Blockchain Forensics:
A Modern Approach to Investigating CyberCrime in the Age of Decentralisation

Saminu Salisu
Bilic
saminu@bilic.io

Velitchko Filipov
Bilic
velitchko.filipov@tuwien.ac.at

Barry Penne
Bilic
barry@bilic.io

30 June 2022

Abstract

Blockchain forensics (the use of scientific methods to manipulate data to create useful and informative descriptions of the manipulated data) takes data from the blockchain to interpret the flow of digital assets. Investigators use sophisticated data manipulation and visualization tools to identify the travel history of stolen assets. With these capabilities, chain hopping, round-tripping, and all attempts to blur transfer trails by cyber criminals become smoke screens with no effect. This paper establishes a framework for investigating financial crimes on the blockchain, starting with a brief explanation of blockchain forensics, types of financial crimes committed by criminals using the blockchain, and *how* they can be mitigated using OSINT[1]'s investigation process of data collection, data preservation, data processing, and data presentation. This paper also presents a community-based approach to financial crime investigations on the blockchain that involves the general public and victims themselves contributing valuable intelligence that can be used to trace and track criminals by authorities and security agencies in the global fight against cybercrime.

[1] (n.d.). OSINT Framework. Retrieved June 27, 2022, from https://osintframework.com/

Introduction: Compliance in the age of decentralisation

Blockchain forensics[2] and cryptocurrency forensics accounting involves both tracking and interpreting the flow of cryptocurrency assets on the blockchain. The data on the blockchain is publicly available, however, a large number of wallet addresses and transactions need to be deciphered, assessed, and interpreted in each and every case in order to properly track the flow of funds and report on it accordingly.

A significant part of the global economy is immersed in dirty practices, especially in the digital financial landscape, making proceeds from illicit business transactions illegal. To the owners of these assets, the ends are all that matter. To clean these proceeds, the typical criminal would route it through several financial stops and different handlers until it gets back to its origin, but as legal and clean money. The typical money launderer loves nothing more than a process which eliminates all trails that could be traced back to the culprit. It is for this reason that cryptocurrencies and their derivatives, such as Decentralised Finance (DeFi)[3] and Non-Fungible-Tokens (NFTs)[4], have become safe havens for stolen money.

On the blockchain, criminals use a variety of methods and services that deliver money to many addresses or corporations. The assets are subsequently delivered to a target location or an exchange to be liquidated from a legal source. This procedure makes tracing laundered monies back to illegal activity extremely difficult.

At this juncture, the very novel feature of the blockchain - its anonymity and decentralised nature - constitutes a significant fear and apprehension towards the technology, especially from the traditional financial sector. Hence, the increasing development of regulations to guide and monitor cryptocurrency usage and ensure strict compliance for cryptocurrency organisations and service providers. These regulations range from registering exchanges and implementing Know Your Customer (KYC) requirements and Anti-Money Laundering[5] (AML) complaint systems by cryptocurrency organizations for the classification of cryptocurrencies.

Business Problem: The cost of blockchain cybercrime

When cryptocurrency and the blockchain appeared on the financial market scene in 2009, it marked the birth of a technology that would threaten the stability of the traditional centralised financial system. Some of the most significant features of the technology were its anonymity and decentralised design and structure, which put it outside the control of the global political elites. However, this was not a problem for the global financial body and its controlling political spine during the early stages of the cryptocurrencies and blockchain revolution since the technologies were patronised by only a handful of seemingly weirding-looking computer geeks and were worth less than today.

[2] (n.d.). Blockchain Forensics | CipherBlade. Retrieved June 27, 2022, from https://cipherblade.com/blockchain-forensics/
[3] (n.d.). What is DeFi? - Coinbase. Retrieved June 27, 2022, from https://www.coinbase.com/learn/crypto-basics/what-is-defi
[4] (n.d.). Non-fungible tokens (NFT) - Ethereum.org. Retrieved June 27, 2022, from https://ethereum.org/en/nft/
[5] (n.d.). Anti-money laundering | The Law Society. Retrieved June 27, 2022, from https://www.lawsociety.org.uk/topics/anti-money-laundering

“What competition could these technologies pose? What damage could they wreck?”

The world would later find out in a very dramatic fashion what magnificent tree these crypto seeds could grow into in just a decade. In November 2021, the cryptocurrency industry reached a whopping $1.03 trillion in capitalisation, according to CoinMarketCap[6]. This was roughly a decade after Laslo exchanged about 10,000 bitcoins for 2 Papa John’s Pizza[7]. Today, the cryptocurrency industry has expanded to include NFTs valued at about $17 billion and DeFi valued at about $200 billion as of February 2022.
Just two short years ago, Binance[8] was the victim of a very swift attack that left the biggest cryptocurrency exchange at that time short of about 7000 bitcoins worth about $40.8 million at the time of the theft, making it one of the biggest cryptocurrency theft of all times[9]. When investigators followed the transfer trail of the Binance hack, it was discovered that about 5000 bitcoins of the total stolen funds were transferred and laundered through a service called Chip Mixer. Mixers came onto the cryptocurrency scene shortly after the emergence of Bitcoin.

