Closing Solana token accounts with an open source DApp to defend against scams

An experiment to find a user-friendly method to revert *delegation NFT scam* attacks in Solana.

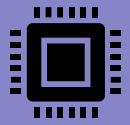
Motivation (I)

Many most up-to-date NFT scam in Solana don't just steal from users after tricking her to interact with a phishing DApp. Instead, they issue an *Approve* instruction to all of the user's ATAs, delegating them to an attacker's account. This effectively give the attacker the ability to keep stealing from the user as she receive more tokens or NFT in the future.

This is particularly egregious when the victim has some NFT or tokens stacked in some DApp that can only un-stake to the user account, from where they would immediately be retired by the attacker.

Furthermore, the subsequent transactions that the attacker performs stealing tokens or NFTs are not signed by the user and would not show on any Solana explorer in the user transaction history.

Motivation (II)



If a user find herself in such situation and she wants to use Phantom, she's out of luck, given that Phantom does not have a feature to remove account delegation (as of the day of writing).

We are assuming that the user does not posses the technical knowledge necessary to break the delegation via programming or CLI.

Motivation (and II)

I propose a user-friendly approach for the user to solve this problem: closing all her ATAs with a DApp called *Free Redeemer*, an open source DApp maintained by a popular Solana community member: **Andreas Schmidhofer**.

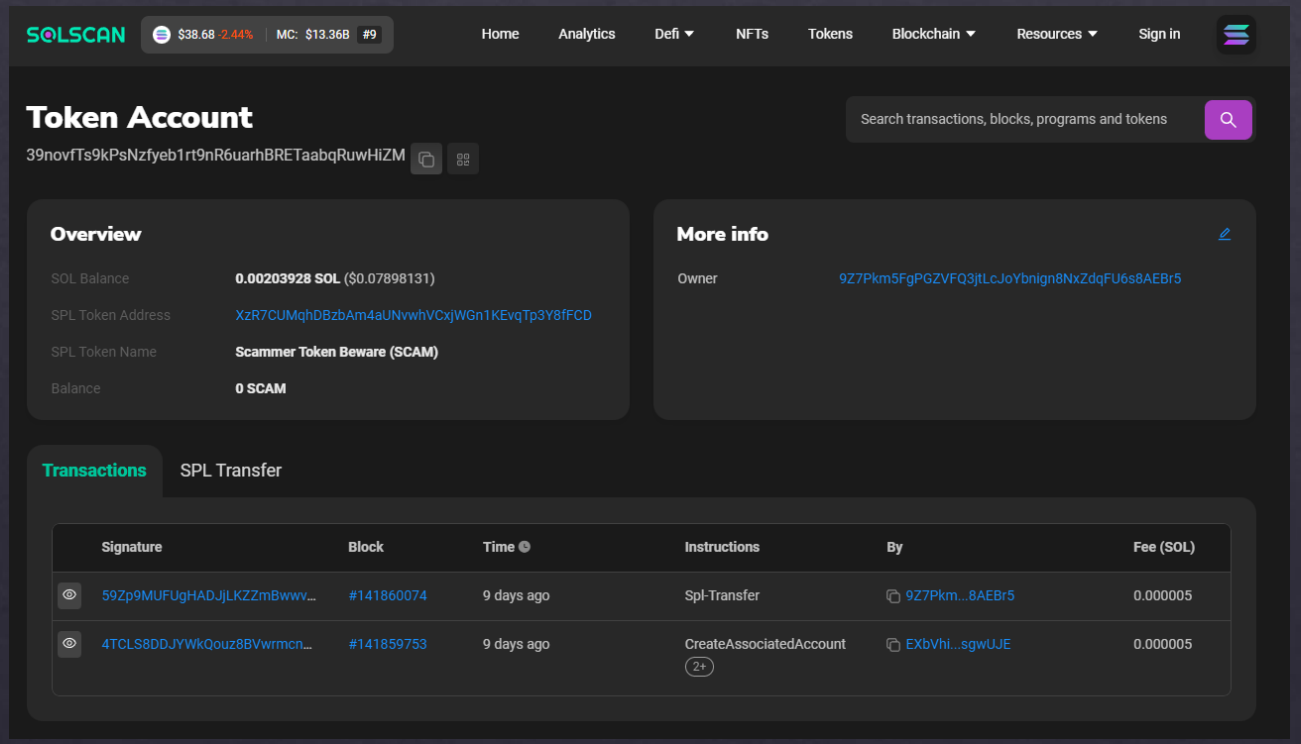
When the user unstack her funds, the ATA for this mint will be reopened but the delegation will be lost, allowing the user to keep her funds.

