Ethereum Guide – Follow the Ether

January 2022

GUIDE FOR INVESTIGATORS

AUTHOR
European Cybercrime Centre (EC3)

Contents

The objective of this guide

The usage of Ethereum has increased over the last years, also by (cyber)criminals. Member States have increasingly reported cases where Ethereum was stolen or used by suspects for criminal payments or money laundering. Europol is receiving an increasing amount of requests to help law enforcement officials in tracing such transactions. With this guide, Europol wants to assist law enforcement colleagues in gaining a better understanding of Ethereum, tokens, smart contracts and more on the Ethereum network. In this way, we hope that our law enforcement partners will have better capabilities to trace Ethereum-related transactions.

What is covered?

- Key Ethereum terminology
- Basics of tracing Ethereum transactions
- Differences in types of Ethereum transactions
- Basics of smart contracts
- Following the money
- Tracing, new developments: DeFi, Staking, NFTs

What is not covered?

- Technical fundamentals of Ethereum
- Detailed explanation of various cryptocurrencies and projects running on the Ethereum network
- Ethereum forks
- Legislation around Ethereum, related coins or other developments

The information in this guide may contain claims you would like to challenge or improve on. If this is the case, please direct your questions / comments / suggestions to O3@europol.europa.eu or the Cryptocurrency community at the European Platforms for Experts.

Key Ethereum terms

In this section, we briefly define some of the key Ethereum terminology[1].

[1] See also https://Ethereum.org/en/glossary/ for other terms and broader descriptions.

Ether is the cryptocurrency of the Ethereum network, the native asset that facilitates payments and other operations on the network.

Ethereum addresses can be shared publicly to receive Ether, tokens and NFTs and to view a balance in relation to the address. They are used for storing Ether assets, tokens, contracts and more. Can be recognised by the fact that they start with 0x.

Ethereum private key allows for cryptographically signing a transaction and sending funds from an associated Ether address.

Ethereum account is the entity in which a user can hold an Ether balance on an address and from which transactions can be sent.

Ethereum transactions are stored in the Ethereum blockchain and signify the transfer of Ether, tokens or NFTs from one address to another.

Smart contracts are lines of code or computer programs that run on the Ethereum blockchain. The code resides in an address on the Ethereum blockchain and runs as programmed, which means they are not executed by a user, but by the program (this is why they are referred to as ‘smart’, still: Etherscan calls them ‘contracts’). They are building blocks of code on the blockchain that can be used to build programs (applications). This combination of decentralised (blockchain) and apps makes decentralised applications or ‘dapps’.

Gas is the computational power that is needed on the Ethereum network to process operations, such as transactions and smart contracts. Gas is a fee required (paid in Ether) to conduct such operations.

Ethereum wallet stores private keys and is used to access Ethereum accounts. Just as with Bitcoin, private keys can also be stored offline in the shape of a mnemonic phrase for example (12 or 24 words).

Ethereum basics

Ethereum is a cryptocurrency. That means that, just like Bitcoin, it has a (public) blockchain to store transactions. The addresses rely on cryptography for security, so a private key of an address is needed to spend funds on that address. Ethereum has some fundamental differences from Bitcoin. The scripting language in Ethereum allows for some additional functionalities. Amongst other things, it allows for the creation of smart contracts, tokens, DeFi platforms, non-fungible tokens (NFTs) and more. Many of these functionalities will be addressed in this guide. Please note that there are no requirements placed on someone that creates and deploys tokens, smart contracts or NFTs in terms of compliance and know-your-customer (KYC). Also, anyone can create them, which has led to many fraudulent projects.

Checking Ethereum addresses

Cryptocurrency investigators and forensic examiners should be familiar with the format of Ethereum addresses, which can be recognised by the fact that they always start with 0x. Addresses contain 40 hexadecimal characters and will look like this:

- 0x00000000219ab540356cBB839Cbe05303d7705Fa

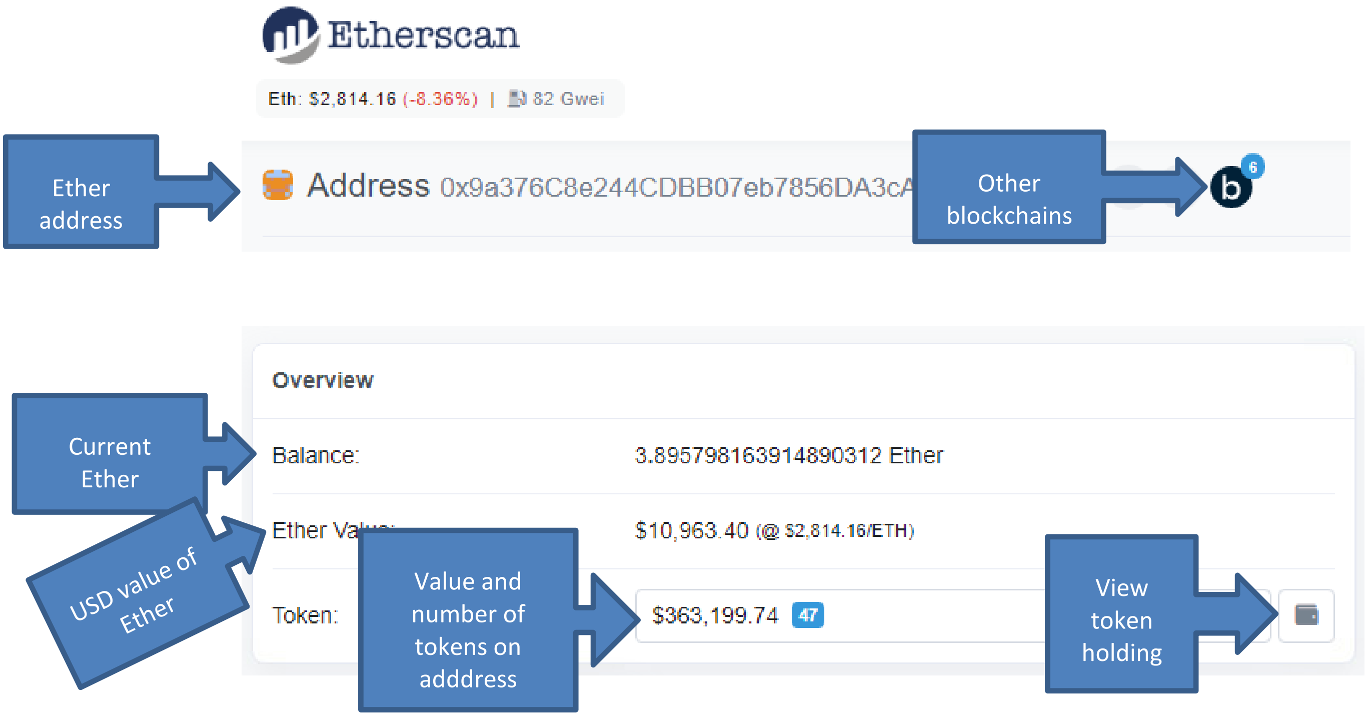
Or:

- 0x9a376c8e244cdbb07eb7856da3cac7f5794b58fa

The investigator with a keen eye for detail will have noticed that these addresses have slightly different formats. The first address uses capitalisation, while the second does not. The address with capitalisation uses a checksum, which is used to verify the validity of data (i.e. the Ethereum address).

The current balance and list of transactions from an Ether address can be checked with websites that show the Ether blockchain. A popular website, which we will use extensively in this guide, is Etherscan.io.

See below an example of the address 0x9a376c8e244cdbb07eb7856da3cac7f5794b58fa on Etherscan:



Etherscan

Eth: $2,814.16 (-8.36%) | 82 Gwei

Address 0x9a376C8e244CDBB07eb7856DA3cA

Overview

Balance: 3.895798163914890312 Ether

Ether Va $10,963.40 (@ $2,814.16/ETH)

Token: $363,199.74 47

Investigator tips

- This address is also valid on other Ethereum based blockchains. Click on the black circle with the white 'b' on the right and you will see this address is also valid on Binance Smart Chain, Polygon (Matic) and more.
- If Etherscan returns a negative result, it might still be worth checking the address on other blockchains, such as Binance Smart Chain.
- Always click on the view token holding to further investigate the tokens held in an address. See 'Understanding Ethereum transactions – Erc20 Tokens' in this guide for more information.

The transaction hash (also known as transaction id) also starts with 0x. However, the transaction hash is 64 hexadecimal characters long and, looks, for example, like this:

- 0x8e6e6fa9734616bd22b546d442fc5840c2d52638de2f378d8c16bf81ccac3b31

Further investigation tips

The following regular expressions can be used to search for Ethereum addresses in seized devices such as laptops and mobile phones:

/^0x[a-fA-F0-9]{40}$/

And this one for transaction hashes:

/^0x([A-Fa-f0-9]{64})$/

This can help in determining if a suspect has owned or transacted Ether.

Ethereum private key

An Ethereum private key consists of 64 random hexadecimal characters or 32 random bytes. The public key can be derived from the private key with Elliptic Curve Digital Signature Algorithm. The private key is needed to access and send a suspect's funds.

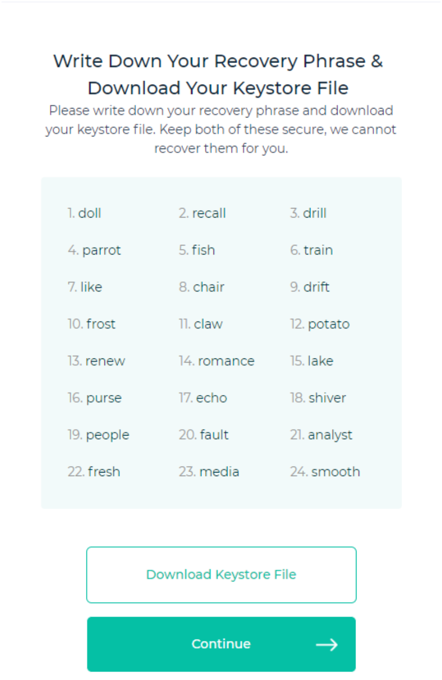
Investigation tip

Look for personal notes on the suspect's devices, especially with titles such as 'key', 'mnemonic', 'phrase', 'wallet' etc. These may hold private keys (or mnemonic phrases) to a suspect's wallets. They might give such files a deliberately misleading name. These type of files are often password protected.

Ethereum seed

Similarly to Bitcoin, *mnemonic phrases* are used in Ethereum to access wallets. These are also known as *recovery seed* or *Secret Recovery Phrase*. A mnemonic phrase is a set of words from which a private key is calculated. With this private key an Ether wallet can be accessed. The user generally writes down this mnemonic phrase as a back-up, to be able to restore their wallet.

A mnemonic phrase often contains 12 or 24 words, but can also contain 16, 18 or 20 words. This is an example of a 24-word seed phrase generated by MyEtherWallet, a software wallet:



Write Down Your Recovery Phrase & Download Your Keystore File

Please write down your recovery phrase and download your keystore file. Keep both of these secure, we cannot recover them for you.

1. doll	2. recall	3. drill
4. parrot	5. fish	6. train
7. like	8. chair	9. drift
10. frost	11. claw	12. potato
13. renew	14. romance	15. lake
16. purse	17. echo	18. shiver
19. people	20. fault	21. analyst
22. fresh	23. media	24. smooth

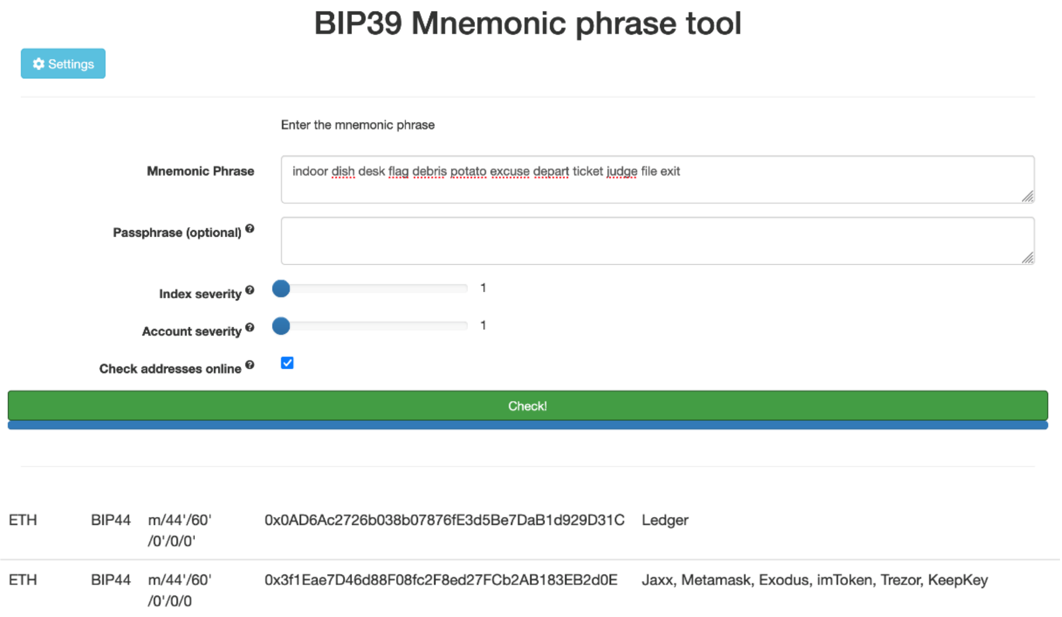
Hardware wallets, such as Trezor, KeepKey and Ledger, also work with mnemonic phrases. See the [Bitcoin Guide for Investigators 2021 on EPE]() for an overview of different types of wallets.

Several law enforcement agencies have created handy tools to quickly verify if a mnemonic phrase is valid, what cryptocurrency addresses could have been created from this phrase and if funds were (ever) on the addresses associated with the phrase. For example, if we insert the below phrase into the Mnemonic Phrase Tool[2]:

[2] Created by the Fiscale Inlichtingen- en Opsporingsdienst (FIOD). Available on the Europol Platform for Experts – Cryptocurrencies (LE Only)

indoor dish desk flag debris potato excuse depart ticket judge file exit

We see the following result for Ether addresses:



BIP39 Mnemonic phrase tool

Enter the mnemonic phrase

Mnemonic Phrase: indoor dish desk flag debris potato excuse depart ticket judge file exit

Passphrase (optional):

Index severity: 1

Account severity: 1

Check addresses online: ☑

ETH	BIP44	m/44'/60' /0'/0/0'	0x0AD6Ac2726b038b07876fE3d5Be7DaB1d929D31C	Ledger
ETH	BIP44	m/44'/60' /0'/0/0	0x3f1Eae7D46d88F08fc2F8ed27FCb2AB183EB2d0E	Jaxx, Metamask, Exodus, imToken, Trezor, KeepKey

There are more results related to other cryptocurrencies as well, as the Mnemonic phrase tool shows the possible addresses that can be derived from different 'derivation paths'[3]. If addresses were used, a green tick appears. The green tick at a certain derivation path basically tells the investigator what type of wallet they should use to open and seize funds.

Investigation tips

- When you find a number of words, for example written on a piece of paper or in a .txt file, use one of the available mnemonic phrase tools created by the Austrian Bundesministerium or the Dutch FIOD, to determine how you can possibly access the funds. These will let you know what public keys could have been created from the mnemonic phrase and with what wallets these can be accessed.
- It is recommended that your law enforcement agency owns different types of hardware wallets and that investigators have installed software wallets before going on a search. Some phrases will be

[3] https://Ethereum.stackexchange.com/questions/70017/can-someone-explain-the-meaning-of-derivation-path-in-wallet-in-plain-english-s

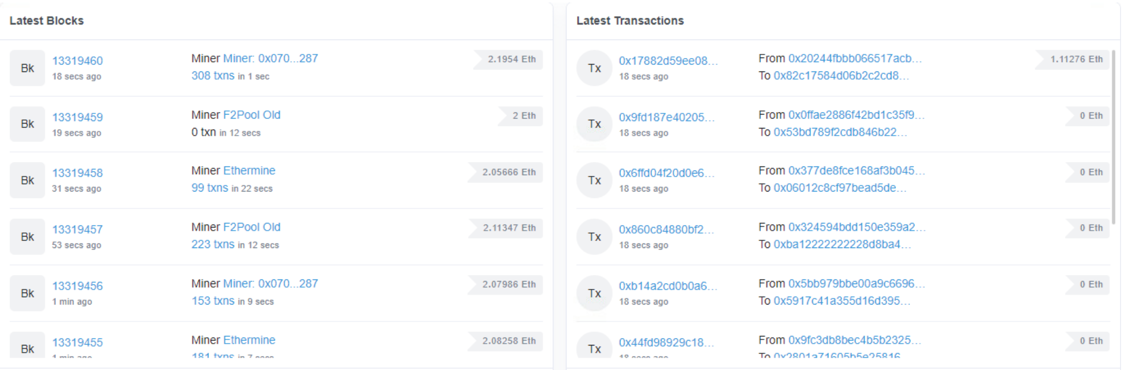
accessible with a certain hardware wallet, but not with the other. See the Bitcoin Guide for Investigators for an overview of wallets.

- When an investigator finds a mnemonic phrase noted down on a sheet of paper, they might have a ‘eureka moment’. In many cases, the criminal funds can now be seized! However, please note that a passphrase can be added on top of the mnemonic, for extra security. This password might also be noted down together with the mnemonic phrase, for example as the 25th word. This is something to keep in mind.

Understanding Ethereum transactions

Similarly to the Bitcoin blockchain, the Ethereum blockchain is formed of blocks containing transactions, which are mined in a proof-of-work system. In this system members of a network (mining computers) make complex calculations to ‘crack’ a mathematical puzzle and as a reward ‘mine’ new cryptocurrency. However, Ethereum is aiming to move to a proof-of-stake system. In this system, users with ‘staked’ Ether are chosen at random to validate the network by ordering transactions and creating new blocks. Less energy and hardware is required for this type of ‘consensus mechanism’[4].

