



BAIL
security

BAILSEC.IO

EMAIL : OFFICE@BAILSEC.IO

TWITTER : @BAILSECURITY

TELEGRAM : @HELLOATBAILSEC

FINAL REPORT:

Prestige Club Forensic Blockchain Tracement

July 2023

Disclaimer:

Security assessment projects are time-boxed and often reliant on information that may be provided by a client, its affiliates, or its partners. As a result, the findings documented in this report should not be considered a comprehensive list of security issues, flaws, or defects in the target system or codebase.

The content of this assessment is not an investment. The information provided in this report is for general informational purposes only and is not intended as investment, legal, financial, regulatory, or tax advice. The report is based on a limited review of the materials and documentation provided at the time of the audit, and the audit results may not be complete or identify all possible vulnerabilities or issues. The audit is provided on an "as-is," "where-is," and "as-available" basis, and the use of blockchain technology is subject to unknown risks and flaws.

The audit does not constitute an endorsement of any particular project or team, and we make no warranties, expressed or implied, regarding the accuracy, reliability, completeness, or availability of the report, its content, or any associated services or products. We disclaim all warranties, including the implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

We assume no responsibility for any product or service advertised or offered by a third party through the report, any open-source or third-party software, code, libraries, materials, or information linked to, called by, referenced by, or accessible through the report, its content, and the related services and products. We will not be liable for any loss or damages incurred as a result of the use or reliance on the audit report or the smart contract.

The contract owner is responsible for making their own decisions based on the audit report and should seek additional professional advice if needed. The audit firm or individual assumes no liability for any loss or damages incurred as a result of the use or reliance on the audit report or the smart contract. The contract owner agrees to indemnify and hold harmless the audit firm or individual from any and all claims, damages, expenses, or liabilities arising from the use or reliance on the audit report or the smart contract.

By engaging in a smart contract audit, the contract owner acknowledges and agrees to the terms of this disclaimer.

Forensic Blockchain Tracement: Prestige Club

Involved addresses:

- a. ethValidator: 0x86ee4072b7427bca3b1109e585a32f2230c515f2
- b. C1: 0x11923d873e2030d45ace9cfc63b12257205ee609
- c. C2: 0xd46f7e32050f9b9a2416c9bb4e5b4296b890a911
- d. C3: 0x2eecbbe4fa4b67b127f50ef8640b30f6c7209d5c
- e. TheSeeder: 0x7dFd9C6CC9a028c3370aFdF041C962Cae5416892
- f. EthValidatorOutgoing: 0x1cd213d2b98f41b35e36f98d2801de05e57a82c8
- g. BlockFiHotOutgoing: 0x2a549b4af9ec39b03142da6dc32221fc390b5533
- h. LinkToEthValidatorOutgoing: 0x6930cec97cb9ad10d8b7735675cd945b744721e0
- i. LinkToEthValidatorOutgoing2: 0x58111e5e9e35eb2a59631486b588cb514a0fbf53

The following report presents the findings of a forensic blockchain investigation conducted to evaluate potential connections between the **ethValidator** address (0x86ee4072b7427bca3b1109e585a32f2230c515f2) and three other addresses:

C1 (0x11923d873e2030d45ace9cfc63b12257205ee609),

C2 (0xd46f7e32050f9b9a2416c9bb4e5b4296b890a911),

C3 (0x2eecbbe4fa4b67b127f50ef8640b30f6c7209d5c).

The objective of this investigation is to address allegations made by a third party accusing the client, who owns all three client addresses, of misappropriating funds and transferring them to the ethValidator address. The client vehemently denies these allegations and has engaged our services to perform an in-depth on-chain analysis to

establish whether there are any substantive links between the ethValidator address and the three client addresses.

This investigation encompasses two key vectors:

a) Full Analysis of the ethValidator Address: This involves examining the transactions, smart contract interactions, and any associated addresses connected to the ethValidator address. By conducting a comprehensive analysis, we aim to identify any potential links between the ethValidator address and other addresses, shedding light on its activities and potential connections.

b) Potential Links to Centralized Exchanges: This phase focuses on investigating whether the ethValidator address has any connections or interactions with centralized exchanges. By scrutinizing relevant transactions and address interactions, we aim to ascertain if the ethValidator address has engaged in any significant trading or transfer activities with exchanges, which may provide insights into its source of funds or potential involvement with the accused client addresses, this information can be used to contact these entities with a valid law enforcement document in an effort to gather more information if the owner of this address has a valid connection to C1, C2 or C3.

