

What Addresses are Potential Fraud Accounts?

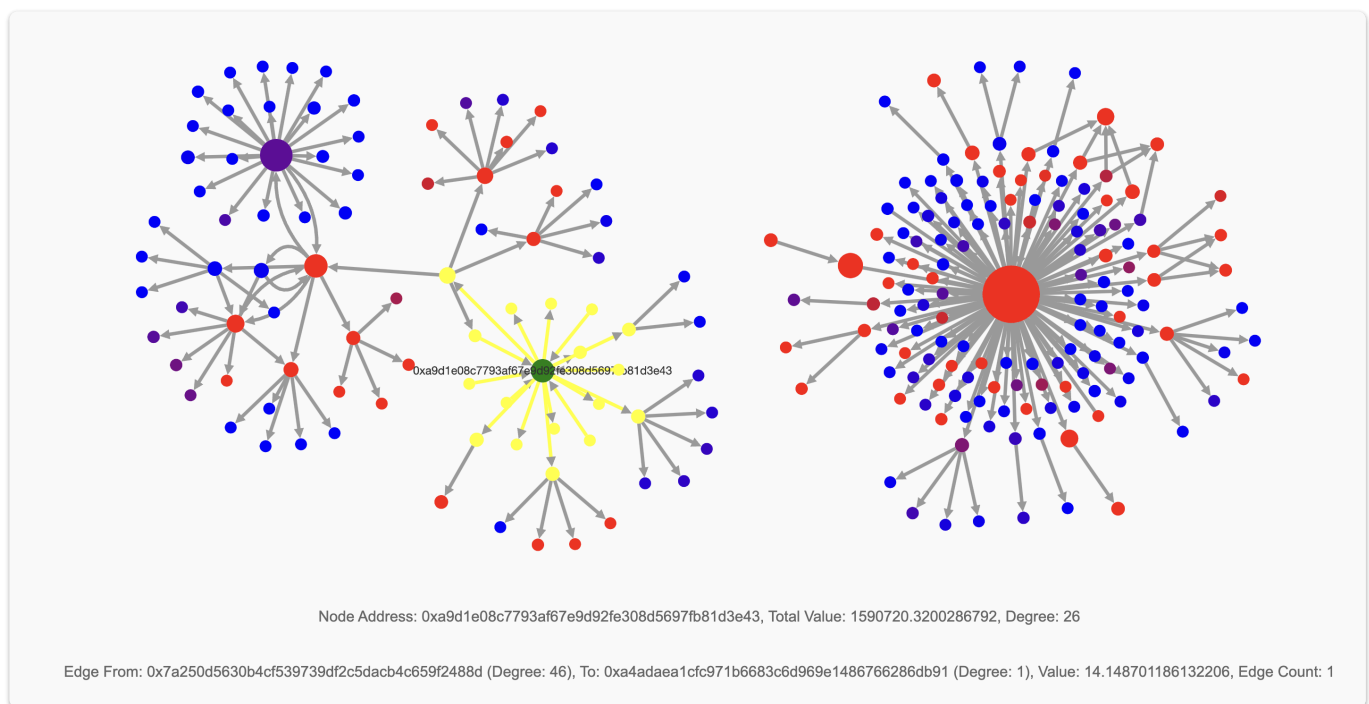
Risk Evaluation Score or Finding Patterns?

Transaction Analysis

- Frequency -> address of burst transaction
- Amount -> unusual amount
- Time -> unusual hours -> can we get ip with address?

