MERKLE SCIENCE

HOW MERKLE SCIENCE DETECTS OTHERWISE CONCEALED CRYPTO CRIME

WHITE PAPER

Table of Contents

How Merkle Science Detects Otherwise Concealed Crypto Crime

Introduction

In the past few years, cryptocurrencies have experienced meteoric growth, shattering predictions of market pundits. Despite (or because of) the Covid-19 pandemic, the adoption of cryptocurrencies continues to grow.

However, amid increased mainstream adoption and the introduction of stringent regulations in many jurisdictions across the globe, cryptocurrency remains one of the preferred choices of currency for criminals, primarily due to its pseudonymous nature and ease of instantly sending funds across the world. But, the sophistication level of crypto crime has changed over the years and criminals are now devising novel ways to bypass regulatory checks and detection by blockchain analytics providers to continue their illicit activities.

This white paper focuses on challenges in crypto crime detection faced by traditional blockchain analytics providers and how Merkle Science has created next-generation crypto threat detection and is flagging otherwise concealed criminal activities.

Challenges in Crypto Crime Detection

Existing cryptocurrency transaction monitoring tools focus on detecting criminal activity based on a database of cryptocurrency addresses that are associated with, or identified as being directly controlled by, criminal entities. Although these methods are sufficient for tracking the movement of funds from sanctioned addresses and known criminal bodies, they fail to assess the risk associated with transactions involving the more privacy-focused cryptocurrencies such as ZCash[1], Dash[2], or Monero, or anonymity features such as the Lightning Network[3] and zk SNARKs[4].

Furthermore, the problem with leveraging a database or sanctioned list-based system is that such systems are not designed to deal with crypto criminals' ever-evolving methods and instead are designed to detect criminals' activities performed in a traditional way, such as using one address repeatedly for committing crimes. For example, in most ransomware attacks, criminals usually create a new address after they lock the systems of the victim organization and demand a ransom deposit to the newly created address. Conventional blockchain analytics fail to detect crime when it is conducted by a new address not part of any database or sanction list. Also, sanction lists such as OFAC are updated only months after a crime has been committed, therefore, relying solely on such lists gives criminals free rein to execute crime during this period.

As criminals are using sophisticated techniques to bypass detection by traditional blockchain analytics, it is imperative to deploy a solution that goes beyond the blacklists, proactively monitors transaction behavior in real-time and detects potential criminal wallets not listed on public or private databases or blacklists.

We will now take a look at how Merkle Science detects sophisticated crime and allows your firm to comply with local and international regulations.

The Science Behind Merkle Science

Merkle Science's transaction screening and wallet monitoring solution is designed to assist crypto businesses and financial institutions in complying with regulatory requirements such as FATF's red flag indicators for virtual assets, FinCEN's guidance on money laundering and terrorist financing, Singapore's MAS PSN02 requirements, and other country-specific AML/CFT laws. Merkle Science focuses on addressing the dual-problem faced by existing cryptocurrency businesses and financial institutions:

- Accurately detecting and preventing crime acrosscryptocurrencies on public blockchains.
- Identifying suspicious transactions conducted using privacy-focused cryptocurrencies or features.

Merkle Science allows you to customize the parameters of our behavior-based rule engine to identify suspicious transactions beyond the blacklists and respond immediately and works on a two-pronged approach:

- A behavior-driven rule engine for classifying the risk level of potential transactions based on transactional history.
- Building a broad cryptocurrency coverage for data ingestion and analytics.

The rules that our transaction monitoring platform supports are broadly classified as:

- Address Rules
- Transaction Rules
- Behavior Rules (also known as the Behavior-based Rule Engines)

Address rules are used to validate whether an address is malicious or if it is trustworthy.

Transactional rules involve all parties in a transaction and analyze not only the incoming funds but also the outgoing funds to determine criminal behavior,

In addition to address-level and transaction-level monitoring that is common among all blockchain analytics providers, Merkle Science allows your firm to detect criminals that are leveraging sophisticated techniques to hide their illicit activities. The above two rules can be categorized as Source of Fund Rules, while the **behavior rule** works based on historical data. This enables customers to set rules based on the transactional history associated with an address and detect crimes that involve sophisticated techniques to conceal their activities. The following are a few examples of how Merkle Science helps your firm detect sophisticated criminal behavior.

