Beosin Follow

Mar 25 · 9 min read · Listen

Save

A Closer Look at the Anti-Sybil Mechanism Under the Arbitrum Airdrop Hype

Recently, the airdrop of Arbitrum, a Layer 2 scaling protocol has become a hot topic in the crypto market.

On-chain data shows that the number of transactions on Arbitrum exceeded 1.21 million which was at a record high on March 22, surpassing the 1.08 million transactions on Ethereum mainnet and the 260,000 transactions on Optimism.

Arbitrum is a Layer 2 scaling protocol with high performance, low cost, and decentralization. After the airdrop on the evening of March 16, a large number of airdrop hunters were restricted by a series of anti-sybil rules. Today, we will study what anti-sybil rules are.

When it comes to a sybil attack, many users should be familiar with it. A Sybil attack uses a single node to simultaneously operate many active fake identities within a blockchain network.

The Airdrop Sybil Attack is an attack method against airdrop activities. Attackers use fake identities and addresses to obtain more airdrop tokens.

let’s start with the rules of the Arbitrum airdrop to learn about the anti-sybil mechanism.

Arbitrum Airdrop Rules and Sybil Detection Model

In the Arbitrum airdrop, airdrop strategies and a distribution model have been formulated to check whether each wallet address on the chain meets the airdrop criteria:

1. If all transactions of the airdrop recipient occur within 48 hours, 1 point will be deducted.

2. If the airdrop recipient's wallet balance is less than 0.005 ETH, and the wallet has not interacted with more than one smart contract, 1 point will be deducted.

3. If the wallet address of the airdrop recipient was identified as a sybil address during the Hop Protocol bounty program, the recipient will be disqualified.

4. There is also a criterion that has not been confirmed by Arbitrum, which is that users who use the same IP to connect to multiple wallets to view the number of airdrop tokens on http://arbitrum.foundation will be disqualified.

Meanwhile, Arbitrum uses on-chain data to identify related addresses owned by a user. They use data from Nansen, Hop, and OffChain Labs to remove addresses such as bridges, exchanges, and smart contracts. Some addresses are removed through manual detection, such as donation addresses.

Use the following data for data cleaning:

1. Raw Eligibility List (from Nansen)

2. Excluded Entities (from Nansen)

3. CEX Deposit Addresses (from Nansen)

4. CEX Deposit Addresses (traced from CEXs hot wallets)

5. Unique transaction and traces (from,to) Arbitrum

6. Unique transaction and traces (from,to) Ethereum

7. Internal Address list from OffChain Labs

8. Hop Blacklist

9. Hop list with eliminated Sybil Attackers

10. Nansen address tags

11. Other active addresses tagged manually

After data cleaning is complete, two types of charts will be generated:

The first type of graph will have each transaction with msg.value is treated as an edge with their (from_address, to_address). In the second graph, each funder/sweep transaction is treated as an edge with their (from_address, to_address). **Funder transaction** is the first ether transfer to an account. **Sweep transaction** is the last ether transfer from an account.

Clusters are generated by partitioning the above graph into strongly connected and weakly connected subgraphs. Large subgraphs are broken down using the Louvain Community Detection Algorithm, providing more refined results and eliminating Sybil addresses more accurately.

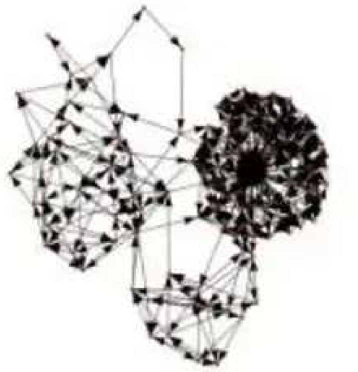
We identify Sybil clusters based on known patterns, here are some examples

● Addresses transferring funds in a cluster of more than 20 addresses

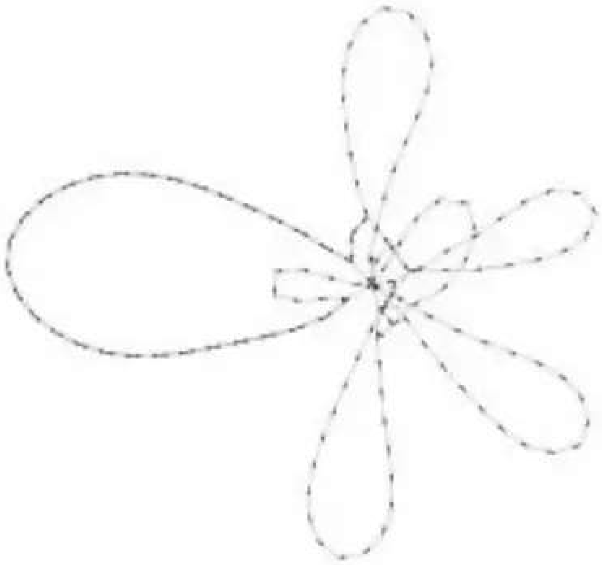
● Addresses that are funded from the same source

● Addresses with similar activity

From these patterns, a cluster was generated as follows:



Cluster 319 with 110 eligible addresses https://github.com/ArbitrumFoundation/sybil-detection



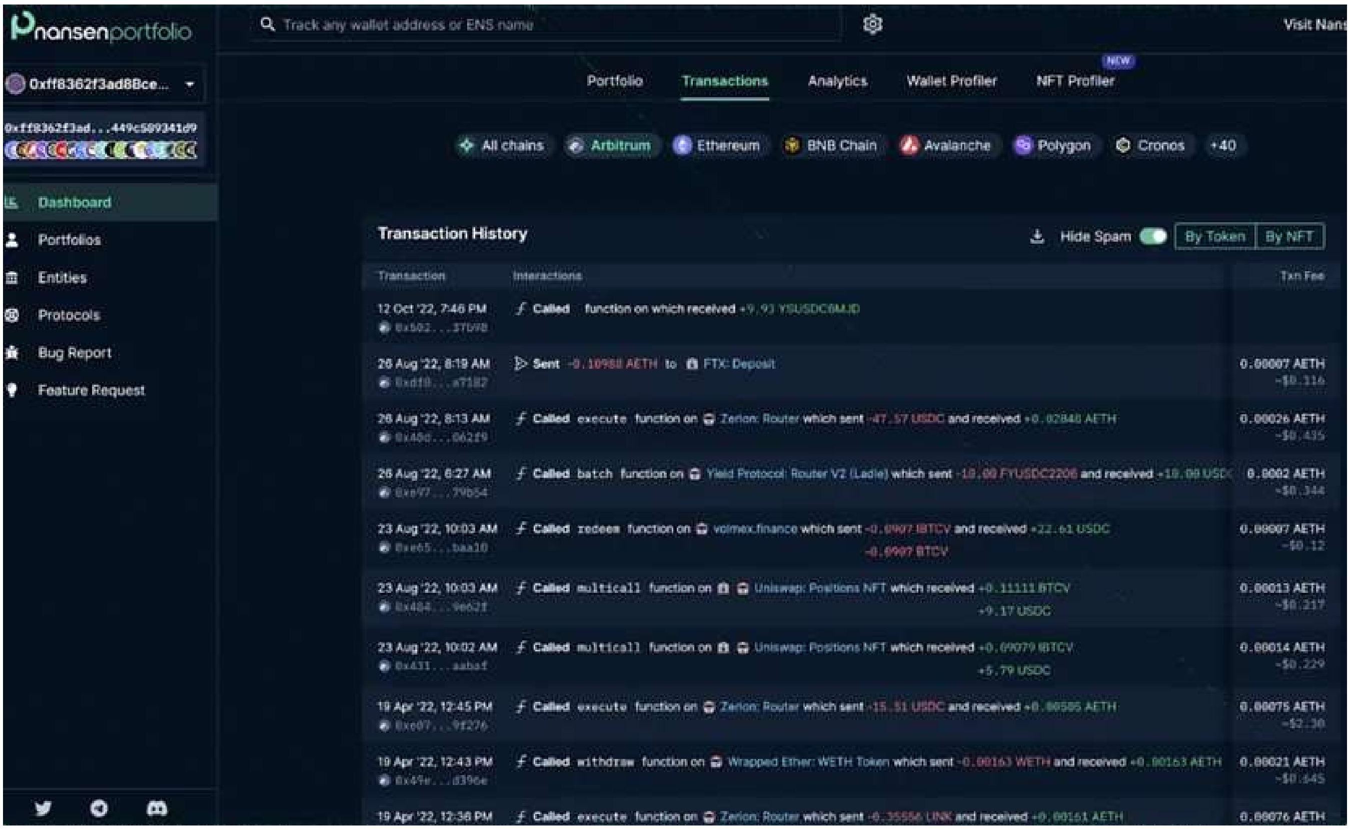
Cluster 1544with 56 eligible addresses https://github.com/ArbitrumFoundation/sybil-detection

How Do Researchers Identify Sybil Addresses?

Researchers with Offchain Labs identified possible Sybil addresses by using a clustering algorithm with from_address / to_address transaction data from Nansen Query, and integrated tracing and token transfers on Arbitrum and Ethereum. Then they manually checked the data for possible false sybil addresses.

Below is an example of a suspected sybil address:

Two addresses in a group of 400 addresses have very similar activities (sending funds to the same CEX deposit address).

