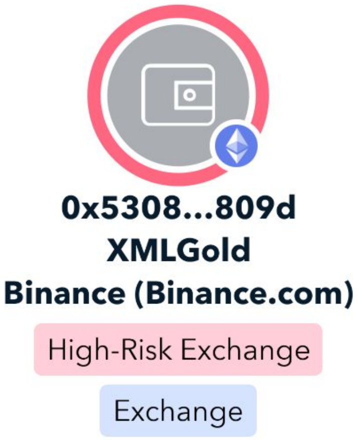
Binary Tree +2



3Arecf...9vmy
Satoshi Tango
Coinbase

Exchange +1

Graphton +1



0x5308...809d
XMLGold
Binance (Binance.com)

High-Risk Exchange

Exchange

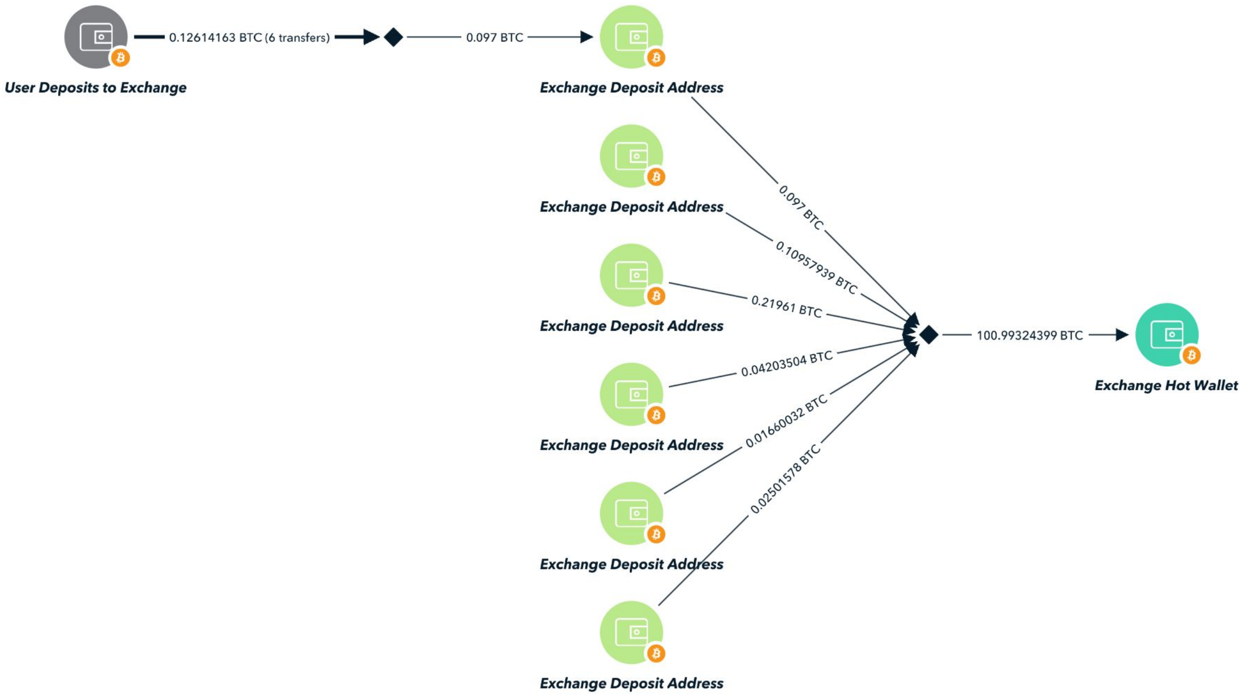
Deposit aggregation

Deposit aggregation is when an exchange combines a large number of customer deposits and sends them to another address at that exchange in a single transaction, usually to save money on transaction fees

The TRM graph depicts the following typology:

- An address deposits bitcoin (BTC) into a deposit address at a exchange (in light green)
- The deposit address then combines the initial deposit with 91 other inputs belonging to the exchange
- The 92 deposits are then sent to a final global exchange address in a single transaction