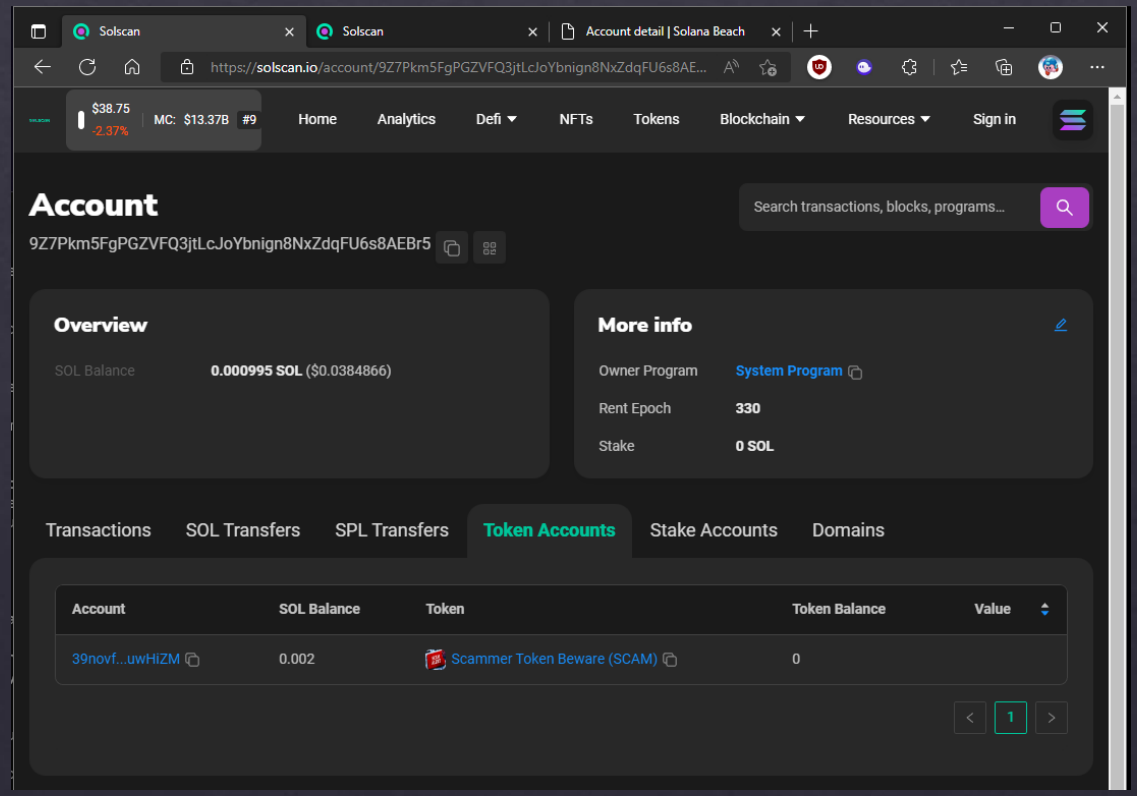
What follow is a small experiment, creating a situation similar to the one caused by this attack, and showing how the user can easily break the delegation.

Experiment outline

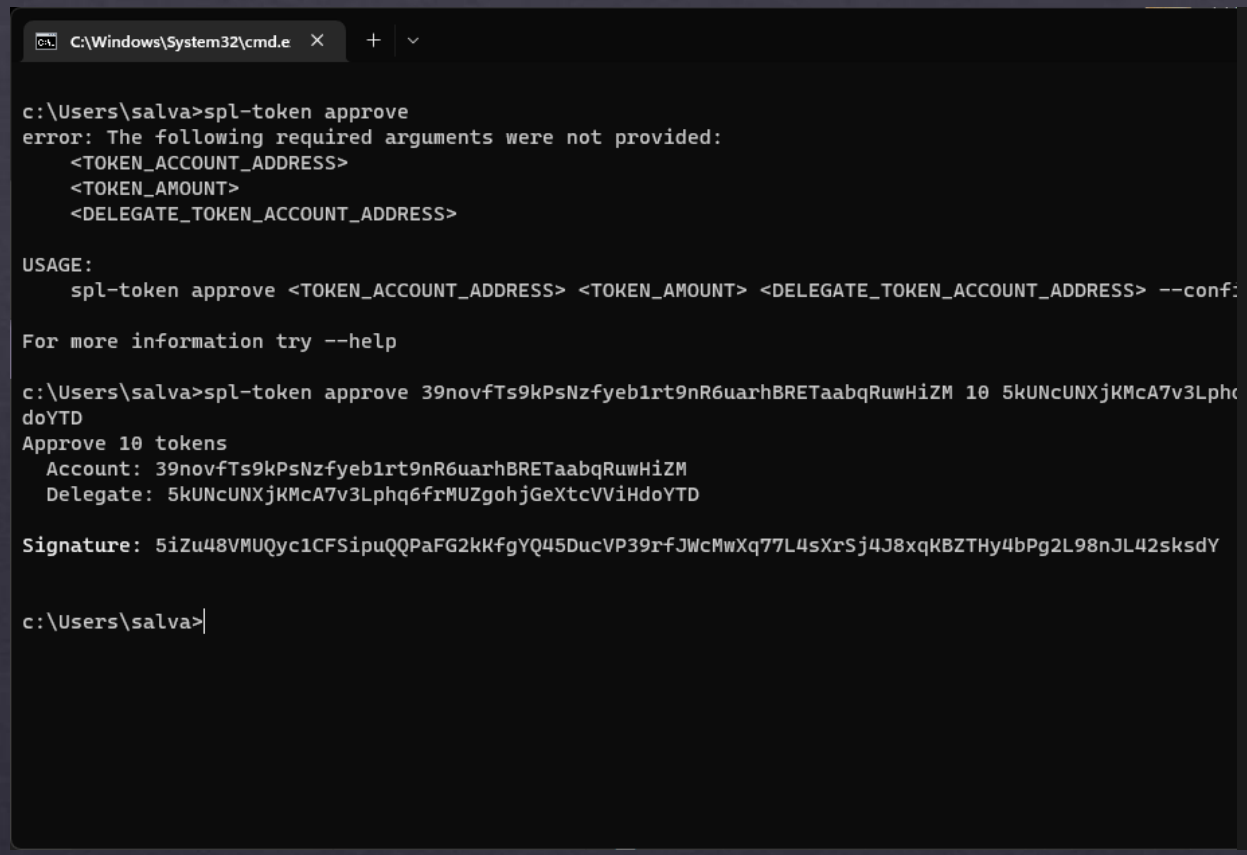
- Starting with a Phantom installation with an account with an ATA with no tokens.
- Export the account private key to the console environment.
- Delegate the ATA with CLI.
- Check the delegation on a Solana explorer.
- Close the ATA with a Dapp (proposed user intervention).
- Send a token of the same mint to reopen the ATA.
- Check that delegation is no longer on place.