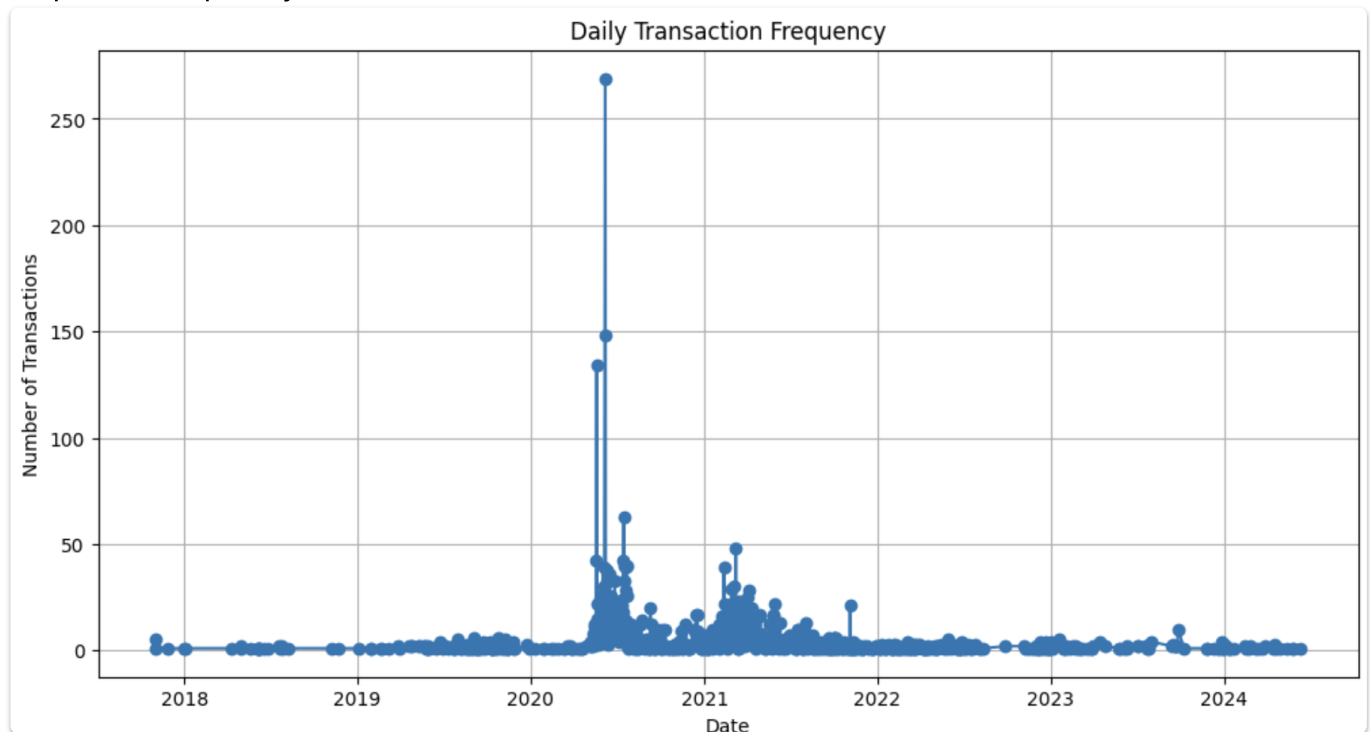
Address Analysis

- Cluster -> groups of addresses frequently transact to each other, indicate potential coordination



By observing the graph we can see a few clusters and huge nodes with massive transactions.