The Ethereum blockchain’s size is very large, which makes it impractical to download for investigators. Therefore, it is easier to use publicly available or commercial tracing tools. A popular free option is Etherscan.io, which can be used to explore blocks, transactions, smart contracts, token transfers, internal transactions and more. On the front page recent blocks and transactions can be seen:



Latest Blocks

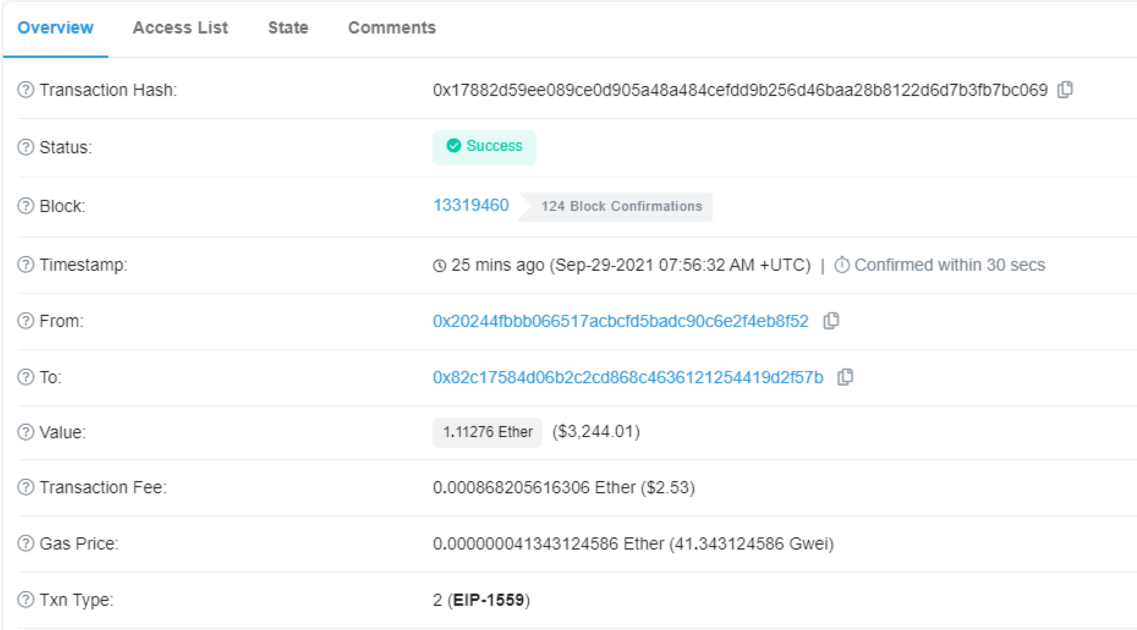
Bk	13319460 18 secs ago	Miner Miner: 0x070...287 308 txns in 1 sec	2.1954 Eth
Bk	13319459 19 secs ago	Miner F2Pool Old 0 txn in 12 secs	2 Eth
Bk	13319458 31 secs ago	Miner Ethermine 99 txns in 22 secs	2.05666 Eth
Bk	13319457 53 secs ago	Miner F2Pool Old 223 txns in 12 secs	2.11347 Eth
Bk	13319456 1 min ago	Miner Miner: 0x070...287 153 txns in 9 secs	2.07986 Eth
Bk	13319455 1 min ago	Miner Ethermine 181 txns in 7 secs	2.08258 Eth

Latest Transactions

Tx	0x17882d59ee08... 18 secs ago	From 0x20244fbbb066517acb... To 0x82c17584d06b2c2cd8...	1.11276 Eth
Tx	0x9fd187e40205... 18 secs ago	From 0x0ffae2886f42bd1c35f9... To 0x53bd789f2cdb846b22...	0 Eth
Tx	0x6ffd04f20d0e6... 18 secs ago	From 0x377de8fce168af3b045... To 0x06012c8cf97bead5de...	0 Eth
Tx	0x860c84880bf2... 18 secs ago	From 0x324594bdd150e359a2... To 0xba1222222228d8ba4...	0 Eth
Tx	0xb14a2cd0b0a6... 18 secs ago	From 0x5bb979bbe00a9c6696... To 0x5917c41a355d16d395...	0 Eth
Tx	0x44fd98929c18... 18 secs ago	From 0x9fc3db8bec4b5b2325... To 0x2801a71605b5e25816	0 Eth

When clicking on the most recent (top right) transaction, we can see the details of a transaction from one Ether address to another:

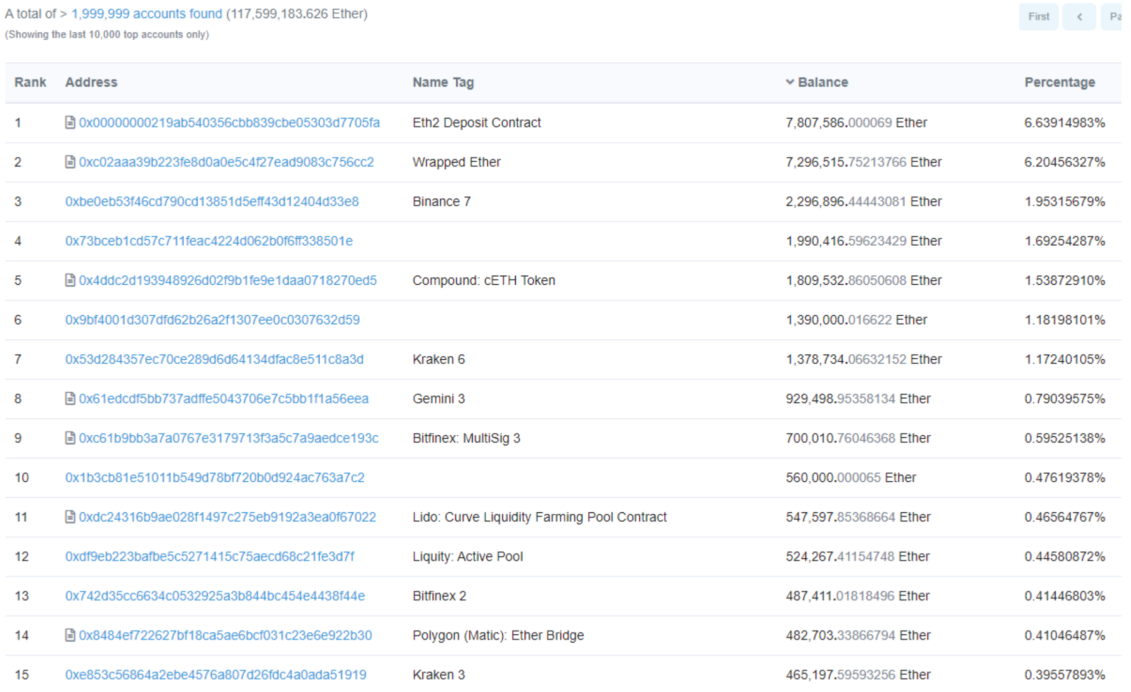
[4] https://Ethereum.org/en/developers/docs/consensus-mechanisms/pos/



Transaction Hash:	0x17882d59ee089ce0d905a48a484cefdd9b256d46baa28b8122d6d7b3fb7bc069
Status:	Success
Block:	13319460 124 Block Confirmations
Timestamp:	25 mins ago (Sep-29-2021 07:56:32 AM +UTC) | Confirmed within 30 secs
From:	0x20244fbbb066517acbcfd5badc90c6e2f4eb8f52
To:	0x82c17584d06b2c2cd868c4636121254419d2f57b
Value:	1.11276 Ether ($3,244.01)
Transaction Fee:	0.000868205616306 Ether ($2.53)
Gas Price:	0.000000041343124586 Ether (41.343124586 Gwei)
Txn Type:	2 (**EIP-1559**)

From this we can see when the transaction took place (i.e. when it was verified by miners), from which address the Ether were sent and where it ended up, how much was sent and what transaction fee needed to be paid to miners to verify the transaction. Contrary to Bitcoin, Ethereum does not use change addresses. This makes it easier to see where funds end up, as ‘regular’ transactions on the Ethereum blockchain go from one address to one other address. This can seem a bit similar to traditional bank account transactions.

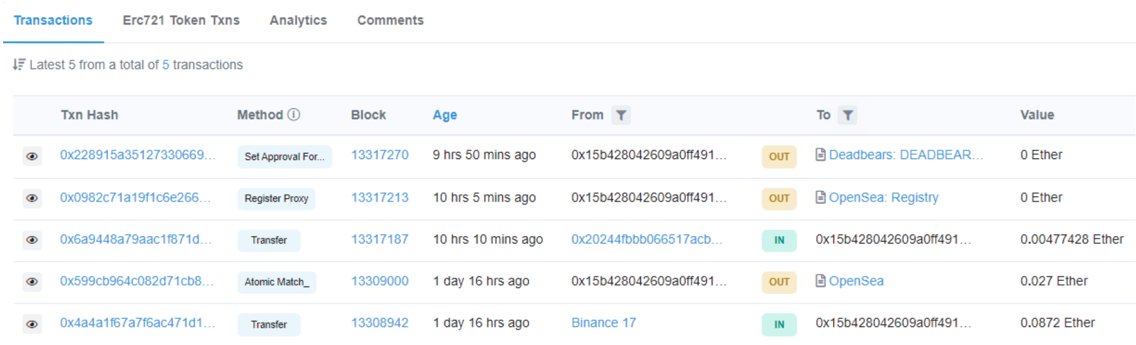
Another advantage is that some services are already ‘tagged’ on Etherscan.io. When tracing bitcoins with sites such as Blockchain.com, this is not the case. Therefore, this is a clear advantage. For example, the list of ‘Top Accounts by ETH Balance’ include several addresses with exchange tags, such as Binance, Kraken, Bitfinex and Gemini:



A total of > 1,999,999 accounts found (117,599,183.626 Ether)
(Showing the last 10,000 top accounts only)

Rank	Address	Name Tag	Balance	Percentage
1	0x00000000219ab540356cbb839cbe05303d7705fa	Eth2 Deposit Contract	7,807,586.000069 Ether	6.63914983%
2	0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2	Wrapped Ether	7,296,515.75213766 Ether	6.20456327%
3	0xbe0eb53f46cd790cd13851d5eff43d12404d33e8	Binance 7	2,296,896.44443081 Ether	1.95315679%
4	0x73bceb1cd57c711feac4224d062b0f6ff338501e		1,990,416.59623429 Ether	1.69254287%
5	0x4ddc2d193948926d02f9b1fe9e1daa0718270ed5	Compound: cETH Token	1,809,532.86050608 Ether	1.53872910%
6	0x9bf4001d307dfd62b26a2f1307ee0c0307632d59		1,390,000.016622 Ether	1.18198101%
7	0x53d284357ec70ce289d6d64134dfac8e511c8a3d	Kraken 6	1,378,734.06632152 Ether	1.17240105%
8	0x61edcdf5bb737adffe5043706e7c5bb1f1a56eea	Gemini 3	929,498.95358134 Ether	0.79039575%
9	0xc61b9bb3a7a0767e3179713f3a5c7a9aedce193c	Bitfinex: MultiSig 3	700,010.76046368 Ether	0.59525138%
10	0x1b3cb81e51011b549d78bf720b0d924ac763a7c2		560,000.000065 Ether	0.47619378%
11	0xdc24316b9ae028f1497c275eb9192a3ea0f67022	Lido: Curve Liquidity Farming Pool Contract	547,597.85368664 Ether	0.46564767%
12	0xdf9eb223bafbe5c5271415c75aecd68c21fe3d7f	Liquity: Active Pool	524,267.41154748 Ether	0.44580872%
13	0x742d35cc6634c0532925a3b844bc454e4438f44e	Bitfinex 2	487,411.01818496 Ether	0.41446803%
14	0x8484ef722627bf18ca5ae6bcf031c23e6e922b30	Polygon (Matic): Ether Bridge	482,703.33866794 Ether	0.41046487%
15	0xe853c56864a2ebe4576a807d26fdc4a0ada51919	Kraken 3	465,197.59593256 Ether	0.39557893%

Investigators may also encounter services’ names in transactions overviews. These include exchanges, but also token contracts and non-fungible token (NFT) platforms, which we will discuss later. See an example of such a transaction overview which includes 'tags' below:



Latest 5 from a total of 5 transactions

Txn Hash	Method	Block	Age	From		To	Value
0x228915a35127330669...	Set Approval For...	13317270	9 hrs 50 mins ago	0x15b428042609a0ff491...	OUT	Deadbears: DEADBEAR...	0 Ether
0x0982c71a19f1c6e266...	Register Proxy	13317213	10 hrs 5 mins ago	0x15b428042609a0ff491...	OUT	OpenSea: Registry	0 Ether
0x6a9448a79aac1f871d...	Transfer	13317187	10 hrs 10 mins ago	0x20244fbbb066517acb...	IN	0x15b428042609a0ff491...	0.00477428 Ether
0x599cb964c082d71cb8...	Atomic Match_	13309000	1 day 16 hrs ago	0x15b428042609a0ff491...	OUT	OpenSea	0.027 Ether
0x4a4a1f67a7f6ac471d1...	Transfer	13308942	1 day 16 hrs ago	Binance 17	IN	0x15b428042609a0ff491...	0.0872 Ether

Etherscan actively looks for information related to Ethereum addresses on the Web. They include name tags, which often point to the owner of the address (company or an individual) and a URL to the source of such information. Furthermore, Etherscan adds labels, such as 'NFT' or 'stablecoin' to provide users with further information on what category saddresses belongs to[5].

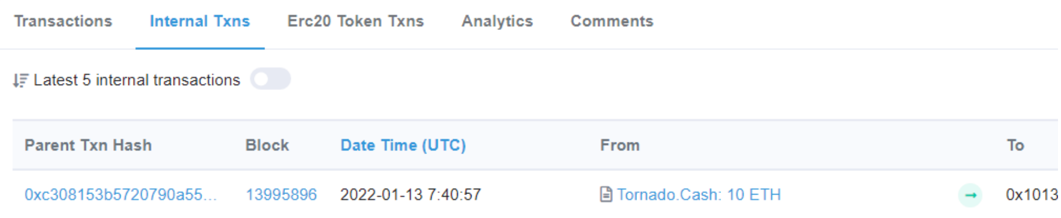
It is important to note that we do not know how accurate these labels are. While Etherscan says to use 'curators' to verify this, they also state that users sometimes falsely claim an address, for example for scamming purposes. It is important for investigators to keep this in mind and to not base an entire case on a single Etherscan tag. Ideally, corroborating evidence provides extra evidence for the label used in an investigation.

Understanding Ethereum transactions – internal txns

The 'Internal txns' tab is visible next to the transactions tab on Etherscan.io, but what are internal transactions? Internal transactions are related to transactions passing through smart contracts as an intermediary.

For investigators, this tab is mainly relevant as it can show the conversion of Ether to other cryptocurrencies or tokens, and vice versa, via smart contracts. Decentralised platforms such as Uniswap or SushiSwap may come up in this tab. Also, you will be able to see incoming transactions from mixers (Tornado.cash for example) as internal transactions. Some wallets do not show internal transactions, so it is always recommended to check this on Etherscan. Also, this tab will not always be visible, only if the address actually executed internal transactions.

In the example below, we see an internal transaction where the address is receiving 10 Ether from the mixer Tornado.cash[6]. As the transactions from this mixer are automated through a smart contract. See below an example of an output visible in the internal transactions tab:



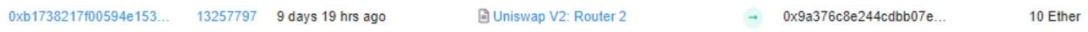
Latest 5 internal transactions

Parent Txn Hash	Block	Date Time (UTC)	From		To
0xc308153b5720790a55...	13995896	2022-01-13 7:40:57	Tornado.Cash: 10 ETH	→	0x1013

[5] https://info.Etherscan.com/public-name-tags-labels/

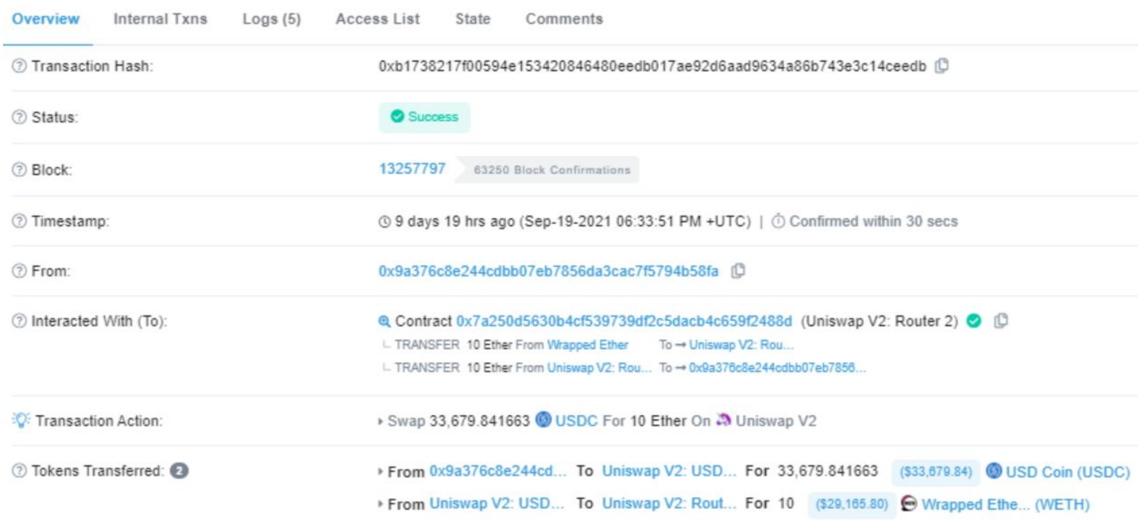
[6] Tornado.cash is the only popular available mixer available for Ethereum and is frequently encountered in investigations

Investigators can for example also see in the internal transaction tab when liquidity is removed from a platform, after an address had sent funds there to stake it (this will be discussed later in this document don't worry if you don't understand it yet).



0xb1738217f00594e153... 13257797 9 days 19 hrs ago Uniswap V2: Router 2 → 0x9a376c8e244cdbb07e... 10 Ether

When clicking on the above transaction hash (on the left), you will see this:



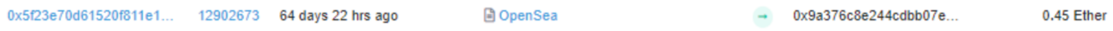
Overview Internal Txns Logs (5) Access List State Comments

Transaction Hash:	0xb1738217f00594e153420846480eedb017ae92d6aad9634a86b743e3c14ceedb
Status:	Success
Block:	13257797 63250 Block Confirmations
Timestamp:	9 days 19 hrs ago (Sep-19-2021 06:33:51 PM +UTC) | Confirmed within 30 secs
From:	0x9a376c8e244cdbb07eb7856da3cac7f5794b58fa
Interacted With (To):	Contract 0x7a250d5630b4cf539739df2c5dacb4c659f2488d (Uniswap V2: Router 2) └ TRANSFER 10 Ether From Wrapped Ether To → Uniswap V2: Rou... └ TRANSFER 10 Ether From Uniswap V2: Rou... To → 0x9a376c8e244cdbb07eb7856...
Transaction Action:	Swap 33,679.841663 USDC For 10 Ether On Uniswap V2
Tokens Transferred: 2	From 0x9a376c8e244cd... To Uniswap V2: USD... For 33,679.841663 ($33,679.84) USD Coin (USDC) From Uniswap V2: USD... To Uniswap V2: Rout... For 10 ($29,165.80) Wrapped Ethe... (WETH)

If we for example look at 'Tokens Transferred', we can conclude that 33.679,84 USD Coin[7] were sent to Uniswap from address 0x9a376c8e244cd..., where these were exchanged for 10 Ether, via Wrapped Ether. The observant investigator will notice a discrepancy: the 10 Ether are worth $ 29.165,80, a loss of over $ 4.000! Fortunately for the trader, this was not the case. The price of 10 Ether presented here is the price at the time of taking the screenshot, not the price during the transaction nine days earlier. At that moment, the price was $3,328.85, which would have been $33.288,50 for 10 Ether, a significantly better exchange rate.

