T&H CONSULTING

B2B SERVICES

CRYPTOCURRENCY FORENSICS

We are T&H Consulting, a Consulting Firm where we provide solutions for individuals and businesses. We are operating from Vármegye u. 3-5, 1052 in Budapest, Hungary and the following is our data:

T&H Consulting International KFT

Registration number 01 09 350838
Hungary

T&H Holdings Limited

Company number 12747126
in the Companies House
United Kingdom

INTRODUCTION

https://tandhconsult.com/

Cryptocurrency, a digital payment system that functions electronically and operates outside of the traditional financial system, is quickly becoming a major issue for law enforcement agencies and financial institutions. Bitcoin is the original and most dominant cryptocurrency, followed by several others that have gained fame and new investors over the previous years. Since 2010, the price of Bitcoin has experienced dramatic upward and downward swings. Between 2016 and 2017 the cryptocurrency market rose to a staggering market cap of nearly $1 trillion USD. Prior to this dramatic increase, cryptocurrencies were largely ignored by the private sector but now many are paving the way to integrate them as a payment system.

This new technology poses several challenges, as many people are willing to hop on the trend of investing in cryptocurrencies despite not knowing the nature of these virtual assets or the inherent risks. For the same reason, many are falling victim to scams related to cryptocurrencies, regardless of whether their aim was to purchase these assets or to use them as a payment method. Furthermore, whether they know it or not, law enforcement agencies and financial institutions are impacted by cryptocurrencies in their communities every day as cryptocurrency-related scams are becoming more and more commonplace.

As this and other related innovations continue to gain a foothold in the economy, criminal exploitation of these systems and methods increase. With cryptocurrency now firmly entrenched in both domestic and international commerce, it is vital that law enforcement, financial institutions and financial crime investigators have a firm understanding of what cryptocurrency is, how it works, and how it can be used in both legitimate and illicit activities.

Difficulties law enforcement agencies may encounter

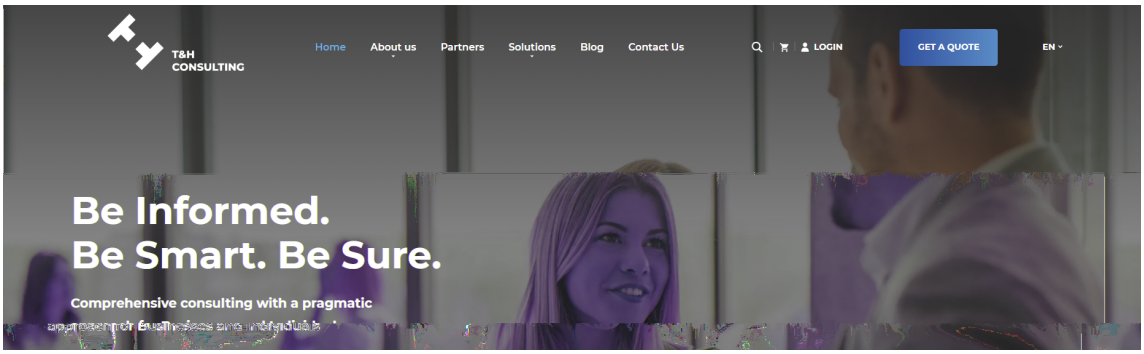
There are many misconceptions about what cryptocurrencies are and how much information is available, viewable, and accessible. Criminals, operating both as individuals and organisations, have come to rely on virtual currencies due to their alleged privacy and confidentiality implications. Law enforcement agencies around the globe are turning to private sector experts in an effort to combat the ever-evolving nature of blockchain technology. These agencies have come to understand the immense effort required to prepare and train their agents in these newfound ideas, and as such, would rather turn to those already proficient in such matters as a time and resource saving measure.

Law enforcement and financial institutions play a key role as the first line of defense in helping identify illicit activity associated with cryptocurrency including but not limited to, money laundering, narcotics, human trafficking, weapons trafficking and terrorist financing. There is an ever-increasing need for the development of appropriate responses to these activities. As technology evolves and the criminal element adopts these new technologies, it is critical that a standardized system of management, training, and guidance be developed, refined, and implemented.

