Exploiting Inattention & Optimism in DAOs

How I stole from a DAO using standard governance tools

(and how to protect yourself)

Isaac Patka (@isaacpatka)

Logos DAO, Metagov

Section 1

🙈 Proof of Inattention 🙉

🥷 Real Exploits 😩

🦸‍♀️ Protecting you & your DAOs 🦸‍♂️

Attention is the most scarce resource in DAOs. Design your governance tooling accordingly.

Optimistic consensus relies on people paying attention 😮

⚡ **SafeSnap** relies on **Reality.ETH**, a Q&A oracle with bonded answers

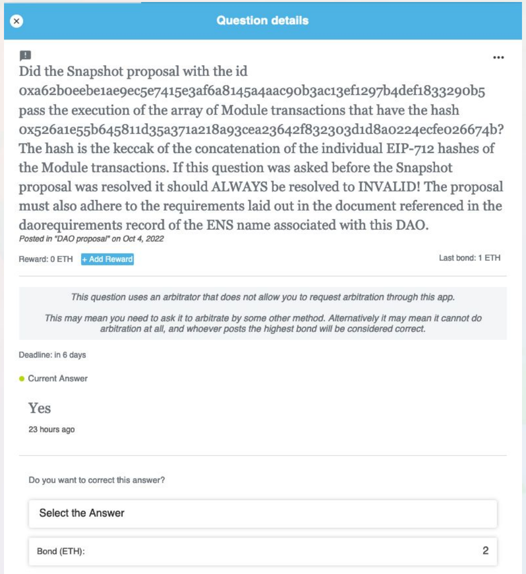
👹 **Moloch DAOs** use *lazy consensus* and have no minimum quorum for proposals to pass*

*but they do need to be sponsored by a member

Reality.ETH is a Q&A Oracle

Many DAOs use Reality.ETH to make **off-chain** votes executable **on-chain**

1. Ask the question


Question details

Did the Snapshot proposal with the id 0xa62b0eebe1ae9ec5e7415e3af6a8145a4aac90b3ac13ef1297b4def1833290b5 pass the execution of the array of Module transactions that have the hash 0x526a1e55b645811d35a371a218a93cea23642f832303d1d8a0224ecfe026674b? The hash is the keccak of the concatenation of the individual EIP-712 hashes of the Module transactions. If this question was asked before the Snapshot proposal was resolved it should ALWAYS be resolved to INVALID! The proposal must also adhere to the requirements laid out in the document referenced in the daorequirements record of the ENS name associated with this DAO.

Posted in "DAO proposal" on Oct 4, 2022

Reward: 0 ETH + Add Reward

Last bond: 1 ETH

This question uses an arbitrator that does not allow you to request arbitration through this app.

This may mean you need to ask it to arbitrate by some other method. Alternatively it may mean it cannot do arbitration at all, and whoever posts the highest bond will be considered correct.

Deadline: in 6 days

● Current Answer

Yes

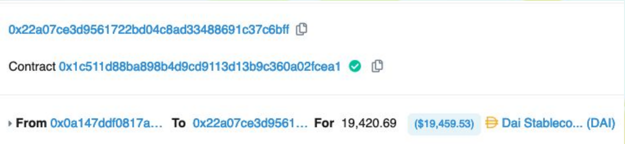
23 hours ago

Do you want to correct this answer?