Through this meticulous investigation, we strive to provide an impartial and evidence-based assessment of the allegations against the client. By examining the aforementioned vectors, we aim to either substantiate or refute the claims of fund

misappropriation and establish whether the ethValidator address is linked in any way to the three client addresses.

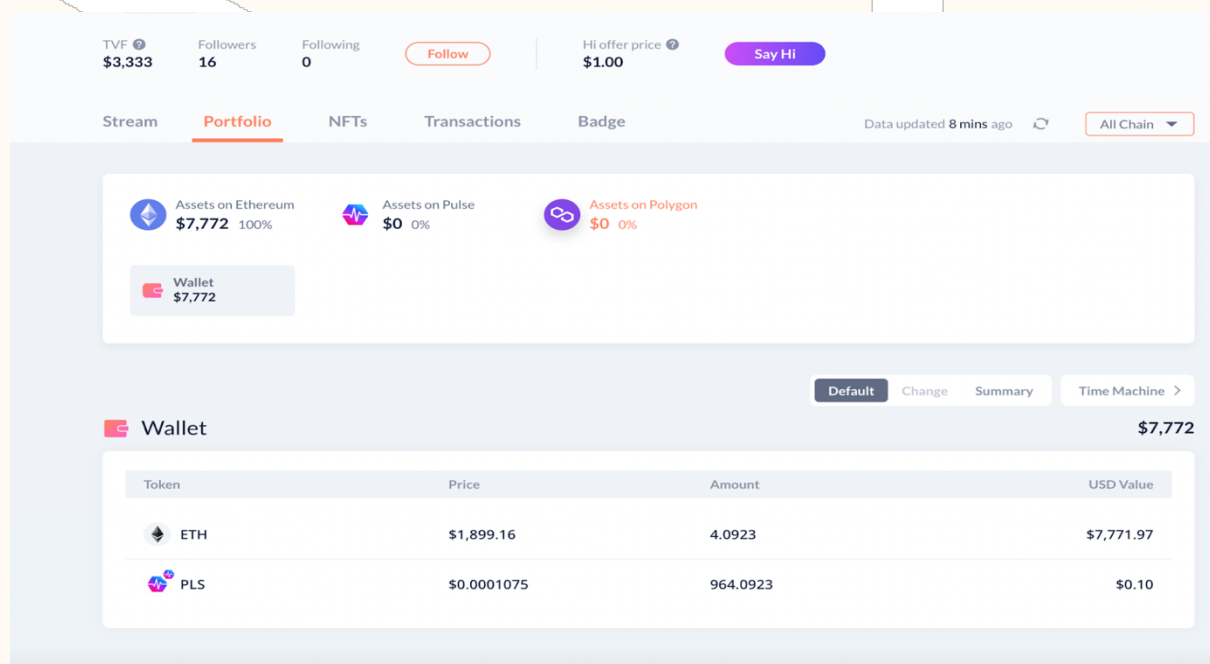
Disclaimer:

The findings and conclusions of this report are based solely on the analysis of on-chain data and should not be considered as definitive proof of guilt or innocence. The report's purpose is to present the discovered evidence, potential connections, and insights derived from the investigation, allowing for a more informed assessment of the allegations made against the client.

Analysis of the ethValidator address

The following deBank portfolio shows all balance of the aforementioned address on all chains:

<https://debank.com/profile/Ox86ee4072b7427bca3b1109e585a32f2230c515f2>

A screenshot of a deBank portfolio page for the address Ox86ee4072b7427bca3b1109e585a32f2230c515f2. The page shows a TVF of \$3,333, 16 followers, and 0 following. The portfolio is divided into three sections: Assets on Ethereum (\$7,772, 100%), Assets on Pulse (\$0, 0%), and Assets on Polygon (\$0, 0%). A wallet section shows a total value of \$7,772. Below this, a table lists the tokens in the wallet: ETH and PLS.