Another recent hack involved the $615 million dollars heist by a North Korean group on the popular play-to-earn game called Axie Infinity[10]. The theft of Ethereum cryptocurrency from a software bridge used for the well-known Axie Infinity play-to-earn game was connected by the US Treasury Department to the North Korean hacking outfit Lazarus. The US agency went as far as placing the Ethereum addresses on the official OFAC sanction list[11].

Presently, billions of dollars exchange hands daily within the crypto market, and with its speed and guaranteed anonymity, the industry, by default, sends an invitation to money launderers, terrorists, hackers, drug traffickers, and other sellers of illicit materials to take advantage of the technology’s ability to protect the identity of its users while allowing them to clean and funnel dirty money back into the financial system.

The global financial system needs an urgent intervention in recovering these stolen funds, creating awareness of cyber safety, and developing innovative tools to tackle this uniquely novel technology increasingly used by cyber criminals to obfuscate and launder illicit assets around the globe.

In the next section, we highlight how criminals are obfuscating funds movement on the blockchain and how they can be tracked and stopped using some of the innovative tools and services offered by Bilic[12].

[6] (n.d.). CoinMarketCap: Cryptocurrency Prices, Charts And Market .... Retrieved June 27, 2022, from https://coinmarketcap.com/

[7] (2018, May 22). Bitcoin Pizza Day 2018: Eight years ago, someone bought two .... Retrieved June 27, 2022, from https://qz.com/1285209/bitcoin-pizza-day-2018-eight-years-ago-someone-bought-two-pizzas-with-bitcoins-now-worth-82-million/

[8] (n.d.). Binance: Buy/Sell Bitcoin, Ether and Altcoins | Cryptocurrency .... Retrieved June 29, 2022, from https://www.binance.com/en

[9] (2019, May 15). Binance loses £31 Million In Well Planned Cyber Attack.. Retrieved June 27, 2022, from https://www.firstsolution.co.uk/blog/binance-loses-31-million-in-well-planned-cyber-attack/

[10] (n.d.). Axie Infinity. Retrieved June 29, 2022, from https://axieinfinity.com/

[11] (2019, September 13). Treasury Sanctions North Korean State-Sponsored Malicious Cyber .... Retrieved June 27, 2022, from https://home.treasury.gov/news/press-releases/sm774

[12] (n.d.). bilic | blockchain data forensics. Retrieved June 27, 2022, from https://www.bilic.io/

Pain Points: How Criminals are obfuscating transactions on the blockchain

Decentralised Finance

Against the design of a centralised finance system which includes third-party intermediaries and leaves a bunch of paper trails, DeFi eliminates the need for a middleman through the use of peer-to-peer financial protocols.

With DeFi, anyone with a computer and internet connection can participate in order to lend, borrow, stake, and trade cryptocurrencies just like in traditional finance. More so, DeFi, unlike cryptocurrency exchanges, has no stringent requirements for identity verification. Thus, users' identities are protected when it comes to participating on these platforms.

The fact that DeFi platforms protect the identity of users offers an invitation to money launderers. Recent reports have revealed that about half of all the recently stolen cryptocurrencies were sent to DeFi platforms. In another report by The Block, about $192.82 billion remains locked in DeFi as of January 2022[13]. The argument for the rise in using DeFi for the cleaning and funnelling of illegal money is due to its present existence outside the regulatory borders.

DeFi is built on blockchain technology; hence, as a platform built on the decentralised ledger technology, transaction data can be accessed and traced. Money launderers, therefore, have to employ other strategies to eliminate the digital footprints of their transactions on platforms. Some of the strategies used include:

Peel Chain [14]

Peel chain is used to funnel very large sums of cryptocurrencies in and out of DeFi platforms in order to make it undetected by authorities that look into very monstrous transactions. Peeling allows money launderers to break small transactions into large amounts of crypto assets and in this piecemeal, maybe even incremental, send large amounts of cryptocurrencies to centralised or decentralised exchanges, where they are converted to fiat currencies or other cryptocurrencies. Money launderers create very long and complex peel chains so that at the time the resources and processes required to trace the transactions to their financial destination become almost impossible and tedious. For instance, an individual wanting to transfer 100 ETH undetected could perform 200 different transactions of 0.5 ETH each. This might be a tedious process, but it lends in with all other normal transactions and thus raises no red flags for the sender.

[13] (2022, June 12). Value Locked - Ethereum and Binance Smart Chain - The Block. Retrieved June 27, 2022, from https://www.theblock.co/data/decentralized-finance/total-value-locked-tvl

[14] (n.d.). Peel Chain | Cryptocurrency Investigation - Hudson Intelligence. Retrieved June 27, 2022, from https://www.fraudinvestigation.net/cryptocurrency/tracing/peel-chain

Chain Hopping[15]

Another strategy money launderers favour is chain hopping. DeFi platforms like Change Finance, which is a multi-chain DeFi application and promotes interoperability, allow users to move their access from one blockchain network to another. Launderers often move from one chain or cryptocurrencies to another in very quick succession. This is to lose trackers and increase the complexity of their transaction history so that it becomes almost impossible to follow the transaction trail to the destination.

Mixers (Tornado Cash)[16]

While blockchain technology makes it impossible to link individuals to wallet addresses, the decentralised public ledger keeps track of all receipts and transactions on the blockchain. Hence, transaction activities between wallets are available and can be tracked until very broad and unrelated data are sifted, cross-referenced, and narrowed down to relatively small variables from which to make better and informed guesses. This, to a large extent, is great news for crypto security and a major deterrent for money launderers on the crypto market.

