Project X Exploit Investigation

Seigniorage Circus

13.07.2022

Introduction

This report focuses on the purported exploit of Project X, an event that resulted in the draining of 500,000 PXT with a value of around 900 AVAX from the project rewards pool.

The authors of this report were contracted to determine if this can be defined a deliberate and malicious act by the protocol management, an act of negligence, or an exploit by an external bad actor.

It is important to state from the outset that this report deals with information that may have legal consequences for the parties involved. The authors have this attempted to gather on-chain evidence as their primary and singular focus as it is irrevocable and without question in its veracity. While the authors do take a position on the question they were contracted to answer, where events are open to multiple interpretations the team has endeavoured to provide them.

In the interest of brevity we have included only information that is directly relevant to the chain of events. Supporting information has been gathered in large amounts but it is too lengthy and not material enough to be of value to the reader.

This report does not constitute financial advice of any kind. All investors are responsible for their own actions and are advised to carry out their own research to verify any information below that they may find relevant. The Author and Seigniorage Circus accept no responsibility for any outcome attributed to the public or private dissemination of the below information

Contracts, Wallets and Glossary of Terms

1. Contracts

- PXT Token V1: 0x40064ce057fb99a5c8e34f61365cc5996e59ab57
- PXT Token V2: 0x9e20af05ab5fed467dfdd5bb5752f7d5410c832e
- PXT Token V3: 0x9adcbba4b79ee5285e891512b44706f41f14cafd
- PXT V3 Proxy: 0x45f6176e253a4cd273822011d065e1fecde8b698

  PXT V3 Node Contract: 0x89a48f08963be9ddeef49796c6f2cae7ad54752
- Smoothing reserve: 0x4a4082ac05a0a6faaf5e2283e24c1b1df2870556
- Treasury: 0x68041dc29775c9ee6e10671204895593e4b6330f
- Operations Pool: 0x92e01e2f29084ddaf3d099fb56191edae066f0e9
- Rewards Pool: 0xADbf6ee98f86D5c234D60662639D0C067818294e

2. Contract Creators (CC)/ Wallets involved

- V1CC: 0x19c7798a756e353f6585302b8cb71fd31dea83af
- V2CC: 0xb244c6db819cff5c32f28f2ba55c027b0f9b8fdc
- V3CC: 0x9dc72782DEAc4Cf25e8319b9ffc1F689F5bF67fd
- V3CC Secondary Wallet: 0x2B0dcBA66631217e1ED23583dC959eaBf42FC090
- Rugster: 0xFbB3A79B276fE81719f24E96b78DfcEa7DCA3987
- V3CC-Rugster Intermediary: 0xfDf7f02Bc2484AFF15DDa407ca48E426668715C1
- Rugster test wallet: 0x44D4937C8B8caF785a0AF22265Ae7AAbB1D97577
- Suspicious wallet 1: 0x222C13939E2eBb2fB91307ee446D4896716C818E
- LeonACosby#9865: 0xEF7aE34d35D1e6eF6f9791aC8be94F3851A6A08C

Timeline

28.12.2021, Project X launches with PXT was its native token [PXT Token V1]. PXT Token V1 soon presented problems for the dev team. The reward system was designed for 24 hr reward allocation and the project devs wanted to change the time horizon to 1 hr.

07.01.2022, 0xdicaprio#7777 announced the replacement of the reward contract. PXT Token V1 contract was untouched. On 15.01.2022, reward contract was successfully replaced. [1.1]

17.01.2022 An announcement is made regarding migration to PXT Token V2 contract. PXT Token V2 had adjusted tokenomics to support Project X's current and future goals. [1.2]

14.04.2022 Miner announces a major upgrade to the protocol, stated to start on 16.04.2022 [1.7]. The announcement stated a high level of flexibility for the protocol moving forwards:

"any further enhancements can simply be attached to the new contract meaning no further downtime in the future!"