By drawing on the expertise of private sector firms such as Chainalysis, law enforcement agencies in the United States have been able to crack terrorism campaigns and retrieve funds from the digital Silk Road. Chainalysis specialises in providing compliance and investigation software to banks, businesses, and governments around the world, mainly in order to track virtual currencies. The company maintains contracts with most federal agencies in the United States, and we also make use of their services. Our diverse and skilled team of professionals is well equipped and ready to take on whatever challenges are presented to them when it comes to blockchain technology. They work to deliver cryptocurrency intelligence and forensics reports. One of our main roles is in the analysis of the blockchain ledger, where all public transactions can be seen. We use proprietary data to correspond real world entities with their presence on the blockchain to determine who is involved. This process can potentially lead law enforcement to the individuals and crime-tainted assets involved in a particular case.

We cooperate with various law enforcement agencies around the globe in our efforts to assist our clients. Our success stories prove the relevance and necessity of private sector firms in combating financial cybercrimes, and our role as a catalyst for law enforcement agencies. Our mature, refined approach enables us to provide solutions to many industries and sectors involved in cryptocurrency.

On our website you can find more information about our different services https://tandhconsult.com/



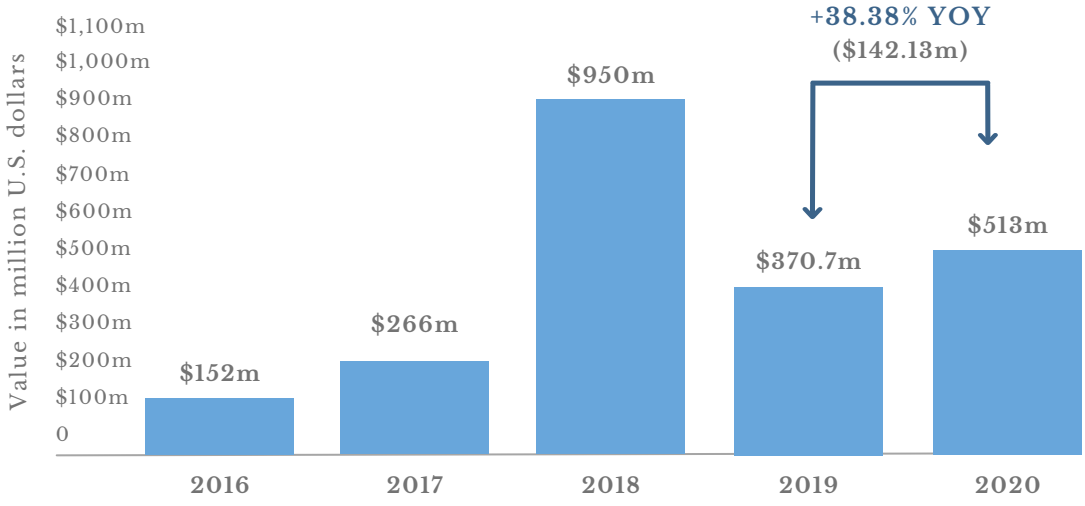
Where do we come in?

We understand the challenges that law firms and various agencies face when dealing with cases involving stolen cryptocurrencies. This is mostly due to the lack of regulation in this sector as well as the relatively unrefined and underdeveloped research units present within law enforcement agencies. Fortunately, at T&H Consulting we have plenty of experience dealing with such cases and we know the procedure to follow. At the same time, we provide our solutions to businesses. When you decide to come on board with us, you can rest assured in the knowledge that the best approaches, experts and researchers currently available are at your disposal.