Detecting Concealed Crypto Crime with Merkle Science's Platform

As stated above, Merkle Science goes beyond blacklists, address-level, and transaction-level crime detection to allow you to customize crime detection parameters to detect sophisticated criminal behaviors that are designed to bypass detection by conventional blockchain analytics providers. Let's take a look at a few examples of how criminals conceal their activities and how Merkle Science can aide your firm in detecting such sophisticated behavior.

Ransomware Attacks

After the Colonial Pipeline ransomware attack in May 2021, the DarkSide hacker group shared a newly created Bitcoin address (bc1q7eqww9dmm9p48hx5yz5gcvmncu65w43wfytpsf) with the Colonial Pipeline for ransom. Within two days of the attack, the DarkSide address received over USD 4.4 million in ransom from the Colonial Pipeline on 9 May 2021.

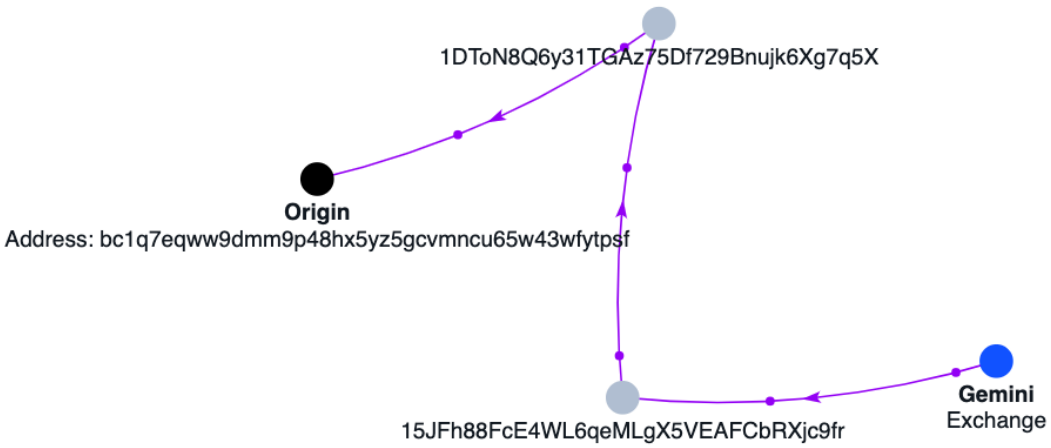

Figure 1: *Fund Movement Of Colonial Pipeline Ransom*

The first incoming transaction to this address was USD 1 and then the next transaction was over $4,433,726.

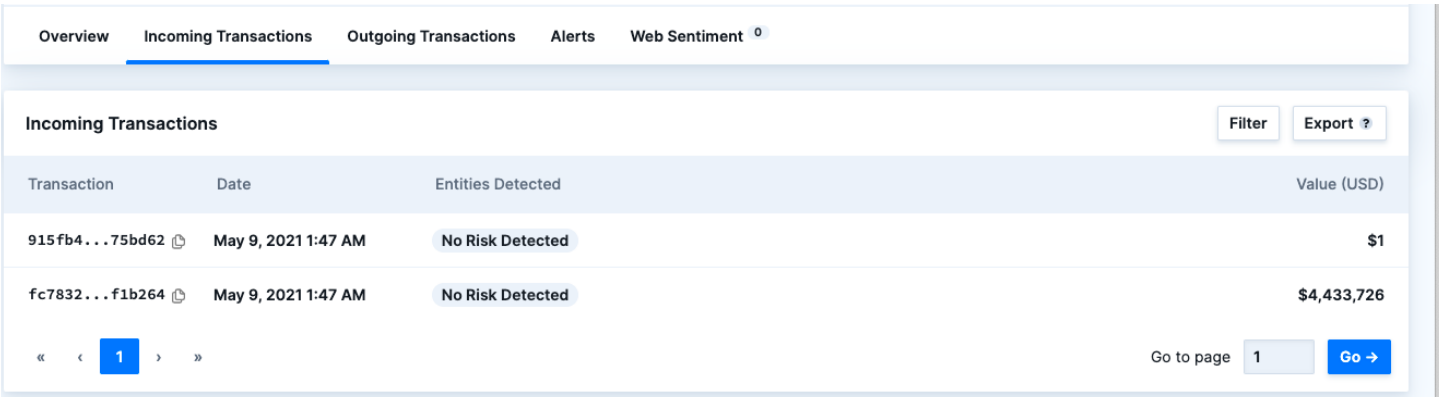

***Figure 2**: All Incoming Transaction To DarkSide Bitcoin Address*

Upon receiving the funds, the criminal then transferred the entire fund (as shown in figure 1) to two different addresses in a row and then to the Gemini exchange.