Enter cryptocurrency mixers. Mixers act as digital shredders that destroy the transaction history provided by the blockchain and in the process make it impossible to track transactions effectively. A very popular mixer is the Tornado Cash mixer[17].

Tornado Cash is an Ethereum DeFi application rumoured to have been used by hackers to launder 100 million in stolen money. With mixers like the Tornado Cash, cryptocurrencies are deposited into the application by the depositing address and the deposits can only be made in specific amounts as stipulated by the application. This could be in ones, tens, or hundreds. The most plausible reason for this is that each one that contributes to the pool contributes the same amount, and when a withdrawal is made it becomes impossible to know which wallets initially deposited which and took out what.

The deposited funds are left for a short period of time to allow the deposited funds to mix with other funds in the system so that no transaction exists as a single transaction but a batch of transactions are layered, bunched, and mashed together to create a single compound transaction that cannot be tied to a single wallet address. The funds are then withdrawn via a different address referred to as the relayer and sent to the recipient's address, which is often different from the deposit address. This breaks the on-chain connection between the deposit address and the recipient address.

[15] (n.d.). Mixing, CoinJoins, Chain Hopping, and Privacy Coins - Chainalysis. Retrieved June 27, 2022, from https://go.chainalysis.com/advanced-obfuscation-techniques-webinar.html

[16] (n.d.). Tornado cash. Non-custodial private transactions on Ethereum.. Retrieved June 27, 2022, from https://github.com/tornadocash/tornado-core

[17] (n.d.). Tornado.cash. Retrieved June 29, 2022, from https://tornado.cash/

It is also important to note that most users of the platform often make use of VPN services to mask their IP addresses so that the deposit IP address is not connected to the withdrawal address.

Tornado Cash mixer's ability to mash and mix transactions to remove the traces of of cryptocurrencies transfers to and from different wallets makes it a very useful tool in the hands of money launderers. In January of 2022, about 4006 ETHs were stolen from crypto.com and investigations[18] into the theft revealed that the stolen ETH had been laundered through Tornado Cash in batches of 100s to unknown wallets.

According to Strom, founder of Tornado Cash, in an interview with CoinDesk, Tornado version 2 would include a cryptographic note in the transaction history of Ether during transactions to help determine the provenance of funds[19]. While this might increase the ability to track the movement of illicit funds through the platform, Tornado continues to attract huge cryptocurrency transactions because of its ability to mask transaction information.

Money Laundering using NFT

The physical art industry has always been attractive to money launderers because of its subjective price, scarcity, unpredictability, and vulnerability to manipulation. Undoubtedly, these factors, including anonymity, which is the icing on the cake, also play out in the NFT industry, resulting in the consequent embrace of the NFT industry by both legitimate and questionable business individuals. A thorough analysis of the NFT market immediately reveals its inorganic financial value explosion and the erratic movement of huge funds to purchase almost worthless digital pieces. But who cares? What is worth nothing to James might be worth gold to John, right? Well, isn't that the right technological recipe for the manipulation and funnelling of dirty money into legally acceptable tender?

One of the popular ways money launderers utilise NFT platforms for laundering dirty money is through Wash Trading[20], which refers to putting up one's NFT for sale, and then purchasing it by oneself multiple times, and, in the process, manipulating the value significantly, increasing the sale price.

What money launderers do is create an account on NFT platforms, create or buy a piece of art on the platform, and wash trade" the NFT asset in their possession, using different accounts on the same platform to increase the price of the asset. When the price of the asset is significantly pumped up, they sell the asset to themselves and receive their dirty illegal money through the sale of an NFT as legitimate money which is withdrawn and circulated in society.

[18] (2022, January 17). Crypto.com's Stolen Ether Being Mixed Through Tornado Cash. Retrieved June 27, 2022, from https://www.coindesk.com/business/2022/01/18/cryptocoms-stolen-ether-being-laundered-via-tornado-cash/

[19] (2022, January 25). Tornado Cash Co-Founder Says the Mixer Protocol Is Unstoppable. Retrieved June 27, 2022, from https://www.coindesk.com/tech/2022/01/25/tornado-cash-co-founder-says-the-mixer-protocol-is-unstoppable/

[20] (2022, April 18). What are wash trading and money laundering in NFTs?. Retrieved June 27, 2022, from https://cointelegraph.com/explained/what-are-wash-trading-and-money-laundering-in-nfts

Chainalysis, in its report[21], identified 262 users who sold an NFT to a self-funded address more than 25 times, creating $8.5 million in profits. Close analysis showed that certain transactions on OpenSea showed very irregular pricing and certain accounts could be traced to have transferred funds to other wallet addresses and then used to purchase NFTs from the foundation account. These practices serve to funnel dirty and illegal money through a legitimate digital art platform back into the economy as legitimate money.

Solutions: Tracking Cyber Criminals on The Blockchain

The anonymity of cryptocurrencies makes it difficult but not impossible to uncover the identities or persons behind wallet addresses. In fact, it is this feature which makes NFTs and other cryptocurrencies slaughterhouses for infected meat.