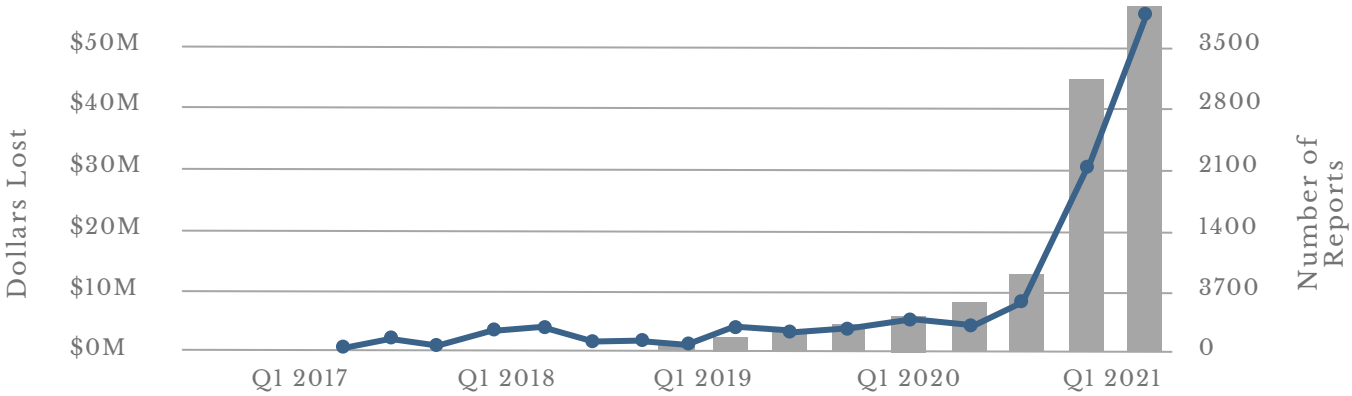
Crypto scams in numbers

According to the Federal Trade Commission in the USA, since October 2020, nearly 7,000 consumers have reported losses due to cryptocurrency scams totalling more than $80 million with a reported median loss of $1,900. Compared to the same period a year earlier, that's about 12 times the number of reports and nearly 1,000% more in reported losses. Cryptocurrency hacks and thefts increased almost 40% in 2020 According to research by Trading Platforms UK.

Value of Cryptocurrency Hacks and Thefts Worldwide
From 2016 to 2020, in million U.S. dollars
Sources: Ciphertrace.com, Statista



There was a huge spike in investment-related scams in 2020 and it is mostly related to the pandemic, as many were staying at home while struggling to make ends meet. These people began seeking out methods with which they can make more money, at which point scammers began capitalising on their lack of knowledge and unfamiliarity. Many specialists argue that such a spike is not real, but as we were experiencing a turmoil in the market it was made more visible. The influx of many new traders and investors in the market made easy victims for scammers seeking to take advantage of their greed and inexperience.



These figures are based on reports to the FTC's Consumer Sentinel Network that were categorized as investments related fraud and indicated cryptocurrency as the payment method
Source https://www.fool.com/research/crypto-investment-scams/

Mapping process

Tracing cryptocurrencies is a process in which many actors are involved: the client, the scammer(s), the cryptocurrency exchanges, and the authorities. For this process, we need the dates of the transactions, the receiver wallet addresses, TX hashes and amounts in crypto.

The blockchain is a public ledger in which everybody can access the information of the transactions, however, the identity of the ones executing the orders is not something visible there. Only specialized software can make it possible to access additional pieces of information.

We use two programs for tracing: Qlue and Chainalysis. Qlue is a software that is in constant development and is always trying to provide innovative solutions in this field. In the case of Chainalysis, this is one of the major providers of software for the tracing of cryptocurrencies and the most prestigious. With them, we can see a representation of the blockchain on a visual graph, upon which it is possible to manually expand and trace. The aim of this process is to follow the money until we find a hosted wallet, in other words, we look for wallet addresses that belong to a known cryptocurrency exchange platform. Even if the funds keep moving, which happens very often, it is important to request information on the hosted wallets.

CHAINALYSIS QLUE™

Cryptocurrency exchanges are a key entity in getting information about the owners of the wallets involved in illicit activities. Even if these platforms are handling non-fiat currencies that lack regulation, they can only be initially acquired with fiat currencies. In other words, the initial purchase of cryptocurrencies necessitates that a payment first be made with a card or bank transfer. In the end, those funds are subject to revision and auditing by the government.

Therefore, crypto exchanges must comply with anti-money laundering policies and with the laws of the countries where they operate.