Select the Answer

Bond (ETH): 2

2. Answer the question

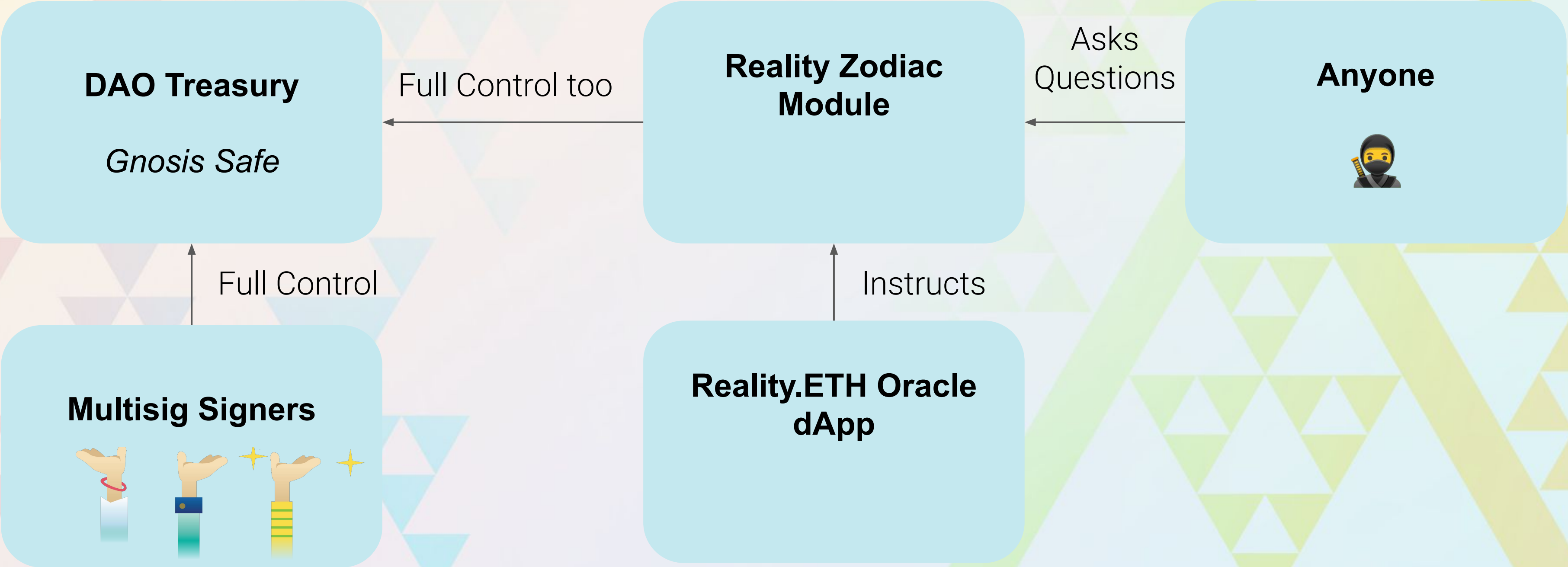

0x22a07ce3d9561722bd04c8ad33488691c37c6bff

Contract 0x1c511d88ba898b4d9cd9113d13b9c360a02fcea1 ✓

From 0x0a147ddf0817a... To 0x22a07ce3d9561... For 19,420.69 ($19,459.53) Dai Stableco... (DAI)

3. Execute

Reality.ETH can execute transactions on a Gnosis Safe through a Zodiac Module ✨



DAO Treasury

Gnosis Safe

Full Control too

Reality Zodiac Module

Asks Questions

Anyone

🥷

Full Control

Multisig Signers

🫴🫴✨🫴✨

Instructs

Reality.ETH Oracle dApp

Multisig Owners Choose the Configuration

Timeout - Duration during which answers can be submitted

Cooldown - Optional duration after Oracle finalization, before execution

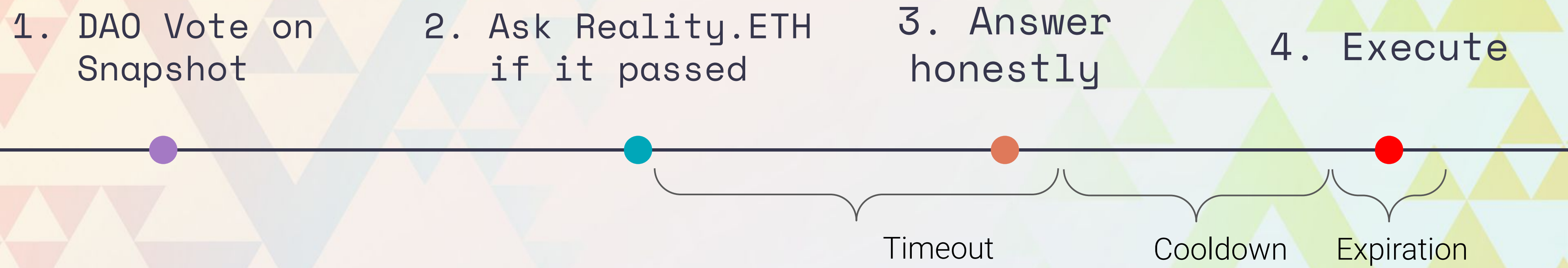
Expiration - Optional duration during which finalized answer can be executed