However, a combination of blockchain investigation tools and expertise can increase precision for tracing and tracking cryptocurrency transactions and identifying their provenance. The processes of attribution and tracking money flow make it possible to reduce the numerous variables and immense amount of data involved in a single transaction to a manageable minimum so that investigators can make the most informed decisions with the information and data at their disposal.

Most people think that crypto trading keeps you anonymous. All you need to show is your wallet address or public key. An address is a string of numbers and letters, 26-35 characters long.
The truth is, crypto trading is pseudonymous. This means that you can't hide your full identity.
This brings us to the big question: **Can a Crypto Transaction be traced?** The short answer is **YES**.
But it's not a 2-minute process. And it requires some expertise.

If a hack or theft occurs, an intelligence agency will need to track the hacker's wallet address. These steps are further highlighted here [22]

Hash functions or strings representing individuals and wallet addresses still present a problem for de-anonymisation[23]. One of the ways to ensure de-anonymisation on the blockchain is the institution of compulsory KYC for NFT and DeFi platform users. This will make sure that wallet addresses can be linked to verifiable user information outside the blockchain, making tracing easier and more effective.

[21] (2022, February 2). NFT Money Laundering and Wash Trading - Chainalysis Blog. Retrieved June 27, 2022, from https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-nft-wash-trading-money-laundering/

[22] (2022, April 23). bilic | Can my transactions on the blockchain be tracked ? - YouTube. Retrieved June 27, 2022, from https://www.youtube.com/watch?v=3NqFKGA_nq4

[23] (n.d.). What is de-anonymization (deanonymization)? - TechTarget. Retrieved June 27, 2022, from https://www.techtarget.com/whatis/definition/de-anonymization-deanonymization

Strengthened policy regulations around using DeFi and NFTs

Such regulations would be aimed at monitoring and arresting the dangerous activities of money launderers. These policy regulations must be dynamic and flexible but with incremental strictness.

Putting in place the necessary AML system to flag suspicious transactions is very appropriate. In August 2021, hackers got hold of $610 million worth of stolen cryptocurrency. About $33 million was converted to the Tether stable coin. The immediate discovery of the activity and swift action of Tether's chief technology officer, Ardoino, led the network to freeze the asset, making it impossible for the hacker to make away with the money. According to Ardoino, the money might have been lost forever had the Tether network wasted more time[24].

Recently, stolen crypto recoveries suggest that the days when cryptocurrencies provided a safe haven for criminals are almost completely over. The recovery of Poly's stolen funds, among others, suggests that blockchain investigators and forensics are improving their methods of tracking down and recovering stolen funds. Examples of tracking successes in the recovery of stolen or dirty money include the $2.3 million paid by the colonial pipeline to hackers who gained access to its computer network and Kucoin's recovery of $281 million in customer assets.

It is general knowledge that the end destination of cryptocurrencies for launderers is exchanges and DeFi platforms. Especially those with no KYC provisions. For this reason, Lisa Monaco stated that the most effective strategy for apprehending money launderers within the crypto space is to follow the money trail made available by the blockchain. The blockchain is sure to document all transactions irrespective of how complex such funds might have been routed to hide their origins and obscure their destinations.

Investigating the Blockchain

To effectively follow the money, crypto investigators use complex tools to investigate the origins of funds, the digital footprints left by the complex layers of transactions, and the destinations of funds.

Investigating sources of funds is an attempt to identify the origin of transactions, especially the address that triggers the beginning of the financial activity. As the transaction commences and goes on, it leaves footprints as it moves from chain to chain, from one exchange to the other, or from wallets to wallets.

Tracking the footprints of crypto fund flow and its analysis is often achieved using complex data mining techniques such as clustering, ownership analysis, and e-discovery:

1. Ownership analysis puts together a confluence of factors and evidence which uncovers the beneficiaries and identities behind wallet addresses under investigation.
2. Clustering algorithms, on the other hand, serve to sift, cross-reference, and identify wallet addresses that belong to the same wallet and owner. Clustering can identify thousands of addresses as belonging to a particular wallet. This helps to reduce the confusion caused by the peeling of funds and concerns the investigator with the end game in mind.

[24] (2021, September 22). Tracking stolen crypto is a booming business - The Washington Post. Retrieved June 27, 2022, from https://www.washingtonpost.com/technology/2021/09/22/stolen-crypto/

3. E-discovery helps to scrape crypto transaction and wallet data off the internet and personal devices and analytically weave the data into a giant digital roadmap which gives the investigator holistic insight. E-discovery often employs different tracing techniques to achieve its purpose.

Lastly, the destination of funds analysis is to identify the wallets that receive funds after they have been laundered through multiple layers of activities.

An important addition to crypto security, presumably the most important one yet, which has turned the tide in favour of forensic experts, is the development and use of sophisticated software for tracking and analysis. An example is Bitquery, which produces analytical tools and software for investigations.