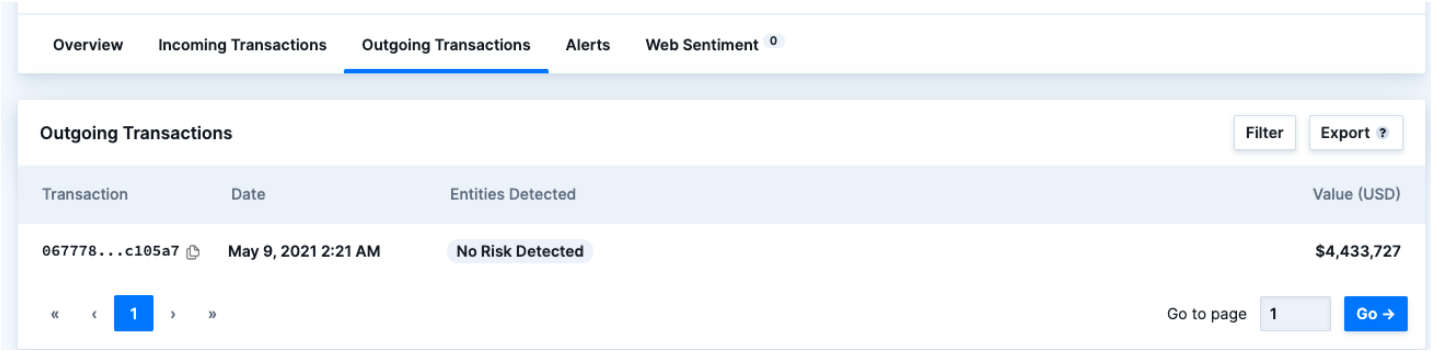

***Figure 3**: Outgoing Fund Analysis From DarkSide Bitcoin Address*

Though the FBI later recovered most of the funds from the hack within a month, in an ideal scenario, Gemini, the recipient exchange of the funds, should have been able to freeze the funds as soon they received it without interference from the FBI. However, it appears that Gemini's blockchain analytics provider missed flagging this transaction given that it wasn't associated with a blacklist/database as it is common with traditional blockchain analytics providers that rely on sanction lists and databases.

Darkside ransomware funds had all the signs of being related to crime. For example, as in most ransomware cases, the criminals created a new address to demand ransom, and then a large amount of crypto was transferred within hours of its creation. Merkle Science's behavior-based rule engine leverages deep learning-based behavior analysis models to detect addresses associated with criminals that leverage sophisticated techniques, such as using 'young addresses,' to bypass detection by traditional blockchain analytics platforms. Merkle Science allows you to set up custom parameters to flag 'young addresses' that start to send or receive large funds within a few days or hours of their creation and are not listed in any sanction list for criminal activity nor associated with any known criminal entity.

Anomaly Detection

This is a case of 'peeling chain' money laundering. A "peel chain" occurs when a large amount of BTC sitting at one address is sent through a series of transactions in which a slightly smaller amount of BTC is transferred to a new address each time.

Our researchers detected this instance when one of the largest cryptocurrency exchanges globally reached out to us last year. The exchange suspected money laundering from a Bitcoin address and when Merkle Science analyzed the address, we came across a sophisticated pattern of money laundering. Let's look at it in detail.

The Bitcoin address (3BMEXgeDvMoXeB2Gx1Kz9jfNP66MxCFpjt) become active on 1 March 2020, at 3:56 PM by receiving $865.59 in Bitcoin, and was active until 28 June 2020, 10:54 PM. During this period, the address received a total of 1.861 BTC.

An anomaly is usually suspected when an address suddenly becomes more active than usual. This rule checks if an address has been transacting significantly more than the average transaction amount during a window of time. But this is not a case of a transaction-