Bond - Minimum bond for answer to be accepted

Arbitrator - Optional 3rd party that can settle Oracle disputes

Question Template - How should questions look to Reality.ETH dApp users

🤗 Scenario 1 - Happy Path



1. DAO Vote on Snapshot

2. Ask Reality.ETH if it passed

3. Answer honestly

4. Execute

Timeout

Cooldown

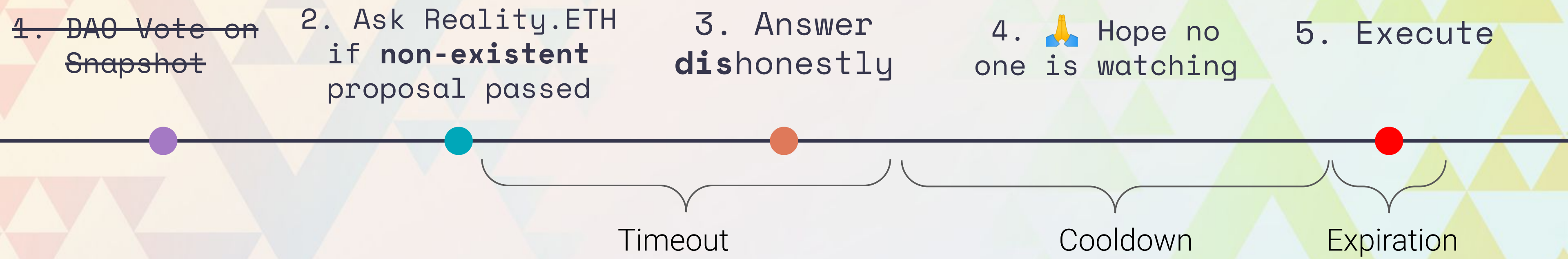
Expiration

Timeout - Duration during which answers can be submitted

Cooldown - Duration after Oracle finalization, before execution

Expiration - Duration during which finalized answer can be executed

🤥 Scenario 2: Dishonest Oracle



~~1. DAO Vote on Snapshot~~

2. Ask Reality.ETH if **non-existent** proposal passed

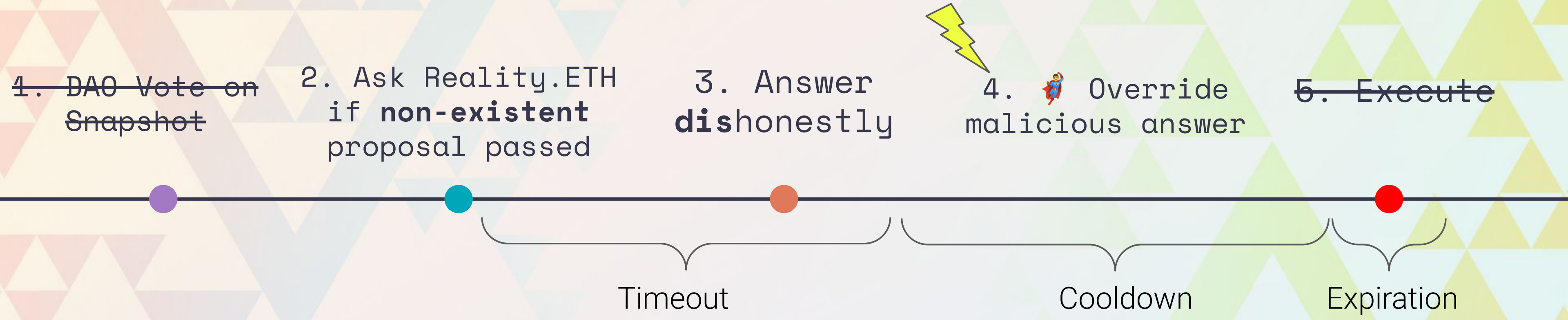
3. Answer **dis**honestly

4. 🙏 Hope no one is watching

5. Execute

An attacker can pose a **non-existent proposal** as a question to Reality.ETH, and submit a **fraudulent** answer by putting down a bond in ETH

🦸 Scenario 2: Dishonest Oracle - **Override**



~~1. DAO Vote on Snapshot~~

2. Ask Reality.ETH if **non-existent** proposal passed

3. Answer **dis**honestly

4. 🦸 Override malicious answer

~~5. Execute~~

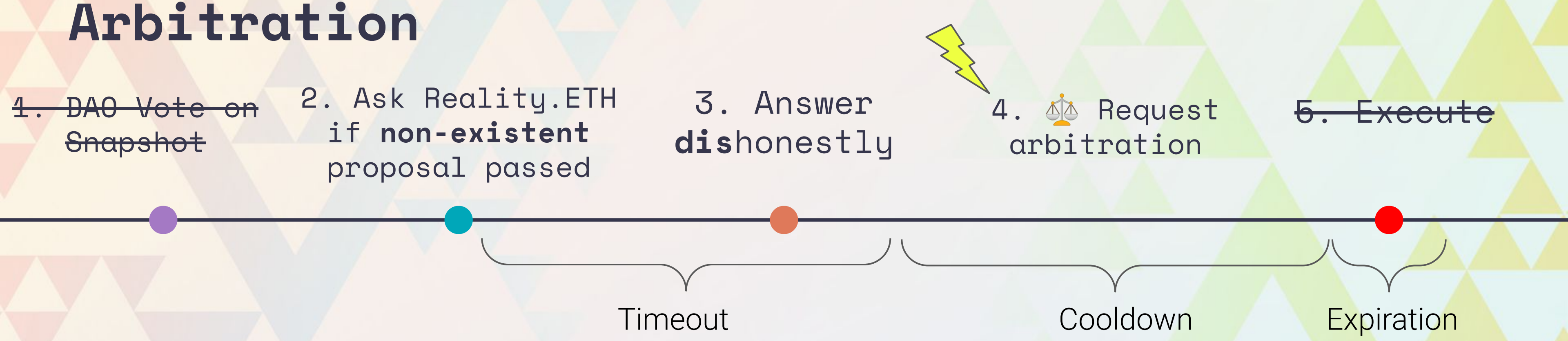
Timeout

Cooldown

Expiration

An **honest** person can override the malicious answer and **claim** the bonded ETH