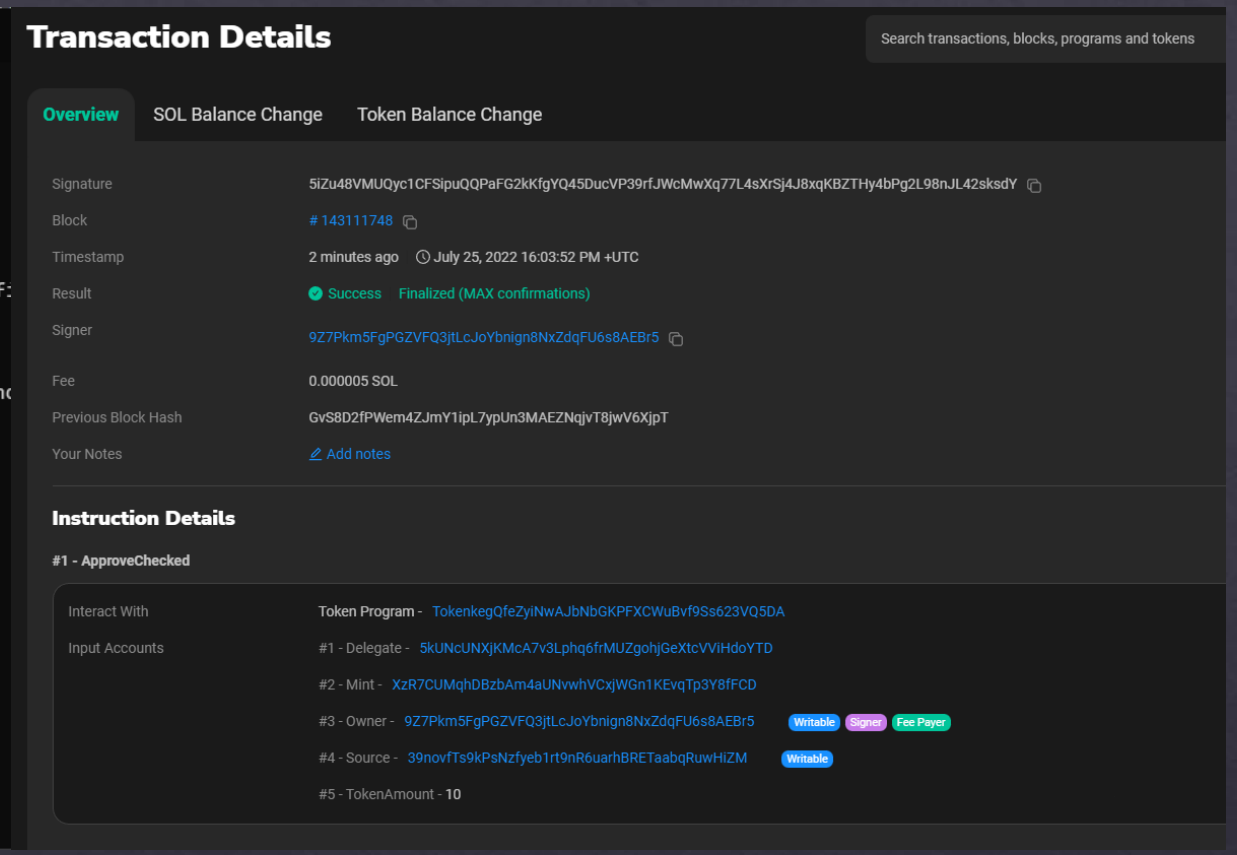
Starting with a Phantom installation with an account with an ATA with no tokens.