V3 proxy contract, V3 Node Contract and PXT V3 token contract were deployed. There is no mention to the community about the V3 dev, or what kind of contract is being deployed. PXT V3 token contract and V3 Node Contract are deployed on top of V3 Proxy contract. Any changes required in the token can be made by the Proxy contract. On 18.04 the upgrade is complete.[1.3]

28.06.22 Rugster Test Wallet ‘practices’ transferring ownership of the Proxy contract to the Rugster. [1.4]

07.07.22 V3 CC transfers the ownership of proxy contract to Rugster. Rugster immediately pulls out 500,000 PXT and patches the contract to its original form. V3 Node contract has approval from Reward pool to spend unlimited V3 token [1.5]

Following these events Zorg makes a community announcement about the Rugster wallet and V3 Proxy contract. He implies that team has no idea what the Rugster wallet and V3 Proxy contract are.

Another announcement by Miner on the same day implies again that the V3 Proxy contract is a rogue and malicious contract with functions to drain rewards pool, put in place by ‘Paulo’ the dev without their knowledge.

07.08.2022 another team announcement states that they have spoken with Paulo and narrowed the issue down to an exploit via information gathered from their Github. [1.6]

3. **Wallet Connections**

Funding

- V1CC funded V3CC. [2.1]

- V2CC wallet was funded by a wallet which in turn was funded by V1 CC wallet [2.2]

- VC22 empties his wallet via a proxy to LeonACosby#9865 [2.11]

Ownership

- PXT V2 token contract ownership was transferred to the PXT V1 Token dev [2.4]

- V3CC transfers the ownership of PXT Token V3 contract to PXT V1 dev, keeps the ownership of Proxy contract. [2.5]

- V3CC transfers the ownership of Proxy contract to Rugster.[2.6]

Other Connections

- V3 has transactions with Rugster-V3 go between wallet. [2.7]

- V3 CC has transactions with Suspicious Wallet 1 [2.8]

- Rugster sends 3 transactions to V3CC. V3CC doesn’t sends any transactions to Rugster.[2.9]

- Suspicious Wallet 1 has transactions with V3CC, Rugster test wallet and LeonACosby#9865. [2.10]

- V2CC also transacts with V3CC secondary wallet [2.3]

Summary of On-Chain Evidence & Conclusions Drawn

Funding & Wallet Ownership

Looking at the interplay between the wallets we can see links of common funding from V1CC to V3CC and via proxy to V2CC also. It is therefore likely that these wallets are highly interlinked if not simply the same person.

Looking at the timeline it appears that - after the issues with PXT V1- the user LeonACosby#9865, a developer funded by The Grape Dao for freelance work on Grape, was brought in for PXT V2. A set of transactions where V2CC emptied their wallet through an intermediary wallet to the wallet owned by LeonACosby#9865 supports this conclusion.

LeonACosby#9865 also shares links with the Rugster Test Wallet via Suspicious Wallet 1 as well as V3CC, so he is nominated as a person of interest and our prime suspect for the owner of Rugster wallet.

Of the developer wallets, V3CC has clear links with the Rugster Wallet (beyond the obvious transfer of ownership), as well as the Rugster Go Between Wallet and Suspicious Wallet 1. We can thus assume that V3CC knows the identity of the Rugster, and link with LeonACosby#9865.

Proxy Deployment

The deployment of the 'Rouge' Proxy contract matches the discord announcements of an upgrade by the Project X Team, and the Proxy contract has been upgrading PXT V3 Token and PXT V3 Node Contract for 3 months with close to 30 total changes made.

There is no feasible way that this was not known by the Project X development team. We must conclude then that the Proxy contract was and is a mechanism for the team to have flexibility over their token and not a compromise of the protocol by bad actor V3CC as they posit in their public facing announcements.

It is unclear to what extent the broader team were aware of the proxy contract but, as the proxy had been active with upgrades for a 3 month period, if no one in the team noticed this it is demonstrative of a level of incompetence or a severe lack of interest in the mechanisms that underlie the protocol.