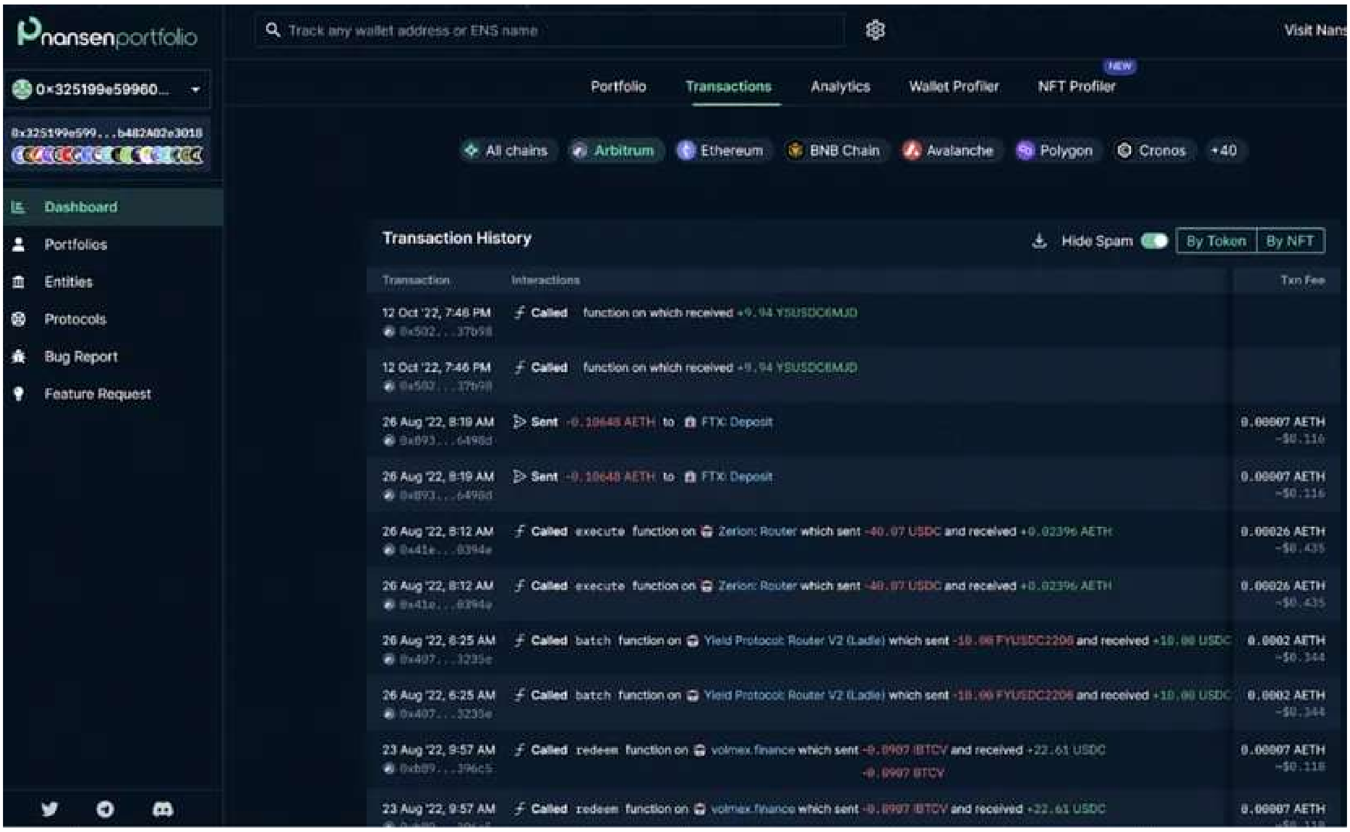


Transaction History

Transaction	Interactions	Txn Fee
12 Oct '22, 7:46 PM 0x502...37b98	Called function on which received +9.93 YSUSDC6MJD	
26 Aug '22, 8:19 AM 0xdf0...a7182	Sent -0.10988 AETH to FTX: Deposit	0.00007 AETH ~$0.116
26 Aug '22, 8:13 AM 0x40d...062f9	Called execute function on Zerion: Router which sent -47.57 USDC and received +0.02848 AETH	0.00026 AETH ~$0.435
26 Aug '22, 6:27 AM 0xe97...79b54	Called batch function on Yield Protocol: Router V2 (Ladle) which sent -10.00 FYUSDC2206 and received +10.00 USDC	0.0002 AETH ~$0.344
23 Aug '22, 10:03 AM 0xe65...baa10	Called redeem function on volmex.finance which sent -0.0907 IBTCV and received +22.61 USDC -0.0907 BTCV	0.00007 AETH ~$0.12
23 Aug '22, 10:03 AM 0x484...9e62f	Called multicall function on Uniswap: Positions NFT which received +0.11111 BTCV +9.17 USDC	0.00013 AETH ~$0.217
23 Aug '22, 10:02 AM 0x431...aabaf	Called multicall function on Uniswap: Positions NFT which received +0.09079 IBTCV +5.79 USDC	0.00014 AETH ~$0.229
19 Apr '22, 12:45 PM 0xe07...9f276	Called execute function on Zerion: Router which sent -15.51 USDC and received +0.00505 AETH	0.00075 AETH ~$2.30
19 Apr '22, 12:43 PM 0x49e...d396e	Called withdraw function on Wrapped Ether: WETH Token which sent -0.00163 WETH and received +0.00163 AETH	0.00021 AETH ~$0.645
19 Apr '22, 12:36 PM	Called execute function on Zerion: Router which sent -0.35556 LINK and received +0.00161 AETH	0.00076 AETH

Source: Nansen

It can be seen that the two addresses performed similar operations at almost the same time.