Product: Bilic® Blockchain AML Product Suite

An all-rounded suite of tools, techniques, and visualization methods provided that empowers analysts and investigators to uncover these stolen/laundered/hacked funds would look like the Bilic framework. Bilic[25] is a blockchain forensic company that aims to help government agencies, businesses, financial institutions, and regulators detect and prevent financial crime involving crypto assets by democratising investigation through an open intelligence marketplace. Bilic's National Institute of Standards and Technology NIST standard-compliant investigative approach[26];

Methodology:

- Data collection: The data collection phase would use sophisticated software to scrape transaction data off the blockchain.
- Data Processing: The processing stage will convert the collected data into useful information used to track the origins, movements, and destinations of stolen funds.
- Group Intelligence Gathering: This phase involves the combination of different intelligence departments in gathering information. This helps to cross-reference information to ensure a confluence point where the different data meets to show that information gathering is credible and would promote informed decision-making.
- Reporting: The final phase involves presenting the findings of investigations for decision making.

Bilic’s AML Product Features

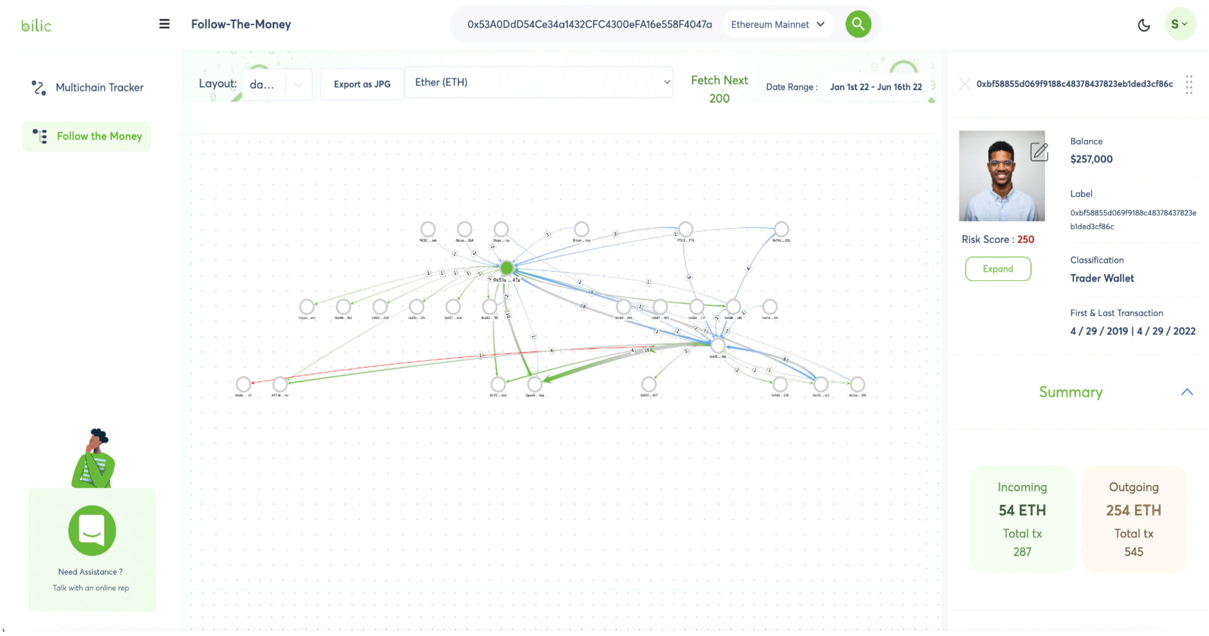
Follow The Money (FTM) AML

FTM is our novel proprietary blockchain investigation dashboard for crypto-asset exploration, visualisations, and wallet transaction tracking. The FTM supports over 47 blockchain networks with multichain graph network visualisation support, meaning analysts can investigate Ethereum and

[25] (n.d.). bilic | blockchain data forensics. Retrieved June 29, 2022, from https://www.bilic.io/
[26] (n.d.). Cybersecurity Framework - NIST. Retrieved June 27, 2022, from https://www.nist.gov/cyberframework

Bitcoinwallets on the same graph.

The FTM dashboard shows the wallet transaction history including funds sent and received, In- and outbound transfers, smart contract interaction, and highlighted activities involving labeled wallets. Investigators can use the FTM tool to investigate transactions, identify nefarious wallets involved in illegal transactions, and track the funds. The FTM dashboard graphically depicts the fund's intake and outflow (see the following figure).



0x53A0DdD54Ce34a1432CFC4300eFA16e558F4047a Ethereum Mainnet

Layout: da...

Ether (ETH)

Date Range : Jan 1st 22 - Jun 16th 22

0xbf58855d069f9188c48378437823eb1ded3cf86c

Risk Score : 250

Balance
$257,000

Label
0xbf58855d069f9188c48378437823eb1ded3cf86c

Classification
Trader Wallet

First & Last Transaction
4 / 29 / 2019 | 4 / 29 / 2022

Incoming
54 ETH
Total tx
287

Outgoing
254 ETH
Total tx
545

Fig. 1. Showing the Follow the Money Wallet Investigation dashboard with a graph network of user transaction and wallet activities

Users can create public and private labels used to tag suspicious wallets, which can be a source of provence for future investigators and valuable intel to both future investigators and intelligence consumers.

Intelligence Marketplace

The Intelligence Marketplace is an open intelligence platform that rewards data generators through funds recovery carrying out investigations of illicit transaction data and reporting. It also offers data consumers such as intelligence agencies, and government organisations access to actionable information in a secure privacy-preserving fashion.