Deposit Aggregation



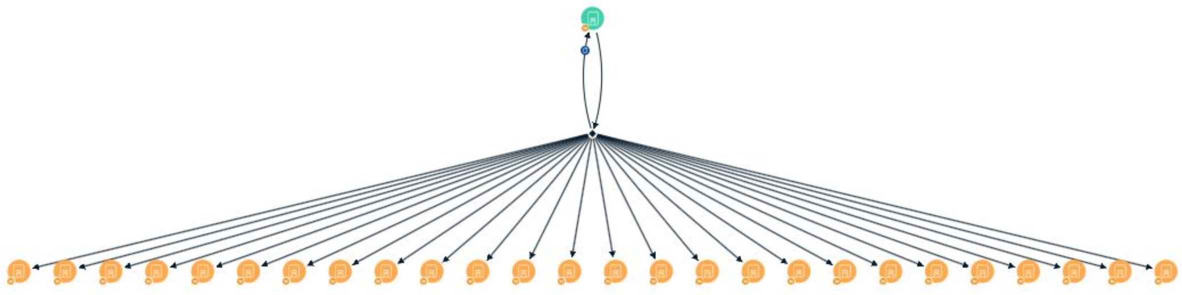
Hot wallet withdrawal

Similarly to deposit aggregation, hot wallet withdrawal is when an exchange combines a large number of customer withdrawals and sends them in one transaction from an exchange hot wallet to multiple customer addresses in a single transaction, usually to save money on transaction fees

The TRM graph depicts the following typology:

- A global exchange (green address) processes multiple customer withdrawals (orange) in one transaction
- The remaining "change" is sent either to another address owned by the global exchange or returns to the originating input address

Hot Wallet Withdrawals



Challenges of tracing through Exchanges

Due to the centralized nature of exchanges, it is extremely difficult to trace funds through an exchange during an investigation for 3 main reasons:

- Change of control of funds from the user to the exchange
- The co-mingling of customer funds
- A lack of key on-chain data due to internal transfers

If an investigation leads to an exchange, exchanges may comply with law enforcement requests for additional details, including customer KYC information

Change of Control: Funds are controlled by the crypto exchange as soon as they are deposited at the service

Co-mingling of Funds: Like regular banks, exchanges internally move and combine funds from various customers before they are withdrawn

Lack of On-Chain Data: Internal transfers conducted by exchanges are recorded on internal, off-chain logs and therefore will not be seen on the blockchain

T3 Collaboration

Freezing USDT

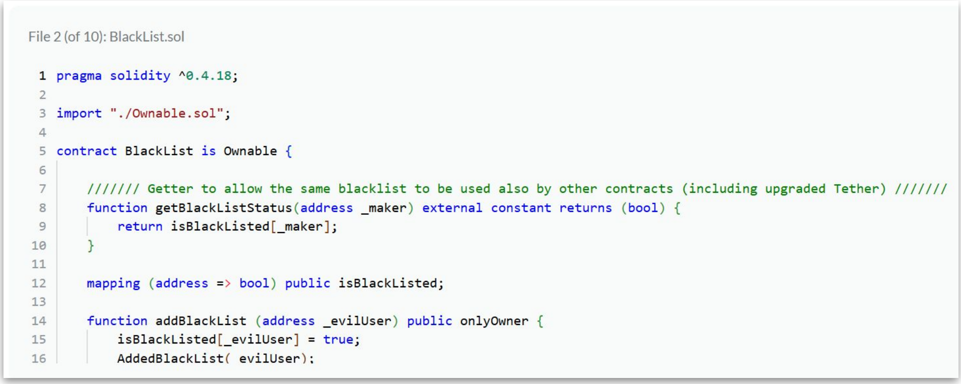
One useful tool to LE is the ability to freeze USDT, this is controlled by Tether. Through the token’s smart contract Tether can restrict access to specific addresses.

Tether can freeze or blacklist a specific wallet address holding USDT on the TRON network. Once frozen the address cannot transfer or redeem the USDT tokens it holds.

Let’s take a look at the USDT contract on tronscan and use the TLM3zA3EWycoDX4ZX4gKze7sgfbdkntTum address linked to Vostok Design Bureau

Freezing USDT

Navigate to the USDT contract address on tronscan: https://tronscan.io/#/token20/TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t/code