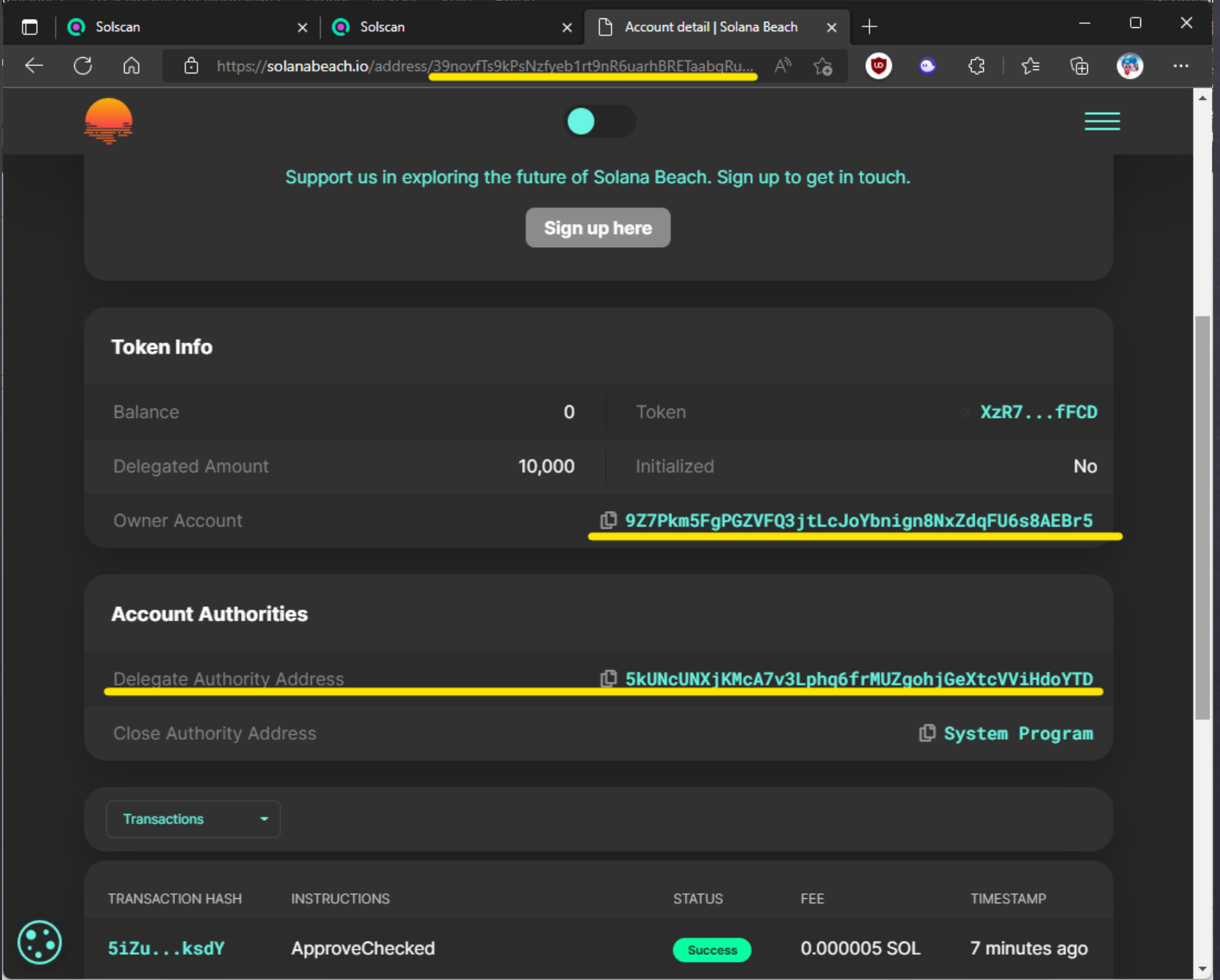


Export the account private key to the console environment (via seed in this case)