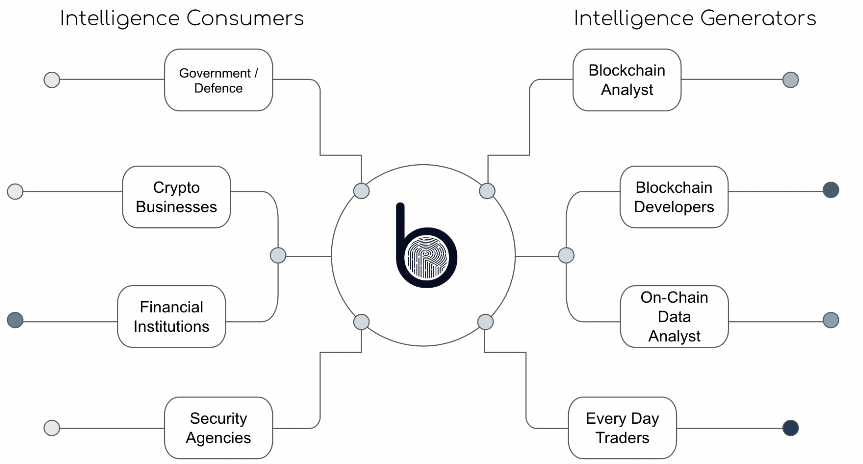
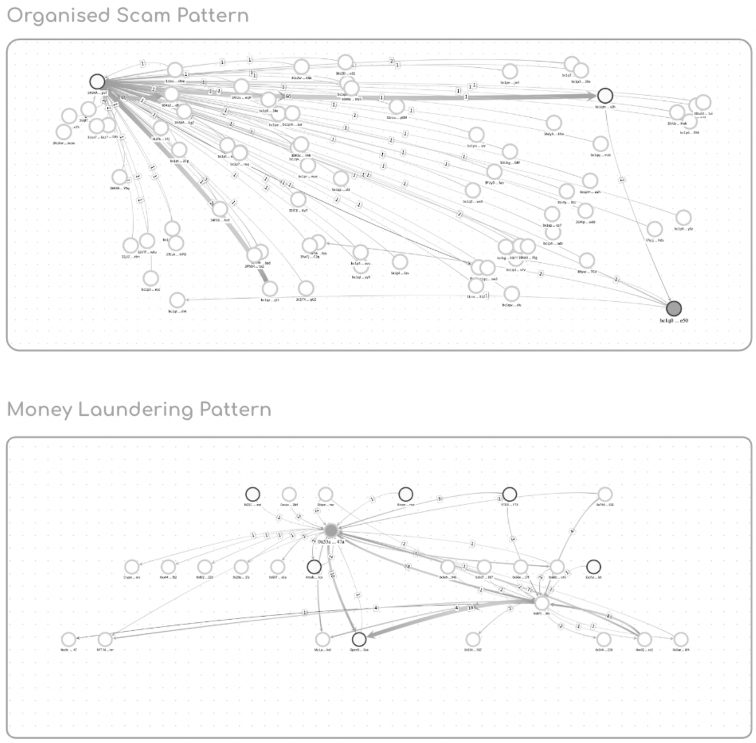


Fig. 2. Showing the Follow the Money The intelligence marketplace information flow, with intelligence generators feeding and accessing data from the market place

As a one-stop-shop for threat intelligence information, the marketplace allows users to report security issues such as malware, hacks, scams, and fraud. Each incident report submitted through the platform is analysed, traced, and verified by our community of security professionals. After each report is examined and determined to be authentic, the information is saved on the Intelligence Data Warehouse without jeopardizing the anonymity of its victims and reporters.

Pattern Recognition Engine (PRE)

Pattern Recognition generally utilises computer algorithms to identify data regularities and patterns in data. Bilic's PRE employs network analysis and machine learning algorithms to automatically detect patterns and irregularities in a user's on-chain activity. Such patterns and irregularities include wallets with fraudulent history, involved in fraud and money laundering, wallets linked to entities, wallets connected to the well-known OFAC sanctioned list etc.


Organised Scam Pattern

Money Laundering Pattern

Fig. 2. Showing 2 examples of pattern recognition from a wallet transaction network; Oraginased scam pattern above and Money laundering Pattern below.

The engine allows the user to automatically detect a series of patterns to speed up investigations and fact-finding. Such as;

- Money laundering transactions patterns: e.g., by tracking money back to another linked wallet or carousel type of patterns. As seen in Fig. 3;
- KYC Pattern: Patterns of regular interaction with KYC platform to allow investigators to easily de-anonymise wallets;
- Mixer Pattern: Network patterns with links to mixers and tumblers;
- Organised Scam Pattern: A networkpattern where funds are moved from one wallet to an operational wallet with a large number of smaller value transactions.

Intelligence Data Warehouse (IDW)

Bilic's IDW is our single source of truth housing large volumes of data from many sources in a centralised and consolidated data warehouse. Institutions can gain useful intelligence insights from this large data set using richness to enhance investigations, threat awareness, and decision-making. We've created a historical record over time of labeled wallets, transaction in- and outflow, off-chain media data, nft transaction history, wallets' association to any irregular patterns from the PRE that instituions and security analysts can use to their advantage. Bilic's IDW can be thought of as the "single source of truth" for blockchain security intelligence.