Token	Price	Amount	USD Value
ETH	\$1,899.16	4.0923	\$7,771.97
PLS	\$0.0001075	964.0923	\$0.10

Portfolio balance

At the time of viewing (19.07.2023; 5PM CET), the address holds the following funds:

- a. Ethereum blockchain: 4.0923 unwrapped ETH
- b. Pulse blockchain: 964.0923 PLS

General activity

To further assess the EOA activity, we will now conduct an activity check of all prominent EVM chains, this activity check is important since malicious actors generally attempt to transact over side-chains since these are often unnoticed by a forensic analysis:

a. Ethereum blockchain: 33 total transactions

ETH BALANCE 0 ETH	PRIVATE NAME TAGS + Add	MULTICHAIN ADDRESSES 0 address found via Blockscan
ETH VALUE \$0.00	LAST TXN SENT 0xaed63eb20560... from 929 days 9 hrs ago	
	FIRST TXN SENT 0xaed63eb20560... from 929 days 9 hrs ago	

Transactions

Internal Transactions

Token Transfers (ERC-20)

Analytics





Comments

Latest 2 internal transactions

ADVANCED MODE: ☐ Advanced Filter

Parent Txn Hash	Block	Age	From	To	Value
0x50a0c6bfeb05e1159...	11563070	929 days 23 hrs ago	BlockFi 4	0x7dFd9C...e5416892	505.15 ETH
0x83fa4600096dac26c...	11563070	929 days 23 hrs ago	BlockFi 4	0x7dFd9C...e5416892	500 ETH

b. BNB chain: no transactions

 Address `0x86ee4072b7427Bca3b1109e585a32f2230c515F2`   

Featured: Build Precise & Reliable Apps with **BscScan APIs**. [Learn More!](#)

Overview

Balance:

0 BNB

BNB Value:

\$0.00

Transactions

BEP-20 Token Txns

Analytics

Comments

Txn Hash

Method ⓘ ▼





Block ▼

Age

From ▼

There are no matching entries

c. Arbitrum: no transactions

 Address `0x86ee4072b7427Bca3b1109e585a32f2230c515F2`   

Overview

Balance:

0 ETH

Ether Value:

\$0.00

Transactions

Erc20 Token Txns

Analytics

Comments

Txn Hash	Method ⓘ	Block	Age	From ▾
There are no matching entries				

d. Polygon: no transactions

More Info

ⓘ My Name Tag:
Not Available, [login to update](#)

Transactions





ERC-20 Token Txns

Analytics

Comments

Txn Hash	Method ⓘ ▾	Block ▾	Age	From ▾	To ▾	Value	[Tx
There are no matching entries							

e. Avalanche: no transactions

 Address `0x86ee4072b7427Bca3b1109e585a32f2230c515F2`   





Overview

Balance:	0 AVAX
AVAX Value:	\$0.00

Transactions ERC20 Token Txns Analytics Comments

Txn Hash	Method ⓘ	Block	Age	From ▾
There are no matching entries				

f. Fantom: no transactions

 Address `0x86ee4072b7427Bca3b1109e585a32f2230c515F2`   

Overview

Balance:	0 FTM
FTM Value:	\$0.00








Transactions ERC-20 Token Txns Analytics Comments

Txn Hash	Method ⓘ	Block	Age	From ▾
There are no matching entries				

g. Pulsechain: no transactions

Address Details

0x86ee4072b7427Bca3b1109e585a32f2230c515F2

 Balance	964.09231971089111029 PLS
 Tokens	0 tokens
 Transactions	0 Transactions
 Transfers	0 Transfers
 Gas Used	0
 Last Balance Update	17825724
 Fee Recipient Blocks	2

Transactions

Internal Transactions

Coin Balance History

Fee Recipient Blocks

Transactions

There are no transactions for this address.

Smart contract interactions

The ethValidator address has conducted 31 smart contract interactions with the Beacon deposit contract:

<https://etherscan.io/address/0x00000000219ab540356cbb839cbe05303d7705fa>

An example tx can be found here:

<https://etherscan.io/tx/0xc41778d6ccd5b38aaeecc7f5e50077f81174cda39455ad53e817a792d0c59a9a>

All transactions were staking transactions where the address has staked 32 ETH.

Outgoing transfers

Besides the address seeding, these sort of transactions promise the highest probability of tracing funds since one can easily identify to which contracts/EOAs the address has sent ETH/ERC20 tokens.