Things that our company cannot do for you

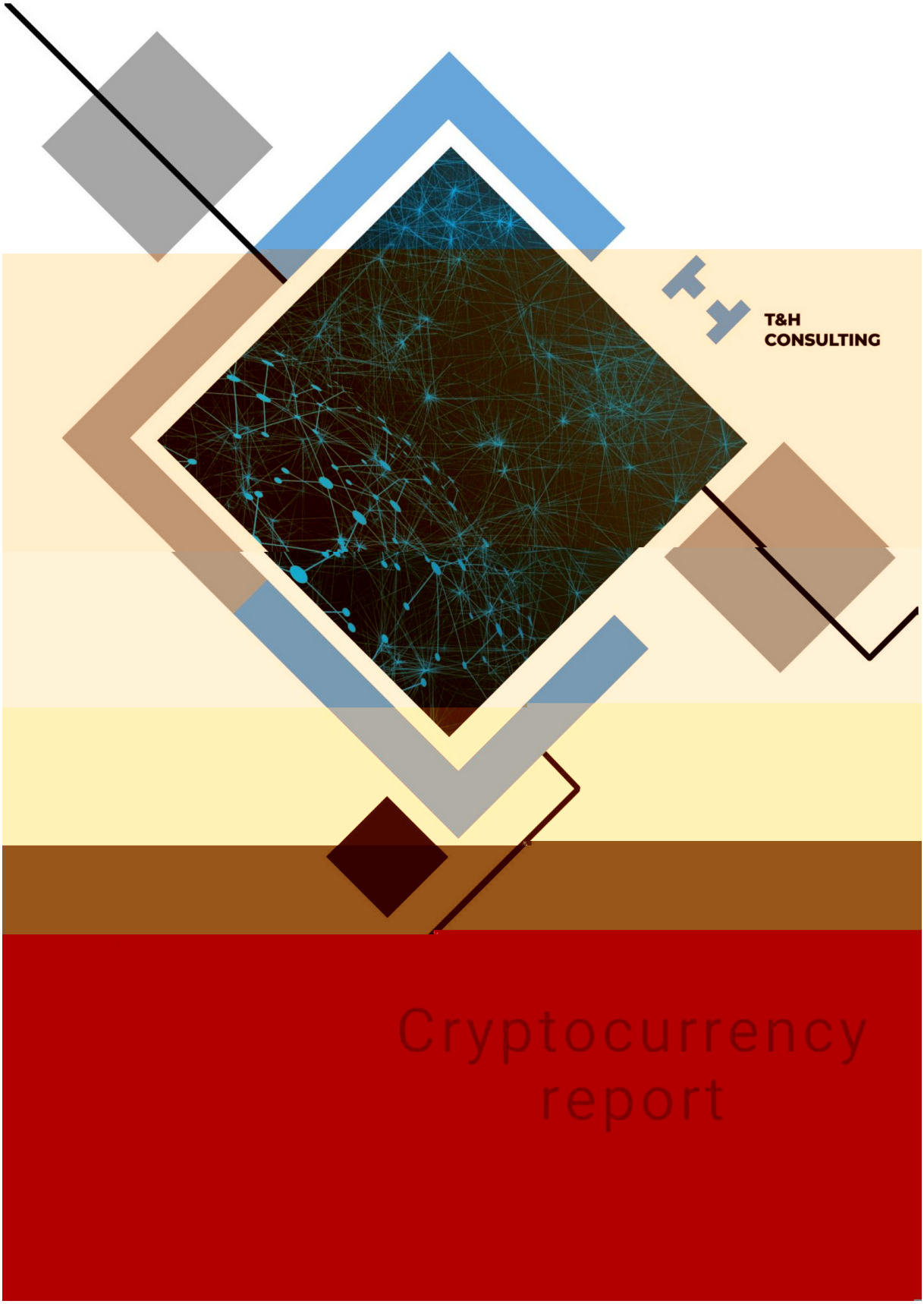
- X **Freeze wallets**
- X **Get the names of the wallets owners**
- X **Compel crypto exchanges to comply with requests**
- X **Reverse cryptocurrency transactions**

Our company's main efforts lie in the tracing process, that is our job. Law enforcement agencies use the information provided by us when contacting the relevant cryptocurrency exchanges. Depending on the jurisdiction and how cooperative the police are, they might request different things from the cryptocurrency exchanges, from the disclosure of information of the owners of the wallet addresses involved in illicit activities to the freezing of those wallets. Again, those actions must be requested by law enforcement agencies or by court rulings, as they are the only ones entitled to request those things.

Why are the Cryptocurrency Intelligence Reports we prepare important for the recovery of stolen crypto assets?