Concluding Statement

The obvious conclusion here is that the V3CC initiated the rug with his transfer of ownership to the Rugster wallet for execution. We have ruled out V3CC as an unknown entity to the team because of the funding source of V1CC. It is our conclusion that the V3CC conducted the Rug while a member of the Project X team, who was originally tasked with the creation and deployment of the 'upgrade' on 18.04 and had since been maintaining and upgrading the protocol via the proxy contract.

The only feasible alternative is that V3CC transferred ownership of the proxy contract to someone who he believed would not abuse the power, or that the Github that the team blame for allowing an exploiter access contained the private keys to VCC3. Even in these most generous of readings, this is gross negligence with community funds.

The gross security risk of the exploit is still present, as the proxy contract is still owned by the Rugster. The Rugster also edited the PXT V3 Node Contract code while interacting with the reward pool and after pulling 500,000 PXT he patched it back up. We can only speculate as to why.

It is the conclusion of the investigators that this was a rug pull of the project by V3CC & potential collaborators, based on a voluntary transfer of the control of the protcols own proxy contract to another wallet, likely his own.

The purported obliviousness which the Project Team have demonstrated in their messaging implies wider involvement, or at the very least a willingness to mislead their community not just about the Rug but also the way that their protocol had been run for the 3 months prior. If the misleading nature of community focused team statements comes instead from a position of ignorance then it is little wonder that one or more predatory team members were able to defraud the investors of this community.

Recommended Follow Up Actions

Confrontation of Project X Core Team with the contents of this report.

Confrontation of LeonACosby#9865.

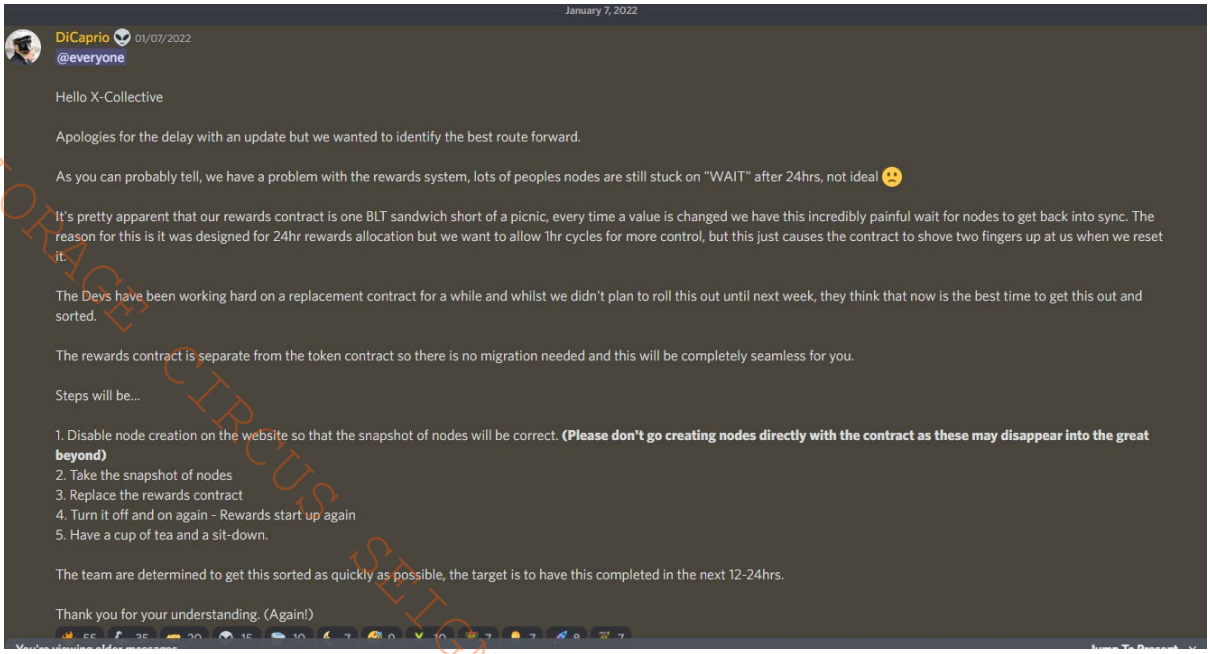
Both of these actors know who V3CC/Rugster are and can reveal the identity to the investigation team

Dissemination of this report to the Project X community and wider LC Community.