This shows that the Ethereum blockchain can give investigators relevant leads on transactions, even when decentralised platforms are used. While it is impossible to trace through traditional exchanges (Coinbase, Gemini, Binance), this is not the case for decentralised exchanges. While requests for information often can not be sent to such decentralised exchanges, as they are (or pretend to be) 'fully decentralised', Ethereum blockchain analysis can give investigators a quick and accurate answer to their questions about the origin and destinations of funds.

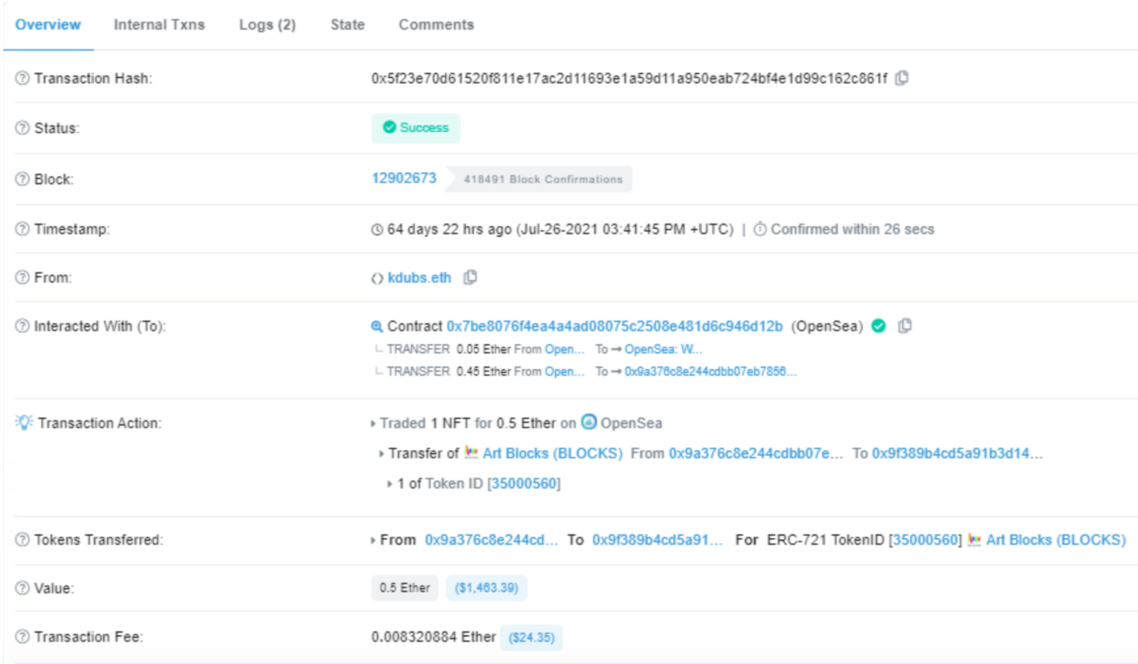
The trading of NFTs is another example that is visible in the 'internal txns' tab. We might see this transaction on this tab:



0x5f23e70d61520f811e1... 12902673 64 days 22 hrs ago OpenSea → 0x9a376c8e244cdbb07e... 0.45 Ether

OpenSea is perhaps the most well-known platform on which NFTs are traded. When we click on the transaction hash, we can see from what address the NFT came:

[7] A stable coin, pegged 1:1 to the US dollar, see https://www.circle.com/en/usdc.



Overview | Internal Txns | Logs (2) | State | Comments

Transaction Hash:	0x5f23e70d61520f811e17ac2d11693e1a59d11a950eab724bf4e1d99c162c861f
Status:	Success
Block:	12902673 418491 Block Confirmations
Timestamp:	64 days 22 hrs ago (Jul-26-2021 03:41:45 PM +UTC) | Confirmed within 26 secs
From:	kdubs.eth
Interacted With (To):	Contract 0x7be8076f4ea4a4ad08075c2508e481d6c946d12b (OpenSea) └ TRANSFER 0.05 Ether From Open... To → OpenSea: W... └ TRANSFER 0.45 Ether From Open... To → 0x9a376c8e244cdbb07eb7856...
Transaction Action:	▸ Traded 1 NFT for 0.5 Ether on OpenSea ▸ Transfer of Art Blocks (BLOCKS) From 0x9a376c8e244cdbb07e... To 0x9f389b4cd5a91b3d14... ▸ 1 of Token ID [35000560]
Tokens Transferred:	▸ From 0x9a376c8e244cd... To 0x9f389b4cd5a91... For ERC-721 TokenID [35000560] Art Blocks (BLOCKS)
Value:	0.5 Ether ($1,463.39)
Transaction Fee:	0.008320884 Ether ($24.35)

When we look at ‘Tokens Transferred’ we see a transaction from one address to another for a certain ‘ERC-721 TokenID’. ERC-721 is the token standard for the transfer of NFTs.

When we look at ‘Interacted with (to)’ we can conclude that an NFT was purchased from an artist on OpenSea, a NFT marketplace. In this case, we can even identify the buyer[8]. If we look at ‘From’ we see ‘kdubs.eth’. This user has (most likely) registered this name with the Ethereum Name Service[9]. Also, when we search for this user name online, we can find that this user uses the Ether address seen above (0x9a376…) and has purchased and sold various NFTs.

Please note that this user was found in a completely random manner. However, if this was a criminal investigation (which it is not), this analysis might have led to useful leads. This Ethereum Name Service could, in theory, also be used to impersonate someone else’s user name. Investigators must keep this in mind and not simply follow one lead.

Investigation tips

- Investigators can obtain interesting info from the ‘Internal txns’ tab on Etherscan, this includes information on:
  - Liquidity removal from decentralised platforms;
  - Transfers of NFTs;
  - The initiator of the trade, especially when it is supplemented with from the Ethereum Name Service or open source information.
- Etherscan.io is a company and will most likely analyse the information that is sent to their platform. This means that they might

[8] The user sent 0,5 Ether to OpenSea at the same time, proving that it is the buyer, not the seller
[9] https://etherscan.io/enslookup-search?search=kdubs.eth

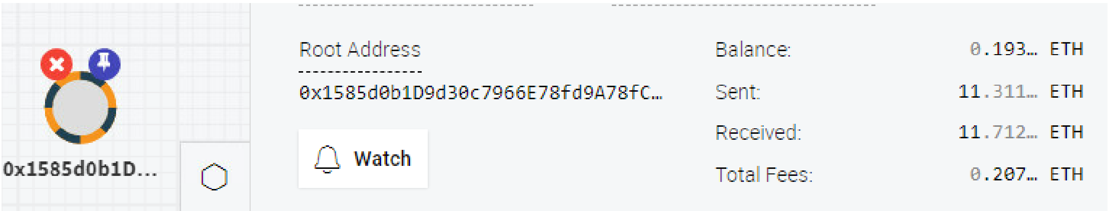
analyse the search queries and addresses inserted in their platform, also by law enforcement agencies. We recommend to consider this potential risk, especially in sensitive cases. Alternative solutions:

- Ask an open source specialist in your agency about this;
- Use paid tracing tools, as these may advertise not to use or sell your search queries.

Understanding Ethereum transactions – Erc20 Tokens

Next to the ‘internal txns’ tab on Etherscan, we find another important element of the Ethereum infrastructure: ERC20 tokens transactions. ERC20 is the technical standard from which tokens can be created on the Ethereum network. The standard defines a set of rules so that every coin, for example a ‘totalSupply’ and that an ERC20 token address has a ‘balanceOf’. The Ethereum system allows users to keep or store both Ethereum’s native currency Ether (ETH) and one or more of these tokens on the same Ethereum address. These addresses are referred to as “accounts”. A token balance is easier to overlook than a balance in Ether and can lead to an investigator forgetting to see (and possibly seize) criminal funds.

For example, if we would look at address 0x1585d0b1D9d30c7966E78fd9A78fCd14D6F7A7D4 in a popular tracing tool, we would see this:



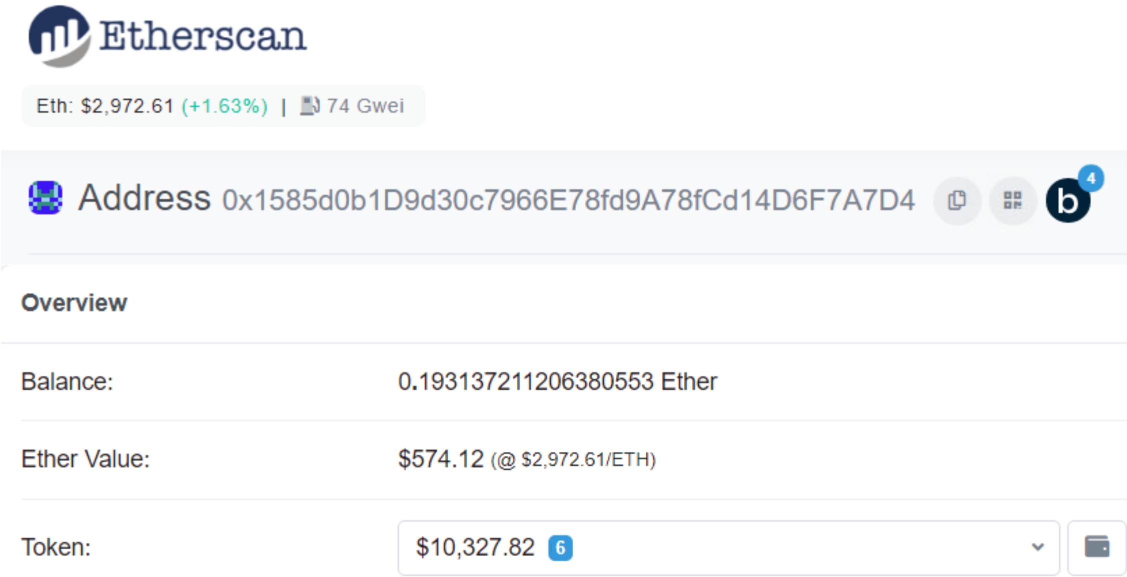
0x1585d0b1D...

Root Address
0x1585d0b1D9d30c7966E78fd9A78fC…

Watch

Balance:	0.193…	ETH
Sent:	11.311…	ETH
Received:	11.712…	ETH
Total Fees:	0.207…	ETH

The address appears to have an active balance of 0,193 Ether. At the time of writing this is just over $ 574, which might not be enough to start thinking about criminal asset seizure. However, when we analyse this address on Etherscan, we see something else:



Etherscan

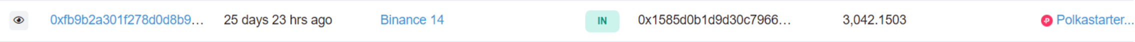
Eth: $2,972.61 (+1.63%) | 74 Gwei

Address 0x1585d0b1D9d30c7966E78fd9A78fCd14D6F7A7D4

Overview

Balance:	0.193137211206380553 Ether
Ether Value:	$574.12 (@ $2,972.61/ETH)
Token:	$10,327.82 6

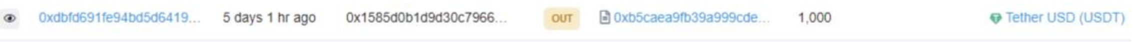
This address also holds a token balance of $ 10.327,82! When clicking on the arrow or wallet symbol on the right, we can see the detailed balance. It turns out this address holds over $ 9.000 in Polkastarter token, more than $ 2.000 in Tether (USDT) and smaller amounts in USD Coin and some other not very well-known coins. When we look at the ‘Erc20 Token Txns’ tab, we can obtain more information on these tokens. An example below:



0xfb9b2a301f278d0d8b9…	25 days 23 hrs ago	Binance 14	IN	0x1585d0b1d9d30c7966…	3,042.1503	Polkastarter…

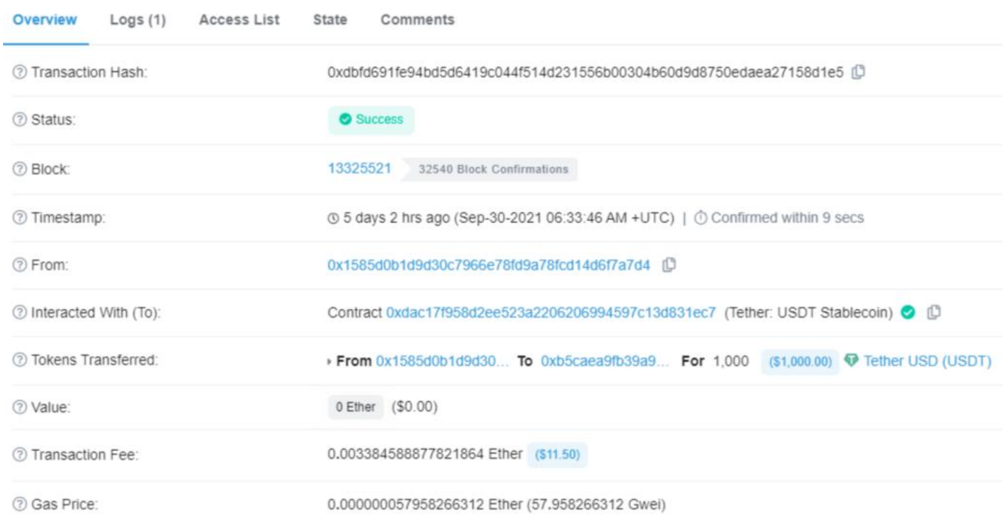
Part of the Polkastarter tokens seem to come from exchange Binance. This could indicate that the owner of the account we are looking at, also has an account at Binance, where they may have purchased these tokens.

Looking at another token transaction from this address, we see the following:



0xdbfd691fe94bd5d6419…	5 days 1 hr ago	0x1585d0b1d9d30c7966…	OUT	0xb5caea9fb39a999cde…	1,000	Tether USD (USDT)

We see that the address transferred tokens to another address that holds a smart contract as well. When clicking on the transaction hash, we see that the address 0x1585d0b1D9d30c7966E78fd9A78fCd14D6F7A7D4 sent 1.000 Tether (which should always be $ 1.000) for this transaction:

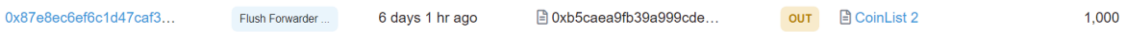


Overview Logs (1) Access List State Comments

Transaction Hash:	0xdbfd691fe94bd5d6419c044f514d231556b00304b60d9d8750edaea27158d1e5
Status:	Success
Block:	13325521 32540 Block Confirmations
Timestamp:	5 days 2 hrs ago (Sep-30-2021 06:33:46 AM +UTC) | Confirmed within 9 secs
From:	0x1585d0b1d9d30c7966e78fd9a78fcd14d6f7a7d4
Interacted With (To):	Contract 0xdac17f958d2ee523a2206206994597c13d831ec7 (Tether: USDT Stablecoin)
Tokens Transferred:	From 0x1585d0b1d9d30… To 0xb5caea9fb39a9… For 1,000 ($1,000.00) Tether USD (USDT)
Value:	0 Ether ($0.00)
Transaction Fee:	0.003384588877821864 Ether ($11.50)
Gas Price:	0.000000057958266312 Ether (57.958266312 Gwei)

The user needed gas to initiate this transaction, but did not transfer any other Ether, only USDT.

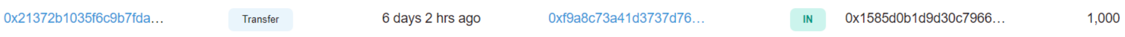
When we further follow this transaction by clicking on the receiving address 0xb5caea…, we see that the 1.000 USDT (and all other transactions) most likely ended up at exchange ‘Coinlist.co’:



0x87e8ec6ef6c1d47caf3…	Flush Forwarder …	6 days 1 hr ago	0xb5caea9fb39a999cde…	OUT	CoinList 2	1,000

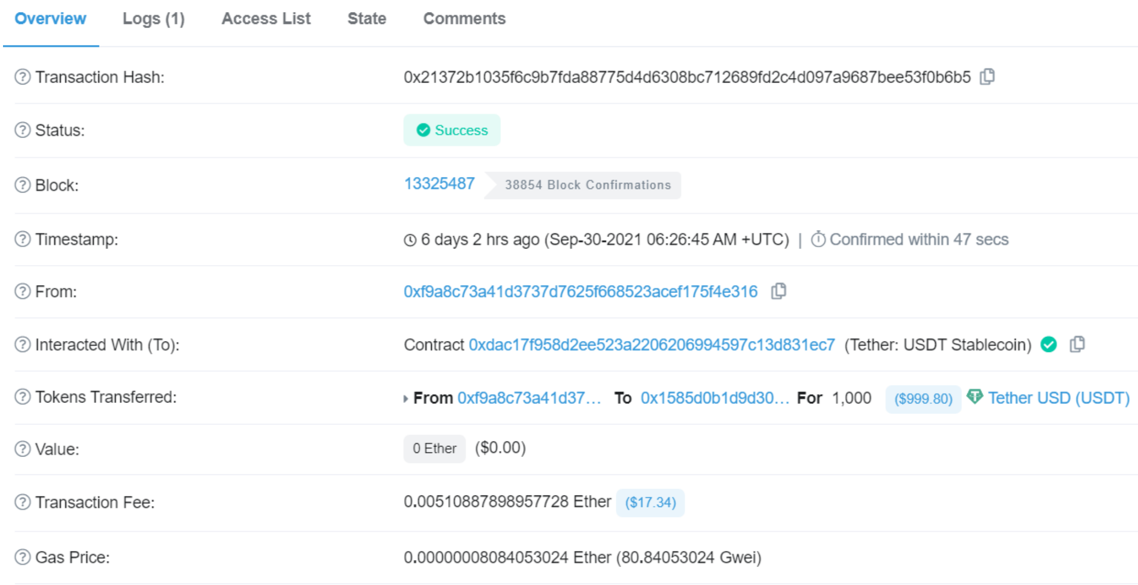
When looking at the contract at this address, we see that it is called ‘Forwarder’. All transactions are forwarded to the owner of the contract.

Below, we also want to show you an opposite type of transaction, where the address receives USDT.



