



## **Course IV:**

# **DeFi Risks and Opportunities**

## **2. Governance, DNS, Oracle Risk, DEX and Custodial Risks**

### **(i) Governance Attack**

# Risks: Governance risk

## *What is governance risk?*

- For some protocols, such as Uniswap, programming risk is the sole threat to the protocol because the application is autonomous and controlled by smart contracts.
- Other DeFi applications rely on more than just autonomous computer code.

# Risks: Governance risk

## *What is governance risk?*

- For example, MakerDAO, the decentralized credit facility described earlier, is reliant on a human-controlled governance process that actively adjusts protocol parameters to keep the system solvent.
- Many other DeFi protocols use similar systems and rely on humans to actively manage protocol risk.
- This introduces a new risk, *governance risk*, which is unique to the DeFi landscape.

# Risks: Governance risk

## *Protocol governance*

- Protocol governance refers to the representative or liquid democratic mechanisms that enable changes in the protocol.
- To participate in the governance process, users and investors must acquire a token that has been explicitly assigned protocol governance rights on a liquid marketplace.
- Once acquired, holders use these tokens to vote on protocol changes and guide future direction.

## Risks: Governance risk

*51% (or less)*

- Governance tokens usually have a fixed supply that assists in resisting attempts by anyone to acquire a majority (51%), nevertheless they expose the protocol to the risk of control by a malicious actor.
- The founders often control traditional fintech companies, which reduces the risk of an external party influencing or changing the company's direction or product.

# Risks: Governance risk

*51% (or less)*

- DeFi protocols, however, are vulnerable to attack as soon as the decentralized governance system launches.
- Any financially equipped adversary can simply acquire a majority of liquid governance tokens to gain control of the protocol and steal funds.
- A financially equipped adversary can attack a protocol if the potential profit exceeds the cost of attack.

# Risks: Governance risk.

## March 13, 2021 \$TSD governance attack

- Hacker amasses governance token
- Devs held only 9% of governance
- Hacker votes to mint him/herself 11.5 quintillion \$TSD
- Hacker dumps 11.8 billion on Pancakeswap DEX

<https://twitter.com/trueseigniorage/status/1370956726489415683?lang=en>



### Thread



**True Seigniorage Dollar** @TrueSeigniorage · Mar 13

A malicious attacker has just utilized [\\$TSD](#) DAO to mint 11.8 billion tokens to his own account and sold all to Pancakeswap. Here is what happened:

1. Due to long Debt phase, people unbond from DAO because they no longer have rewards from expansion..



22



103



193



**True Seigniorage Dollar** @TrueSeigniorage · Mar 13

2. Dev account has only 9% of the DAO. We failed once when proposing the Implementation to enable the crosschain bridge. In this case, Dev account does not have enough stack to vote against the attacker.



1



3



20



**True Seigniorage Dollar** @TrueSeigniorage · Mar 13

3. What has been done by him? He gradually bought [\\$TSD](#) at low price to accumulate until he has more than 33% of the DAO. Then he proposed an Implementation and voted for it. Because he possess enough stack to finish the voting process, the Implementation went through successfully



6



16



40



**True Seigniorage Dollar** @TrueSeigniorage · Mar 13

In the Implementation, the attacker added code to mint for himself 11.8 billion [\\$TSD](#). Then he sold all of the tokens to Pancakeswap. That's sad, it is an attack but it is how a decentralized DAO works.



5



9



63



# True Seigniorage Dollar (TSD) Price Chart