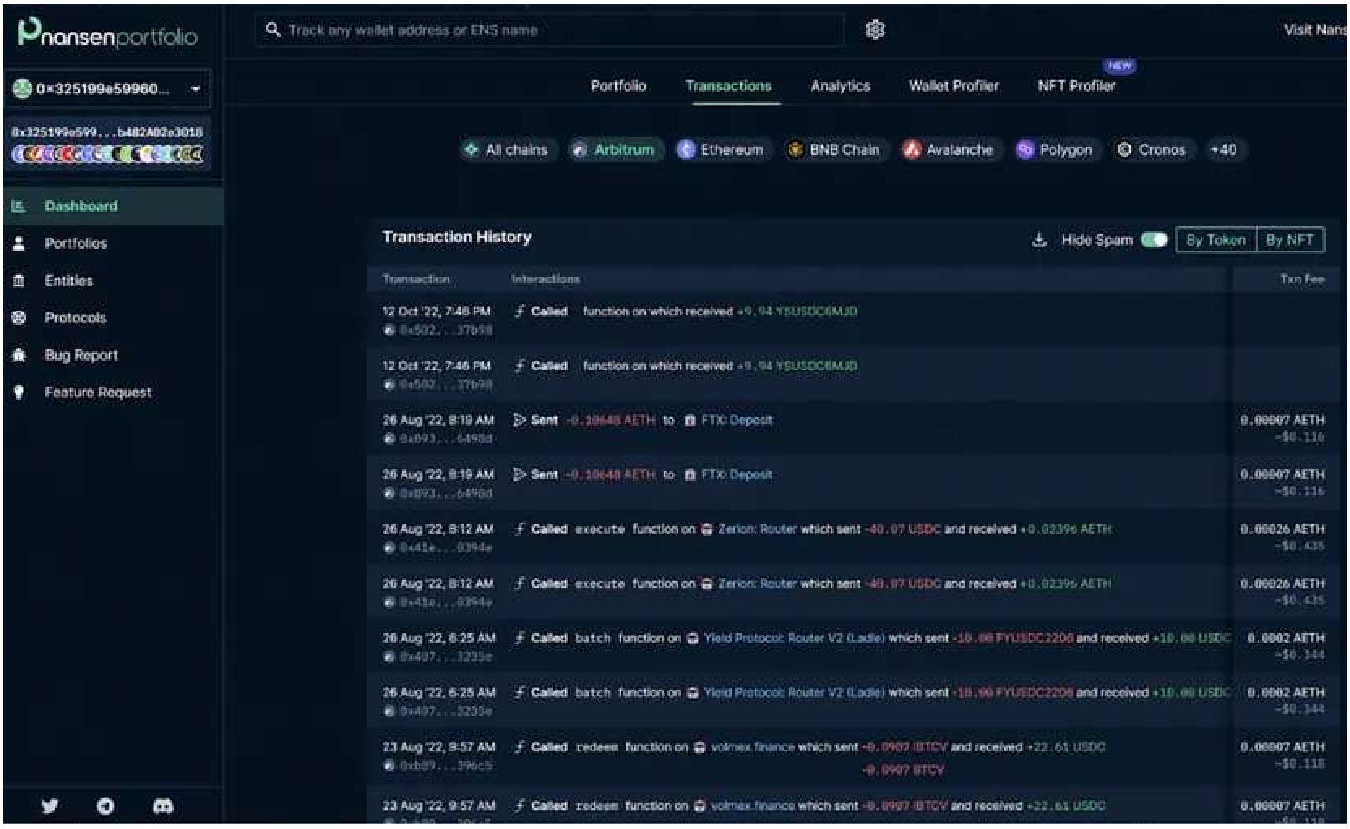


Transaction History

Transaction	Interactions	Txn Fee
12 Oct '22, 7:46 PM 0x502...37b98	Called function on which received +9.94 YSUSDC6MJD	
12 Oct '22, 7:46 PM 0x502...37b98	Called function on which received +9.94 YSUSDC6MJD	
26 Aug '22, 8:19 AM 0x893...6498d	Sent -0.10648 AETH to FTX: Deposit	0.00007 AETH ~$0.116
26 Aug '22, 8:19 AM 0x893...6498d	Sent -0.10648 AETH to FTX: Deposit	0.00007 AETH ~$0.116
26 Aug '22, 8:12 AM 0x41e...0394e	Called execute function on Zerion: Router which sent -40.07 USDC and received +0.02396 AETH	0.00026 AETH ~$0.435
26 Aug '22, 8:12 AM 0x41e...0394e	Called execute function on Zerion: Router which sent -40.07 USDC and received +0.02396 AETH	0.00026 AETH ~$0.435
26 Aug '22, 6:25 AM 0x407...3235e	Called batch function on Yield Protocol: Router V2 (Ladle) which sent -10.00 FYUSDC2206 and received +10.00 USDC	0.0002 AETH ~$0.344
26 Aug '22, 6:25 AM 0x407...3235e	Called batch function on Yield Protocol: Router V2 (Ladle) which sent -10.00 FYUSDC2206 and received +10.00 USDC	0.0002 AETH ~$0.344
23 Aug '22, 9:57 AM 0xb89...396c5	Called redeem function on volmex.finance which sent -0.0907 IBTCV and received +22.61 USDC -0.0907 BTCV	0.00007 AETH ~$0.118
23 Aug '22, 9:57 AM	Called redeem function on volmex.finance which sent -0.0907 IBTCV and received +22.61 USDC	0.00007 AETH

Source: Nansen

Despite this, some people still complain about the flaws in Arbitrum's airdrop strategy. The strategy regards sybil addresses as normal, but the wallet addresses of real users are restricted instead.