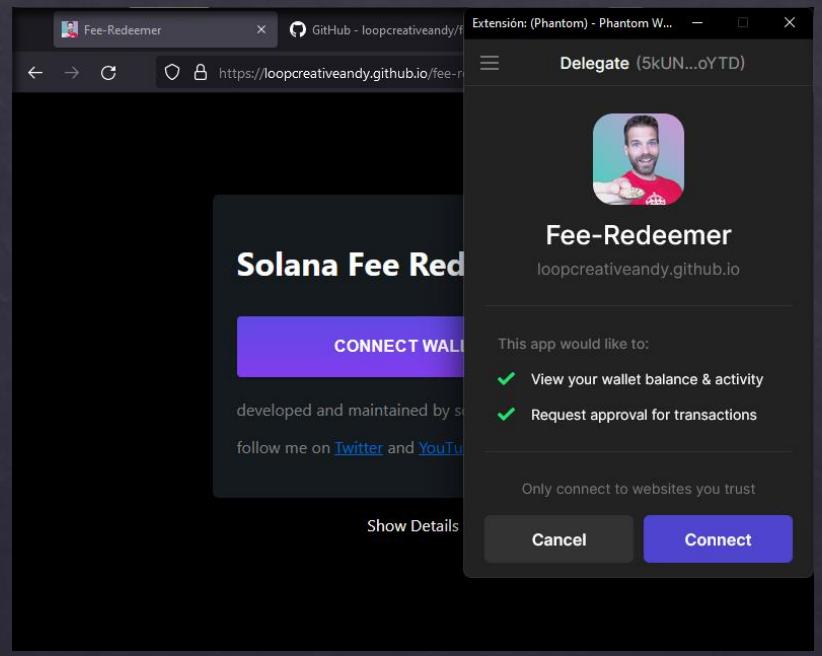
Delegate the ATA with CLI

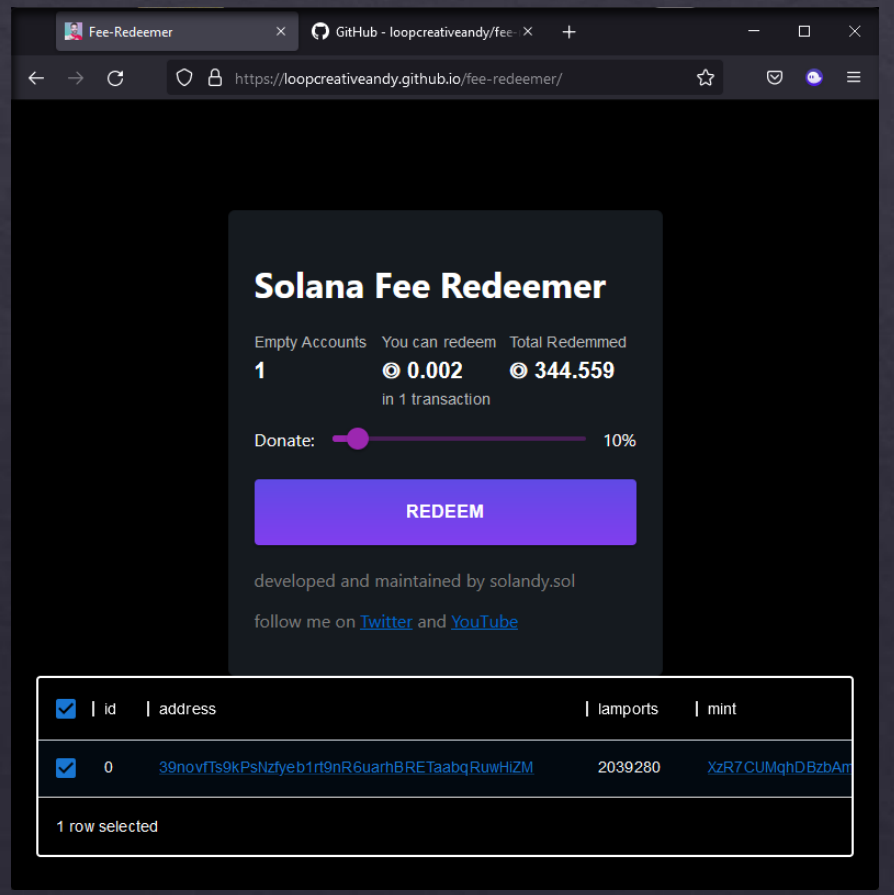


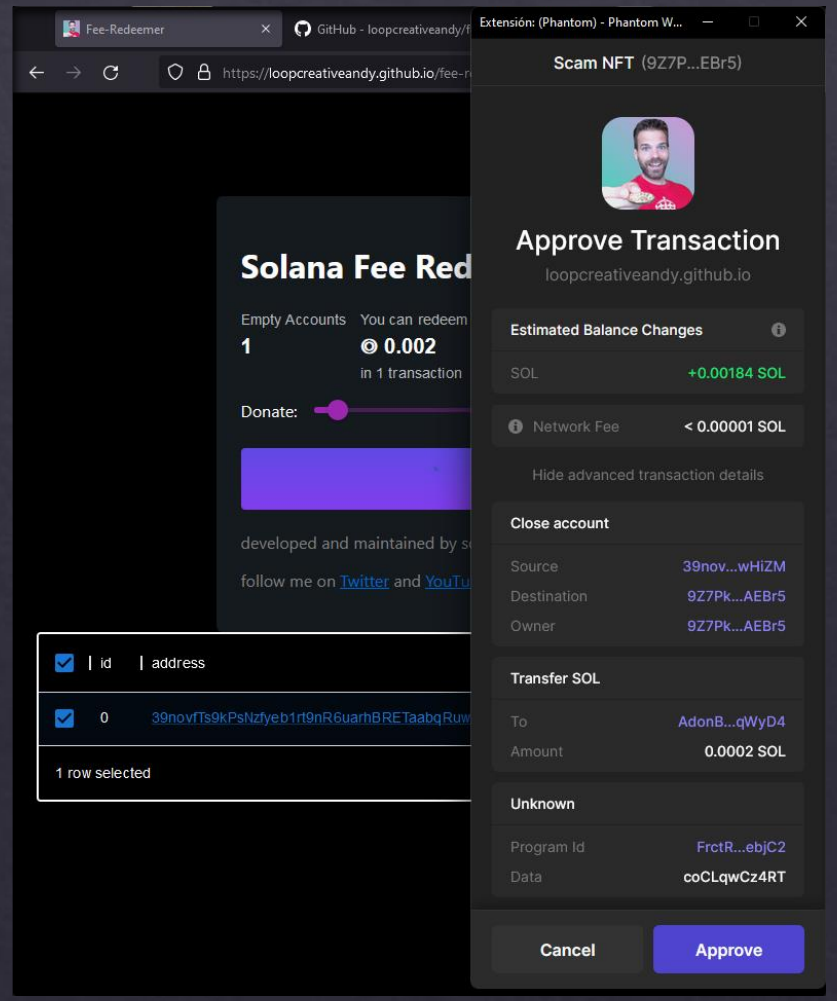
Check the delegation on a Solana explorer (solanabeach.io)

Close the ATA with a Dapp (user intervention)

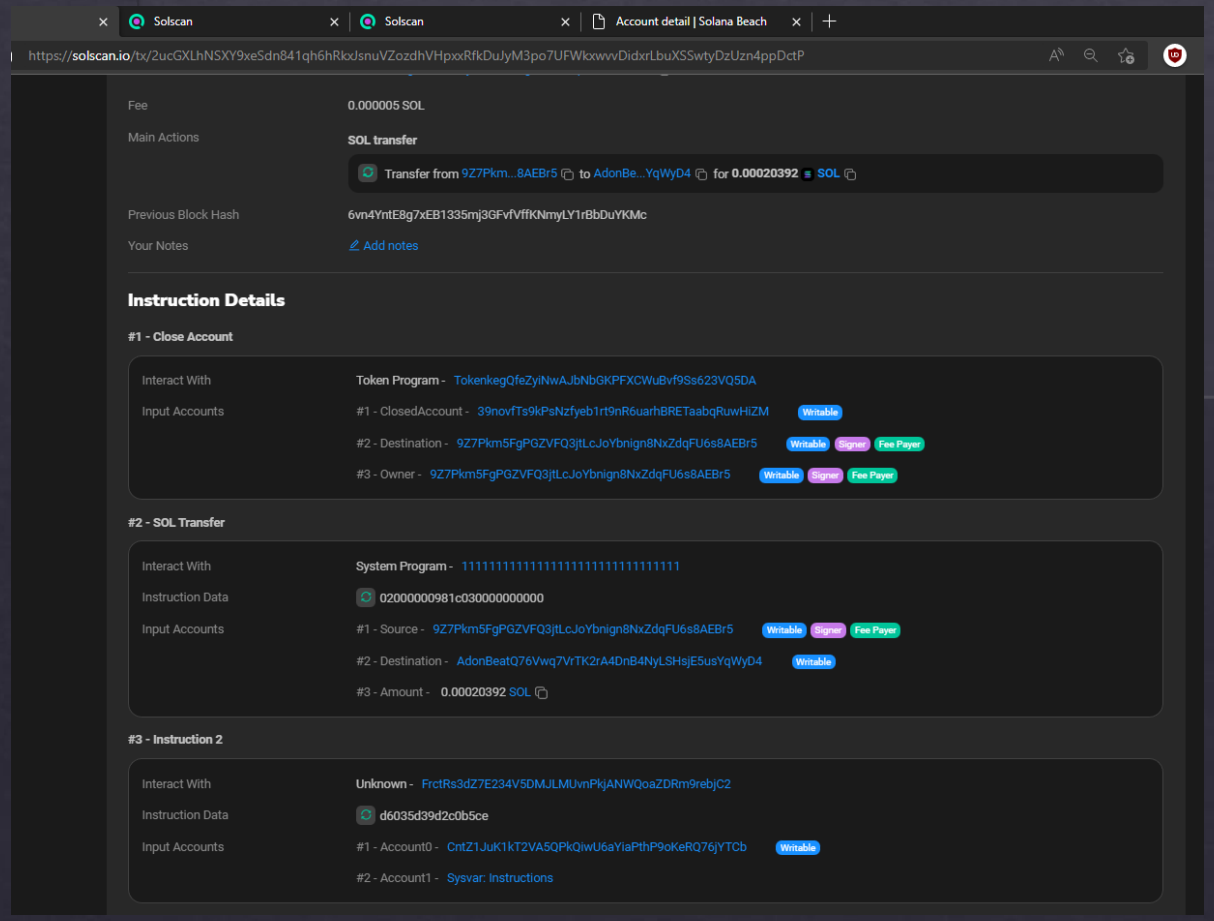
- DApp: https://loopcreativeandy.github.io/fee-redeemer/
- Github repo: https://github.com/loopcreativeandy/fee-redeemer