Investigation of Rugster Test Wallet links via additional wallet with contract deployment for AHE (Abeats), a large gamefi project, and cross-reference their records with Assure KYC to identify Rugster.

Timeline References

1.



January 7, 2022

DiCaprio 01/07/2022

@everyone

Hello X-Collective

Apologies for the delay with an update but we wanted to identify the best route forward.

As you can probably tell, we have a problem with the rewards system, lots of peoples nodes are still stuck on "WAIT" after 24hrs, not idea!

It's pretty apparent that our rewards contract is one BLT sandwich short of a picnic, every time a value is changed we have this incredibly painful wait for nodes to get back into sync. The reason for this is it was designed for 24hr rewards allocation but we want to allow 1hr cycles for more control, but this just causes the contract to shove two fingers up at us when we reset it.

The Devs have been working hard on a replacement contract for a while and whilst we didn't plan to roll this out until next week, they think that now is the best time to get this out and sorted.

The rewards contract is separate from the token contract so there is no migration needed and this will be completely seamless for you.

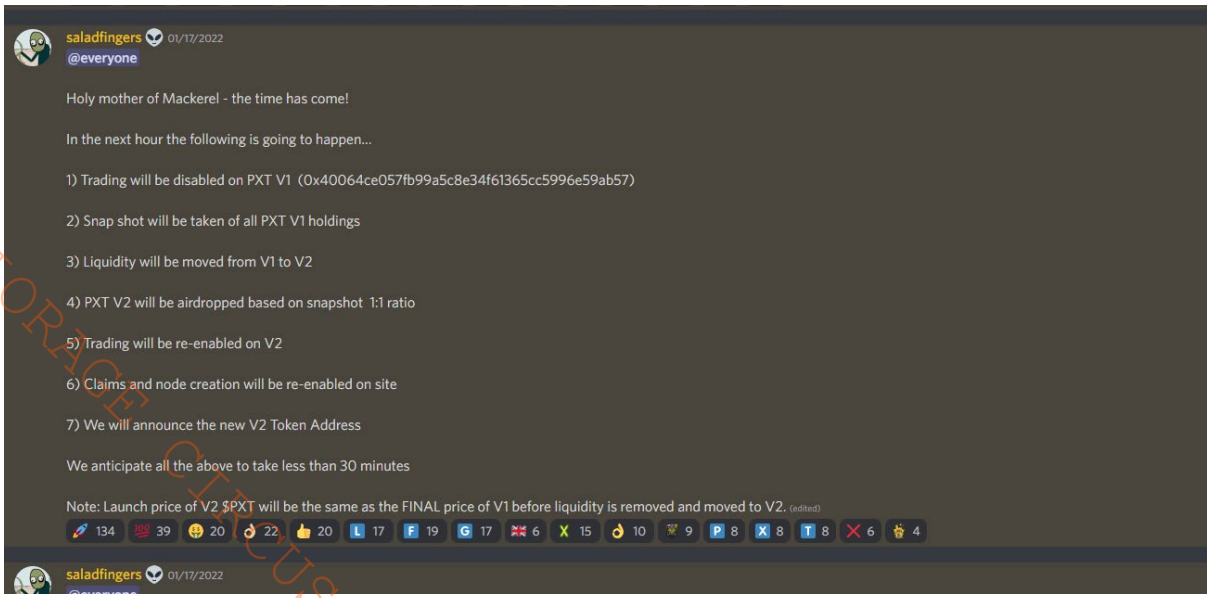
Steps will be...

1. Disable node creation on the website so that the snapshot of nodes will be correct. **(Please don't go creating nodes directly with the contract as these may disappear into the great beyond)**
2. Take the snapshot of nodes
3. Replace the rewards contract
4. Turn it off and on again - Rewards start up again
5. Have a cup of tea and a sit-down.