0x21372b1035f6c9b7fda…	Transfer	6 days 2 hrs ago	0xf9a8c73a41d3737d76…	IN	0x1585d0b1d9d30c7966…	1,000

When we click on the transaction hash (on the left), we see the following:

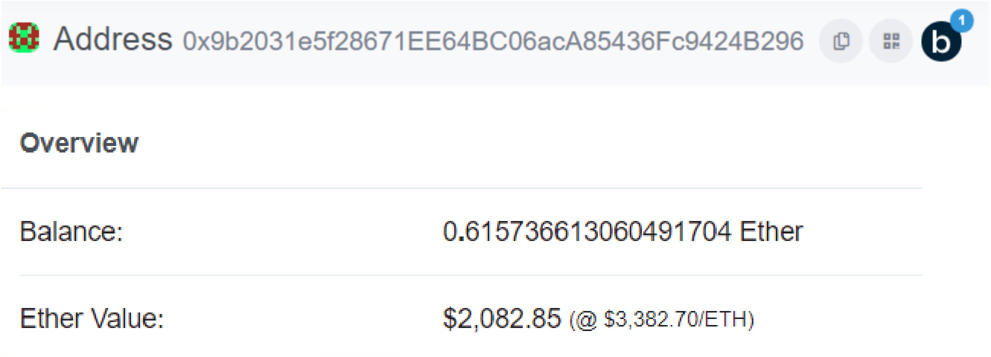


? Transaction Hash:	0x21372b1035f6c9b7fda88775d4d6308bc712689fd2c4d097a9687bee53f0b6b5
? Status:	✓ Success
? Block:	13325487 38854 Block Confirmations
? Timestamp:	6 days 2 hrs ago (Sep-30-2021 06:26:45 AM +UTC) | Confirmed within 47 secs
? From:	0xf9a8c73a41d3737d7625f668523acef175f4e316
? Interacted With (To):	Contract 0xdac17f958d2ee523a2206206994597c13d831ec7 (Tether: USDT Stablecoin) ✓
? Tokens Transferred:	**From** 0xf9a8c73a41d37… **To** 0x1585d0b1d9d30… **For** 1,000 ($999.80) Tether USD (USDT)
? Value:	0 Ether ($0.00)
? Transaction Fee:	0.00510887898957728 Ether ($17.34)
? Gas Price:	0.00000008084053024 Ether (80.84053024 Gwei)

Similarly, here we see that gas was needed to initiate the transaction, but no further Ether was sent. From the transaction details alone, it can be a bit confusing to see who sent and received a token. Therefore, we recommend to always look at the transactions tab as well, to see if the transaction was 'IN' (incoming) or 'OUT' (outgoing).

Some famous examples of tokens created with ERC20 include stablecoin Tether (USDT)[10], Binance Coin (BNB) and ChainLink (LINK)[11]. It must be noted that some of these tokens also run on other blockchains, meaning that investigative leads can sometimes be spread across platforms and chains.

For example, when looking at address 0x9b2031e5f28671EE64BC06acA85436Fc9424B296, we see the following balance on Etherscan:



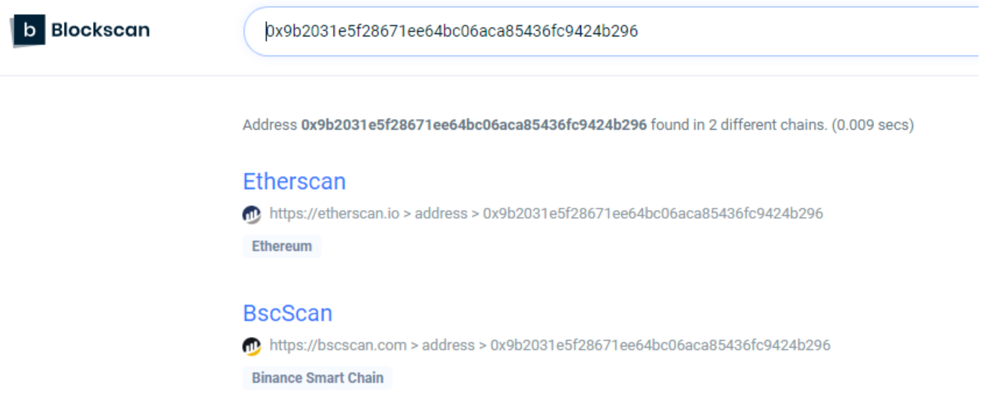
Address 0x9b2031e5f28671EE64BC06acA85436Fc9424B296

Overview

Balance:	0.615736613060491704 Ether
Ether Value:	$2,082.85 (@ $3,382.70/ETH)

When looking at the black 'b', we see a blue '1'. This means that this address holds tokens on one other blockchain. When clicking on it, we see the relevant blockchains:

[10] https://Etherscan.io/token/0xdac17f958d2ee523a2206206994597c13d831ec7
[11] https://Etherscan.io/token/0x514910771af9ca656af840dff83e8264ecf986ca



Blockscan

0x9b2031e5f28671ee64bc06aca85436fc9424b296

Address **0x9b2031e5f28671ee64bc06aca85436fc9424b296** found in 2 different chains. (0.009 secs)

Etherscan

https://etherscan.io > address > 0x9b2031e5f28671ee64bc06aca85436fc9424b296

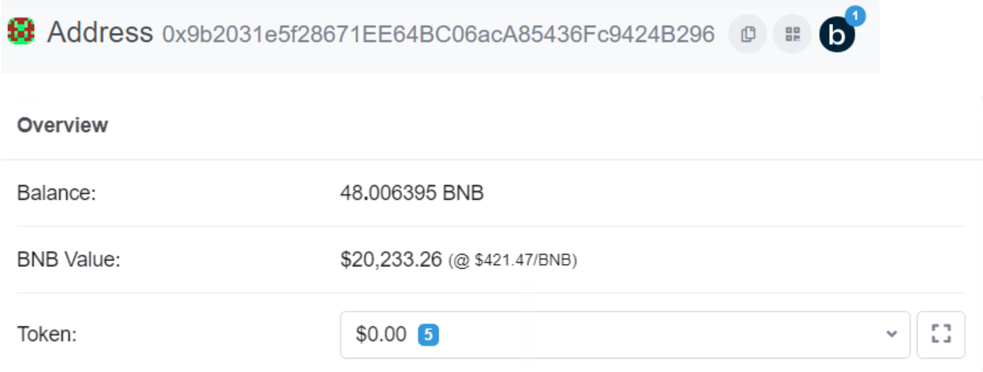
Ethereum

BscScan

https://bscscan.com > address > 0x9b2031e5f28671ee64bc06aca85436fc9424b296

Binance Smart Chain

We have just seen Etherscan, so we click on BscScan, a block explorer for Binance 'Smart Chain'[12]. We see here that the address holds another $ 20.000 in BNB!



Address 0x9b2031e5f28671EE64BC06acA85436Fc9424B296

Overview

Balance:	48.006395 BNB
BNB Value:	$20,233.26 (@ $421.47/BNB)
Token:	$0.00 5

In some cases, the address can be used on various blockchains, such as Polygon (Matic), HECO chain, Fantom and different types of testnets. Testnets are not relevant for asset seizure, as they do not contain 'real' coins, but are used for testing purposes.

Investigation tips

- Never forget to check a token balance of an Ether address. It may hold tokens that may be worth a lot. These are not always shown in tracing tools and can be easily overlooked.
- When looking at the 'Erc20 Token Txns' tab more information can be gained on token balances and their origin and destination.
- Be aware that one address may be used by a suspect on various blockchains, such as Ethereum, Binance Smart Chain and Polygon, and can hold tokens on all of them.

[12] While this block explorer was created by Binance, it runs on decentralised nodes and they do not have information on all transactions that you can see on this platform. Still, as Binance's native coin BNB is used for paying fees, it is in many cases likely that transactions will (at some point) lead to Binance.

Understanding and investigating smart contracts

Smart contracts are an important element of Ethereum. They are pieces of code that will run when certain prerequisites are met. They are often a type of contract between a buyer and seller. Smart contracts use the same address format as the accounts. When you see an Ethereum address sending funds to another Ethereum address, you are sometimes actually observing an account interacting with a smart contract.

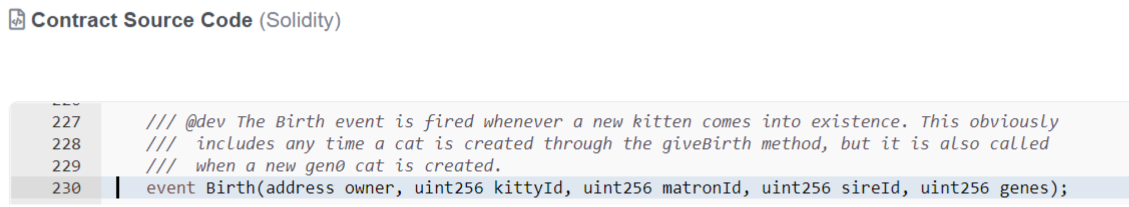
Smart contracts are in the end just a type of Ethereum account that have a balance and can send transactions. They 'live' in a specific address on the Ethereum blockchain. In the smart contract you can always see who (more specifically: what Ether address) has created the contract. Smart contracts attempt to, in some cases, replace intermediaries such as exchanges or banks, as they can, for example, automate cryptocurrency conversions and the 'printing' of cryptocurrency (i.e. token creation).

Smart contracts are programs that run on the Ethereum blockchain and operate by 'if, then' logic, meaning: that **if** the requirements of the contract are met, **then** a certain action will be executed. This can, for example, be a conversion of Ethereum for another cryptocurrency at a decentralised exchange. Famous types of services running on smart contracts are decentralised exchanges (such as Uniswap), Decentralised Autonomous Organisations (or 'DAOs', such as MakerDAO) and decentralised applications (or 'dapps', such as Serious Dice) and non-fungible tokens (such as CryptoKitties). To better understand how such services running on smart contracts work, it makes sense to dive deeper into the code of the smart contract and to look at what happens when transfers are made.

Let's imagine you have overheard your suspects in a wiretap, saying that they decided to launder all of his criminally gained Ether by purchasing hundreds of cute non-fungible tokens: CryptoKitties! Before you have any idea how to find and seize the CryptoKitties, it is a good idea to understand how they work first.

How would you go about better understanding CryptoKitties? By analysing the smart contract. Analysing the code of a smart contract can show ownership, total supply, balance, creation date and more. In the case of CryptoKities, we can find the smart contract when we go to its dedicated Ether address[13] and click on the tab 'Contract'.

We can for example learn more about the creation (birth) of a CryptoKitty from the Contract Source Code:

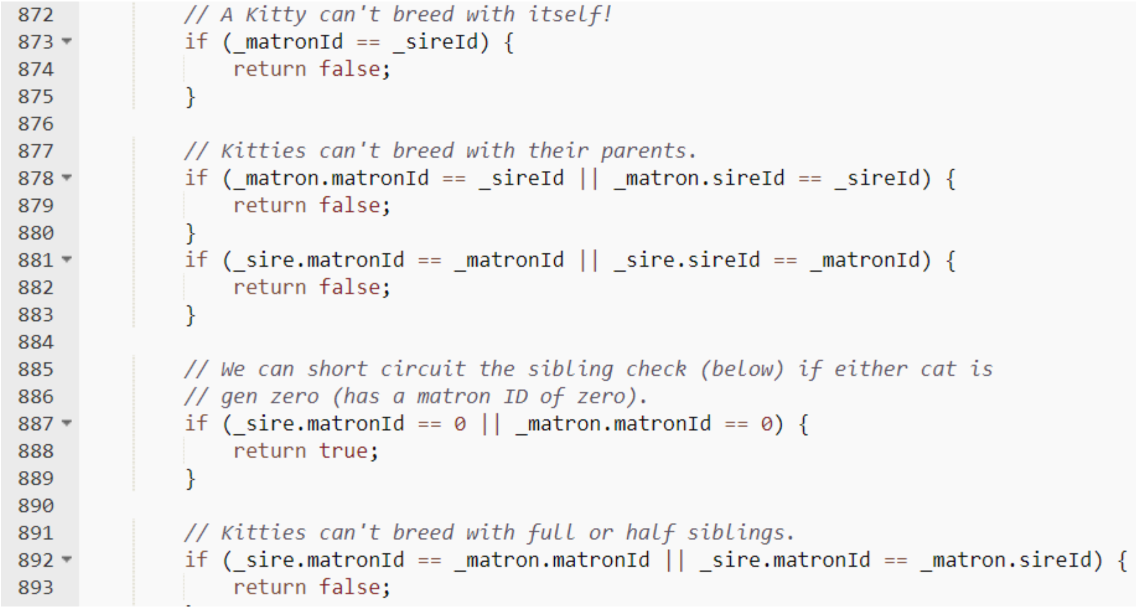


```
/// @dev The Birth event is fired whenever a new kitten comes into existence. This obviously
///  includes any time a cat is created through the giveBirth method, but it is also called
///  when a new gen0 cat is created.
event Birth(address owner, uint256 kittyId, uint256 matronId, uint256 sireId, uint256 genes);
```

It shows that every CryptoKitty that is created in a 'Birth' is owned by an address and has a kittyID, matronID, sireID and genes. This for example already tells you that a CryptoKitty has a mother (matron) and a father (sire).

When digging deeper into the code, we can find some more funny rules, such as these:

[13] 0x06012c8cf97BEaD5deAe237070F9587f8E7A266d



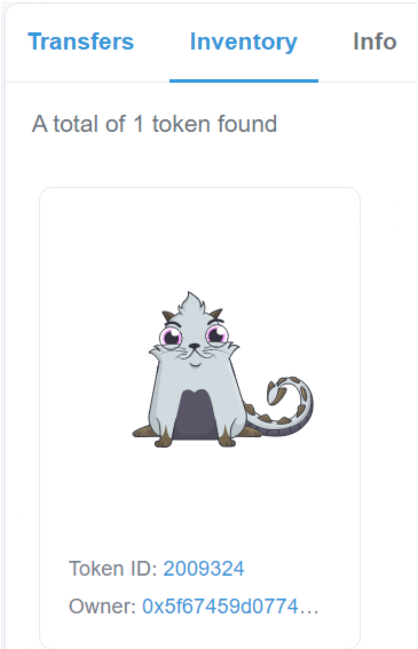
```
// A Kitty can't breed with itself!
if (_matronId == _sireId) {
    return false;
}

// Kitties can't breed with their parents.
if (_matron.matronId == _sireId || _matron.sireId == _sireId) {
    return false;
}
if (_sire.matronId == _matronId || _sire.sireId == _matronId) {
    return false;
}

// We can short circuit the sibling check (below) if either cat is
// gen zero (has a matron ID of zero).
if (_sire.matronId == 0 || _matron.matronId == 0) {
    return true;
}

// Kitties can't breed with full or half siblings.
if (_sire.matronId == _matron.matronId || _sire.matronId == _matron.sireId) {
    return false;
```

Now, let's say you find hundreds of pictures of CryptoKitties with their IDs written on them, during a house search of your suspect. What could you do? Let's start with one CryptoKitty.

When typing in the word 'CryptoKitties' on Etherscan, you will find their page here: https://Etherscan.io/token/0x06012c8cf97bead5deae237070f9587f8e7a266d. When clicking on the 'Inventory' tab, you will see all CryptoKitties in existence. When looking for any tokenID of a CryptoKitty, you can change the above link by adding **a=** and the **KittyID** at the end. So, for example, if you found the following ID: 2009324, you will get the below link:

https://Etherscan.io/token/0x06012c8cf97bead5deae237070f9587f8e7a266d?a=2009324

When going to this link and clicking on 'inventory', we see a CryptoKitty:

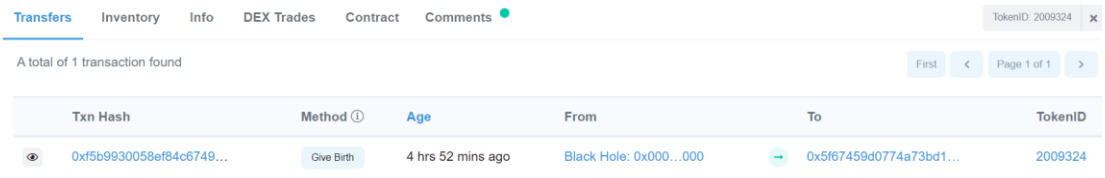


A total of 1 token found

Token ID: 2009324

Owner: 0x5f67459d0774...

When clicking on the Transfers tab, we see details of when the CryptoKitty was born:

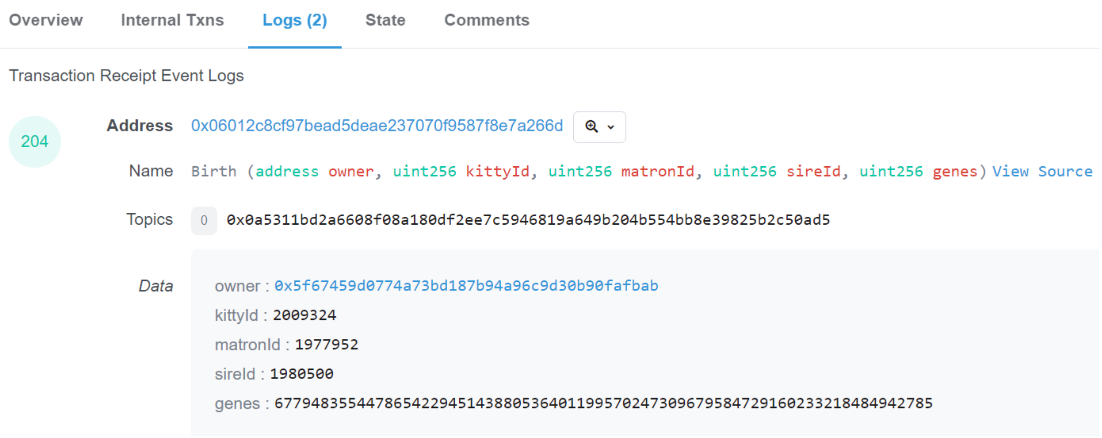


A total of 1 transaction found

Txn Hash	Method	Age	From	To	TokenID
0xf5b9930058ef84c6749…	Give Birth	4 hrs 52 mins ago	Black Hole: 0x000…000	0x5f67459d0774a73bd1…	2009324

We can see here that the CryptoKitty came from a ‘Black Hole’ or address 0x0000000000000000000000000000000000000000. This means that it was created or ‘born’ at this moment. This process is sometimes referred to as ‘minting’.