Because law enforcement agencies are overwhelmed with their workload and usually, many are uncertain of which steps to follow in cases involving cryptocurrencies. As this technology is still new and we, as a society, are not yet properly educated or knowledgeable in their intricacies, it is a matter of course that neither the victims nor the authorities know how they should proceed. In addition, the tracing process is time-consuming and requires expertise in both the nature of cryptocurrencies and the software used to track them. Time is crucial since scammers are developing new, increasingly complex ways to hide and merge stolen funds in an effort to make them impossible to find. As a result, some investigations might take up to a year or even more.

The following are samples of our Cryptocurrency Intelligence Report and our Forensics Report. The length of these reports depends on the case as well as on the information we can obtain. The information and the graphs displayed may vary depending on the software we use.


T&H
CONSULTING
Cryptocurrency
report

Profile

Name: Client's Name

Report issued: March 30, 2021

Reason: Fraud / Cybercrime

Asset: BTC

Contents

1. Glossary

Address

A digital destination used to send and receive cryptocurrency funds. It is similar to a physical house address or an email address, however, cryptocurrency wallets often contain many addresses. A Bitcoin address is a hash of the public key and consists of 26-35 alphanumeric characters.

Asset

The type of cryptocurrency used in a transfer (Bitcoin, Ethereum, etc.). Can also refer to non-fungible representations of value (e.g. cryptokitties).

Cluster

A collection of cryptocurrency addresses that T&H Consulting has identified to be controlled by one entity.

Counterparty

The other party that participates in a cryptocurrency transaction.

Deposit Address

Deposit addresses are addresses that an organization or service manages on behalf of their users, where users receive funds into their account at the service.

Cold Wallet

A type of wallet that is not connected to the internet. This is also referred to as cold storage.

Paper Wallet

A type of cold storage wallet where private keys are printed on a piece of paper, written down, or exist on another physical medium.

Hosted Wallet

A wallet that resides on a third-party service. The third-party service may hold both the user's private and public keys.

Hot Wallet

A wallet that resides on a device connected to the internet, like a desktop computer or smartphone. If a user has the wallet on their device, their private keys will be stored on the device.

Transaction

A transaction consists of one or more fund transfers. A bitcoin transaction comprises: a unique transaction ID (the transaction hash); input(s), which are the source of the coins; and output(s), which are the destinations of the coins.

Transaction Hash

Also known as a transaction ID, the transaction hash is a unique identifier of a transaction.

Transfer

The part of a transaction that moves funds from one address to another address. For some asset types like Ethereum each transaction is one transfer, but for asset types like Bitcoin, a transaction can contain multiple transfers.

UTXO

An acronym for Unspent Transaction Output. UTXO is used to describe the transaction model used by most blockchains. In the UTXO model, you spend previously unspent chunks of cryptocurrency.

Wallet

A software program that generates and stores a user's addresses and private keys. It is used to send and receive cryptocurrency and monitor balances.

Withdrawal address

A withdrawal address is the address to which funds are sent externally. Multiple users may send funds to the same withdrawal address.

2. Transactions

a. Payments that were done in favour of Suspects

The following table lists the initial movement of cryptocurrencies initiated by our client to the following suspect addresses. It also includes the amount that was sent in each transaction.

For a quick reference, a transaction should be understood as a collection of transfers. For asset types like Bitcoin, a transaction can contain multiple transfers. A transfer is the movement of value from one address to another.

Type of Asset: BTC

Date	Transaction hash	Wallet address	Asset amount
16/07/21 10:33	619423c3f94693bd35aa669d04c63bb5abf28d0dd535c7fdddcfaf9354adaff7	3LDUMcxnWZQAqUkeNwEtf7s9LWazqh41QW *Suspect 1	0.02200052
16/08/21 13:25	7ca4ac24521c04adc896d308eb03ca0981746b8b367b671373c24113b81ea22e	3LDUMcxnWZQAqUkeNwEtf7s9LWazqh41QW *Suspect 1	0.11
14/10/21 10:10	e19e73e61dd598ecd40d446ec144d2[illegible]411	3DVa1dMufnDGpa8kYzksdi6rJEui5X8zqy *Suspect 2	[illegible]
14/10/21 13:44	4c563eaabc3e0af81460a02db602e3ba4c94dc9dfab8144223616109df698706	3DVa1dMufnDGpa8kYzksdi6rJEui5X8zqy *Suspect 2	0.04387624
19/10/21 11:07	d69872f9c91363fb0d7ded2a386d95fb075bf194a313d3850e55602da6304061	3DVa1dMufnDGpa8kYzksdi6rJEui5X8zqy *Suspect 2	0.10008292
Total			**0.38344739**