The ethValidator address has only one outgoing ETH transfer to the following address: 0x1cd213d2b98f41b35e36f98d2801de05e57a82c8 ("ethValidatorOutgoing"), with the following transaction hash:

<https://etherscan.io/tx/0x4709ae3f7038788eca6a8c483e49959c4981fd6449fe012a04424a91b7a0adb9>

The aforementioned address seems to be a **BlockFi smart contract wallet**, as one can see in the transaction, a simple ETH transfer was made to this contract, which then triggers the contracts fallback function and sends the ETH directly to the **BlockFi hot wallet**:

Transaction Receipt Event Logs

154

Address [0x2a549b4af9ec39b03142da6dc32221fc390b5533](#) 🔍

Name Deposited (address from, uint256 value, bytes data) [View Source](#)

Topics 0 0x6e89d517057028190560dd200cf6bf792842861353d1173761dfa362e1c133f0

Data from: 0x1cd213d2b98f41b35e36f98d2801de05e57a82c8
value: 45065904941826968436
data: Dec Hex

155

Address [0x1cd213d2b98f41b35e36f98d2801de05e57a82c8](#) 🔍

Name ForwarderDeposited (address from, uint256 value, bytes data) [View Source](#)

Topics 0 0x69b31548dea9b3b707b4dff357d326e3e9348b24e7a6080a218a6edeec48f9b

Data from: 0x86ee4072b74278ca3b1109e585a32f2230c515f2
value: 45065904941826968436
data: Dec Hex

with the address `0x2a549b4af9ec39b03142da6dc32221fc390b5533` (“**BlockFi Hot Outgoing**”).

Interestingly, there are two other transactions to the **ethValidatorOutgoing** address:

1)

<https://etherscan.io/tx/0x1d5f8270732b891a7e8f5198564dbb2bf5678b9e55454a8c8b2fb63fd71a49f2> , a transfer incoming from **Gemini** over 100 ETH

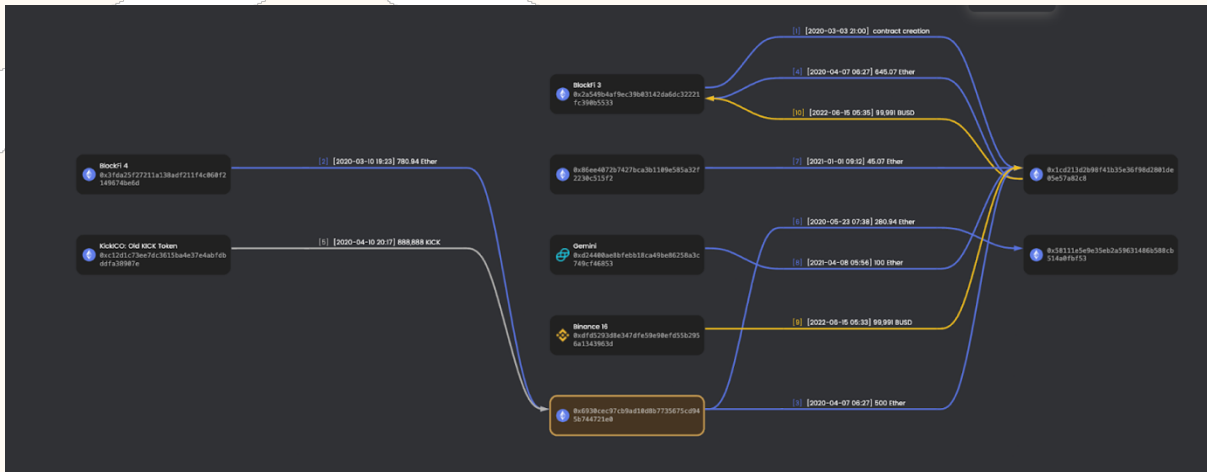
2)

<https://etherscan.io/tx/0xb726273eea54b7f81e86bfdcb375fec2fec79f142a875b2020c659f8fee34734> , a transfer incoming from **Binance** over 99,991 BUSD

3)

<https://etherscan.io/tx/0x9c83116602e5ece33422ec524fdf4c6e47515727901da4a059fd61f7d6dda279> , a transfer incoming from `0x6930cec97cb9ad10d8b7735675cd945b744721e0` (“**LinkToEthValidatorOutgoing**”)

The aforementioned address is the only real possibility to trace further steps since all other transactions, including the seeding are done **by/from exchange wallets** where a tracing is almost impossible without a law enforcement enquiry.