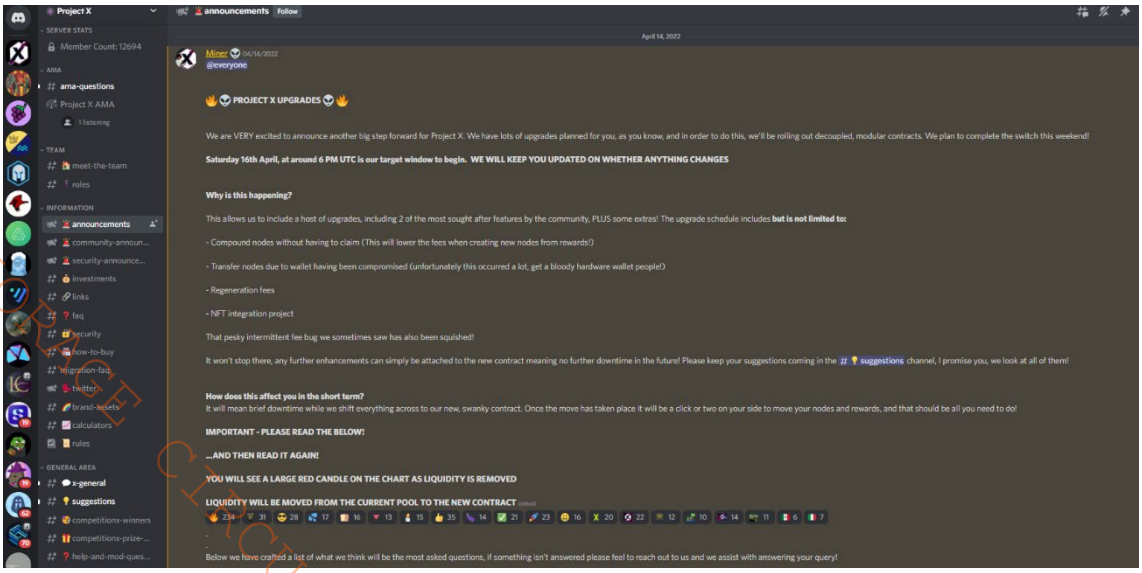
The team are determined to get this sorted as quickly as possible, the target is to have this completed in the next 12-24hrs.

Thank you for your understanding. (Again!)

2.



3.



4.

https://snowtrace.io/tx/0x8209c8ea6f0cb3260e1ead07c607f5abfd54c6a5e5023c69b2bf8177852386cc

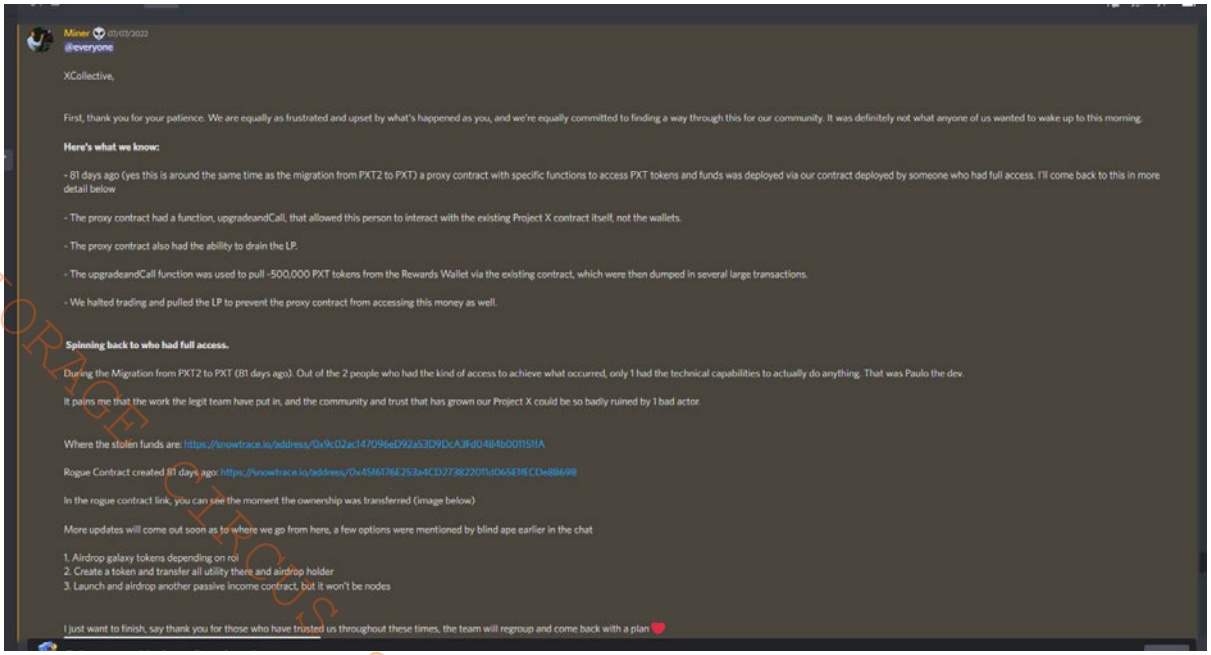
5.