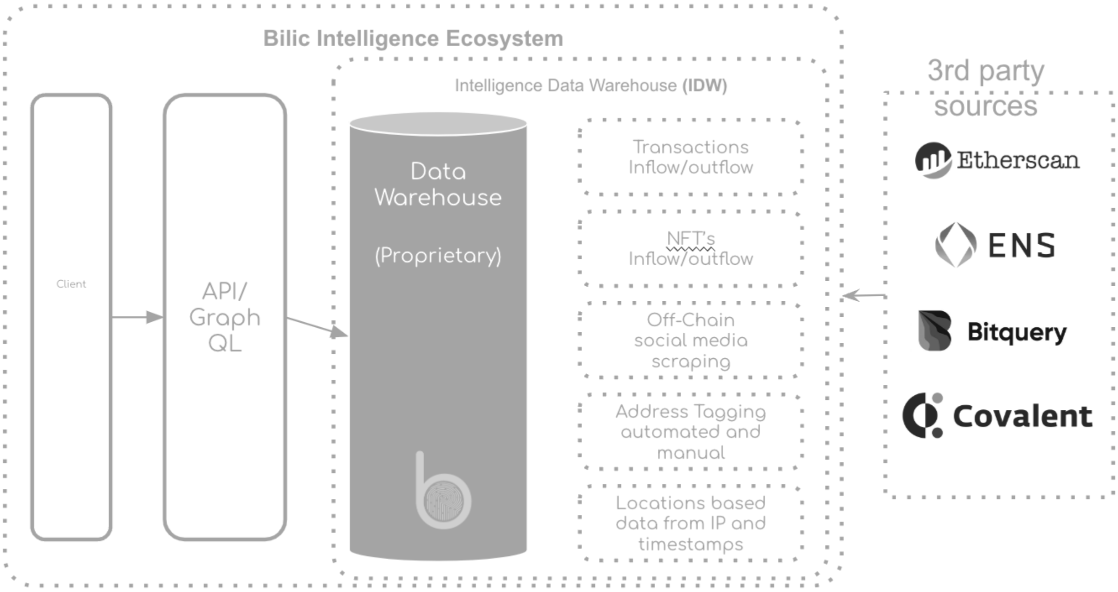
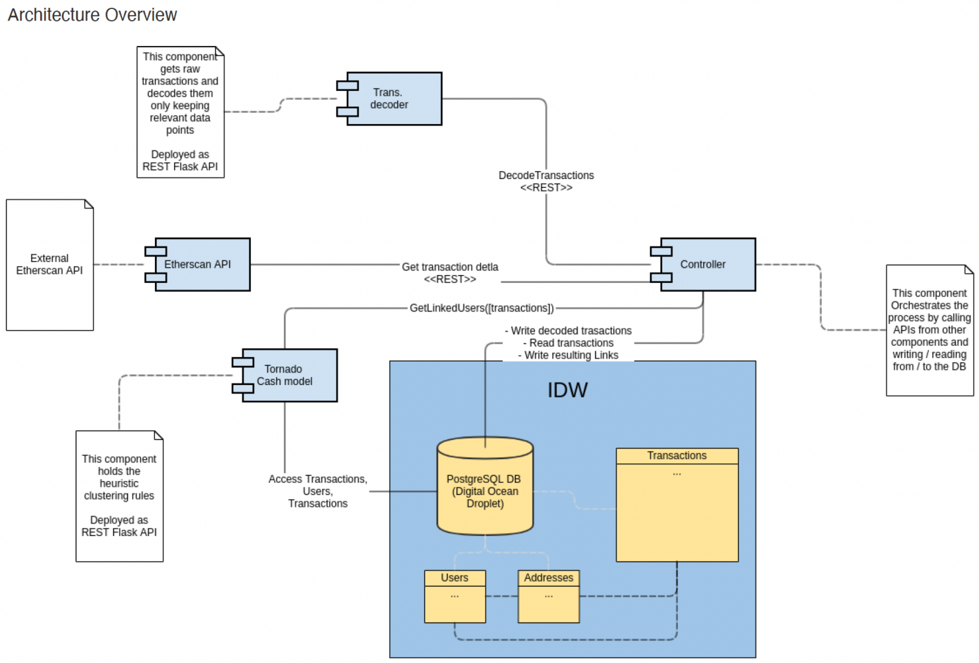

Bilic Intelligence Ecosystem
Client
API/ Graph QL
Intelligence Data Warehouse (IDW)
Data Warehouse
(Proprietary)
Transactions Inflow/outflow
NFT's Inflow/outflow
Off-Chain social media scraping
Address Tagging automated and manual
Locations based data from IP and timestamps
3rd party sources
Etherscan
ENS
Bitquery
Covalent

Fig. 4. Showing the Intelligence Data Warehouse Architecture, with data types, storage method, providers and micro processors clearly identified.

The IDW data is gathered from a variety of sources to create an data warehouse that no one else can match. The IDW is a critical component of the Bilic intelligence ecosystem since it allows for extensive high-level profiling, transaction segmentation, data scraping, and address tagging.

Address Linkability Model

The most popular non-custodial coin mixer on Ethereum, Tornado Cash, is frequently used to safeguard address anonymity. Due to the chance of privacy leakage as a result of various unsuitable transactional behaviors in the Tornado Cash mixing process. We built a model to take advantage of this data leakage to identify bad actors by specifically linking them to addresses in the output during the mixing attempts.