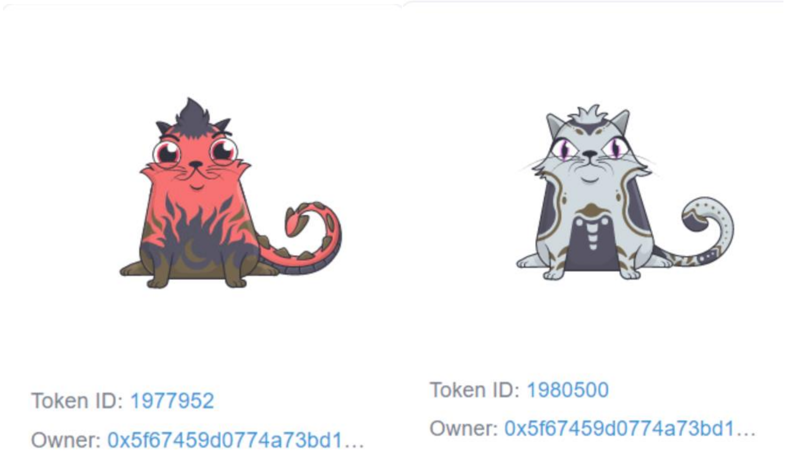
When clicking the Txn Hash and then ‘logs’, we find further information:



Transaction Receipt Event Logs

```
204   Address  0x06012c8cf97bead5deae237070f9587f8e7a266d
      Name     Birth (address owner, uint256 kittyId, uint256 matronId, uint256 sireId, uint256 genes) View Source
      Topics   0  0x0a5311bd2a6608f08a180df2ee7c5946819a649b204b554bb8e39825b2c50ad5
      Data     owner : 0x5f67459d0774a73bd187b94a96c9d30b90fafbab
               kittyId : 2009324
               matronId : 1977952
               sireId : 1980500
               genes : 677948355447865422945143880536401199570247309679584729160233218484942785
```

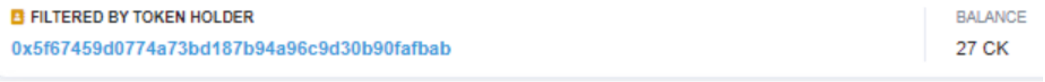
Here we can see the matronID (mother) and sireID (father) of our CryptoKitty. When we use the URL ‘trick’ again as described above, we find two CryptoKitties, the mother and father of 2009324:



Token ID: 1977952
Owner: 0x5f67459d0774a73bd1…

Token ID: 1980500
Owner: 0x5f67459d0774a73bd1…

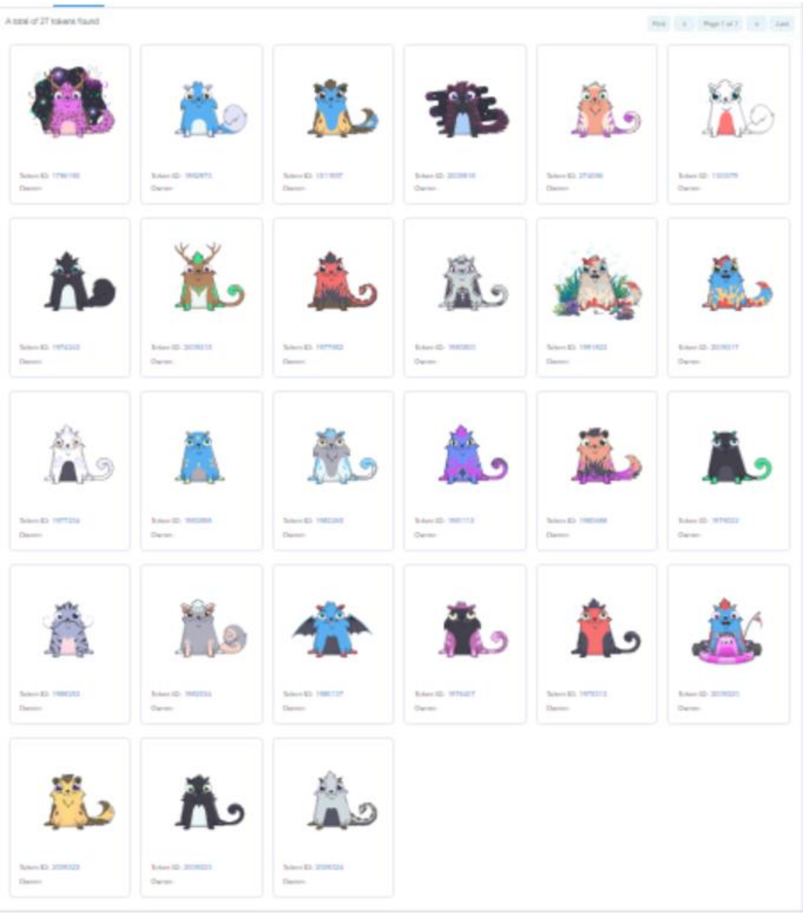
Interestingly, we see the parents have the same owner as the child. When clicking on this address, we are sent to the CryptoKitties address. However, Etherscan filters the results for us and shows the number of CryptoKitties (CK) held by address 0x5f67459d….



FILTERED BY TOKEN HOLDER
0x5f67459d0774a73bd187b94a96c9d30b90fafbab

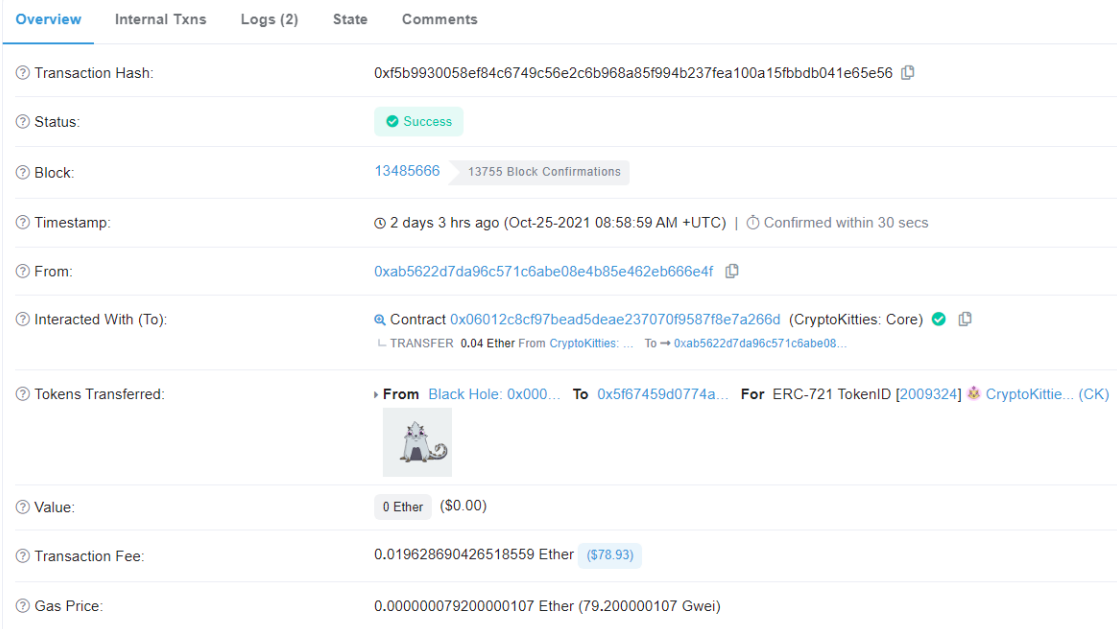
BALANCE
27 CK

When clicking on 'inventory' we see the entire collection of the CryptoKitties held by this address:



This person is a kitty hoarder!

We can even find further information from before the 'birth', i.e. the payment for the creation of the CryptoKitty. When we click on the transaction hash from the transfers tab, we see the following:

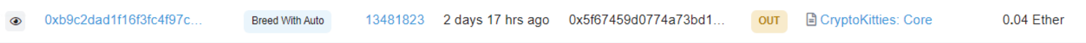


Transaction Hash:	0xf5b9930058ef84c6749c56e2c6b968a85f994b237fea100a15fbbdb041e65e56
Status:	Success
Block:	13485666 13755 Block Confirmations
Timestamp:	2 days 3 hrs ago (Oct-25-2021 08:58:59 AM +UTC) | Confirmed within 30 secs
From:	0xab5622d7da96c571c6abe08e4b85e462eb666e4f
Interacted With (To):	Contract 0x06012c8cf97bead5deae237070f9587f8e7a266d (CryptoKitties: Core) └ TRANSFER 0.04 Ether From CryptoKitties: ... To → 0xab5622d7da96c571c6abe08...
Tokens Transferred:	From Black Hole: 0x000... To 0x5f67459d0774a... For ERC-721 TokenID [2009324] CryptoKittie... (CK)
Value:	0 Ether ($0.00)
Transaction Fee:	0.019628690426518559 Ether ($78.93)
Gas Price:	0.000000079200000107 Ether (79.200000107 Gwei)

We see that before the kitty was transferred from a ‘Black Hole’ to address 0x5f67…., this address interacted with contract 0x06012c… (the CryptoKitty smart contract). A transfer of 0.04 Ether was made! When we go to the address 0x5f67 and click on transactions, we see that many transactions were made to the CryptoKitty smart contract.

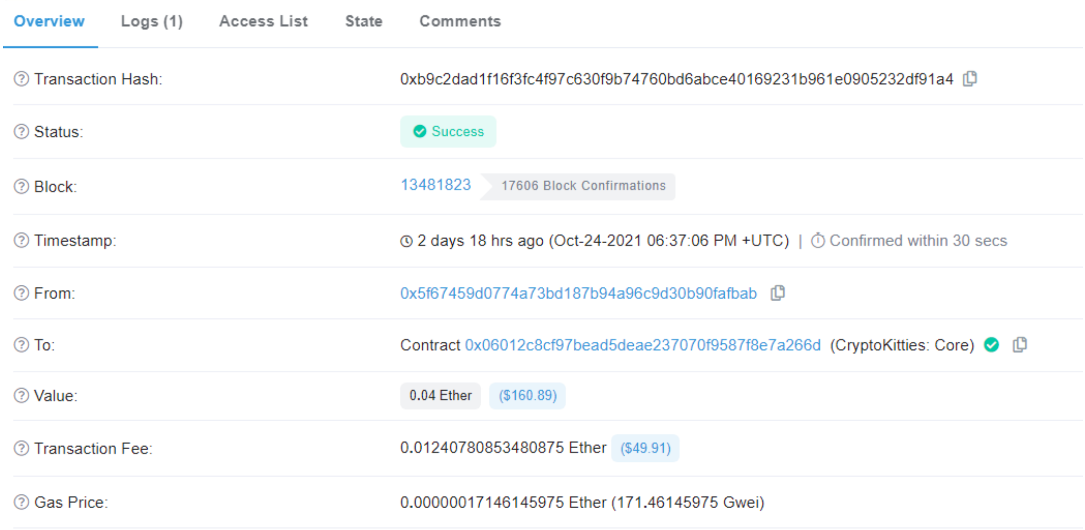
However, when we spent some time looking at the different transaction hashes and event logs, we find the following:

- A transaction of 0.04 Ether to the CryptoKitty smart contract:



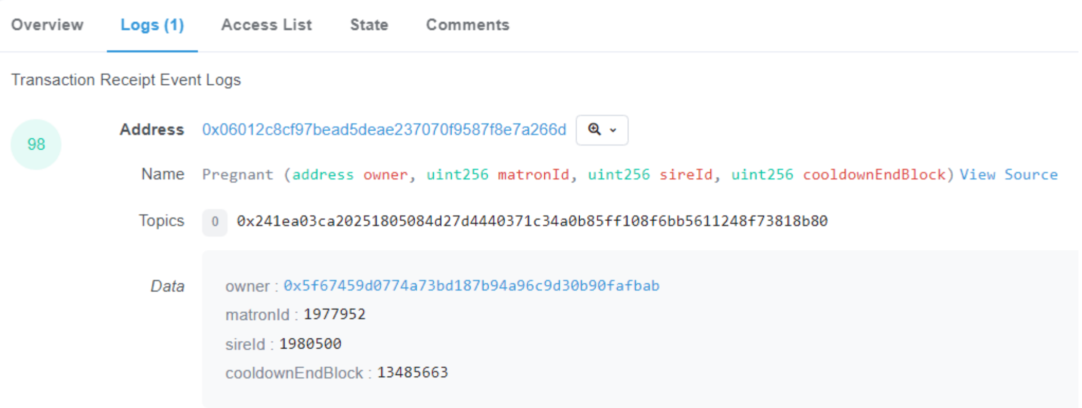
0xb9c2dad1f16f3fc4f97c…	Breed With Auto	13481823	2 days 17 hrs ago	0x5f67459d0774a73bd1…	OUT	CryptoKitties: Core	0.04 Ether

- More details of the transaction:



Transaction Hash:	0xb9c2dad1f16f3fc4f97c630f9b74760bd6abce40169231b961e0905232df91a4
Status:	Success
Block:	13481823 17606 Block Confirmations
Timestamp:	2 days 18 hrs ago (Oct-24-2021 06:37:06 PM +UTC) | Confirmed within 30 secs
From:	0x5f67459d0774a73bd187b94a96c9d30b90fafbab
To:	Contract 0x06012c8cf97bead5deae237070f9587f8e7a266d (CryptoKitties: Core)
Value:	0.04 Ether ($160.89)
Transaction Fee:	0.01240780853480875 Ether ($49.91)
Gas Price:	0.00000017146145975 Ether (171.46145975 Gwei)

- The matronID and sireID of our CryptoKitty’s parents. Evidence that a payment was made to let the parents mate:



Transaction Receipt Event Logs

98

Address 0x06012c8cf97bead5deae237070f9587f8e7a266d

Name `Pregnant (address owner, uint256 matronId, uint256 sireId, uint256 cooldownEndBlock)` View Source

Topics 0 `0x241ea03ca20251805084d27d4440371c34a0b85ff108f6bb5611248f73818b80`

Data

```
owner : 0x5f67459d0774a73bd187b94a96c9d30b90fafbab
matronId : 1977952
sireId : 1980500
cooldownEndBlock : 13485663
```

Of course, it may be quite unlikely that your suspect launders money through CryptoKitties. Still, intelligent criminals may (in the future) try to use these type of purchases for money laundering. As you can find information on smart contracts in the same way, we wanted to explain this process to you. If you want to find out anything about a smart contract, you can follow the above processes to learn more about it.

You can have a look yourself at some other details of the code of the smart contract of CryptoKitties and see if you can discover other interesting details (for example have a look at the different roles of the CEO, CFO and COO of CryptoKitties; can you discover their Ether addresses?).

Also, have a look at some other smart contracts to see what you can find out about their workings.

By viewing interactions between the suspect and the smart contract, investigators can also find out whether a suspect has deposited, withdrawn or traded cryptocurrency at a decentralised exchange. We will discuss this below in the 'DeFi' section.

Investigation tips

- Smart contracts can give an investigator insights into ownership, technical characteristics and creators of tokens on the Ethereum network.
- Further analysis on Etherscan can lead to many leads on owners of tokens, number of purchases, dates and time, and amounts spent.

DeFi

Decentralised Finance (DeFi) offers services similar to traditional finance, but does so without intermediaries, i.e. companies or other entities. The platforms used are pieces of code (smart contracts) and facilitate direct interaction between traders. DeFi is essentially a collection of smart contracts offered through a platform that users can directly connect their hardware or software wallets to, to buy, sell, or swap coins or tokens. The platform only facilitates the trades, but there is no central party in the middle. Famous examples of DeFi exchanges include SushiSwap and Uniswap.

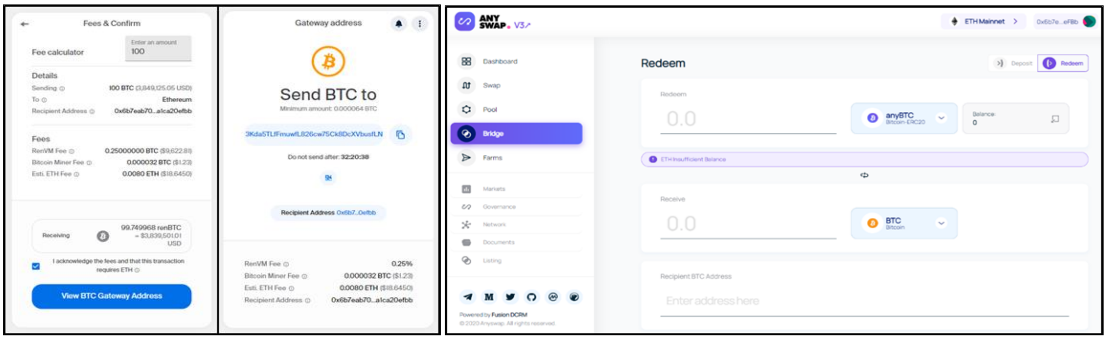
The DeFi ecosystem allows users to supply liquidity (cryptocurrencies or tokens) to platforms via smart contracts. These are called 'liquidity pools'. For a small reward, users make sure DeFi platforms have liquidity for other users to trade on the platform. There are also examples of DeFi platforms that offer services for borrowing and earning interest on cryptocurrencies, without the intervention of third parties, such as AAVE and Yearn.finance.

For now, the most relevant development in the field of DeFi for investigators is the exchange of tokens without intervention of an intermediary. In theory, this complicates the job of an investigator, as there is no cooperative exchange to send a subpoena to. DeFi exchanges can not help with requests, as they are pieces of code and execute transactions automatically without employees looking at the transactions. Still, there often are some possibilities in tracing these type of transactions. As everything is recorded on the blockchain and is publically available, it allows for the investigation of the swaps performed on such DeFi platforms by following the code in the contract.

At traditional exchanges it is not possible to swap, for example, Bitcoin directly against an ERC20 token. To fix this, some DeFi companies created specific tokens that have a perfect 1:1 correlation between a crypto asset in their reserves and the token in circulation. This is similar to stablecoins, such as Tether and USD Coin, where one 'coin' always equals one USD in fiat currency. However, these ERC20 tokens serve as a bridge between the Bitcoin and Ethereum blockchain: WBTC, renBTC, anyBTC.

The DeFi swap process is as follows (also works the other way around, token_BTC to BTC): Alice sends 100 BTC to the DeFi deposit address (reserve). The service mints (creates) 100 token_BTC through a smart contract on Ethereum (minus fees). The 100 token_BTC are received on Alice's Ethereum wallet.

There are several scenarios when investigating transactions going into DeFi platforms:



Fees & Confirm

Fee calculator: 100

Details
Sending: 100 BTC (3,849,125.05 USD)
To: Ethereum
Recipient Address: 0x6b7eab70...a1ca20efbb

Fees
RenVM Fee: 0.25000000 BTC ($9,622.81)
Bitcoin Miner Fee: 0.000032 BTC ($1.23)
Esti. ETH Fee: 0.0080 ETH ($18.6450)

Receiving: 99.749968 renBTC = $3,839,501.01 USD

☑ I acknowledge the fees and that this transaction requires ETH

Gateway address

Send BTC to

Minimum amount: 0.000064 BTC

3Kda5TLfFmuwfL826cw75Ck8DcXVbusfLN

Do not send after: 32:20:38

Recipient Address 0x6b7..0efbb

RenVM Fee: 0.25%
Bitcoin Miner Fee: 0.000032 BTC ($1.23)
Esti. ETH Fee: 0.0080 ETH ($18.6450)
Recipient Address: 0x6b7eab70...a1ca20efbb

Redeem

Redeem: 0.0 anyBTC Bitcoin-ERC20 Balance: 0

ETH Insufficient Balance

Receive: 0.0 BTC Bitcoin

Recipient BTC Address: Enter address here

Powered by Fusion DCRM
© 2020 Anyswap. All rights reserved.