#1 plot tx frequency and list amount



#1.1 Bin data by day

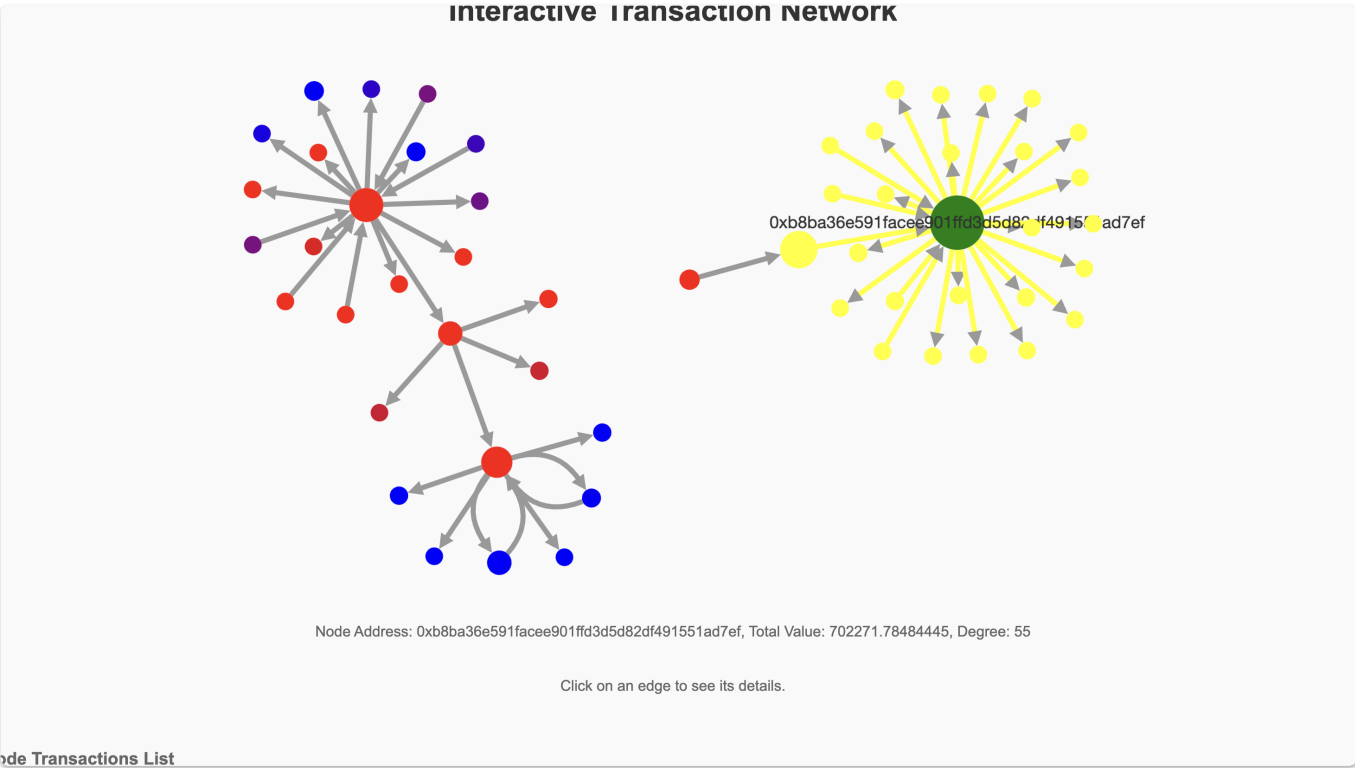
-> Result not useful

#1.2 Flatten the dimension

#1.3 List Top 20 tx frequency address

```
0xb8ba36e591facee901ffd3d5d82df491551ad7ef: 1188.0
0x7a250d5630b4cf539739df2c5dacb4c659f2488d: 470.0
0x8fd587b5ea5abd65ad3439d9e58c63222866baa9: 386.0
0x28c6c06298d514db089934071355e5743bf21d60: 329.0
0x569c1f1fcced968120e631466a55fa7acfec5b79: 265.0
0xb4e16d0168e52d35cacd2c6185b44281ec28c9dc: 262.0
0x168c612157ffca2b8e1bc89cb4a1afdf81e31edb: 236.0
0x3f5ce5fbfe3e9af3971dd833d26ba9b5c936f0be: 227.0
0x4a5cf9ecc6fdd4750df92a33ced79d477d9298c8: 223.0
0x51b6ccb815ee46ac94733099d7d281bbb952e26: 208.0
0x3e2ae8cc6584ad5011b498dc338f8bcd863b12ac: 138.0
0x5fff56c053d5428af6c34341535e0f6f9d5ebb4e: 120.0
0x5237eb109c66125c63907b91ac1473df8a4768b6: 105.0
0xebc18d25d8122da21f73a6bcb78971671f21f6ff: 95.0
0x092a106bd981df3415dcf931f10216a093b5ba1c: 88.0
0xae6aa86232e7892e973899f885584ce530fafd5: 64.0
0x2d62e6b6a8e1c4495b1255c2e558b93eb962925f: 59.0
0xd520294ec8b6cc2f8252412c14f83e937fe6a7a5: 56.0
0x49f9316eb22de90d9343c573fbd7cc0b5ec6e19f: 49.0
0x194d1ba9edb4bd849ca844870c05ac5cfb632b14: 47.0
```

Filtering out only the first Layer



The green node is the one with the highest tx frequency. And now we can see that his tx actions are mostly based on the 1 Layer, with value with 702271, 55 degree on 1 layer and value 145920, 125 degree on the second layer