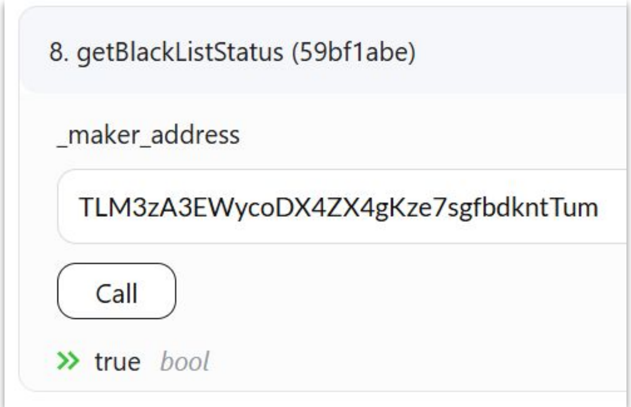


File 2 (of 10): BlackList.sol

```
pragma solidity ^0.4.18;

import "./Ownable.sol";

contract BlackList is Ownable {

    /////// Getter to allow the same blacklist to be used also by other contracts (including upgraded Tether) ///////
    function getBlackListStatus(address _maker) external constant returns (bool) {
        return isBlackListed[_maker];
    }

    mapping (address => bool) public isBlackListed;

    function addBlackList (address _evilUser) public onlyOwner {
        isBlackListed[_evilUser] = true;
        AddedBlackList(_evilUser);
```

We can get some sense of the contracts functions

Using the Read Contract tab we can check if an address is blacklisted. Let's look at TLM3zA3EWycoDX4ZX4gKze7sgfbdkntTum



8. getBlackListStatus (59bf1abe)

_maker_address

TLM3zA3EWycoDX4ZX4gKze7sgfbdkntTum

» true *bool*

T3 FINANCIAL CRIME UNIT

TRON | tether. | TRM

Objectives

Combat illicit activity associated with the use of USDT on the TRON blockchain

Create a safer and more secure crypto community for all by sending a clear message that illicit finance is not welcome in crypto

Form the first of its kind initiative aimed at facilitating a public-private partnership

T3 FCU

Stakeholders

First-of-its-kind private sector initiative aimed at combating illicit activity associated with the use of USDT on the TRON blockchain

TRON is a decentralized, blockchain-based operating system with smart contract functionality, proof-of-stake principles as its consensus algorithm

Tether is a cryptocurrency stablecoin, launched by the company Tether Limited Inc. in 2014. As of May 1, 2024, Tether had excess reserves of $6.3 billion

TRM

TRM is a blockchain intelligence platform that blends blockchain data with advanced analytics to help financial institutions and governments fight fraud, money laundering, and financial crime

Threat Tier Prioritization

Resources will be applied based on the threat level of the alleged illegal activity and value threshold. Exceptions can be made if agreed.

Severe Risk - Highest priority violations: Terrorism, CSAM, proliferation, sanctions, pig butchering

High Risk - Second priority violations: Large fraud schemes, hacks/exploits, ransomware, real-time-money laundering

Medium Risk - Lowest priority violations: Cybercrime, smaller fraud schemes, money launderers

Non-prioritized violations: All other categories of illicit use of cryptocurrency

96,076

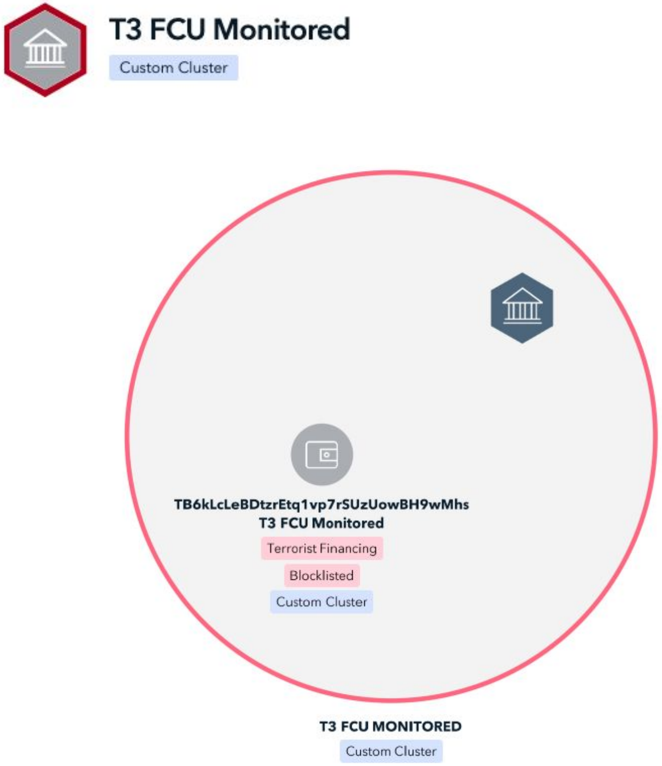
Total Transfers

105

Addresses

$3,122,081,126

Total Volume



T3 FCU Monitored

Custom Cluster

TB6kLcLeBDtzrEtq1vp7rSUzUowBH9wMhs

T3 FCU Monitored

Terrorist Financing

Blocklisted

Custom Cluster

T3 FCU MONITORED

Custom Cluster