- Best case scenario: When discovering a transaction deposited into a DeFi service investigators will have to perform further tracing in another blockchain and not anymore in the one investigated up until this point. Carefulness is required! The difficult part is to know which blockchain / new asset should be investigated.

- Worst case scenario: The main issue for investigators is when the tracing tool they are using does not identify the deposit into the DeFi service. In the best case they will notice that something is wrong while tracing and will stop tracing forward. In the worst case, they will continue tracing and will start discovering elements that are not related to their investigation.

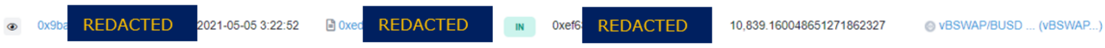
So how can we identify transactions going into DeFi platforms and easily investigate their smart contracts? We will use a case with a multimillion hack as an example.

DeFi hack example

Criminals are using cross-chain liquidity and the bridges between Bitcoin and smart chains protocols, such as Ethereum or Binance Smart Chain, without having to rely on a centralised and regulated exchanges. DeFi exchanges are used anonymously, without any form of registration, identification or KYC/AML rules. They also give access to thousands of tokens that can be swapped instantly with a few clicks. This creates difficulties for LEAs in tracing, especially if the investigator is not confident in interpreting smart contracts. Tracing tools also often do not properly cluster and attribute DeFi structures on the Bitcoin blockchain yet. We recommend investigators to be really careful while tracing, especially with large BTC transactions.

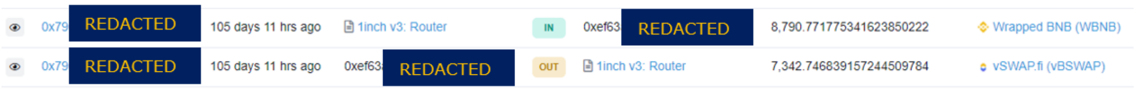
Still, there are possibilities in investigating decentralised exchanges. We can have a look at a hack on the vStake smart contract of the DeFi company 'valuedefi.io'. A loss of millions was reported.

On the 5th of May 2021, an unknown perpetrator exploited the smart contract of the vStake pool by using a specific function that had led to the transfer of the reserve of the pool corresponding to ***10 839 vBSWAP/BUSD*** to his own BSC address ***0xef6-REDACTED***.



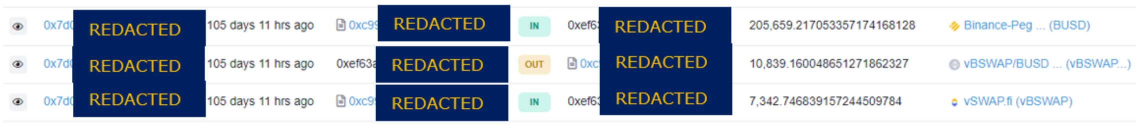
0x9ba REDACTED 2021-05-05 3:22:52 0xed REDACTED IN 0xef6 REDACTED 10,839.160048651271862327 vBSWAP/BUSD ... (vBSWAP...)

Immediately after gaining access to the **10 839 vBSWAP/BUSD**, the suspect removed all the liquidity from the smart contract and received **7 342 vBSWAP** and **205 659 BUSD.**



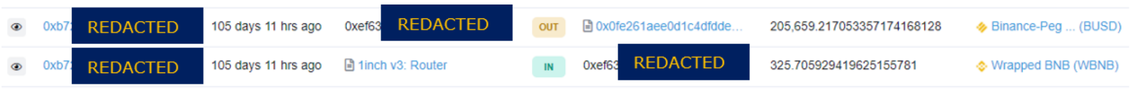
0x79 REDACTED	105 days 11 hrs ago	1inch v3: Router	IN	0xef63 REDACTED	8,790.771775341623850222	Wrapped BNB (WBNB)
0x79 REDACTED	105 days 11 hrs ago	0xef63 REDACTED	OUT	1inch v3: Router	7,342.746839157244509784	vSWAP.fi (vBSWAP)

Immediately again, the suspect converted the **7 342 vBSWAP** into **8 790 Wrapped BNB** (WBNB) using **1inch** decentralized exchange platform.



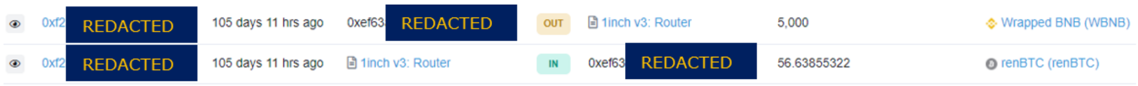
0x7d0 REDACTED	105 days 11 hrs ago	0xc9 REDACTED	IN	0xef6 REDACTED	205,659.217053357174168128	Binance-Peg ... (BUSD)
0x7d0 REDACTED	105 days 11 hrs ago	0xef63 REDACTED	OUT	0xc REDACTED	10,839.160048651271862327	vBSWAP/BUSD ... (vBSWAP...)
0x7d0 REDACTED	105 days 11 hrs ago	0xc9 REDACTED	IN	0xef6 REDACTED	7,342.746839157244509784	vSWAP.fi (vBSWAP)

The suspect did the same with the **205 659 BUSD** converted into **325 Wrapped BNB** (WBNB).



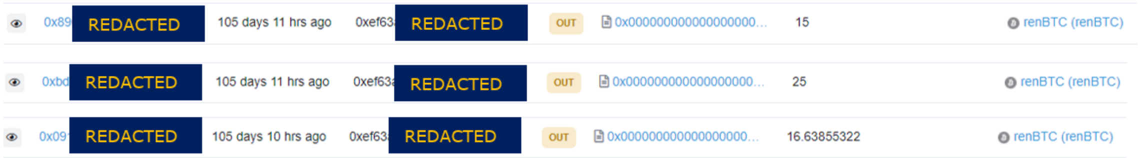
0xb7 REDACTED	105 days 11 hrs ago	0xef63 REDACTED	OUT	0x0fe261aee0d1c4dfdde...	205,659.217053357174168128	Binance-Peg ... (BUSD)
0xb7 REDACTED	105 days 11 hrs ago	1inch v3: Router	IN	0xef63 REDACTED	325.705929419625155781	Wrapped BNB (WBNB)

Still using **1inch**, the suspect converted subsequently the freshly received WBNB in to **56.63 RenBTC**.



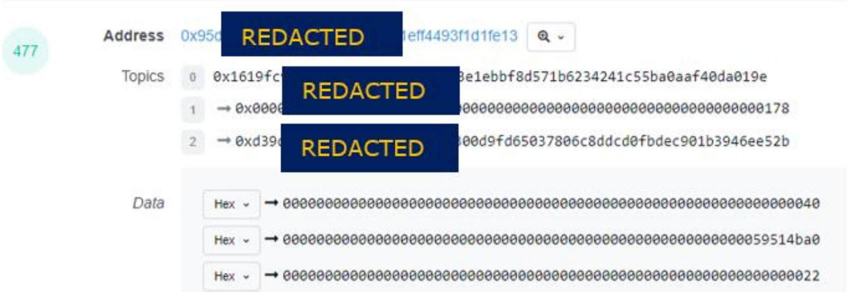
0xf2 REDACTED	105 days 11 hrs ago	0xef63 REDACTED	OUT	1inch v3: Router	5,000	Wrapped BNB (WBNB)
0xf2 REDACTED	105 days 11 hrs ago	1inch v3: Router	IN	0xef63 REDACTED	56.63855322	renBTC (renBTC)

We can see that right after receiving the RenBTC the perpetrator started to spend them in 3 different transactions to a strange BSC smart contract address (0x00000000000…).



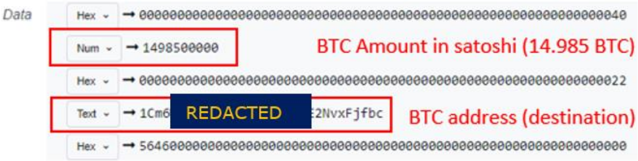
0x89 REDACTED	105 days 11 hrs ago	0xef63 REDACTED	OUT	0x000000000000000000...	15	renBTC (renBTC)
0xbd REDACTED	105 days 11 hrs ago	0xef63 REDACTED	OUT	0x000000000000000000...	25	renBTC (renBTC)
0x09 REDACTED	105 days 10 hrs ago	0xef63 REDACTED	OUT	0x000000000000000000...	16.63855322	renBTC (renBTC)

This address corresponds to a specific function into the smart contract that is doing a BURN (destruction) of the token. But, what happened to the renBTC? Is the suspect crazy? In fact, they just converted renBTC into BTC using the REN bridge service. Should you ask RENproject.io what happened to the renBTC? No, there is an easier way to find what you are looking for. For this purpose, you can click on the Transaction hash and then on "Logs (x)" in the transaction details page. You should get the details shown below:



```
477   Address  0x95d REDACTED 1eff4493f1d1fe13
      Topics   0   0x1619fc REDACTED 3e1ebbf8d571b6234241c55ba0aaf40da019e
               1   → 0x0000 REDACTED 000000000000000000000000000000000000178
               2   → 0xd39 REDACTED 00d9fd65037806c8ddcd0fbdec901b3946ee52b
      Data     Hex → 0000000000000000000000000000000000000000000000000000000000000040
               Hex → 000000000000000000000000000000000000000000000000000000000059514ba0
               Hex → 0000000000000000000000000000000000000000000000000000000000000022
```

Nothing interesting here at first sight, a huge disappointment indeed. However if you convert the second line on the data field from HEX to NUM and the fourth (redacted above) from HEX to TEXT, you will get the following:

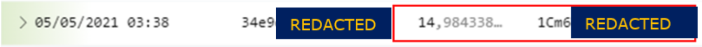


```
Data  Hex  → 0000000000000000000000000000000000000000000000000000000000000040
      Num  → 1498500000
      Hex  → 0000000000000000000000000000000000000000000000000000000000000022
      Text → 1Cm6 REDACTED E2NvxFjfbc
      Hex  → 5646000000000000000000000000000000000000000000000000000000000000
```

BTC Amount in satoshi (14.985 BTC)

BTC address (destination)

By looking at the BTC address discovered on the Bitcoin blockchain, we should see an incoming transaction of 14,985 BTC (minus Tx fee). Here is where the perpetrator transferred the stolen funds, but this is just the start of a long trail. Now the investigator can attempt to follow the BTC.



```
> 05/05/2021 03:38     34e9 REDACTED     14,984338…     1Cm6 REDACTED
```

Investigation tips

- Decentralized services can be investigated quite easily, if investigators know how to interpret a smart contract.
- Suspects may use DeFi exchanges to exchange one token for the other. This is not the end of your investigation, there are possibilities in tracing these conversions.
- Tracing tools are limited in terms of DeFi services’ identification and this could have a huge impact on an investigation. Therefore, we recommend to also use public blockchain explorers, such as Etherscan.

Non Fungible Tokens (NFTs)

Non-fungible tokens (NFTs) are digital goods that are unique, tradeable and (partly) stored and searchable through a blockchain. Recently, many pieces of collectibles and digital art have been sold as NFTs, meaning that these art pieces are recorded in the blockchain and have a unique hash value which enables the owner to prove that it is theirs. According to some, NFT was the word of the year 2021[14]. Famous platforms on which one can purchase and sell NFTs is OpenSea.io, Valuables and Makersplace. However, exchanges are also increasingly getting involved in the NFT trade, such as Binance, Coinbase and FTX.

Whereas EC3 has not yet seen many cases where NFTs were used by suspects, they can potentially be used for money laundering. Some possible criminal modi operandi with NFTs:

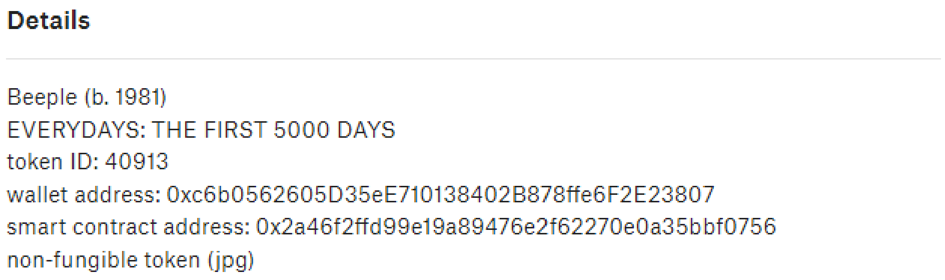
- Cryptocurrency coming from an illicit source could be used to purchase NFTs, after which they are sold again;

[14] https://decrypt.co/86742/nft-is-collins-dictionarys-2021-word-year

- Ownership of NFTs could be used as an 'explanation' for the large growth in fortune of a suspect, while in reality there is another source of criminality;
- NFTs can be stolen from artists if their wallet is hacked.

As NFTs are often created on platforms and signed with the private key of the wallet of the artist, this leaves them vulnerable to hacks. EC3 has seen a case in which an attacker obtained the private key of the MetaMask wallet of an NFT artist. The artist had created NFTs with the private key of the MetaMask wallet and received funds on the same address every time he sold an NFT. The hacker emptied the account every time the artist received funds, making it impossible for the artist to keep on selling the NFTs he created with the MetaMask wallet without losing his funds. These kind of new cases require novel approach by LEAs.

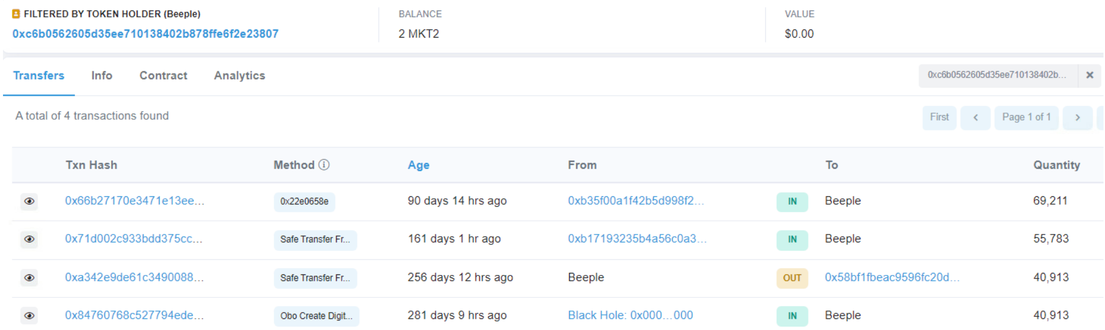
The movement of NFTs from one owner can generally be tracked relatively easily. Let's for example look at the most expensive NFT of all time: Beeple's 'Everydays: the First 5000 Days', which sold for over $ 69 million. As Etherscan has tagged Beeple's Ethereum address[15], we can investigate. By looking at open sources, we know that the piece was auctioned on the 11th of March 2021 at Christie's. When looking at their site we find some extra information about the piece:



Details

Beeple (b. 1981)
EVERYDAYS: THE FIRST 5000 DAYS
token ID: 40913
wallet address: 0xc6b0562605D35eE710138402B878ffe6F2E23807
smart contract address: 0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756
non-fungible token (jpg)

We do not know if the NFT was actually transferred on that day. But we know now that the token ID is 40913. We also see that the wallet address on Christie's site is the same as the one Etherscan labelled 'Beeple'. The smart contract is owned by Makersplace.com, a NFT marketplace, which we see at this link: https://etherscan.io/token/0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756. A trick in this case is to add **?a=** and the address of Beeple to this link, i.e.: https://Etherscan.io/token/0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756?a=0xc6b0562605d35ee710138402b878ffe6f2e23807. Now we see all the interactions of Beeple with this smart contract.



FILTERED BY TOKEN HOLDER (Beeple)
0xc6b0562605d35ee710138402b878ffe6f2e23807

BALANCE
2 MKT2

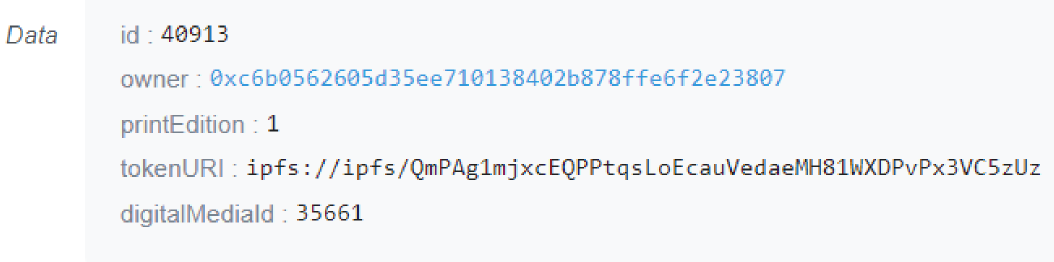
VALUE
$0.00

A total of 4 transactions found

	Txn Hash	Method	Age	From		To	Quantity
👁	0x66b27170e3471e13ee...	0x22e0658e	90 days 14 hrs ago	0xb35f00a1f42b5d998f2...	IN	Beeple	69,211
👁	0x71d002c933bdd375cc...	Safe Transfer Fr...	161 days 1 hr ago	0xb17193235b4a56c0a3...	IN	Beeple	55,783
👁	0xa342e9de61c3490088...	Safe Transfer Fr...	256 days 12 hrs ago	Beeple	OUT	0x58bf1fbeac9596fc20d...	40,913
👁	0x84760768c527794ede...	Obo Create Digit...	281 days 9 hrs ago	Black Hole: 0x000...000	IN	Beeple	40,913

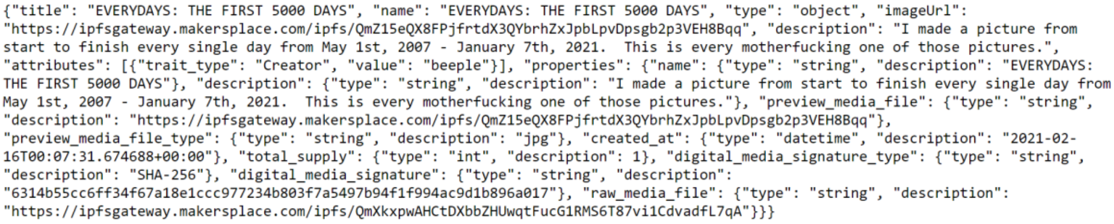
[15] 0xc6b0562605D35eE710138402B878ffe6F2E23807

The first transaction took place 281 days ago (at the time of writing) and shows the creation of the NFT on Makersplace. The transaction 256 days ago shows the movement of the NFT to the winner of the auction at Christie's. When we look at the minting transaction and click on 'logs' we see the following data about the NFT:



```
Data    id : 40913
        owner : 0xc6b0562605d35ee710138402b878ffe6f2e23807
        printEdition : 1
        tokenURI : ipfs://ipfs/QmPAg1mjxcEQPPtqsLoEcauVedaeMH81WXDPvPx3VC5zUz
        digitalMediaId : 35661
```

While the cryptographic data of NFTs is stored on the blockchain, the actual NFT (picture in this case) is not. In this case, it is stored on the Interplanatery File System, a distributed system for storing files. We can access it through the gateway ipfs.io[16], where we will find the following information:



```
{"title": "EVERYDAYS: THE FIRST 5000 DAYS", "name": "EVERYDAYS: THE FIRST 5000 DAYS", "type": "object", "imageUrl":
"https://ipfsgateway.makersplace.com/ipfs/QmZ15eQX8FPjfrtdX3QYbrhZxJpbLpvDpsgb2p3VEH8Bqq", "description": "I made a picture from
start to finish every single day from May 1st, 2007 - January 7th, 2021.  This is every motherfucking one of those pictures.",
"attributes": [{"trait_type": "Creator", "value": "beeple"}], "properties": {"name": {"type": "string", "description": "EVERYDAYS:
THE FIRST 5000 DAYS"}, "description": {"type": "string", "description": "I made a picture from start to finish every single day from
May 1st, 2007 - January 7th, 2021.  This is every motherfucking one of those pictures."}, "preview_media_file": {"type": "string",
"description": "https://ipfsgateway.makersplace.com/ipfs/QmZ15eQX8FPjfrtdX3QYbrhZxJpbLpvDpsgb2p3VEH8Bqq"},
"preview_media_file_type": {"type": "string", "description": "jpg"}, "created_at": {"type": "datetime", "description": "2021-02-
16T00:07:31.674688+00:00"}, "total_supply": {"type": "int", "description": 1}, "digital_media_signature_type": {"type": "string",
"description": "SHA-256"}, "digital_media_signature": {"type": "string", "description":
"6314b55cc6ff34f67a18e1ccc977234b803f7a5497b94f1f994ac9d1b896a017"}, "raw_media_file": {"type": "string", "description":
"https://ipfsgateway.makersplace.com/ipfs/QmXkxpwAHCtDXbbZHUwqtFucG1RMS6T87vi1CdvadfL7qA"}}}
```

If you click on the imageUrl link included in the above text, you will find a picture of the NFT.