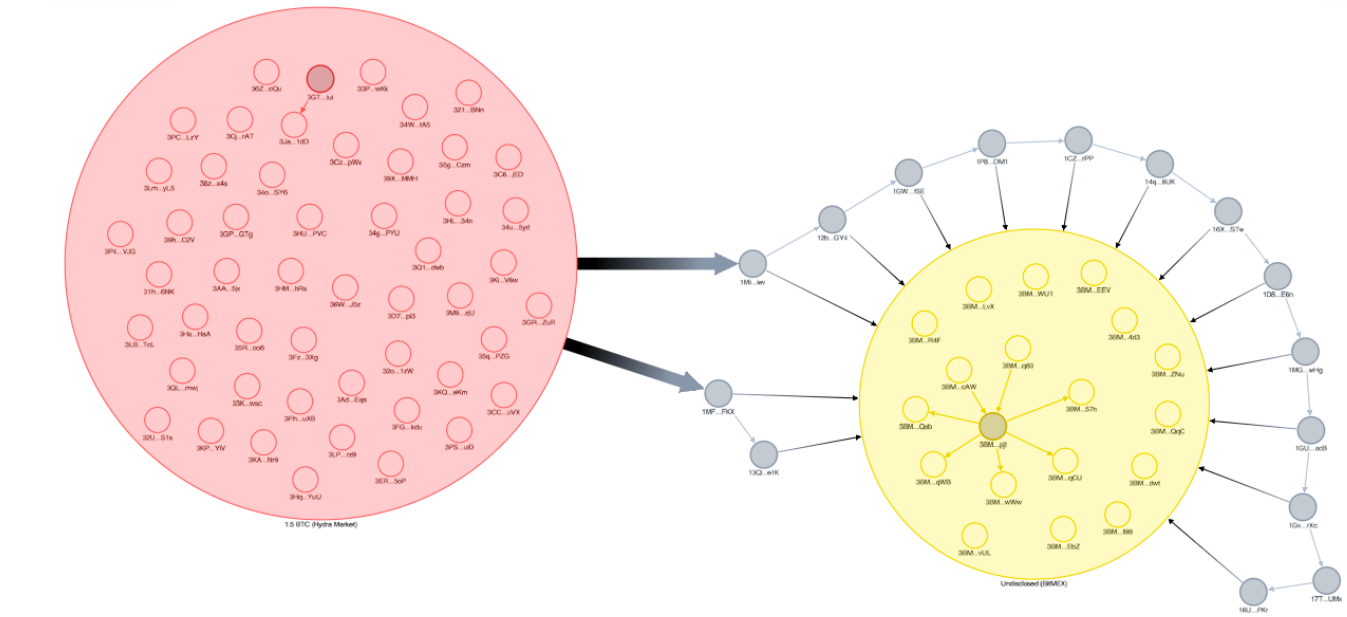

Figure 4: *Transfer Of Funds In A Peeling Chain Pattern*

based anomaly. For example, looking at the transfers as shown in figure 4, a compliance officer or a conventional transaction monitoring solution would not know if there was something suspicious going on.

Overview | Incoming Transactions | Outgoing Transactions | Alerts | Web Sentiment 0

Outgoing Transactions — Filter | Export ?

Transaction	Date	Entities Detected	Value (USD)
3b732a...e683ba	Jun 29, 2020 10:54 PM	Exchange	$1,005.24
4cb29d...650ef2	Jun 28, 2020 9:24 PM	Exchange	$6,237.66
e71960...c238ee	Jun 27, 2020 9:36 PM	Exchange	$2,493.69
78275b...57d5b5	May 20, 2020 9:39 PM	Exchange	$1,173.81
e05f20...3c4f55	May 20, 2020 1:56 AM	Exchange	$1,958.17
46dba7...ecc79e	May 6, 2020 9:09 PM	Exchange	$933.07
8467f4...e2d622	May 3, 2020 9:14 PM	Exchange	$2,085.58
b45cea...00b60f	Mar 4, 2020 1:22 AM	Exchange	$1,339.18

« ‹ 1 › » Go to page 1 Go →

Figure 5: *Outgoing Fund Analysis Of A Peeling Chain Anomaly*

But when our data scientists looked at the pattern of transfers, the wallet had a total of 1.861 BTC which was then transferred to addresses indirectly associated with darknet marketplace Hydra Market in a chain peeling pattern (as shown in figure 4) to evade detection by blockchain analytics firms and government agencies. This is another case in which a particular type of behavior is at play trying to commit a crime and any solution that does not analyze transaction behavior would not be able to detect it.

Dormant Addresses

The following outlines an example of a dormant Litecoin address that was involved in criminal activities as suspected by one of our client exchanges. This Litecoin address (LXMiwvHKvWZy7TBbN5mxRokqnLU4WbY4Uf) was inactive since 8 November 2019, for all outgoing transactions but was receiving smaller chunks of funds on a regular basis, making it a point of suspicion. It suddenly became active on 6 May 2021 and transferred $303.08 to another address and, subsequently transferred $355.55

on May 8 at 2:24 AM. Three minutes after transferring $355.55 of Litecoin on May 8, the address transferred another $71,113.08 worth of Litecoins at 2:27 AM.