Transaction History

Transaction	Interactions	Txn Fee
12 Oct '22, 7:46 PM 0x502...37b98	Called function on which received +9.94 YSUSDC6MJD	
12 Oct '22, 7:46 PM 0x502...37b98	Called function on which received +9.94 YSUSDC6MJD	
26 Aug '22, 8:19 AM 0x893...6498d	Sent -0.10648 AETH to FTX: Deposit	0.00007 AETH ~$0.116
26 Aug '22, 8:19 AM 0x893...6498d	Sent -0.10648 AETH to FTX: Deposit	0.00007 AETH ~$0.116
26 Aug '22, 8:12 AM 0x41e...0394e	Called execute function on Zerion: Router which sent -40.07 USDC and received +0.02396 AETH	0.00026 AETH ~$0.435
26 Aug '22, 8:12 AM 0x41e...0394e	Called execute function on Zerion: Router which sent -40.07 USDC and received +0.02396 AETH	0.00026 AETH ~$0.435
26 Aug '22, 6:25 AM 0x407...3235e	Called batch function on Yield Protocol: Router V2 (Ladle) which sent -10.00 FYUSDC2206 and received +10.00 USDC	0.0002 AETH ~$0.344
26 Aug '22, 6:25 AM 0x407...3235e	Called batch function on Yield Protocol: Router V2 (Ladle) which sent -10.00 FYUSDC2206 and received +10.00 USDC	0.0002 AETH ~$0.344
23 Aug '22, 9:57 AM 0xb89...396c5	Called redeem function on volmex.finance which sent -0.0907 iBTCV and received +22.61 USDC -0.0907 BTCV	0.00007 AETH ~$0.118
23 Aug '22, 9:57 AM	Called redeem function on volmex.finance which sent -0.0907 iBTCV and received +22.61 USDC	0.00007 AETH

Source: Nansen

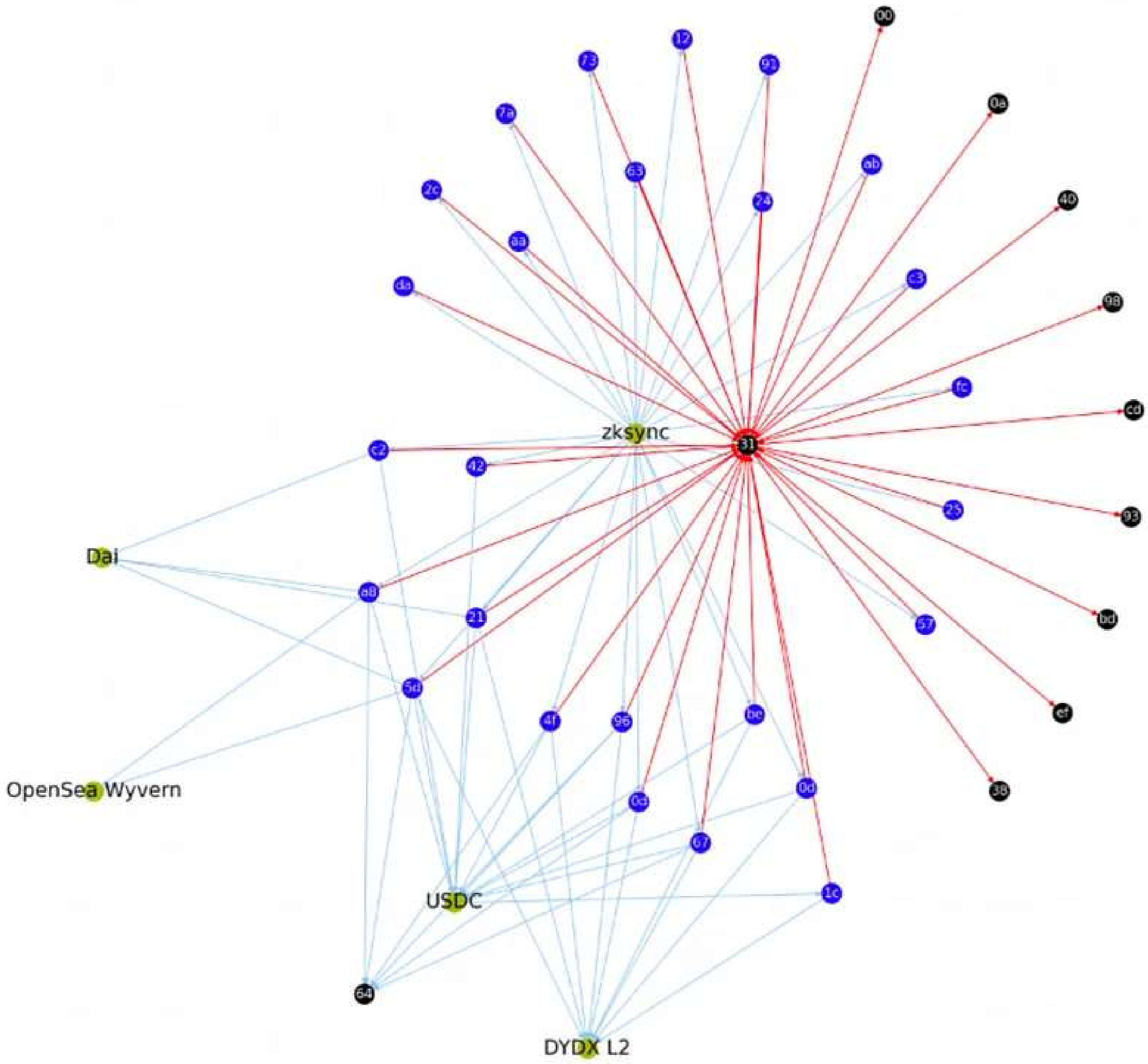
In addition to Arbitrum, Hop Protocol airdrop identified many sybil attackers through anti-sybil rules last year.