The NFT moved from Beeple to 0x58bf1fbeac9596fc20d87d346423d7d108c5361a, after which, within two hours, it was transferred to another address which has a user name as its tag. Please try to find this name (and their website) yourself!

Please be aware that a token id is not unique. It is only unique to one specific token or smart contract. A smart hacker can thus recreate a very similar smart contract to, for example, the one by Makersplace's, let's say Makkersplace. In this way, buyers and sellers of NFTs can be misled and transfer funds or valuable NFTs to addresses of the fraudsters. These kind of cases may increase in the future.

In 2021, some 'rug pull' cases were reported. In such cases, a so-called NFT projects announced a big release of NFTs, after which investors started sending Ether to the projects. The 'developers' suddenly shut down the projects and ran off with investors' funds. In these cases, NFTs do not actually have to be investigated, as they were (most likely) never created. The stolen funds can be tracked as in any other Ether investigation.

Investigation tips

- NFTs could be used for money laundering, fraud and other types of crimes, but EC3 has not yet seen many cases of this.
- NFTs can be tracked with Etherscan and additional information on the tokens can be found in log information.

[16] https://ipfs.io/ipfs/QmPAg1mjxcEQPPtqsLoEcauVedaeMH81WXDPvPx3VC5zUz

- Similar to tokens, you can go to an address, click on the drop-down menu after ‘Token:’ and see (at the bottom) whether an Ethereum address holds NFTs. These are called ‘ERC-721 Tokens’ in the list.

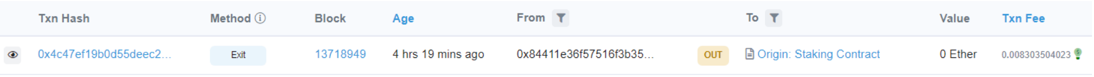
Staking

Similarly to Bitcoin, Ethereum has historically used proof-of-work to mine new coins (Ether). However, Ethereum is moving to proof-of-stake. Participants in the network staking enough[17] Ether can become ‘validators’ and have a similar role as proof-of-work miners, i.e. verify transactions and create new blocks. With proof-of-stake, verifiers are chosen at random to create and validate blocks.

Staking is thus the process of participating in transaction validation on a proof-of-stake blockchain. Solana, Cardano and Algorand are some other examples of cryptocurrencies that use proof-of-stake.

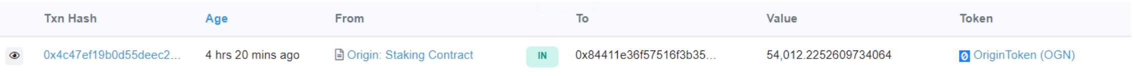
Suspects could, in theory, stake to temporarily invest illicit earnings and passively earn income over it. When you know the Ether addresses of your suspect, it is still not immediately obvious whether they have staked or not.

Let’s look at an example of a staking withdrawal on Etherscan, first we look at the Transaction tab:



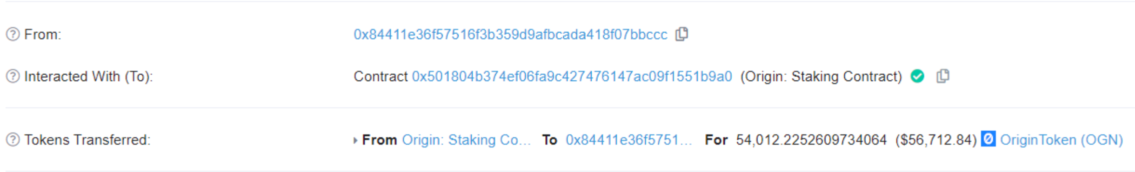
Txn Hash	Method ⓘ	Block	Age	From		To	Value	Txn Fee
0x4c47ef19b0d55deec2...	Exit	13718949	4 hrs 19 mins ago	0x84411e36f57516f3b35...	OUT	Origin: Staking Contract	0 Ether	0.008303504023

Then at the ERC20 tab:



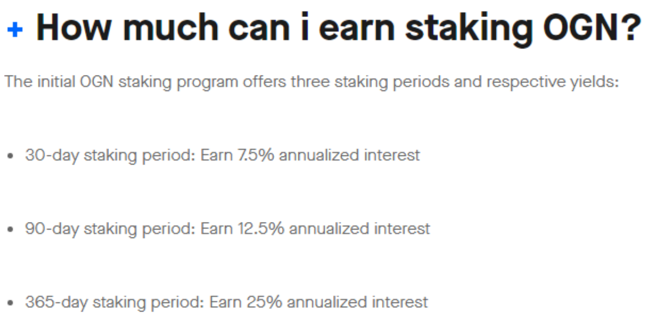
Txn Hash	Age	From		To	Value	Token
0x4c47ef19b0d55deec2...	4 hrs 20 mins ago	Origin: Staking Contract	IN	0x84411e36f57516f3b35...	54,012.2252609734064	OriginToken (OGN)

And when clicking on the Txn hash:



ⓘ From:	0x84411e36f57516f3b359d9afbcada418f07bbccc
ⓘ Interacted With (To):	Contract 0x501804b374ef06fa9c427476147ac09f1551b9a0 (Origin: Staking Contract) ✓
ⓘ Tokens Transferred:	▸ **From** Origin: Staking Co... **To** 0x84411e36f5751... **For** 54,012.2252609734064 ($56,712.84) OriginToken (OGN)

Investigators could be confused by the ‘OUT’ transfer in the Transactions tab, where it appears as if a transfer occurred from 0x84411e… to Origin. However, this is merely the gas fee paid for the transaction in Ether. The user actually receives over 54.000 OriginToken, from the staking contract. This means that the user purchased OriginToken and held (staked) it on the platform for a period of time to receive interest. When Googling OriginToken and ‘staking’, we found this:



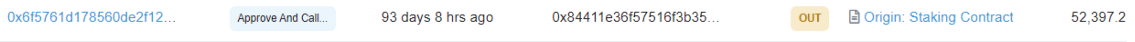
+ How much can i earn staking OGN?

The initial OGN staking program offers three staking periods and respective yields:

- 30-day staking period: Earn 7.5% annualized interest
- 90-day staking period: Earn 12.5% annualized interest
- 365-day staking period: Earn 25% annualized interest

[17] 32 Ether in November 2021

When looking at the address 0x84411e36f57516f3b359d9afbcada418f07bbccc in the OriginToken contract[18], we can see a transaction rougly 90 days before the withdrawal from the OriginToken staking contract:



0x6f5761d178560de2f12...	Approve And Call...	93 days 8 hrs ago	0x84411e36f57516f3b35...	OUT	Origin: Staking Contract	52,397.2

So the user staked 52.397,2 OriginTokens for 93 days ago. The user would get 12.5% annualised interest over a 90-day period, which would be 52.397,2 * 1.125 = 58.947. This would be a 6.549,8 gain over a year. However, as the tokens were only held for one fourth of a year, three months, we can divide this amount by four, which is 1.637,45. Adding this to initial investment (52.397,2) leads to 54.034,65. This is very close to the amount that was withdrawn after 90 days (54.012,23). The slight difference may be explained by the fact that the user held the coins 93 days and not 90 days. Also, these kind of platforms may alter staking yields over time, as OriginToken also explains on a blog[19]. Yet another explanation for the slight difference could be platform fees for withdrawing funds.

What this example shows it that the tokens 'disappeared' from the user's account for over 90 days. However, in reality, the user was earning interest over the tokens by staking them on a platform.

Investigation tips

- Investigators may miss staked tokens when looking at a suspect's balance.
- To see whether an Ether address is staking, look for interactions with staking contracts.
- If possible, connect the users' hardware wallet to their computer to see on what platforms they hold and stake tokens.
- Suspects might mention staking as explanation of increased earnings, whereas they in reality could come from illicit sources. The blockchain can prove or disprove this. However, beware that suspects could have also re-invested illicit earnings, which makes the profits from staking illicit as well.

Following the money

The tracing of Ether and tokens, similarly to Bitcoin, usually starts with an address or a transaction made by the suspect and the objective is usually to find the most convincing route to a LE friendly exchange or a payment processor. Unfortunately, suspects often do not send criminally obtained funds straight to an exchange. The investigator often has to follow the flow of funds from one address to another. With Ether and related tokens, an extra layer of complexity is added as one cryptocurrency

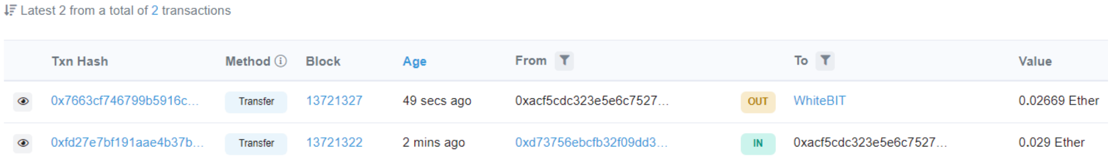
[18] Remember the trick to add '?a=' to URL of the contract address and add the Ether address you are interested in, i.e.: https://Etherscan.io/token/0x8207c1ffc5b6804f6024322ccf34f29c3541ae26?a=0x84411e36f57516f3b359d9afbcada418f07bbccc

[19] https://blog.originprotocol.com/stake-origin-tokens-ogn-to-earn-up-to-25-yield-c26db1970bbb

can be staked, swapped for the other, sold for tokens or NFTs. The previous paragraphs should have given you an idea how to follow these types of conversions.

Still, it is important to know, when to continue and when to stop with the analysis. After all, it is always better to fail to identify a service used by the suspect than coming to a wrong conclusion and follow funds of users that are completely unrelated to the suspect.

Contrary to Bitcoin, there are no change addresses in Ethereum and related tokens, which makes tracing, in principle, easier. Let's say that in a hypothetical case, we have seen a suspect do a transaction seconds before we arrested her with the laptop still open. We see the Ether address she used in her wallet, it is 0xaCF5CDc323E5e6C7527087eF67d82D7628d5273f. When we want to know the deestination of funds, we simply insert the address in Etherscan.io:

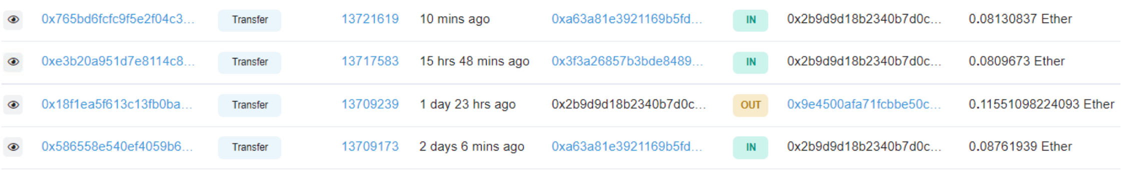


Latest 2 from a total of 2 transactions

Txn Hash	Method	Block	Age	From		To	Value
0x7663cf746799b5916c...	Transfer	13721327	49 secs ago	0xacf5cdc323e5e6c7527...	OUT	WhiteBIT	0.02669 Ether
0xfd27e7bf191aae4b37b...	Transfer	13721322	2 mins ago	0xd73756ebcfb32f09dd3...	IN	0xacf5cdc323e5e6c7527...	0.029 Ether

We can immediately see that the Ether was sent to exchange WhiteBIT[20].

Of course, it is not always so simple. In many cases you will simply see transfers where it is not immediately clear where the funds go to:

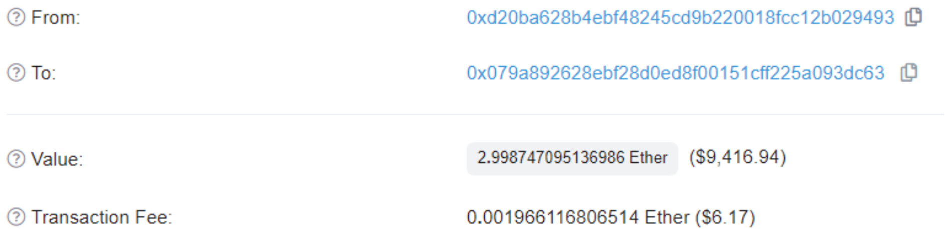


0x765bd6fcfc9f5e2f04c3...	Transfer	13721619	10 mins ago	0xa63a81e3921169b5fd...	IN	0x2b9d9d18b2340b7d0c...	0.08130837 Ether
0xe3b20a951d7e8114c8...	Transfer	13717583	15 hrs 48 mins ago	0x3f3a26857b3bde8489...	IN	0x2b9d9d18b2340b7d0c...	0.0809673 Ether
0x18f1ea5f613c13fb0ba...	Transfer	13709239	1 day 23 hrs ago	0x2b9d9d18b2340b7d0c...	OUT	0x9e4500afa71fcbbe50c...	0.11551098224093 Ether
0x586558e540ef4059b6...	Transfer	13709173	2 days 6 mins ago	0xa63a81e3921169b5fd...	IN	0x2b9d9d18b2340b7d0c...	0.08761939 Ether

Unfortunately, without context, it is hard to derive whether such transactions constitute payments from one person to the other, a transfer to another wallet of the same person or even transactions by entities such as exchanges.

Fortunately, Etherscan often provides us with some context. When looking at the Transactions tab there is a 'Method' header, which is a function based on decoded input data and describes what type of transaction took place. For example, there are some obvious ones such as 'transfer', 'swap exact ETH for tokens', 'deposit Ether for' and 'stake start'. However, there are also weirder functions, such as 'Add Many To Safari and pack', 'claim volts' and 'increase custody allowance'. When looking at the logs of these types of transactions, investigators can find out what they mean.

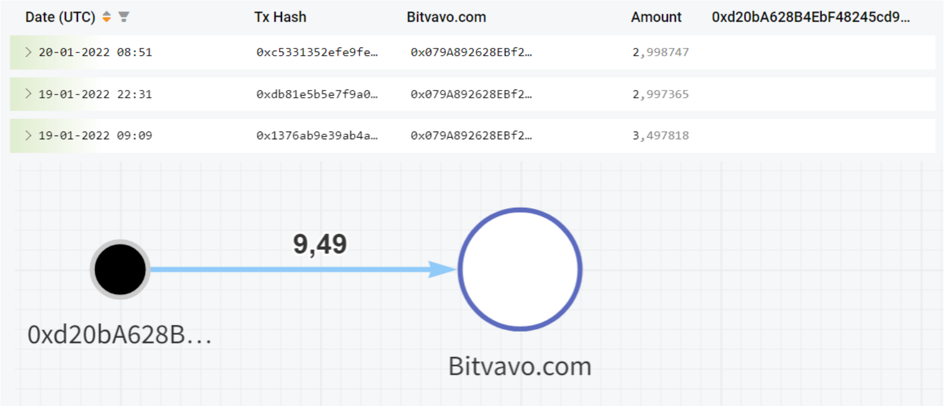
The tagging of Etherscan is not always correct, as can be seen from the below example:



From:	0xd20ba628b4ebf48245cd9b220018fcc12b029493
To:	0x079a892628ebf28d0ed8f00151cff225a093dc63
Value:	2.998747095136986 Ether ($9,416.94)
Transaction Fee:	0.001966116806514 Ether ($6.17)

[20] The transaction fee here was 0.00231 Ether, which explains the difference in the two amounts.

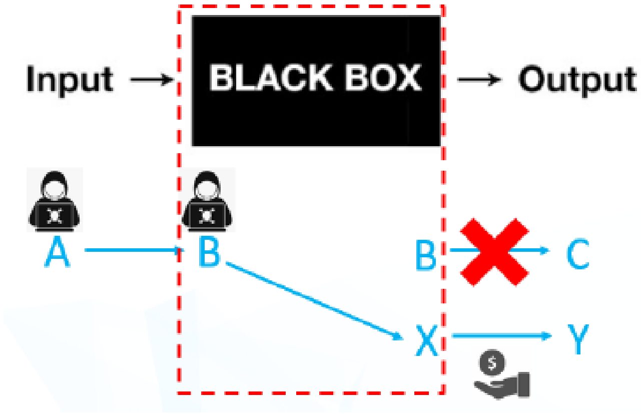
Etherscan does not recognise these addresses as part of a cluster. However, a popular tracing tool has identified the ‘to’ address as belonging to Dutch exchanges Bitvavo (see below). This is why it is recommended to always check the addresses in your investigation both in Etherscan and available tracing tools.