https://snowtrace.io/tx/0x018afe1a612f6b4f1a1dea163f2d91a484444a9f460b2fe0a1318e433d71fc0e

https://snowtrace.io/tx/0xfc1e56015a5b856f01c744dd91725695e819ed0b3930945522e9f498cb167f81

https://snowtrace.io/tx/0x128c0c8416704b426615676f73e34ab190592ba9debd5349c115d9a9536ed562

6.



Miner 07/07/2022
@everyone

XCollective,

First, thank you for your patience. We are equally as frustrated and upset by what's happened as you, and we're equally committed to finding a way through this for our community. It was definitely not what anyone of us wanted to wake up to this morning.

Here's what we know:

- 81 days ago (yes this is around the same time as the migration from PXT2 to PXT) a proxy contract with specific functions to access PXT tokens and funds was deployed via our contract deployed by someone who had full access. I'll come back to this in more detail below

- The proxy contract had a function, upgradeandCall, that allowed this person to interact with the existing Project X contract itself, not the wallets.

- The proxy contract also had the ability to drain the LP.

- The upgradeandCall function was used to pull ~500,000 PXT tokens from the Rewards Wallet via the existing contract, which were then dumped in several large transactions.

- We halted trading and pulled the LP to prevent the proxy contract from accessing this money as well.

Spinning back to who had full access.

During the Migration from PXT2 to PXT (81 days ago). Out of the 2 people who had the kind of access to achieve what occurred, only 1 had the technical capabilities to actually do anything. That was Paulo the dev.

It pains me that the work the legit team have put in, and the community and trust that has grown our Project X could be so badly ruined by 1 bad actor.

Where the stolen funds are: https://snowtrace.io/address/0x9c02ac147096eD92a53D9DcA3Fd04Bf4b0011511A

Rogue Contract created 81 days ago: https://snowtrace.io/address/0x45f6176E253a4CD27382201fd066Ef1ECDe88698