🦸‍♀️ Scenario 2: Dishonest Oracle - **Arbitration**



~~1. DAO Vote on Snapshot~~

2. Ask Reality.ETH if **non-existent** proposal passed

3. Answer **dis**honestly

4. ⚖️ Request arbitration

~~5. Execute~~

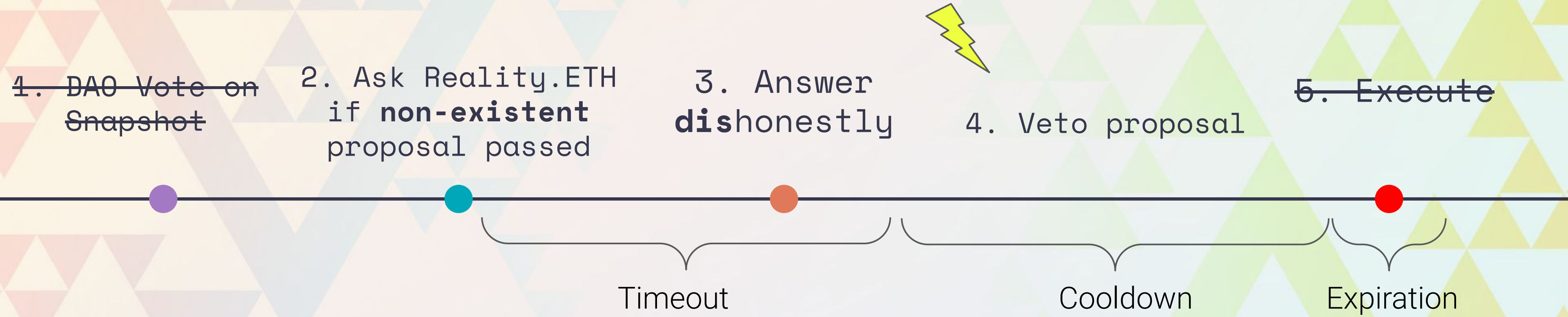
Timeout

Cooldown

Expiration

An **arbitrator** can step in to override the malicious answer (IF one is configured)

Scenario 2: Dishonest Oracle - **Veto**



~~1. DAO Vote on Snapshot~~

2. Ask Reality.ETH if **non-existent** proposal passed

3. Answer **dis**honestly

4. Veto proposal

~~5. Execute~~

Timeout

Cooldown

Expiration

Multisig owners can **veto** the malicious answer during **cooldown** (if it is configured)

Misconfiguration can make exploits **trivial**

Timeout - Too short of a timeout can make it hard to catch malicious transactions

Cooldown - 0 second cooldown removes veto period

Bond - Low minimum bond makes it cheap to try and exploit

Arbitrator - Absent arbitrator removes final safeguards

Vetoer - Absent or negligent multisig signers remove veto safeguard

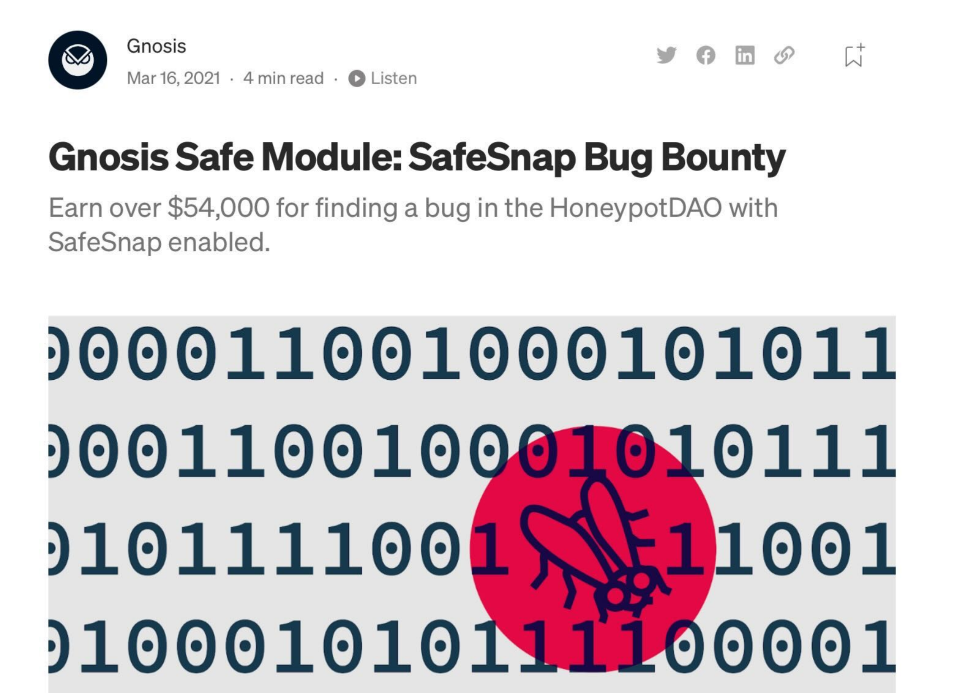
We will see examples of ALL of these misconfigurations in mainnet exploits (coming up next…)