Date (UTC)	Tx Hash	Bitvavo.com	Amount	0xd20bA628B4EbF48245cd9…
20-01-2022 08:51	0xc5331352efe9fe…	0x079A892628EBf2…	2,998747	
19-01-2022 22:31	0xdb81e5b5e7f9a0…	0x079A892628EBf2…	2,997365	
19-01-2022 09:09	0x1376ab9e39ab4a…	0x079A892628EBf2…	3,497818	

Private vs. Service wallets

In the Bitcoin Guide for Investigators we said ‘never ever trace through services’. Once the suspect sends bitcoins to an exchange, this is the endpoint and the investigator should send a request for information to this exchange. With Ethereum and related tokens, this is more nuanced. Centralised services (for example: Kraken, Coinbase, Binance) are still black boxes, because we do not know what happens when funds are deposited there. We explained this in the last guide with the following schema:



The diagram depicts the transaction where a cryptocurrency is sent from a suspect to his account at a centralised exchange is visible in the blockchain. He may use the platform to convert cryptocurrency to fiat, which can be withdrawn – either to a bank account or to an online services such as Skrill, Webmoney or Perfect Money. A conversion to other cryptocurrencies, such as privacy coins, is also possible. However, the bottom line is, this is **not** visible in the public blockchain, as an investigator is not aware of the methods centralised exchanges use to exchange funds for their customers.

In an ideal situation, tracing tools and publicly available services such as Etherscan would always be correct in identifying services. Unfortunately, they are not, which leads to the fact that the investigator has to be careful not to trace through a service. So how do we identify unidentified services? There are a couple of points to check, which are indications that an address is part of a service:

- In tracing tools, an unidentified cluster might be recognisable by the fact that it has, for example, a yellow circle around it (Chainalysis);
- In a tracing tool, you may see that the cluster you are looking at is enormous (hundreds or thousands of addresses);
- You might see one address with hundreds or thousands of transactions and a very high balance;
- You might also see many connections to different services from one address. Individual users may not use many services, as this is not practical;
- An address might receive and / or send its funds to one specific service. This may indicate that the address you are looking at is actually part of this service.

It must be noted that this is not a 'hard science'. Exceptions exist, there will for example be individuals who have done huge amounts of transactions or use many different services. Therefore, this type of analyses always requires your own judgement based on the context as well.

As shown in previous paragraphs, DeFi platforms are different. We can actually trace through them! The interactions users have with these platforms are publicly traceable on the blockchain. Investigators should not simply look at the transactions tab, but also at the transaction hash and look at the logs to obtain further information. As these transactions are automated according to smart contracts, they follow expected routes. This offers opportunities for investigators, without sending requests for information, which can also make your investigation a lot more efficient!

Contacting exchanges

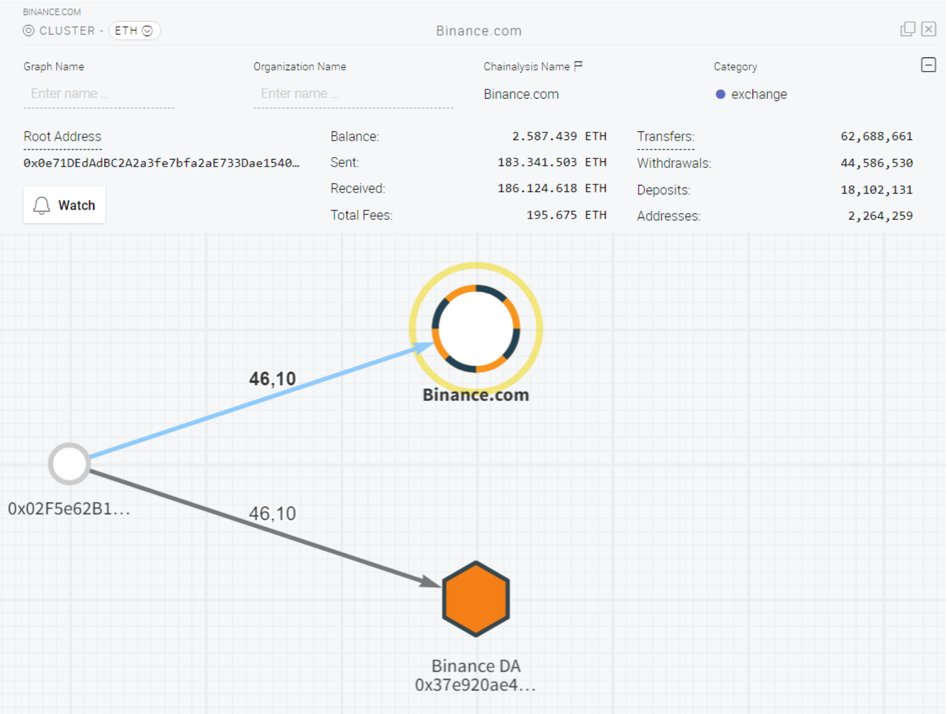
The majority of centralised exchanges and other services comply with law enforcement requests and can provide useful information.

In order to properly request data from an exchange, be sure to attach searchable unique identifiers to your request. This will simplify the process for an exchange and they might be able to return information more quickly. Scanned copies containing addresses or transactions always have to be accompanied by an Excel spreadsheet, .txt or .csv file containing the unique identifiers in an editable format.

The standards for contacting the services differ considerably. For a list of recommended contacts, tips on how to request data from each exchange and evaluation of their cooperation with law enforcement please refer to the Cryptocurrency Services Review Guide released in January 2021 and the updated Contact Details on Cryptocurrency Exchanges, released in December 2021. Access to the Guide can be obtained via your liaison officer.

What exactly should be requested?

Generally, investigators will identify a deposit address within a service. Pay attention to include a correct address – i.e. not the address of the cluster provided by commercial tools, but the deposit address of the client you are interested in:



BINANCE.COM

CLUSTER - ETH

Binance.com

Graph Name	Organization Name	Chainalysis Name	Category
Enter name ...	Enter name ...	Binance.com	● exchange

Root Address				
0x0e71DEdAdBC2A2a3fe7bfa2aE733Dae1540…	Balance:	2.587.439 ETH	Transfers:	62,688,661
	Sent:	183.341.503 ETH	Withdrawals:	44,586,530
Watch	Received:	186.124.618 ETH	Deposits:	18,102,131
	Total Fees:	195.675 ETH	Addresses:	2,264,259

In the example above, we can for example see that 46,10 ether is sent to Binance. However, this is not sent to the root address of Binance, but to one specific deposit address (see Binance DA 0x37e920ae4…). The exchange will need to receive this deposit address to be able to provide you with identifying information on your target.

For clarity, it is a good idea to request the following info to make sure the exchange can identify the correct client.

- Deposit address at exchange, not the exchange's main address;
- Tx hash;
- Timestamp of transaction;
- Amount deposited at exchange by suspect.

For withdrawals, it is still important to include the withdrawal addresses, even though the address is outside of the exchange. In this case, it is again good practice to mention the:

- Suspect's withdrawal address;
- Transaction hash;
- Withdrawal amount;
- Timestamp of the transaction(s).

Seizing Ether, tokens and NFTs

An important aspect of understanding Ethereum, tokens and NFTs for investigators is knowing how to seize them. Seizing in this case means the transfer of a suspect's Ether, tokens or NFTs to a government-controlled wallet. Before you start seizing, it is also important to know what the policy in your country is regarding cryptocurrency seizure. Some countries use an exchange to immediately convert the seized cryptocurrency to fiat currency (Euros), but other countries safely store the seized cryptocurrency on a hardware wallet or use professional third parties to store seized assets. Please see EPE for discussions on countries using these services.

Accessing a wallet

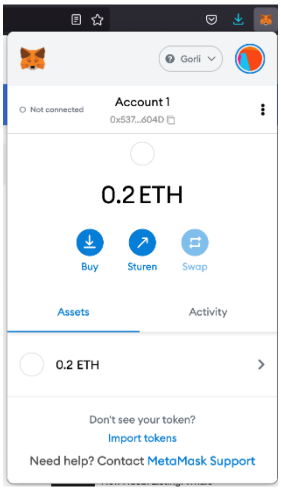
But how do you access a wallet? In an ideal situation, during a house search, you would encounter your suspect's open laptop with a software cryptocurrency wallet running, after which you can simply transfer the funds to a government-held wallet. Additionally, when the suspect's computer is open, you can check[21] whether they have accounts at exchanges. From these exchanges, funds can also be transferred to government-controlled wallets. You can for example look for the browser bookmarks of a suspect or see if they have a password manager, in which you might find (user names and passwords for) exchange accounts of the suspect.

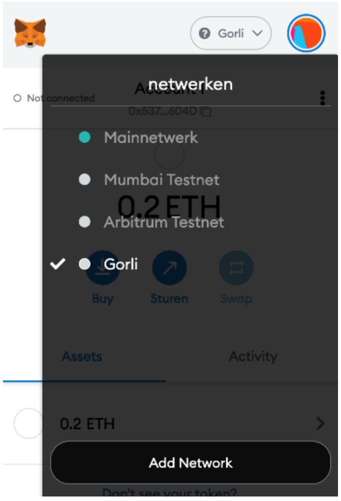
It is also advisable to try to connect the suspect's hardware wallet (if you find one) to their computer. They may, for example, use software wallets in combination with a hardware wallet for extra security. MetaMask is an example of a software wallet that can be used in combination with a hardware wallet (Trezor, Ledger etc.)[22].

When transferring funds from the suspect's wallet, it is important to remember to transfer **tokens first**. This is important, as you need gas to pay the transaction costs of every transaction. These are paid in Ether.

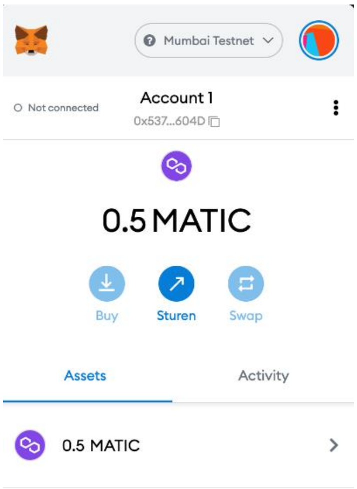
Tip: when you encounter a MetaMask wallet, make sure to not only check the different tokens and to seize them first, but also all the different networks the wallet connects to. Some other cryptocurrencies are supported by MetaMask, but do not run on the Ethereum network. Examples are xDai, Avalanche, Binance Smart Chain, Polygon (Matic) and HECO (Huobi Eco Chain).

In the below screenshots you can see that there are different coins in different networks. While these are testnet transactions (i.e. these have no value), Ethereum is available through the 'Gorli' network, whereas the Matic is in the 'Mumbai testnet'. Matic also requires its own gas to be transferred, i.e. Matic tokens. If these were real transactions with value, the networks to connect to would be 'Ethereum Mainnet' and Matic would be on the 'Matic Mainnet'.





[21] If your national legislation allows it, discuss with your prosecutor.
[22] https://MetaMask.zendesk.com/hc/en-us/articles/360020394612-How-to-connect-a-Trezor-or-Ledger-Hardware-Wallet



Networks can be deleted as well, so if you know that your suspect has a large amount of a certain Ethereum-related cryptocurrency, you could try adding the networks back into MetaMask to see if there are more hidden funds available.

Difficulties in accessing funds

Many suspects that own cryptocurrency will secure them with passwords and / or mnemonic seed phrase. We will not discuss password cracking further in detail, as this is more of a task for your forensic unit. However, as mentioned before, there are various tools available for interpreting mnemonic phrases. It is essential that investigators in your country are aware of the importance of mnemonic phrases. Without context, they look like some random words on a piece of paper, which an unknowing investigator may fail to recognise. However, this could lead to seizure of cryptocurrency, which could be worth millions of euros. Therefore, during every house search where there is a possibility that the suspect possesses cryptocurrency, investigators should be actively looking for pieces of paper with 'random' words on it (i.e. mnemonic phrases).

Also, there can be legal difficulties, as your national legislation may not allow for the seizure of cryptocurrencies at foreign exchanges during a house search. Some prosecutors may require an international freezing order (via MLAT or EIO). However, seizing cryptocurrencies during the house search can be a lot quicker and easier when national legislation is used. It is advisable to discuss this with your prosecutor before the house search, so you do not have to decide on the spot.

The numerous developments on the Ethereum ecosystem lead to new issues when seizing. For example, criminal funds in Ether can now be staked, sent to liquidity pools and/or sold for NFTs.

- *Staking*
  - If a suspect stakes, their cryptocurrency can be locked into a platform for a set period of time. In some cases, it is impossible to take the cryptocurrency out until the end of the staking period. For example, for Ethereum 2.0[23] the staking period is at least two years. As discussed, other examples of coins that can be staked are Cardano,

[23] See the Eth2.0 deposit contract here: https://Etherscan.io/address/0x00000000219ab540356cbb839cbe05303d7705fa

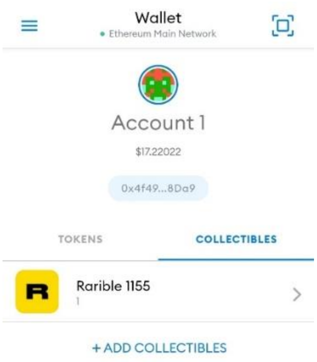
Algorand, Polkadot, Cosmos, Tezos and many more. In theory, it may be possible for an investigator to talk to the developers of the staking platform, who could return the staked criminal funds when they are locked in for an extended period of time. However, these are uncharted territories and we are happy to hear from you if you have any experience in this regard.

- Tip: on Etherscan at the top of the page, you can see if an address has staked to Ethereum 2.0. You will see the tag 'Eth2 Depositor'.

- *Liquidity Pools*
  - Liquidity pools allow for DeFi platforms to have liquidity for other users to trade. Users are motivated to provide liquidity, as they earn liquidity pool (LP) tokens or other forms of interest. For example, when a user lends Ether to the platform Compound, they will receive cETH tokens that demonstrate the deposit of funds. These tokens gain interest. They are used to get the deposited Ether back from Compound. The longer the user keeps the cETH, the more interest they get on their Ether and the more Ether they can get back from the Compound platform.
  - Tip: When a user receives tokens for liquidity providing, the tokens are created or 'minted'. When the user returns the tokens to the platform, they are destroyed or 'burned'. An investigator can recognise such a transaction on Etherscan as it will come from (mint) or go to (burn) a 0x00000… address. These tokens are often 'pegged' 1:1[24] to the value of the underlying asset that is deposited to the platform. An example of a platform Examples include Wrapped Ethereum, AnyBTC, goETH, goBTC and many more.

- *NFTs*
  - NFTs can be stored in a variety of ways. Popular options are, similarly to storing cryptocurrencies, software and hardware wallets.
  - If a law enforcement agency would obtain access to a wallet with NFTs from a suspect, the agency could transfer them to their own wallet or offer them for sale on an NFT platform from a government account. EC3 does not have experience in this yet, and would be happy to discuss and learn from partners about this.

[24] See for example: https://aave.com/aTokens/



- Software wallets are frequently used to store NFTs. A common example of such a wallet is MetaMask. You can find NFTs under the tab ‘collectibles’ on MetaMask. On the right you can see an example. Popular NFT platform OpenSea, for example, integrates MetaMask. This makes it an attractive option for the storage of NFTs and should be checked by investigators when they have a suspicion of the possession of NFTs by a suspect.
- When NFTs are created on a network (such as Ethereum) that is already supported by a hardware wallet, they can also be stored on such device. An NFT will generally first be created locally or purchased on a platform such as OpenSea or Rarible, but after the owner can send it to an address created on a hardware wallet.

Investigation tips

- First seize tokens, then Ether. If your forget this, you may run out of gas and will not be able to transfer the tokens.
- If possible, connect the suspect’s software and / or hardware wallet to their computer. Browse to the platforms that they may have used and see if there are balances on the platforms and wallets. In some occasions, such funds are only accessible when you connect the right wallet to the right platform (for example MetaMask on OpenSea).
- Make sure to enter a mnemonic phrase in the correct derivation path. See further guidance on the use of mnemonic phrase tools on EPE.
- Smart contracts are immatubale when deployed on the blockchain. However, sometimes new versions (updates) are published. This can give investigators chances, if developers are willing to cooperate. In theory, addresses that received criminal funds can also be blacklisted if there is a variable in the contract that allows for it[25]. This would mean that other entities in the network can not interact with blacklisted addresses anymore. Addresses could for example be blocked by DeFi platforms, which will make it impossible for criminal funds to be deposited. Investigators can explore these opportunities

[25] See for example Tether’s (USDT) blacklist here: https://bloxy.info/txs/calls_sc/0xdac17f958d2ee523a2206206994597c13d831ec7?signature_id=37757

by contacting the developers or companies behind such smart contracts. Partners of EC3 have previously done this successfully, please contact us for more information.

- Many developments in this field are novel and many LEAs do not have much experience in these kinds of seizing. We encourage the sharing of experiences with EC3. Ideally, we would provide guides on all relevant cryptocurrencies, tokens, NFTs and platforms, but unfortunately there are too many developments. Via the EPE we are happy to share experiences more broadly.

Next steps

We recommend you to practise as much as you can by checking out new types of wallets, tokens, NFTs, liquidity pools and more. By making some test transactions, you can see what happens on the blockchain and prepare yourself for future investigations. The best learning material is hands-on practice – interaction with cryptocurrency wallets, services and on the job experience!

We are not aware of many courses specifically focusing on the tracing of Ethereum and related tokens. However, there are still some resources out there to increase your understanding of Ethereum, DeFi and related topics:

- Many different online free courses, one good example is The University of Nicosia's Massive Online Open Course (MOOC) → Introduction to Decentralized Finance (DeFi).
- Tracing tools and security companies offer trainings related to cryptocurrency tracing, increasingly related to Ethereum and DeFi as well.

Europol materials

- Strategic publications, such as the *Cryptocurrency Services Review Guide*, evaluating exchanges and the assistance they provide to LE agencies. The most similar to this guide is the *Bitcoin Guide for Investigators*. A number of shorter reports and thematic Cyber Bits are also available.
- EPE (Europol Platform for Experts):
- https://epe.europol.europa.eu - if you do not have login credentials please send us a request at o3@europol.europa.eu
- Cryptocurrencies Group contains a list of contacts on over 3 100 investigators and private sector contactcs, as well as relevant publications and presentations from previously hosted

cryptocurrency conferences: https://epe.europol.europa.eu/group/europol-virtual-currencies-taskforce

- This group also has a restricted law enforcement only section, on which you can find guides such as this one and the *Cryptocurrency Services Review Guide*, *Contact List on Cryptocurrency Exchanges* and a space where you can ask fellow international investigators questions.
- SIRIUS – a great resource on online service providers:
  - https://epe.europol.europa.eu/group/sirius

Please let us know if you encounter any mistakes in this guide via O3@europol.europa.eu and we will update it as soon as possible!