b. Located wallets

These wallets correspond to the last known addresses where the client's cryptocurrency was transferred to by the suspects, or the last identified and traced service wallet that the suspect moved funds to. Thus, all the subsequent wallets are the last known destinations that received transactions from the aforementioned suspect addresses. We have to clarify that the amounts transferred between the different clusters may or may not correspond to the initial amount transferred in favour of the scammers. This is because any transaction can be sent partially, along with other UTXOs, and may potentially include fees. However, all the displayed transactions correspond to movements made from the scammers' clusters to service wallets (which are most often cryptocurrency exchanges).

The complete path and partitions of the asset after being transferred from the suspect addresses can be seen in detail in the completed diagram labelled "Mapping of the cryptocurrency".

In this table you can see the wallet addresses whose location was identified:

Wallet number	Platform	Name on the Graph
3HayRDiQaT1h3CtMejoLPozE9E5oRUbUGo	Kraken.com	Kraken.com 1
3LFPetKV1tzMY3UgiiTxt15gCDFiePEd6S	KuCoin.com	KuCoin.com 1
1Mf55Ndu78dDEv7Lcs5cUdqr7QpdujFHjD	Binance.com	Binance.com 1
1ApMtA2icPjjjgkR3ictqaEjoe7iKzXvbh	Binance.com	Binance.com 2

3. Detailed information of the fraudulent wallet transactions

a. Information about the transactions (fraudulent wallets)

The following table contains an extract from the complete information that corresponds to all the transactions made from the suspect clusters. If more information is needed about any transaction, it can be provided upon request.

Suspect's 1 cluster with root address:

34KQBmcpmk9rPWPxWtYvbEkJjymJ8FARGE

Transaction Hash	Date	Receiving Address	Counterparty Root Address	Value
5b658ac19850a616781f3d239ee5ea8b3fc9c62f043d87174258590f4a5c442b	7/15/2021 8:43	34KQBmcpmk9rPWPxWtYvbEkJjymJ8FARGE	1Je3RohZT6mH1AofjcjMJXgbVgKrJNVohD Coinbase.com	0.01022285
619423c3f94693bd35aa669d04c63bb5abf28d0dd535c7fdddcfaf9354adaff7	7/16/2021 10:33	3LDUMcxnWZQAqUkeNwEtf7s9LWazqh41QW	3Erc3ZBbWpX6BTLHnWTRg8qHKDv6MFvt2X	0.02200052
3623848a873b3a16aed03bb6bbbe144c090c1636235f8f765804577f5b199672	7/21/2021 15:03	368Lus9fqwiquZT26ZGk9W6eYW9sbfPr96	1HhVMYrxCUriKL3jnbXa6y595xCWhHj7sG Bitstamp.net	0.04236
83cde32cba9e1d16a7479f070c42074e5b5aec0e8692c5e2470e28594731be47	7/23/2021 14:28	3LFPetKV1tzMY3UgiiTxt15gCDFiePEd6S	1C1bm3mQPpep9wJsVpQ8Fjx1GErqXhurxy KuCoin.com	-0.07457081
7ca4ac24521c04adc896d308eb03ca0981746b8b367b671373c24113b81ea22e	8/16/2021 13:25	3LDUMcxnWZQAqUkeNwEtf7s9LWazqh41QW	3KoX7XLdh24UJBfVyZFfB4T8F4FSuhHvG4	0.11
eee216e54427ca1fa1ca15249f8709f291eb03bea20d621a527addca1b929196	8/16/2021 13:57	3HayRDiQaT1h3CtMejoLPozE9E5oRUbUGo	157EDTdFDEymZDPjKX8RWbuxVYREForUAP Kraken.com	-0.07539054
eee216e54427ca1fa1ca15249f8709f291eb03bea20d621a527addca1b929196	8/16/2021 13:57	3AREXymZdnwfzrZvRkDRZaTPW2DsjzFbwp	3AREXymZdnwfzrZvRkDRZaTPW2DsjzFbwp	-0.03460274