Architecture Overview
This component gets raw transactions and decodes them only keeping relevant data points

Deployed as REST Flask API
Trans. decoder
DecodeTransactions <<REST>>
External Etherscan API
Etherscan API
Get transaction detla <<REST>>
Controller
GetLinkedUsers([transactions])
This component Orchestrates the process by calling APIs from other components and writing / reading from / to the DB
- Write decoded trasactions
- Read transactions
- Write resulting Links
Tornado Cash model
IDW
This component holds the heuristic clustering rules

Deployed as REST Flask API
Access Transactions, Users, Transactions
PostgreSQL DB (Digital Ocean Droplet)
Transactions
...
Users
...
Addresses
...

Fig. 5. Showing the Intelligence Data Warehouse Architecture, with data types, storage method, providers and micro processors clearly identified.

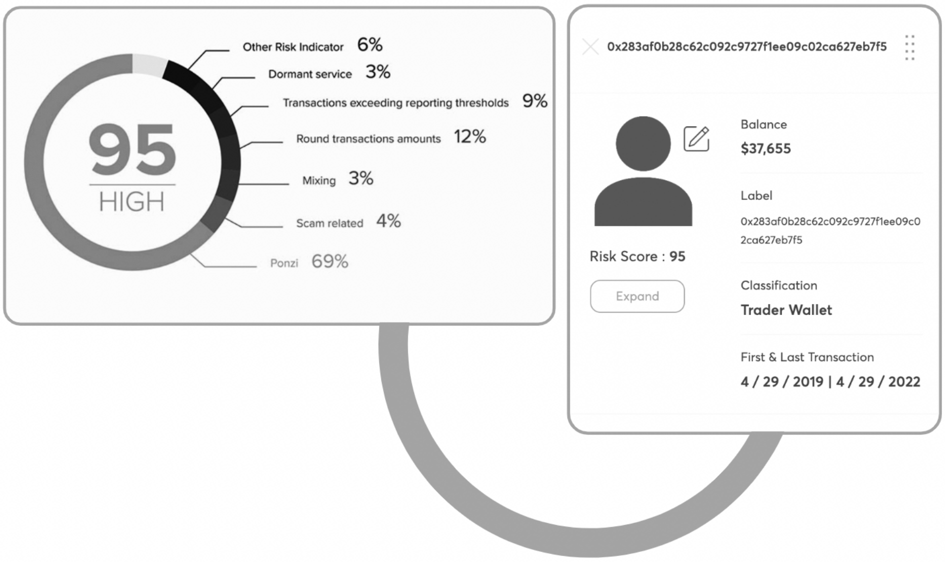
The Architecture above describes shows how the address linakbility model fits into the global bilic data architecture for wallet tracking and user de-anonymisation.

Tornado Cash is a protocol ensuring that users can break a link in on-chain activity for the purpose of improving transaction privacy between the recipient and destination address. Acting as a complex token mixer, Tornado Cash utilises smart contracts that accept deposits made in ETH that are then withdrawn to other addresses. This hides the flow of funds and makes it harder to track the funds, turning the protocol into a good option to be explored for AML purposes.

Bilic Verify

Bilic Verify is our novel AML tool for wallet risk factor check. Intelligence consumers and retail market such as financial institutions, companies, custodians, exchanges, security agencies, trading desks, and fintech users can utilise Bilic verify as a digital shield. This solution protects consumers from transmitting their digital assets to a fraudulent wallet address in an irreversible manner.

Users can simply query an endpoint or search for the bilic verify rating for a specific wallet and they get a detailed wallet breakdown and risk rating as seen in Fig. 6.



0x283af0b28c62c092c9727f1ee09c02ca627eb7f5

Risk Score : 95

Balance
$37,655

Label
0x283af0b28c62c092c9727f1ee09c02ca627eb7f5

Classification
Trader Wallet

First & Last Transaction
4 / 29 / 2019 | 4 / 29 / 2022

Fig. 6. Showing the Bilic Verify result and risk factor for a user wallet

Intel-as-a-Service (IAAS)

Bilic as anIAAS provider, gives it's clients access to a suite of intelligence software, including APIs, databases, and machine learning algorithms, that will act as a large ecosystem to protect them from fraud and hacking. This will include features such as an automated wallet analytics engine to investigate asset movement, a database of blacklisted wallets suspected or involved in illegal activities, APIs, and more.

Conclusion

This paper has argued against the *myth* that cryptocurrency is untraceable and safe heaven for criminals. We have highlighted the impacts of blockchain crimes on businesses, how to find criminals attempting to eliminate their digital footprints on the blockchain, and discussed and presented tools to track and trace these footprints along with a framework to follow when investigating blockchain-related crimes. The cryptocurrency space and its associated technologies, especially its security design, are still emerging, making it highly vulnerable to attacks. However, the days when hackers and money launderers funnel stolen money back into the economy easily are gone. There are emerging sophisticated technologies and methods for tracking and apprehending suspicious transactions on the blockchain. The increasing capability of expert blockchain investigators and crypto forensic analysts is challenged by the availability and use of transaction mixers, round-tripping, and complex layering, among other strategies used by criminals to hide their footprints on the blockchain.