Figure 6: *Fund Movement Of A Dormant Address*

Upon investigating the fund movement, we found that the address was associated with three different mining pools

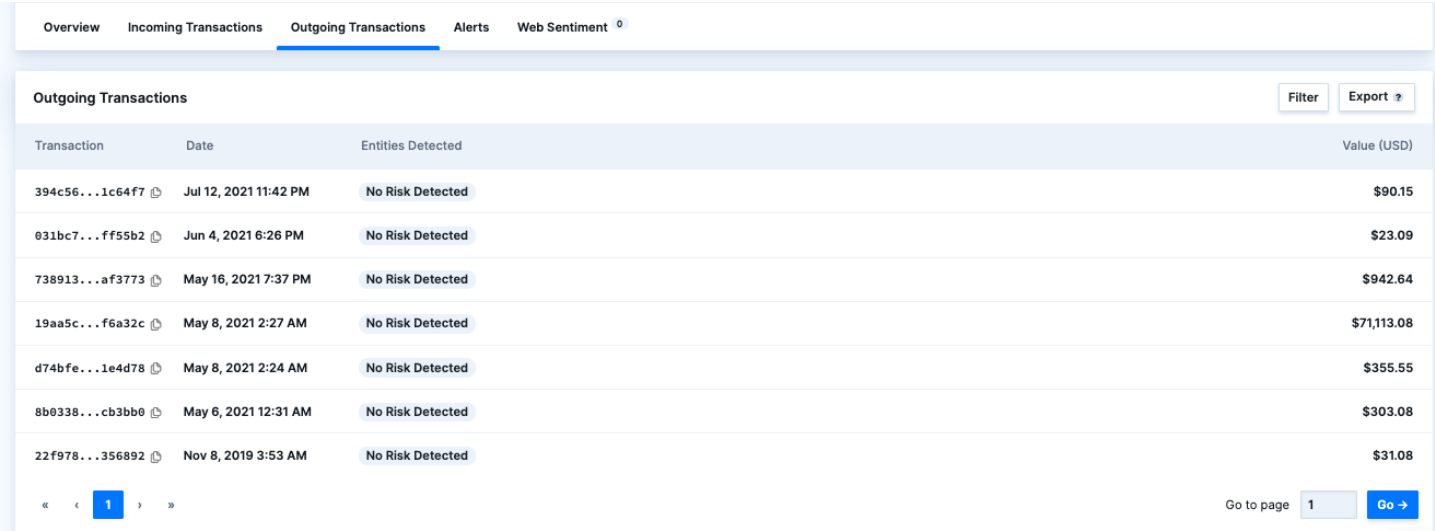

Figure 7: *Outgoing Fund Analysis Of A Dormant Address*

The exchange, upon finding out that the address was associated with miners, later opened a case and decided to report it to authorities. Behavior analysis is crucial in these instances as conventional solutions cannot detect such sophisticated patterns because this address was not associated with a sanction list or a known criminal entity.

Transit Address

Transit addresses are a type of address that have received funds within a specified time - usually a few hours - and have withdrawn at least 50% of the deposited funds. Detecting and flagging such addresses requires custom rules.

For example, from 30 November 2019 to 4 December 2019, a Bitcoin address (1PXfgCjaBYvbQphAKuDNQoGrUSUbJ1NgRk) received 1.42 BTC and withdrew all the funds subsequently by 4th December. Criminals involved in extortion follow the same pattern as ransomware criminals and use one address once or for one campaign - as they did in this case - and then discard that address.