Section 2

🥷 Real Exploits 😩

How I exploited a DAO and how others are attacking them as we speak

$100Ms of DAO treasuries are at risk of inattention attacks



Gnosis

Mar 16, 2021 · 4 min read · Listen

Gnosis Safe Module: SafeSnap Bug Bounty

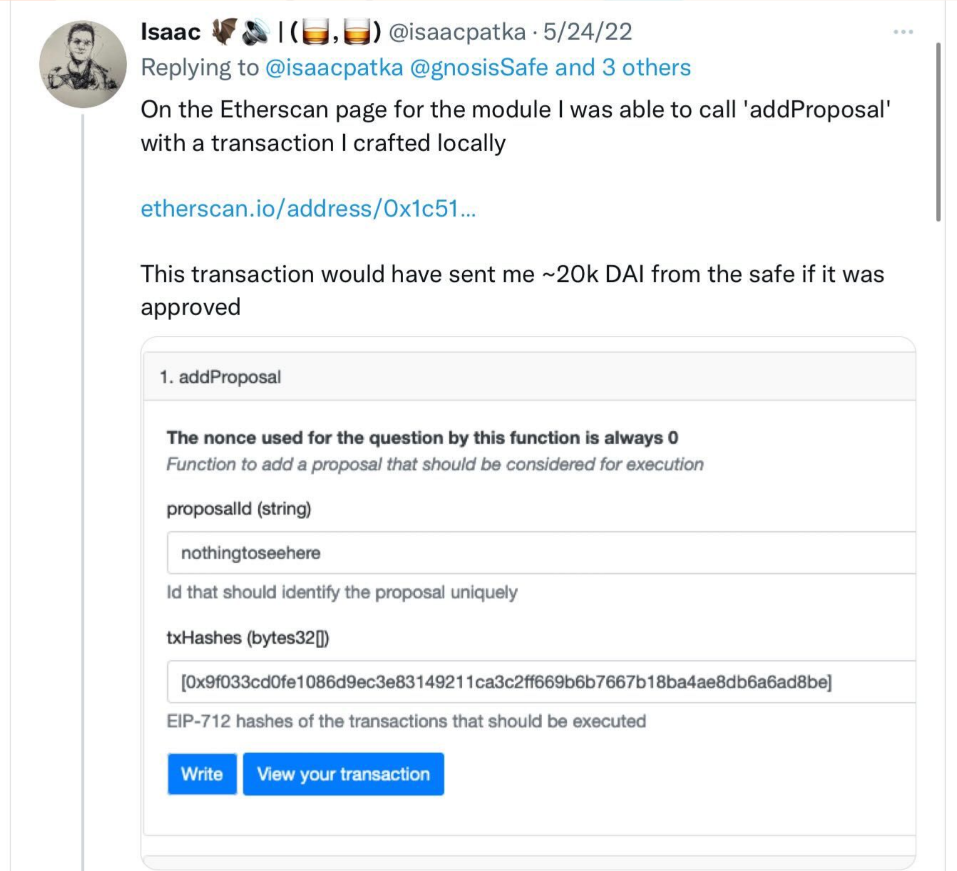
Earn over $54,000 for finding a bug in the HoneypotDAO with SafeSnap enabled.

🍯 Exploiting the SafeSnap Honeypot

Gnosis set up a bug bounty for the Reality.ETH module in Spring 2021 and it sat dormant for over a year

https://etherscan.io/address/0x0a147ddf0817ade664eb9cb343d96a21ed857d11

😏 Crafting the Exploit



Isaac 🦅🔊 | (🥃,🥃) @isaacpatka · 5/24/22

Replying to @isaacpatka @gnosisSafe and 3 others

On the Etherscan page for the module I was able to call 'addProposal' with a transaction I crafted locally

etherscan.io/address/0x1c51…

This transaction would have sent me ~20k DAI from the safe if it was approved

1. addProposal

The nonce used for the question by this function is always 0

Function to add a proposal that should be considered for execution

proposalId (string)

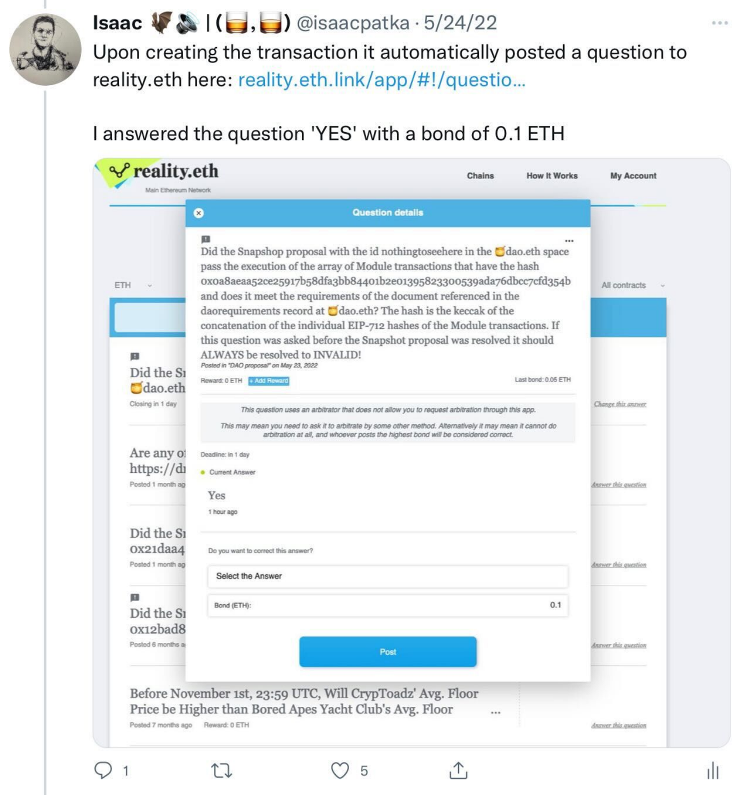
nothingtoseehere

Id that should identify the proposal uniquely

txHashes (bytes32[])

[0x9f033cd0fe1086d9ec3e83149211ca3c2ff669b6b7667b18ba4ae8db6a6ad8be]