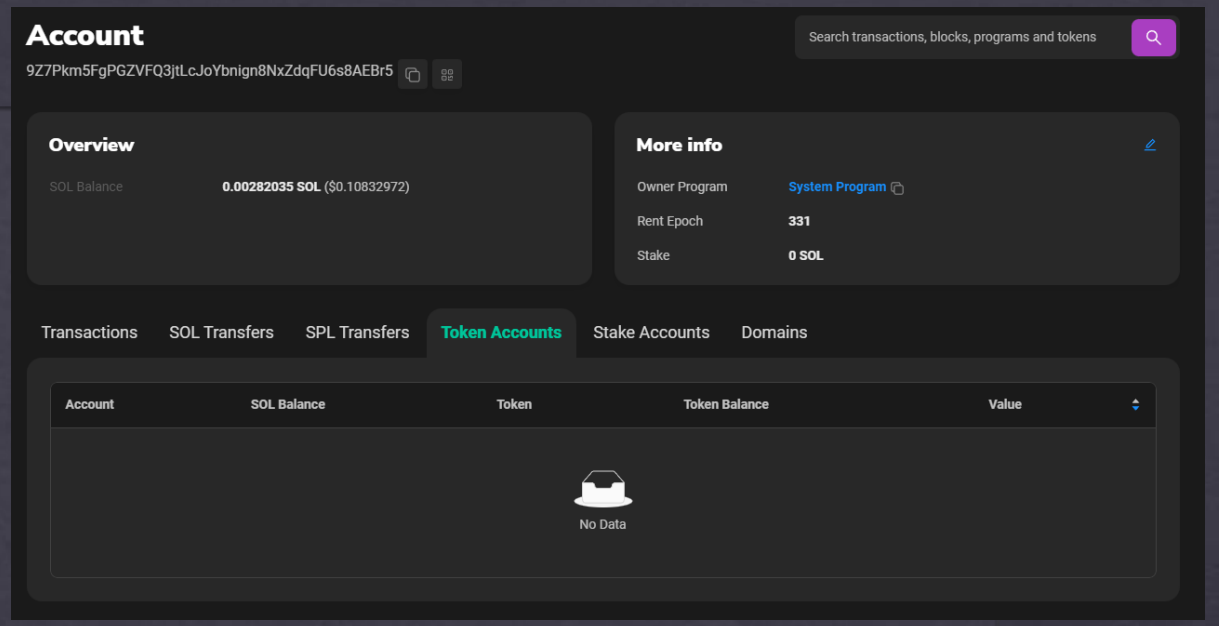


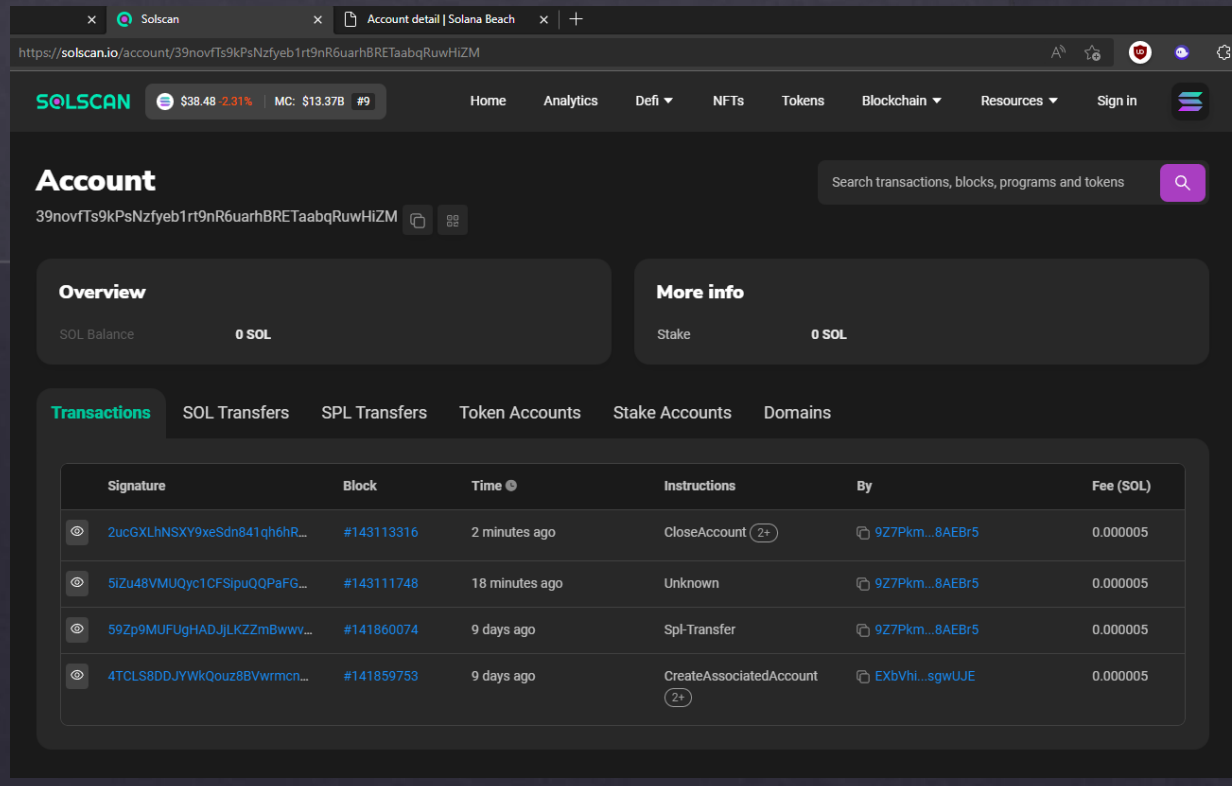




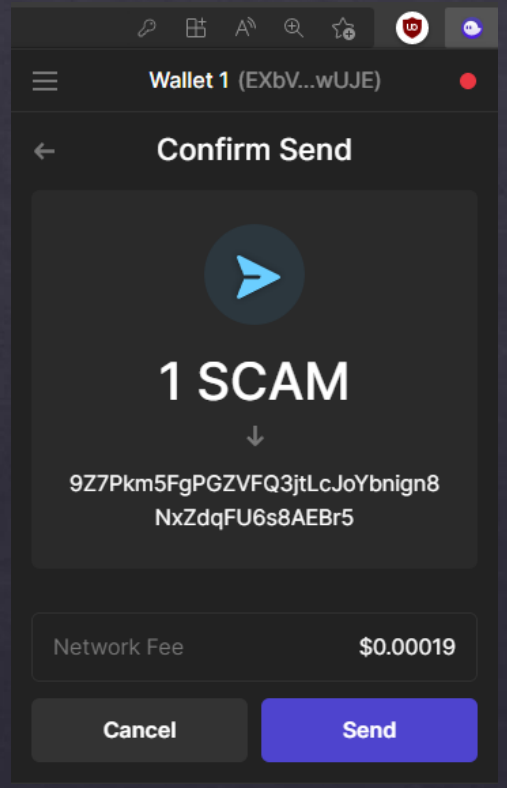
Token account is now closed

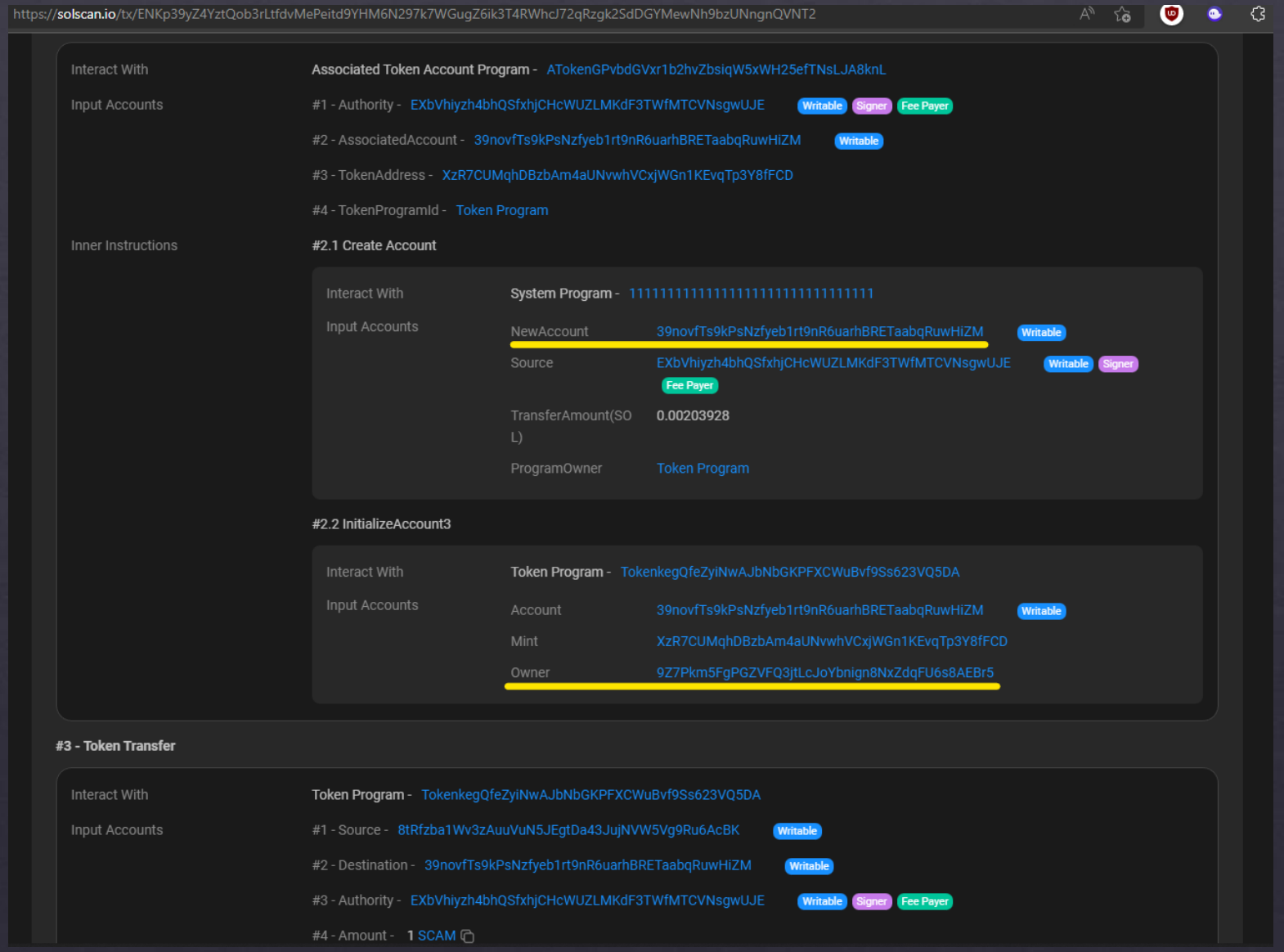