Sybil Attackers During Hop Protocol Airdrop

On May 6, 2022, after Hop Protocol officially announced the airdrop rules, it stated that among the 43,058 addresses which were initially eligible for the airdrop, 10,253 were identified as sybil attackers.

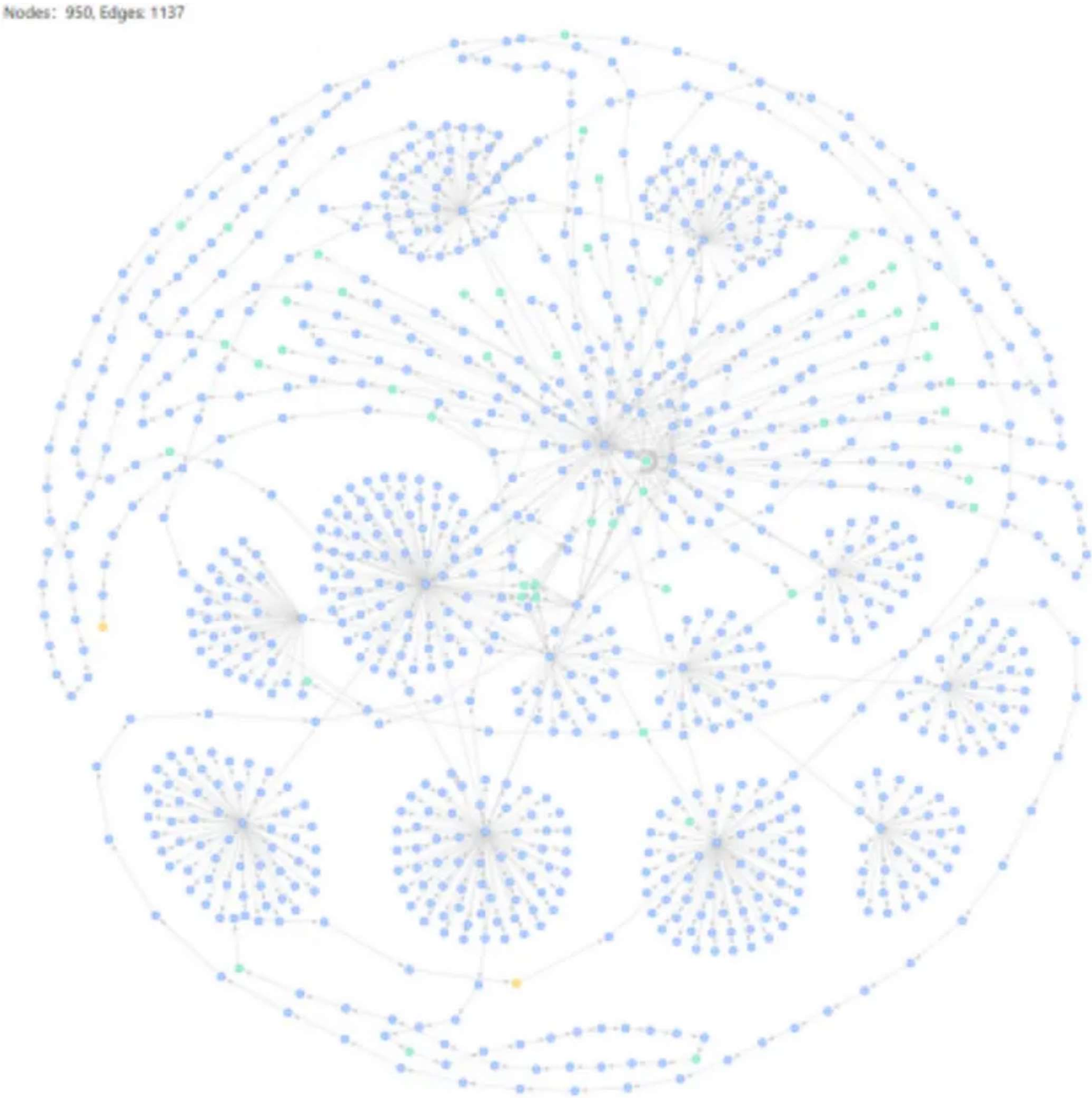
The following are some of the rules for judging sybil attackers by Hop Protocol:

1. Multiple addresses have a parent fund distribution or collection address, which proves that it was a sybil attacker:



Source: Sybil Attacker Report # 275

2. Multiple addresses have obvious correlations in transactions:



Source: Sybil Attacker Report # 367

3. Sybil attacks have similar operations at almost the same time, including batch transfers in a short period of time, the same gas value, and the similar number of assets used to interact with smart contracts.

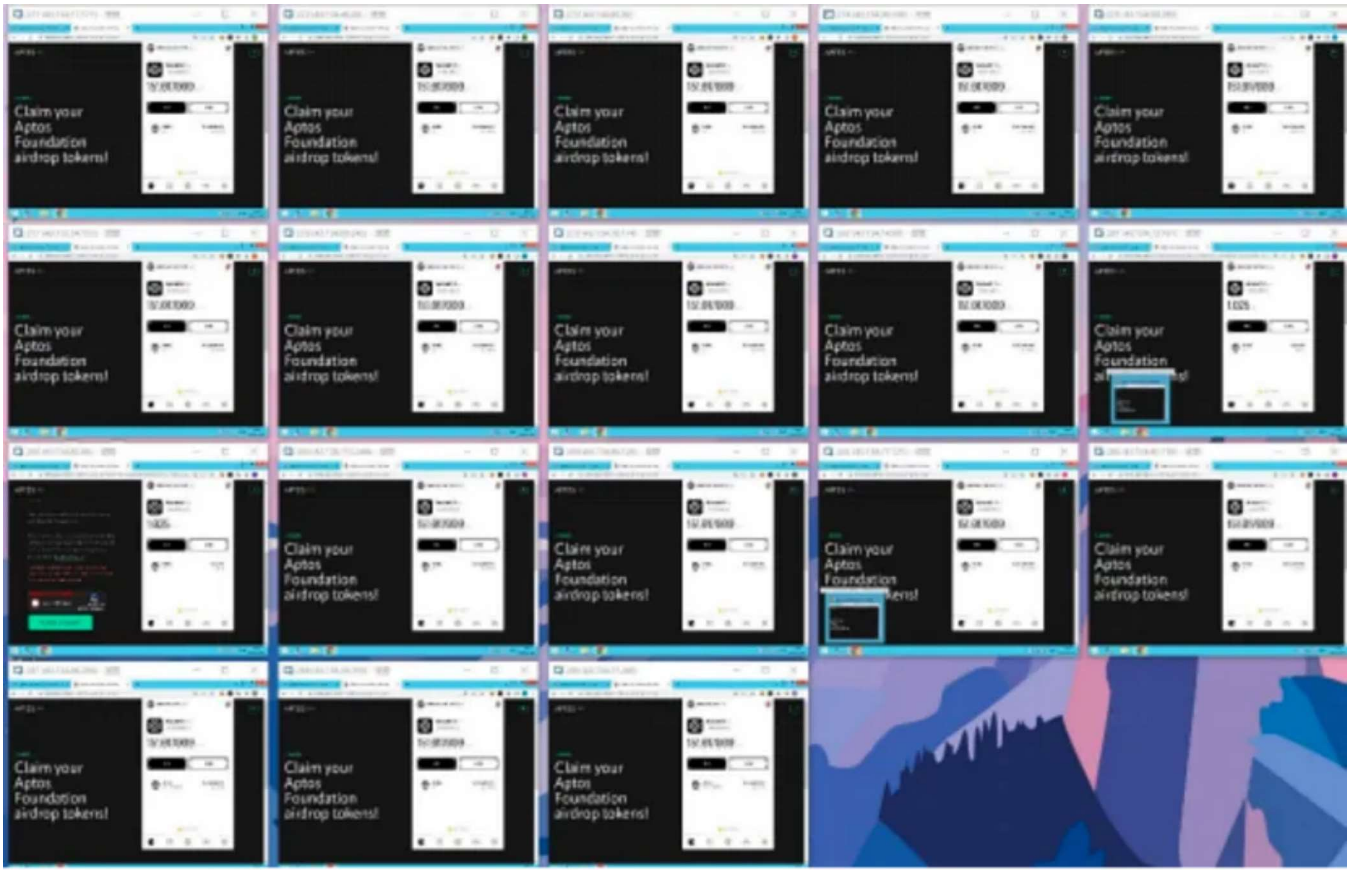
4. The interaction history of sybil addresses has the attack records of other projects in the past.