Listing Node Transactions

Node Transactions List

From	To	Value	Degree	Time
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x33e6ab970b5a87a327e6bc13d65760697b4f5527	20	26	2023-12-26T14:15:11
0x0459c357f79a9f6efd3ccceda2239bffe69dd204	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	1502.0858537291438	3	2024-03-12T03:10:11
0xd7b1f3ca8e76206b2a6b13e405913b52f87a3b04	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	500	1	2022-07-19T00:24:27
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x33e6ab970b5a87a327e6bc13d65760697b4f5527	824.63116124	26	2023-12-27T20:08:11
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0xe6f30fb267ddc6ee5e2d4b44c2f7ad3543b0408b	2.5	26	2022-07-19T20:14:20
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0xe6f30fb267ddc6ee5e2d4b44c2f7ad3543b0408b	1.5	26	2022-07-20T02:18:03
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x33e6ab970b5a87a327e6bc13d65760697b4f5527	8.52927989	26	2023-12-28T00:16:11
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x87e7d106fe75fcd26d9ac311ef29ac1398dd4441	5	26	2022-07-20T02:18:03
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x33e6ab970b5a87a327e6bc13d65760697b4f5527	837.1023514	26	2023-12-30T23:57:23
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0xe6f30fb267ddc6ee5e2d4b44c2f7ad3543b0408b	1.5	26	2022-07-22T23:15:01
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x33e6ab970b5a87a327e6bc13d65760697b4f5527	2152.56414342	26	2024-01-01T03:22:11
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x87e7d106fe75fcd26d9ac311ef29ac1398dd4441	1	26	2022-07-22T23:16:11
0xeb1580f074ca7ea3d51cf6e3ad57e731faa9341	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	500	1	2022-07-19T00:24:27
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x87e7d106fe75fcd26d9ac311ef29ac1398dd4441	1	26	2022-07-22T23:19:56
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0xe6f30fb267ddc6ee5e2d4b44c2f7ad3543b0408b	1.5	26	2022-07-22T23:19:56
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x49b952d032098ff9aaba04ea4a14d0dec7ccccc	196	26	2022-07-27T02:20:18
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x23d65814f48d01680732c9d7200633cee3692a37	457.2	26	2022-07-27T02:30:06
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0xbce185e39b58d78d9b511feb472724d7d103b6ce	9999.85105	26	2022-07-27T02:30:39
0xea96b85b55c1c5370627cc52f8ee21ffc3164a30	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	1551340.1	1	2022-07-19T00:24:27
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x7f70faadba649d734e419586f61240774915a8c8	2853.756189	26	2022-07-27T02:34:00
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x8656b09057e750f485bb2b851c480150df0bdcbb	905	26	2022-07-27T02:37:52
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x00449d5cb9545742af2ee91e1f63716ae2e7d996	1001	26	2022-07-27T02:54:23
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x1ef4194853360e5662b0f54d56928f3be101c4e	4471	26	2022-07-27T02:55:32
0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x43d62b5f0e241a2a4fe07dd8dd27c13f5f5bf	103	26	2022-07-27T02:58:07
0x7e62ae4672e0acd4258ef5b763a23610fa9b519	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	12778.5	1	2022-07-19T00:29:53
0x80d10505e0bda9201ed113525adf68483082e062	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	256	1	2022-07-19T00:29:53

Select time range: 2018-04-29 → 2024-04-17

Select layer range: 0 1 2

Show Top 10 Transactions Highlight High Frequency Nodes Reset Graph

#1.4 How can we tell the difference between fraud tx and big investments?

-> trace origin, check whether it is from known risky addresses

-> if the dest of funds are going to multiple addresses in short period of time, may indicate laundering(smurfing technique)

#1.5 Color Tagging the Clusters

#1.6 Observing the visualization graph, there exists some back and forth swaps, I want to check the tx frequency of these addresses and check cycles in this graph.