EIP-712 hashes of the transactions that should be executed



Isaac 🦅🔊 | (🥃,🥃) @isaacpatka · 5/24/22

Upon creating the transaction it automatically posted a question to reality.eth here: reality.eth.link/app/#!/questio…

I answered the question 'YES' with a bond of 0.1 ETH

reality.eth

Main Ethereum Network

Question details

Did the Snapshop proposal with the id nothingtoseehere in the 🍯dao.eth space pass the execution of the array of Module transactions that have the hash 0x0a8aeaa52ce25917b58dfa3bb84401b2e01395823300539ada76dbcc7cfd354b and does it meet the requirements of the document referenced in the daorequirements record at 🍯dao.eth? The hash is the keccak of the concatenation of the individual EIP-712 hashes of the Module transactions. If this question was asked before the Snapshot proposal was resolved it should ALWAYS be resolved to INVALID!

Posted in "DAO proposal" on May 23, 2022

Reward: 0 ETH + Add Reward

Last bond: 0.05 ETH

This question uses an arbitrator that does not allow you to request arbitration through this app.

This may mean you need to ask it to arbitrate by some other method. Alternatively it may mean it cannot do arbitration at all, and whoever posts the highest bond will be considered correct.

Deadline: in 1 day

● Current Answer

Yes

1 hour ago

Do you want to correct this answer?

Select the Answer

Bond (ETH): 0.1

Did the Sı
🍯dao.eth
Closing in 1 day

Change this answer

Are any o
https://dı
Posted 1 month ag

Answer this question

Did the Sı
0x21daa4
Posted 1 month ag

Answer this question

Did the Sı
0x12bad8
Posted 6 months a

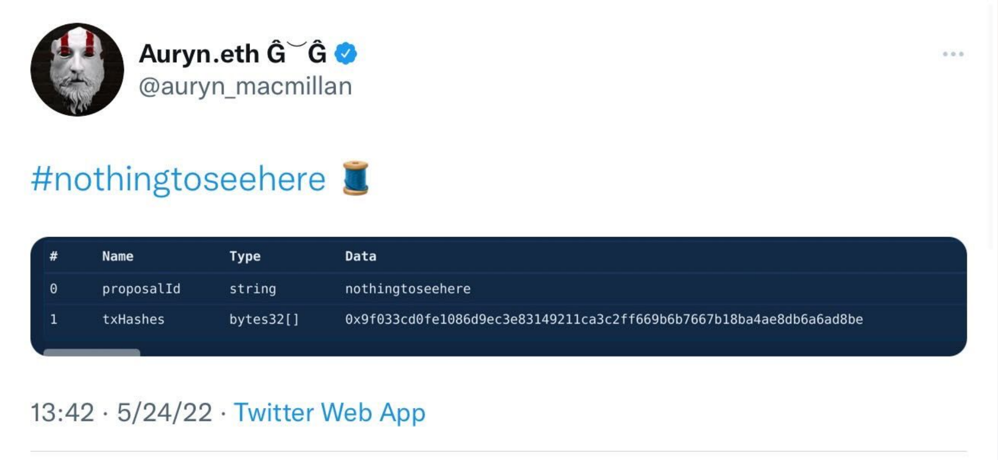
Answer this question

Before November 1st, 23:59 UTC, Will CrypToadz' Avg. Floor Price be Higher than Bored Apes Yacht Club's Avg. Floor …