The analysis of the “**LinkToEthValidatorOutgoing**” address has shown that the address was seeded by BlockFi

Parent Txn Hash	Block	Age	From	To	Value
0xae843fbd73fbdedd8...	9645568	1225 days 20 hrs ago	BlockFi 4	0x6930cE...744721e0	780.9403345 ETH

and executed an ether transfer to address:

0x58111e5e9e35eb2a59631486b588cb514a0fbf53

(“**LinkToEthValidatorOutgoing2**”) with the following transaction hash:

<https://etherscan.io/tx/0x286a1224c3d6bd479d5370035ecf7cf2682fe89ba39f2a53b35ce35db6f22d96>

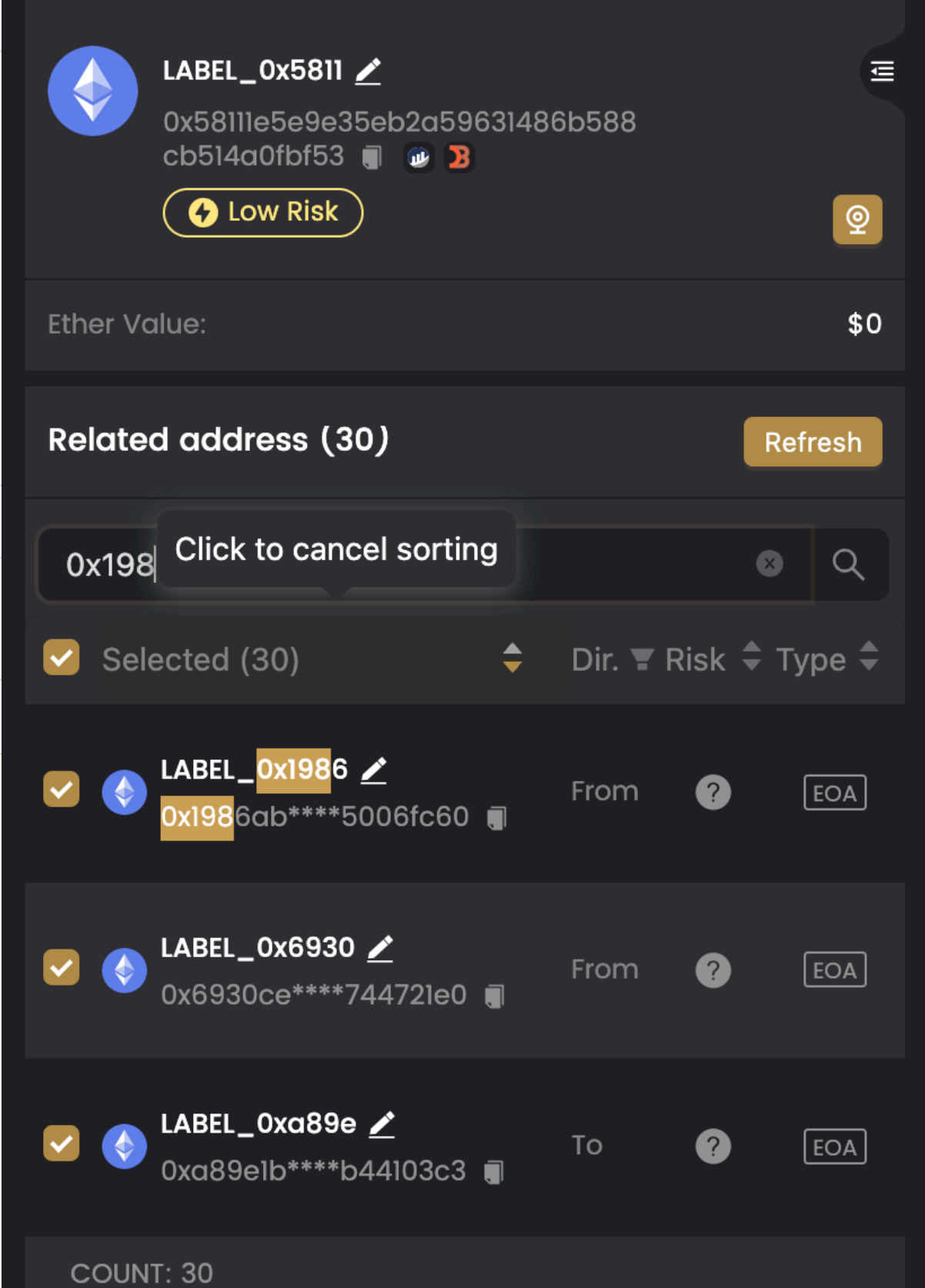
Moreover, the **KickToken** was minted:

<https://etherscan.io/tx/0x9300b14bfaec55870d3178d520c47bbea3d079eb7f5ccc6b4c6d1d27aec6bb03>

The only tracing possibility is now the **LinkToEthValidatorOutGoing2** address which has the following transactions

As one can see from the above screenshot the LinkToEthValidatorOutgoing2 has executed several transfers to other addresses, the next step is to identify possible connections to the above mentioned **C1, C2, C3** addresses.

The following screenshot displays an example of a linked address:



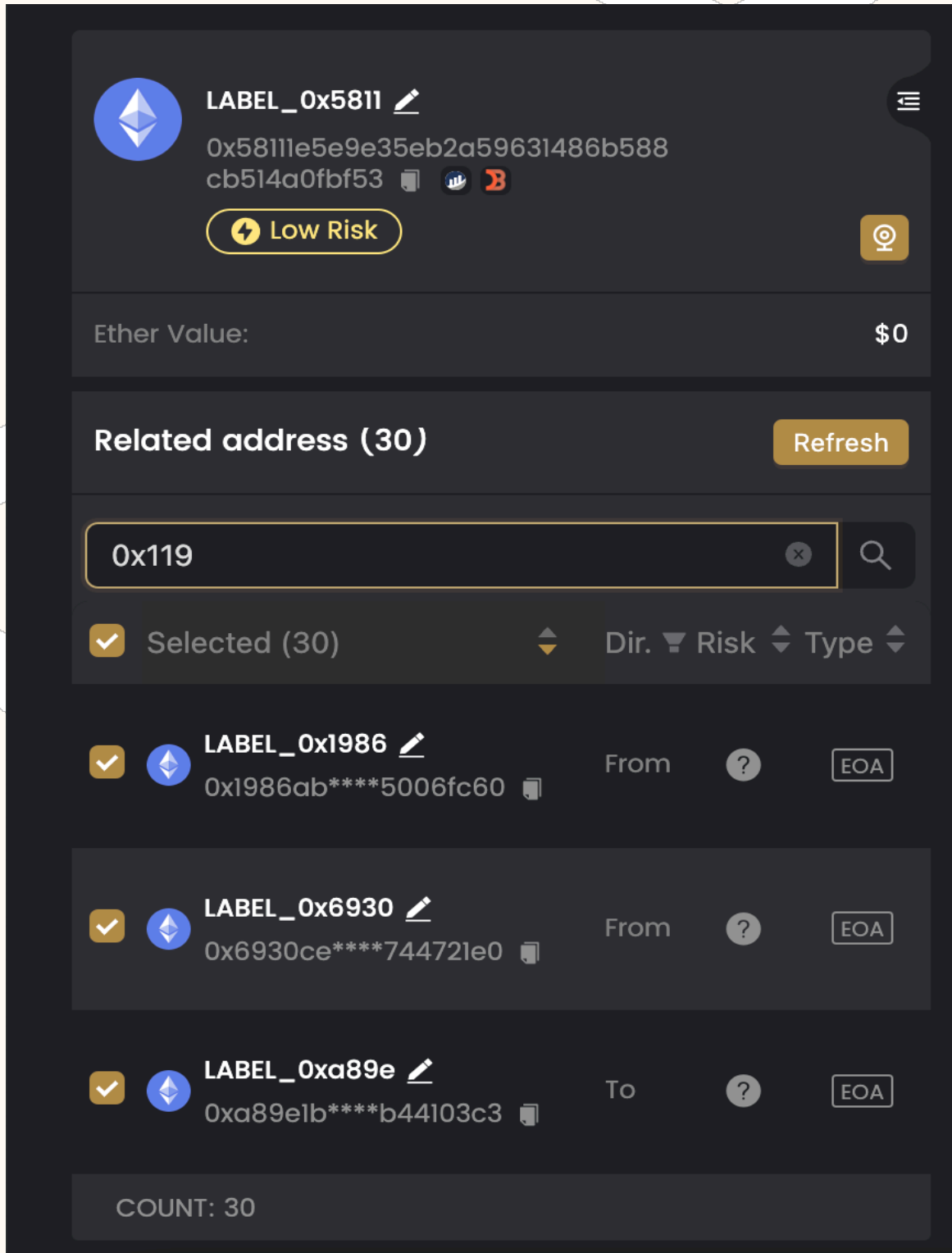
The screenshot displays the BAIL security interface for a linked address. At the top, the address **LABEL_0x5811** is shown with its Ethereum icon, a pencil icon for editing, and a "Low Risk" status. Below this, the "Ether Value" is listed as **\$0**. A section titled "Related address (30)" includes a "Refresh" button and a search bar containing "0x198". Below the search bar, a table lists related addresses, each with a checkbox, an Ethereum icon, a label, a risk status, and a type (EOA).