Suspect's 2 cluster with root address: 3DVa1dMufnDGpa8kYzksdi6rJEui5X8zqy

Transaction Hash	Date	Receiving Address	Counterparty Root Address	Value
e19e73e61dd598ecd40d446ec144d2ed9aba1179cbef095af1cccdd54a6d4411	10/14/2021 10:10	3DVa1dMufnDGpa8kYzksdi6rJEui5X8zqy	3G5YvWWQ7ADdLgezsj2m68xAXpGLDMJe6r	0.10748771
b722798f04a1949af5933f5f9f395e60f33e708b388f9148aa592371fa2c4426	10/14/2021 10:37	1Mf55Ndu78dDEv7Lcs5cUdqr7QpdujFHjD	1128Ev6iMRQ25SuGAnrekSqbW8aQpX5PZQ Binance.com	-0.10747431
4c5636eabc3e0af81460a02db602e3ba4c94dc9dfab8144223616109df698706	10/14/2021 13:44	3DVa1dMufnDGpa8kYzksdi6rJEui5X8zqy	3GZQ[illegible]EWmaY R8XA7nh3ma8C8ixuQDW4	0.04387624
d69872f9c91363fb0d7ded2a386d95fb075bf194a313d3850e55602da6304061	10/19/2021 11:07	3DVa1dMufnDGpa8kYzksdi6rJEui5X8zqy	3KygEie4zx5f7AE3itasbj7hPDPMi3DsUE	0.10008292
c393abac5e79e3b5bc15e7beaca38b5c93f5a8d1ac98203aa4b1c31060571c6b	10/20/2021 11:16	1ApMtA2icPjjjgkR3ictqaEjoe7iKzXvbh	1128Ev6iMRQ25SuGAnrekSqbW8aQpX5PZQ Binance.com	-0.14393676

4. Mapping of the cryptocurrency

The following diagram showcases the complete path and partitions the Asset took from when it was first sent by our client to the suspect wallets. However, it may or may not correspond with the final destination the cryptocurrency arrived at, rather it should be understood as the movements and partitions it had up to this point. T&H consulting has to clarify that due to the nature of assets such as BTC, it can move and divide further from the final destination displayed in this report.

To better understand the layout of the following diagram, please note it should be read from left to right. This will facilitate the visualization of how the initial transactions made to the suspect wallets were divided and transferred to other wallets, and their last traceable location.