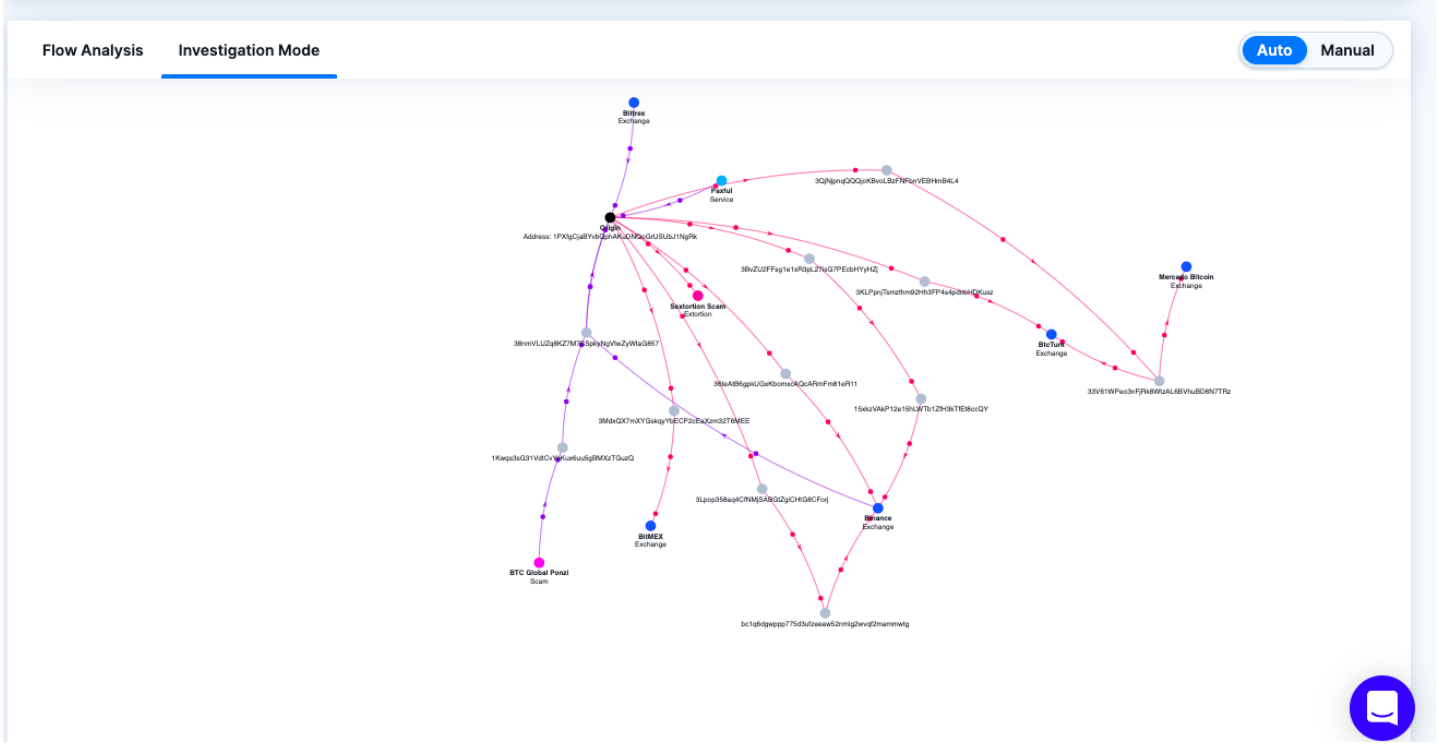

Figure 8: *Fund Movement Analysis Of A Transit Address*

The address that is associated with the extortion scam — illustrated above in Figure 8 — started to receive funds on 30 November 2019, at 6:01 PM with a starting fund of $60.8 and within four days, received a total of $10,429.7 (1.42 Bitcoins).

Overview | Incoming Transactions | Outgoing Transactions | Alerts | Web Sentiment 163

Incoming Transactions — Filter | Export

Transaction	Date	Entities Detected	Value (USD)
e8a3f5...ee9f14	Dec 4, 2019 7:17 AM	No Risk Detected	$2,582.16
f0e530...1dc90b	Dec 4, 2019 4:34 AM	Service	$714.45
8a9ed1...ae4f40	Dec 4, 2019 1:00 AM	No Risk Detected	$590.21
44d9ad...171c92	Dec 4, 2019 12:30 AM	Service	$1,032.86
1d478f...6225d3	Dec 3, 2019 8:22 PM	No Risk Detected	$708.25
1cc327...b4a0a2	Dec 3, 2019 2:06 PM	Service	$256.81
a6a63a...08be98	Dec 3, 2019 1:37 PM	Service	$708.25
2a51d0...9c59bc	Dec 3, 2019 1:37 PM	Service	$333.39
0bef2b...8a6b92	Dec 3, 2019 9:41 AM	No Risk Detected	$627.46
493bd3...85b319	Dec 3, 2019 9:00 AM	No Risk Detected	$25.76