-> The tool should let me easy filter out the selected address, perhaps with listing frequency or recent transactions

#2 Finding Cycles

When observing the graph using visualization tool, we can see obvious cycles and clusters

#2.1 Defining Suspicious Cycle

i set my definition of "suspicious" as :

```
if cycle_length <= 3 and cycle_value > 500:  
    cycle is suspicious
```

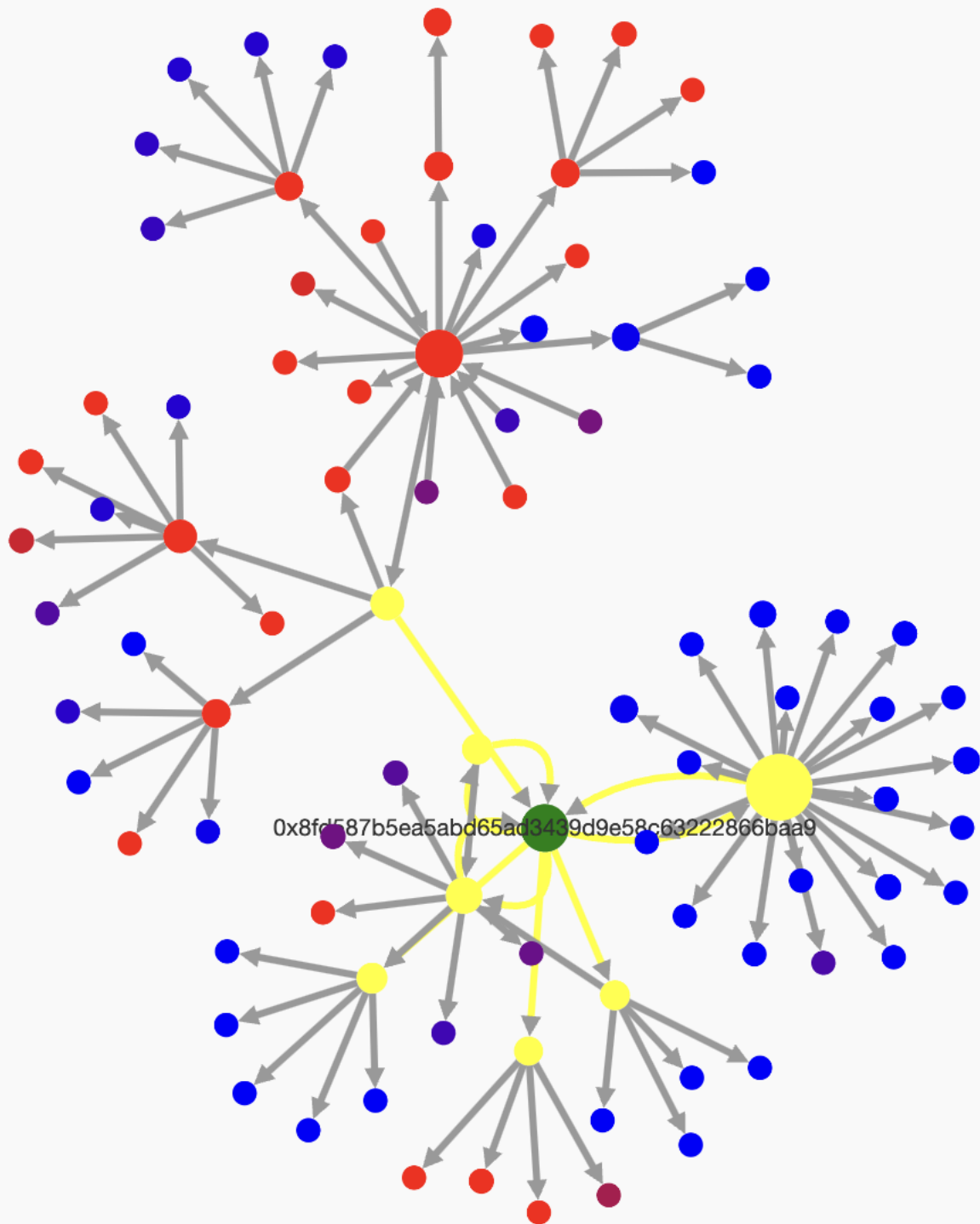
#2.2 List out top 20 sus cycles

We can see that both top sus cycles and top frequency address have duplications. A lot of them are also the same as some of the address @Manchien and I observed weird behaviors earlier

#2.3 The cycle doesn't guarantee fraud/laundrying. The swap may happen in a wide span of time. We need to check the frequency of these cycles. Wondering is there a way to visualize graph + a vector of time?