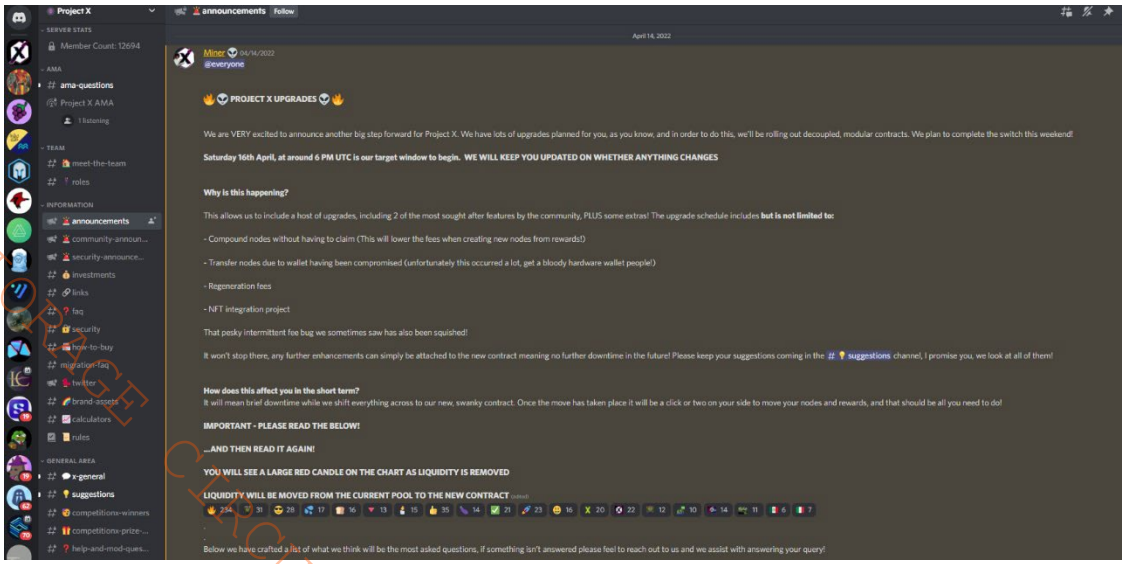
In the rogue contract link, you can see the moment the ownership was transferred (image below)

More updates will come out soon as to where we go from here, a few options were mentioned by blind ape earlier in the chat

1. Airdrop galaxy tokens depending on roi
2. Create a token and transfer all utility there and airdrop holder
3. Launch and airdrop another passive income contract, but it won't be nodes

I just want to finish, say thank you for those who have trusted us throughout these times, the team will regroup and come back with a plan ❤️

7.



TXN References

1. https://snowtrace.io/tx/0xfb2d132ce697b0d263fe4d46fe7a371c39b0d3fce5c397159896621df3989c0d

2. https://snowtrace.io/tx/0xea49324e93b2242737af2391b00726bd62302de7ab9532b57abc0abda137f10c

3. https://snowtrace.io/tx/0x411604ccb6ebf1f8c1a190d974e4ff8c701c1dd9cd1624cb6dedfbd190636db84

4. https://snowtrace.io/tx/0x411604ccb6ebf1f8c1a190d974e4ff8c701c1dd9cd1624cb6dedfbd190636db8

5. https://snowtrace.io/tx/0x7819b3ca9220effde91bc6dd586c3980d0a4b9ae400d7b0eb1d34e2521185243

6. https://snowtrace.io/tx/0x018afe1a612f6b4f1a1dea163f2d91a484444a9f460b2fe0a1318e433d71fc0e

7. https://snowtrace.io/tx/0x8409307b029403ed711524bf63ab38a24f9b44556aadb19ea69d5323ac60daaf

   https://snowtrace.io/tx/0xcc3a4e9b8342b5ef6c91b16c3a9aae244605b2553103ceeb276f8a81e9059e9d

   https://snowtrace.io/tx/0x093ff1859b5ea40ba43bae12a97ccd7b713f904d21b3cd5c5f1dd99f32ae6a69

8. https://snowtrace.io/tx/0xa5be5e5dbb9daac3a7eef65c5f9c7612fb7624215f920bb3462adbc319c84464

9. https://snowtrace.io/tx/0x9b26a8ec80e348a782e7e4b9f0d1364b405cdef8be27a0ce7fc5e890fd4e196e

10. https://snowtrace.io/tx/0x1f5d6197b6b27beb07b9c0936433bd5450fbf52037c054380a7bee3774459e28

    https://snowtrace.io/tx/0x613d95312cc5b4b0a41340d0bfaaffe8e22643403f7aa97adeef093ab1aa26d4

    https://snowtrace.io/tx/0x4877609bb375effdd4bf8aa035c5bbca9b9c0ae0ee591cb8c09d74d8fa0015d2

11. https://snowtrace.io/tx/0x9f7ce480365d1af092b3952698668e704784e4ed0bce09eb024721b5bfa0e855

    https://snowtrace.io/tx/0x53073f39864300079971583e2e8671bddb581ef321b39600546e4a92c5780ead