There are teams with little anti-sybil experience who did not have anti-sybil rules when launching their airdrop, such as Aptos.

Looking back at Aptos' airdrop, did airdrop hunters have a big win?

During the Aptos airdrop event in October last year, many airdrop hunters received a large number of tokens because the Aptos team did not prevent sybil attacks.

Someone shared a screenshot of his/her application for Aptos test network on Twitter and communities, and there were multiple accounts on the VPS host. According to users who claimed Aptos airdrop, each testnet application account can get 300 tokens, and users who mint NFTs have 150 tokens. If you have 100 accounts, you can get 30,000 tokens, and if you have 1,000 accounts, you can get 300,000 tokens.



After Aptos was listed on Binance, the price pumped instantly, and then there was a huge dump. **According to researchers' analysis, sybil attack addresses accounted for 40% of the Aptos tokens deposited into Binance at that time.**

It can be seen that sybil attack will have an impact on the project and users, such as **the impact on the token price, the damage to the reputation of the project, and the impact on community builders and participants.**

How to Determine Anti-sybil Rules?

When airdropping, the project team will use an anti-sybil mechanism to prevent airdrop hunters from obtaining too many tokens through multiple wallet addresses or other means to airdrop tokens to real users.

From airdrops in the past, we can see the features of sybil attacks:

1. The funds of addresses are distributed/collected by the same parent address

2. Exactly the same interaction process, time, and projects

3. The same gas value, transaction amount, and time

4. There are frequent transfers between addresses

The following are some anti-sybil mechanisms that project teams may use:

Snapshot: The project team can take a snapshot of all addresses at a specific time, and airdrop tokens to those addresses that have activities and interactions before that time. This prevents airdrop hunters from creating new addresses to acquire tokens after the snapshot time.

Interaction route: Take the addresses that interact with a project within a period of time, and check the consistency of the interaction route of these addresses before/after participating in this project according to the interaction time.

Fund flow: mainly check the flow direction of funds and check the situation of one-to-many or many-to-one transfers of wallets.

Interaction amount: View the amount of each interaction and the reuse rate of funds.

Interaction Frequency: Export addresses that interact with a project within a certain period of time, and use Excel or the project's self-developed board to take the data in the abnormal peak period for further research. The project team can check whether the activities of these addresses are similar.

Interaction times: Take the details of the addresses that participated in the interaction of this project within a certain period of time. Check whether the number of past interactions and the number of interactions after participating in this project are sufficient.

Proof of Stake: Proof of Stake (PoS) is a consensus mechanism used by some blockchains to validate transactions. In PoS, users need to hold a certain amount of tokens to participate in the network. Some project teams can require participants to hold a certain amount of tokens to be eligible for airdrops, raising the requirement for airdrops.

KYC/AML verification: The project teams can require participants to pass the KYC (Know Your Customer) or AML (Anti-Money Laundering) verification process. This process can help verify the identity of participants, which helps prevent sybil attacks.

For example, Beosin KYT virtual asset anti-money laundering compliance and analysis platform **can help customers avoid interacting with potential risk addresses (sybil addresses), and at the same time identify abnormal behaviors, and Beosin Path Tracing can intelligently find more suspicious addresses to allow risk verification to be easier.** Further reading: https://medium.com/@Beosin_com/beosin-kyt-an-on-chain-expert-to-meet-all-your-aml-needs-257e0b306416

Social media verification: The project teams can require participants to follow, like, or repost their social media posts to be qualified for airdrops. This helps ensure that participants are real people and not bots.

Whitelist: The whitelist is a list of addresses eligible for an airdrop. The project teams can limit airdrops to a whitelist of participants, which helps prevent sybil attacks.

Limit on the number of transactions: The project teams can limit the number of transactions that can be made by each address. This prevents sybils from acquiring too many tokens by making a large number of transactions.

Holding time limit: The project teams can require that each address eligible for an airdrop hold its tokens for a certain period. This prevents users from rapidly buying and selling tokens.

Other supporting references:

Social media activities: registration time, frequency of posting, quality of posting (likes and retweets), fans, followers, avatar, profile, etc.

IP address: the number of wallet addresses of the same IP/device and the frequency of changing the IP of a wallet address, etc.

What should we pay attention to when participating in an airdrop?

Beosin has also noticed users' enthusiasm for airdrops. As a security company, we need to share security suggestions as follows.

1. **Obtain information from the official website**: Before participating in an airdrop, you should go to the project's official website and social media pages to check relevant information, including the specific details and rules of the airdrop, the contract address of the token, etc.

2. **Do not easily disclose personal information and wallet addresses**: Some projects may require participants to provide personal information and wallet addresses, but you should be careful about your wallet privacy and security, and not disclose your sensitive information to unknown websites and projects.

3 **Pay attention to risk warnings and precautions**: Before participating in an airdrop, you must carefully read the risk warnings and precautions issued by the project to understand the relevant risks and precautions and understand your risk tolerance.