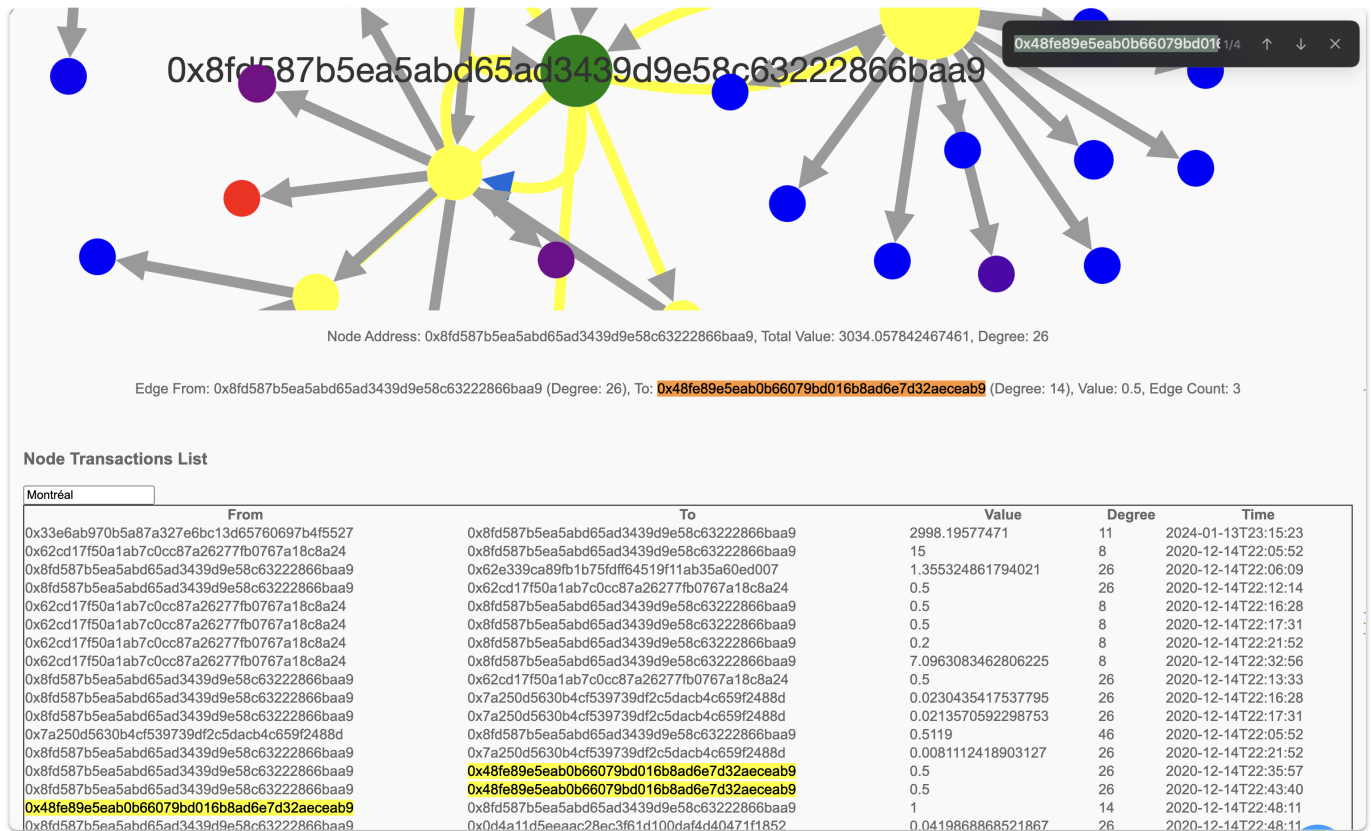
-> A time slider?

#2.4 Filter by frequency or amount



Observing this part of graph we can see the node `0x8fd587b5ea5abd65ad3439d9e58c63222866baa9` is a potential intermediate node, which is also the node with 3rd highest transaction frequency, with total value of 3024 units.