Posted 7 months ago Reward: 0 ETH

Answer this question

🦸‍♂️ Defenders take notice

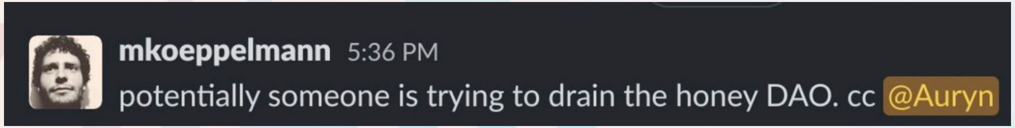


Auryn.eth Ĝ‿Ĝ
@auryn_macmillan

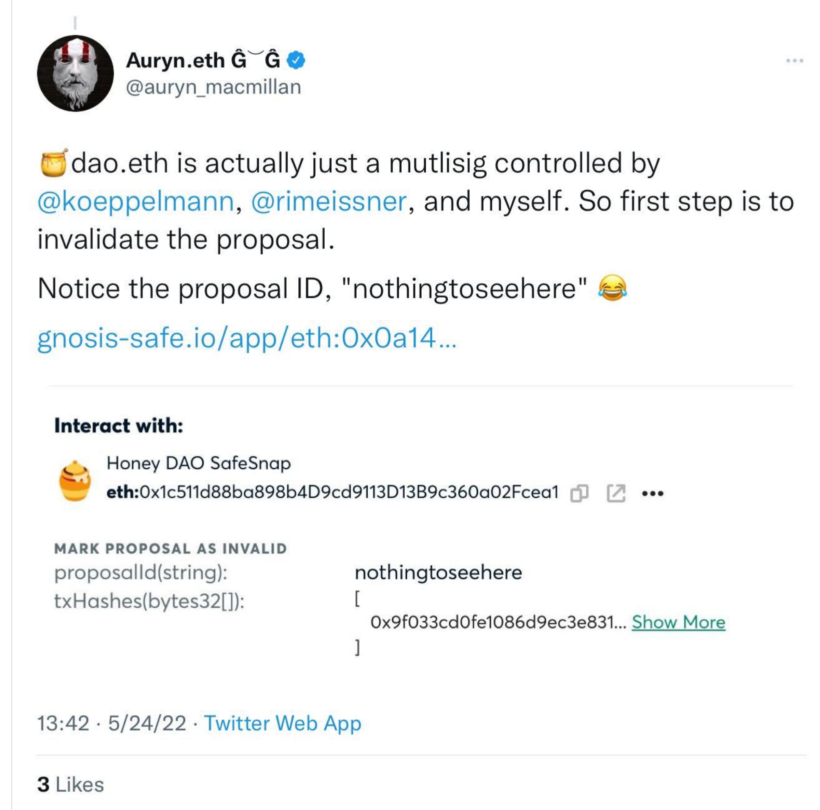
#nothingtoseehere 🧵

#	Name	Type	Data
0	proposalId	string	nothingtoseehere
1	txHashes	bytes32[]	0x9f033cd0fe1086d9ec3e83149211ca3c2ff669b6b7667b18ba4ae8db6a6ad8be

13:42 · 5/24/22 · Twitter Web App



mkoeppelmann 5:36 PM
potentially someone is trying to drain the honey DAO. cc @Auryn



Auryn.eth Ĝ‿Ĝ
@auryn_macmillan

🍯dao.eth is actually just a mutlisig controlled by @koeppelmann, @rimeissner, and myself. So first step is to invalidate the proposal.

Notice the proposal ID, "nothingtoseehere" 😂

gnosis-safe.io/app/eth:0x0a14...

Interact with:

Honey DAO SafeSnap
eth:0x1c511d88ba898b4D9cd9113D13B9c360a02Fcea1

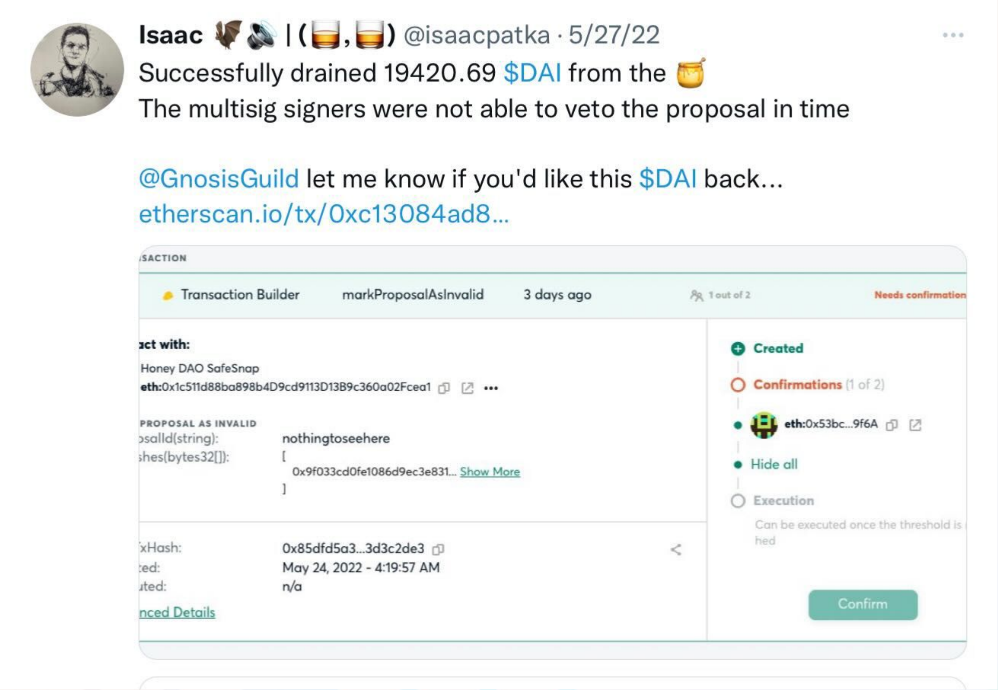
MARK PROPOSAL AS INVALID
proposalId(string): nothingtoseehere
txHashes(bytes32[]): [
0x9f033cd0fe1086d9ec3e831... Show More
]

13:42 · 5/24/22 · Twitter Web App

3 Likes

“Is anyone available to sign this transaction?”

🙃 But it was too late



Isaac 🦇🔊 | (🥃,🥃) @isaacpatka · 5/27/22

Successfully drained 19420.69 $DAI from the 🍯
The multisig signers were not able to veto the proposal in time

@GnosisGuild let me know if you'd like this $DAI back...
etherscan.io/tx/0xc13084ad8...