« ‹ 1 2 › » Go to page 1 Go →

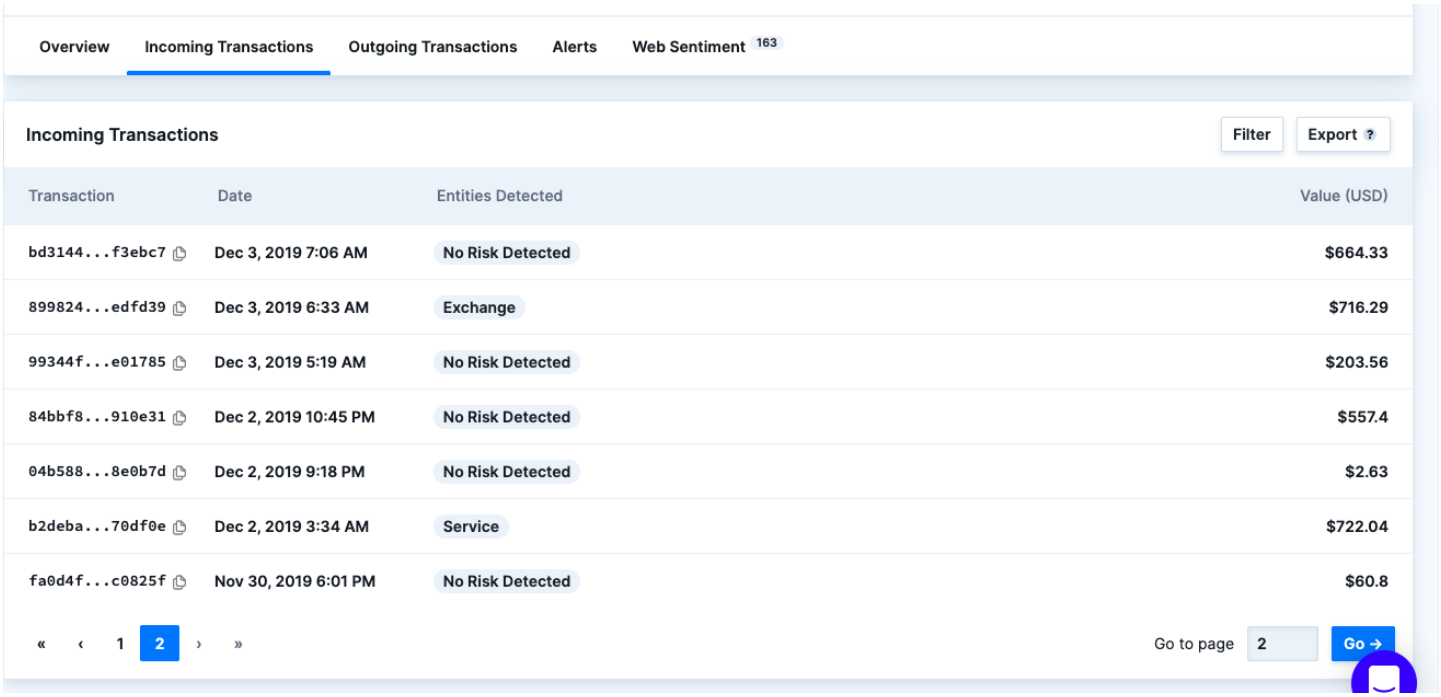

Figure 9: *Incoming Fund Analysis Of A Transit Address*

The criminals then used Binance, BitMex, Mercado Bitcoin, and BtcTurk to transfer funds, and yet none of these exchanges detected this instant fund transfer. Our investigation shows that the address was active for just four days and has since been inactive.