-> It is also very obvious that this node contains many cycles, which is a strong sign of potential laundering or high risk address



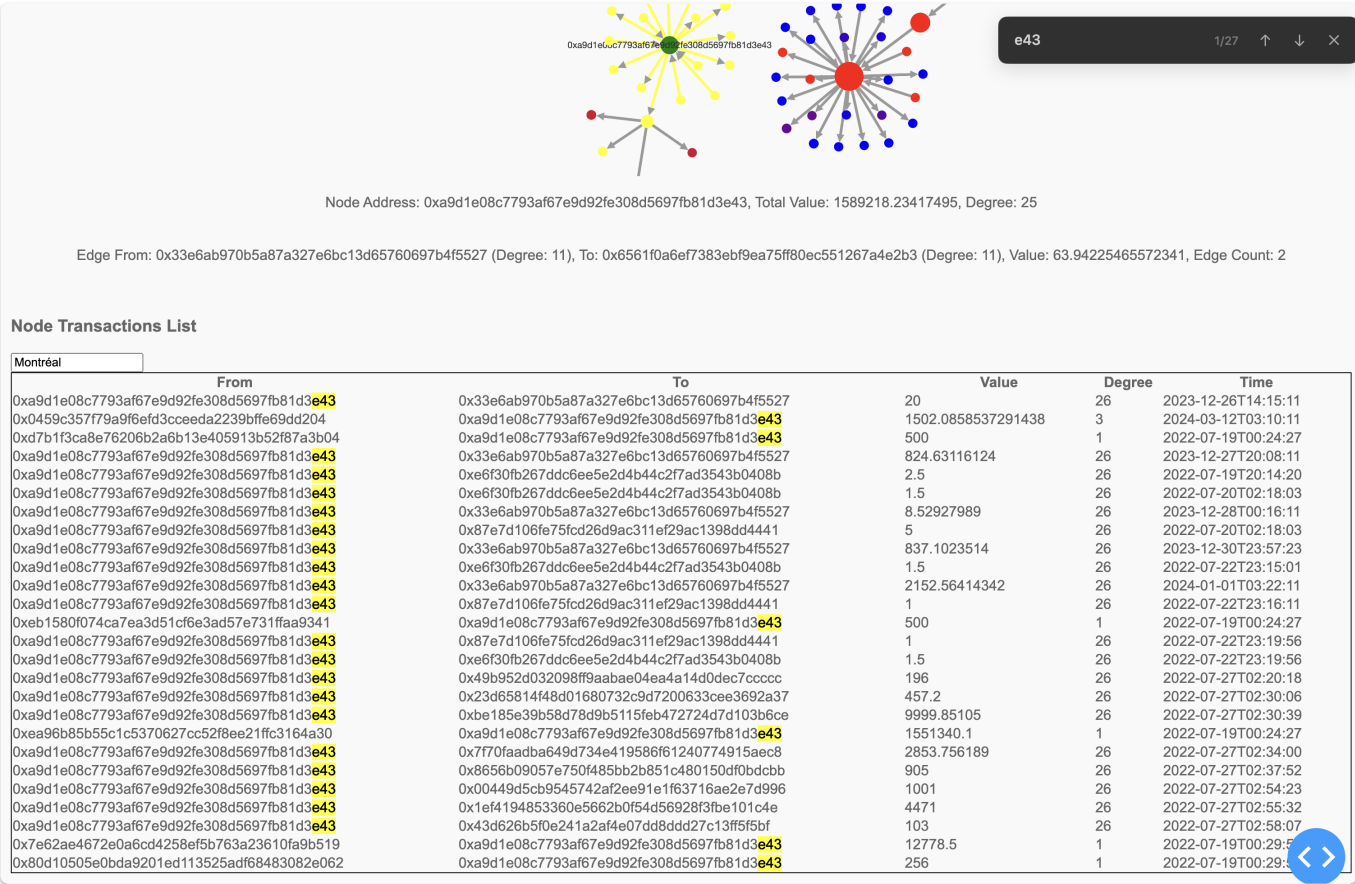
when highlighting out part of the tx, though they happened in a short period of time, their amount is too small

from other cycles we can see similar signs, which may be micro laundering or perhaps smart contract(dev) testings?