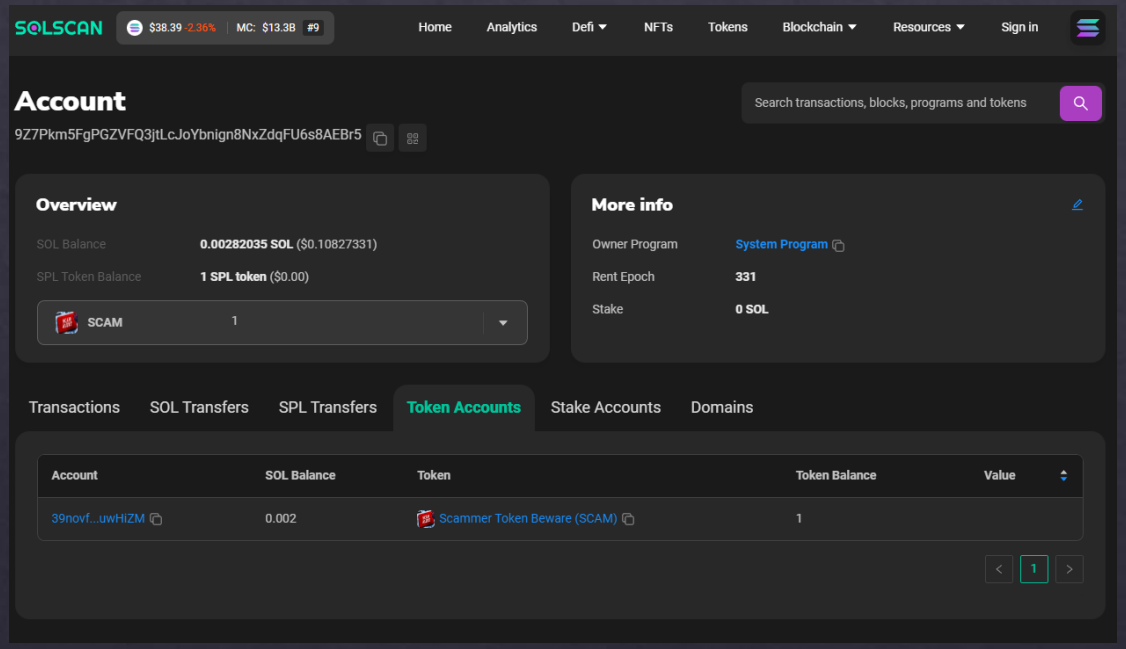


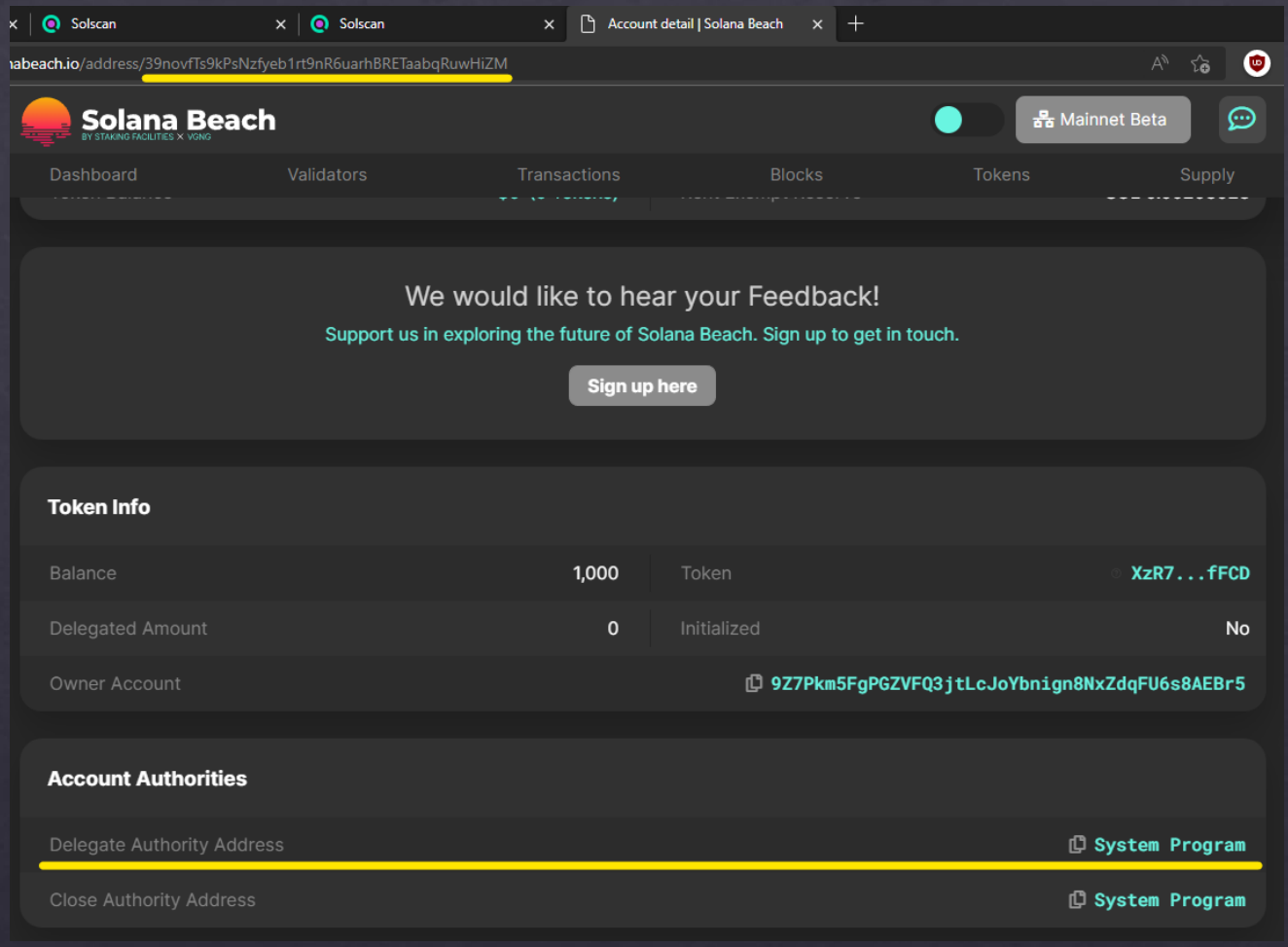
Send a token of the same mint to reopen the ATA





ATA is reopened, same address, no delegation





Conclusion

- Using the Open Source, well regarded DApp *Free Redeemer* to close her Token accounts is an easy and user-friendly way for a victim of a delegation attack to recover control over her ATAs.