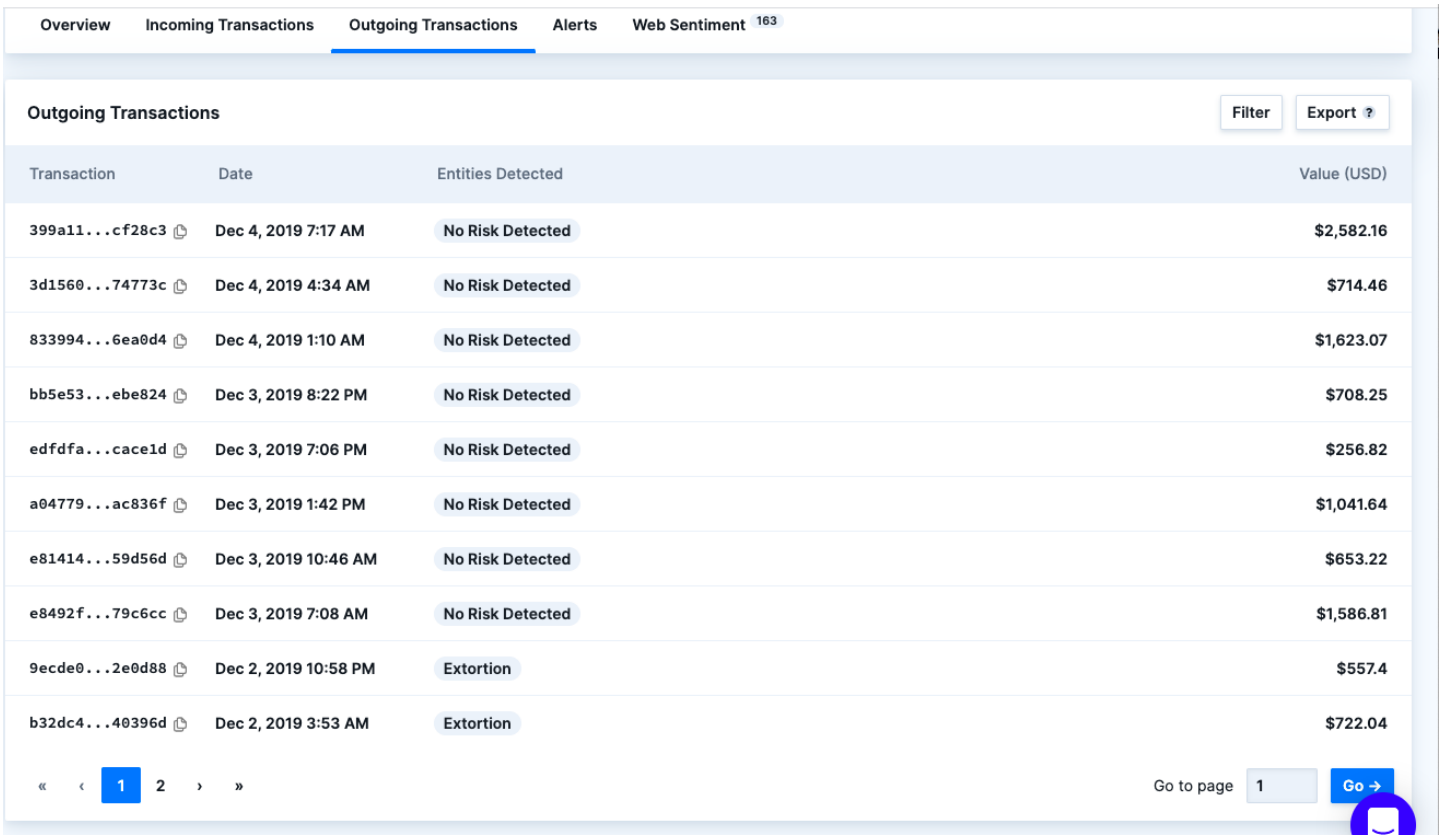

Figure 10: *Outgoing Fund Analysis Of A Transit Address*

This is another case where a particular type of behavior is involved and any system that relies on a database will fail to detect such crimes because criminals do not follow one pattern and constantly evolve their approach to evade detection.

Conclusion

As criminals continue to devise highly sophisticated techniques to launder funds and/or perform illicit trades via cryptocurrencies, it is imperative that the systems used by financial services institutions, cryptocurrency exchanges, and government agencies are a step ahead of them. Relying on a section list that is updated after months of a crime is committed allows criminals free run to execute crime during the gap period. And, as criminals move from sanctioned addresses and opt for more sophisticated techniques, tools from organizations such as Merkle Science that leverage deep behavior analysis are crucial to fighting ever-evolving crypto crimes.

References:

1. https://z.cash/technology/
2. https://docs.dash.org/en/stable/
3. http://lightning.network/how-it-works/
4. https://z.cash/technology/zksnarks/

About Merkle Science

Merkle Science is the next-generation predictive cryptocurrency risk and intelligence platform that helps crypto companies, financial institutions, and government entities detect, investigate, and prevent illegal activities involving cryptocurrencies. Merkle Science's proprietary Behavior Rule Engine enables our tools to go beyond blacklists so that compliance teams may fulfill their local KYC/AML obligations and industry players may stay keep pace with the industry's increasingly complex illicit activities. Merkle Science envisions a world powered by crypto and is creating the infrastructure necessary to ensure the safe and healthy growth of the cryptocurrency industry as it becomes a key pillar of the $22 trillion financial services ecosystem. We enable businesses to scale and mature so that a full range of individuals, entities, and services may transact with crypto safely. For more information on Merkle Science, please visit merklescience.com.

Contact Us

Contact@merklescience.com

Follow Us merklescience @MerkleScience merklescience Merkle Science