This is another Huge node within a suspicious cycle, the cycle consists of
 ['0x0459c357f79a9f6efd3cceeda2239bffe69dd204',
 '0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43',
 '0x33e6ab970b5a87a327e6bc13d65760697b4f5527'] with total value 2830.053840053603

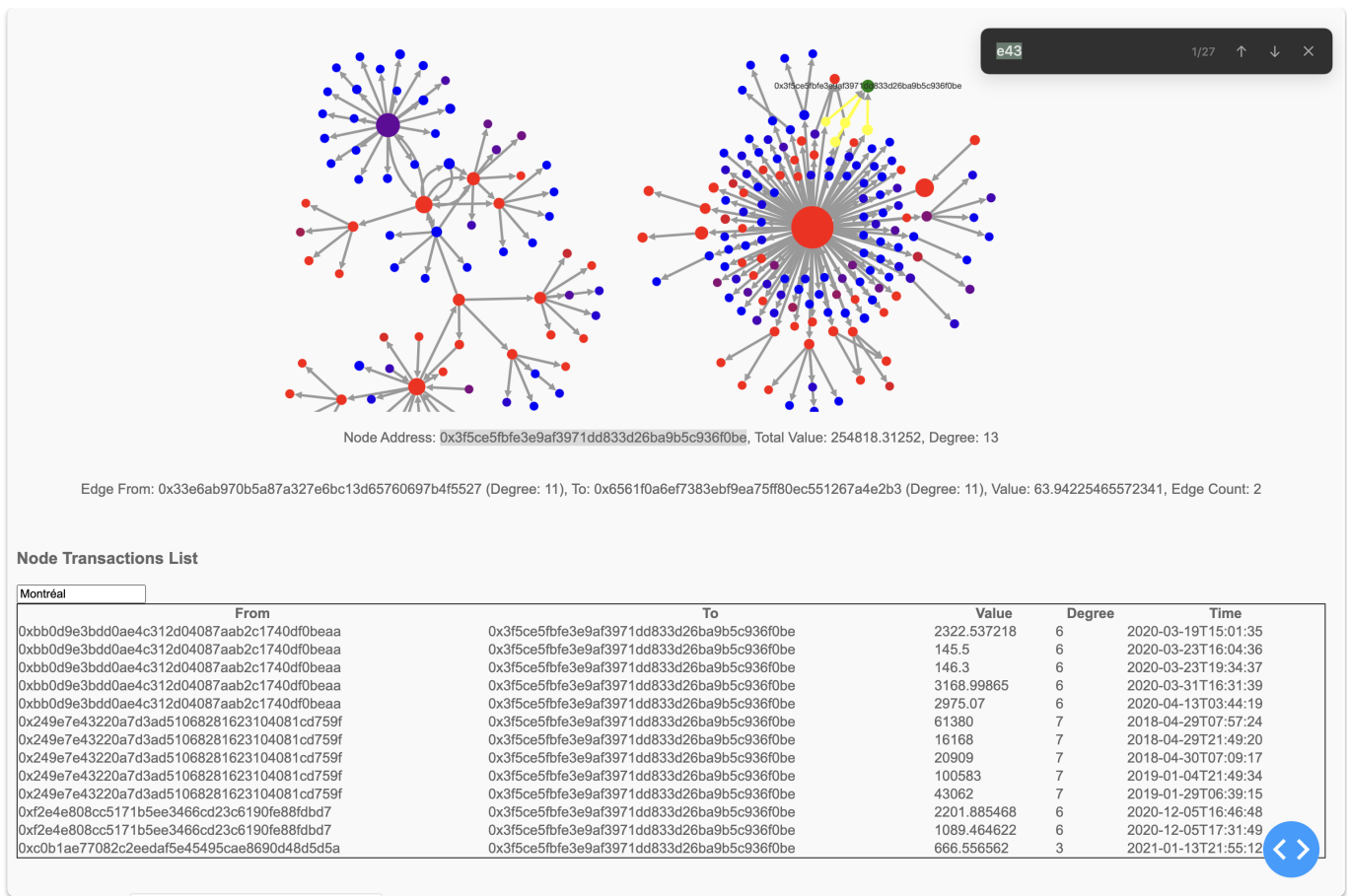
```
e43 -> 527, 20 uni on 2023/12/26 14:15:11
204 -> e43, 1502 unit on 2024/3/12 3:10:11
...
```

The maining point is the following image



e43 doing multiple high frequency transactions with high amount within a very short period of time, concentrated at July, 2022

There are also some interesting nodes that are single-way dumping tokens to big nodes, or nodes gathering humungous funds from several leaf nodes



#3 Finding Cross Chain Transactions (Chain Hopping)