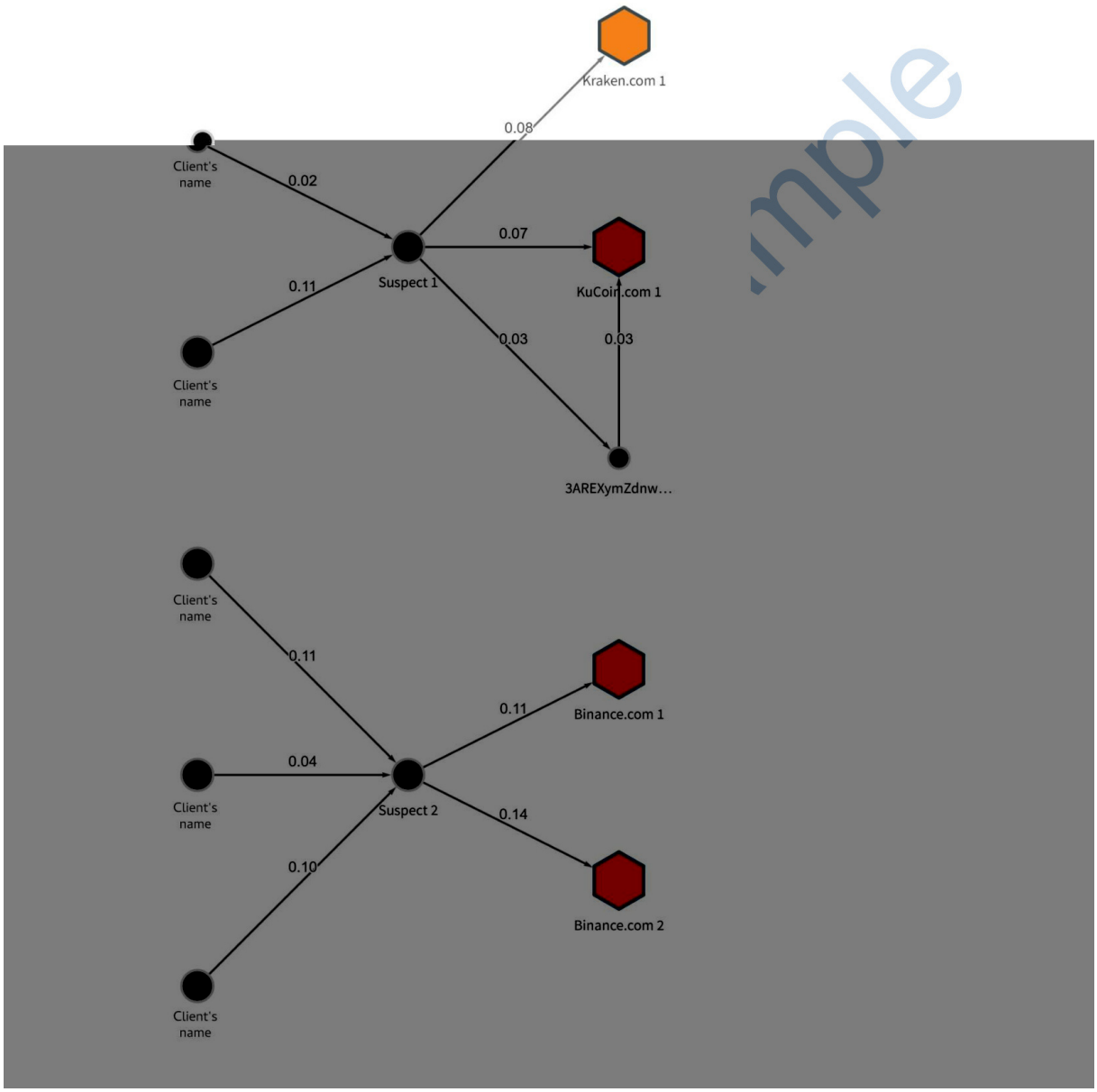
In the mapping, each black circle represents a certain wallet (or cluster), and its size corresponds to the amount of cryptocurrency involved with it on this period. The arrows coming out from each circle represent the destination or relation every wallet has had with other elements displayed in the diagram. The grey and black circles represent unknown no hosted clusters, and the final circles or hexagons containing names ending with .com represent cryptocurrency exchanges.

a. List of Root addresses & Entities represented on the graph below

The root address is the first used (oldest) address in a cluster. This is the first step in how T&H Consulting can identify and attribute entities on the blockchain.

Root Address	Organization Name
34KQBmcpmk9rPWPxWtYvbEkJjymJ8FARGE	Suspect 1
3Erc3ZBbWpX6BTLHnWTRg8qHKDv6MFvt2X	Client's Name
3KoX7XLdh24UJBfVyZFfB4T8F4FSuhHvG4	Client's Name
3DVa1dMufnDGpa8kYzksdi6rJEui5X8zqy	Suspect 2
3G5YvWWQ7ADdLgezsj2m68xAXpGLDMJe6r	Client's Name
3GZQJ7Nt7EWmXjR8XA7nh3ma8C8ixuQDW4	Client's Name
3KygEie4zx5f7AE3itasbj7hPDPMi3DsUE	Client's Name
3AREXymZdnwfzrZvRkDRZaTPW2DsjzFbwp	
3ea95101-926b-45b3-b821-c9954c7a9e73	KuCoin.com 1
3a94ddf2-82e8-4f72-bafb-ae9f2d95d0f2	Kraken.com 1
8fc81320-2e2d-4299-b467-0125350c8711	Binance.com 1
7c2fc557-7cbf-47ba-b6bc-cfb8c19f6832	Binance.com 2

b. Cryptocurrency flow visualization graph



T&H Consulting International KFT

Registration number 01 09 350838
Hungary

T&H Holdings Limited

Company number 12747126
in the Companies House
United Kingdom

https://tandhconsult.com/