<input checked="" type="checkbox"/>	Selected (30)	Dir.	Risk	Type
<input checked="" type="checkbox"/>	LABEL_0x1986 0x1986ab****5006fc60	From	?	EOA
<input checked="" type="checkbox"/>	LABEL_0x6930 0x6930ce****744721e0	From	?	EOA
<input checked="" type="checkbox"/>	LABEL_0xa89e 0xa89e1b****b44103c3	To	?	EOA






COUNT: 30

In the next steps, we display the attempt to link



C1: 0x11923d873e2030d45ace9cfc63b12257205ee609

The screenshot shows the BAIL security interface. At the top, there's a wallet profile for "LABEL_0x5811" with a blue diamond icon. Below the profile, the address "0x5811e5e9e35eb2a59631486b588cb514a0fbf53" is displayed. A yellow "Low Risk" badge is visible. The "Ether Value:" is shown as "\$0". Below this, a section titled "Related address (30)" has a "Refresh" button. A search bar contains "0x119". A table of related addresses is shown with columns for "Selected", "Dir.", "Risk", and "Type". The first two rows are highlighted. The first row shows "LABEL_0x1986" with address "0x1986ab****5006fc60" and "From" direction. The second row shows "LABEL_0x6930" with address "0x6930ce****744721e0" and "From" direction. The third row shows "LABEL_0xa89e" with address "0xa89e1b****b44103c3" and "To" direction. All three are marked as "EOA". A "COUNT: 30" bar is at the bottom.


C2: 0xd46f7e32050f9b9a2416c9bb4e5b4296b890a911



 **LABEL_0x5811** 


0x58111e5e9e35eb2a59631486b588
cb514a0fbf53



 


Ether Value: \$0


Related address (30) 



 


☒ Selected (30)  Dir. ▼ Risk ▲ Type ▲


☒  **LABEL_0x1986** 



From  EOA


0x1986ab****5006fc60 


☒  **LABEL_0x6930** 

From  EOA

0x6930ce****744721e0 




☒  **LABEL_0xa89e** 




To  EOA



0xa89e1b****b44103c3 

COUNT: 30


C3: 0x2eecbbe4fa4b67b127f50ef8640b30f6c7209d5c



 **LABEL_0x5811** 


0x58111e5e9e35eb2a59631486b588
cb514a0fbf53   



 


Ether Value: \$0


Related address (30) 



 


☒ Selected (30)  Dir. ▼ Risk ▲ Type ▲


☒  **LABEL_0x1986** 



From  EOA


0x1986ab****5006fc60 


☒  **LABEL_0x6930** 

From  EOA

0x6930ce****744721e0 

☒  **LABEL_0xa89e** 

To  EOA

0xa89e1b****b44103c3 

COUNT: 30

to the **LinkToEthValidatorOutgoing2** address.

As one can see from the screenshots attached - **no linkage has been identified.**

Result of the investigation

While the ethValidator address has several shows several ties to Gemini, BlockFi and Binance, it is not possible to conclude any results from this information without a valid law enforcement report.

Moreover, forensic investigation **has not shown any direct linkage from ethValidator to C1, C2 or C3.**

While this report shows that **no linkage has been found**, due to the nature of the blockchain technology, it is **not 100% proven that this address has no linkage**. An experienced blockchain user can blur tracement between wallets without leaving an indication that the tracement has been maliciously blurred (e.g. tornadocash).