ısaction

Transaction Builder | markProposalAsInvalid | 3 days ago | 1 out of 2 | Needs confirmation

ıct with:
Honey DAO SafeSnap
eth:0x1c511d88ba898b4D9cd9113D13B9c360a02Fcea1

PROPOSAL AS INVALID
ɔsalId(string): nothingtoseehere
ɛhes(bytes32[]): [
0x9f033cd0fe1086d9ec3e831... Show More
]

ʈxHash: 0x85dfd5a3...3d3c2de3
ɛed: May 24, 2022 - 4:19:57 AM
ɩted: n/a

ɴced Details

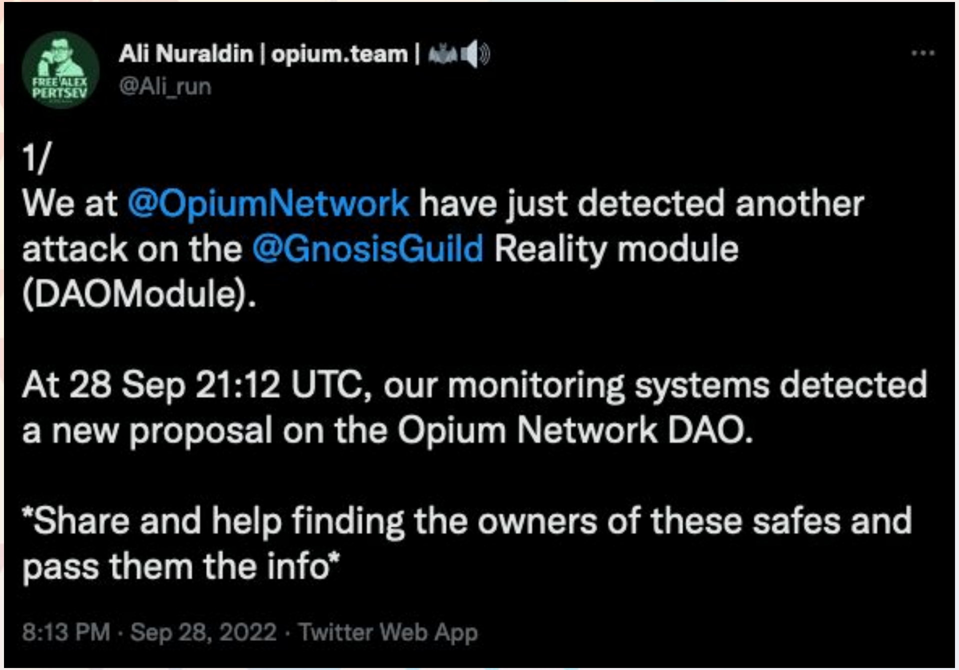
This exploit was successful because...

Arbitration could not be requested

Cooldown was a short 24hr and the vetoers were AFK

No one else on Reality.ETH was paying attention

Then it started happening for real…



Ali Nuraldin | opium.team | 🦇🔊
@Ali_run

1/
We at @OpiumNetwork have just detected another attack on the @GnosisGuild Reality module (DAOModule).

At 28 Sep 21:12 UTC, our monitoring systems detected a new proposal on the Opium Network DAO.

Share and help finding the owners of these safes and pass them the info

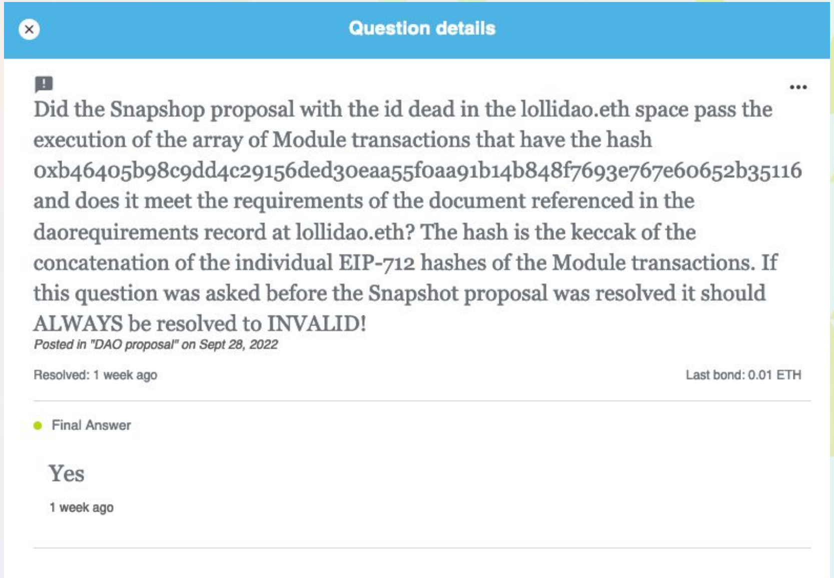
8:13 PM · Sep 28, 2022 · Twitter Web App

While monitoring their own Gnosis Safe & Reality module, the Opium Network team discovered a series of fraudulent transactions attacking DAO treasuries

🎯 Attack 1 - easy target

The attacker found a DAO with a Reality module configured with just **24hr** cooldowns, little activity, and **no minimum bond**

They stole **7.5 ETH** after putting down a 0.01 ETH bond



Did the Snapshop proposal with the id dead in the lollidao.eth space pass the execution of the array of Module transactions that have the hash 0xb46405b98c9dd4c29156ded30eaa55f0aa91b14b848f7693e767e60652b35116 and does it meet the requirements of the document referenced in the daorequirements record at lollidao.eth? The hash is the keccak of the concatenation of the individual EIP-712 hashes of the Module transactions. If this question was asked before the Snapshot proposal was resolved it should ALWAYS be resolved to INVALID!

Posted in "DAO proposal" on Sept 28, 2022

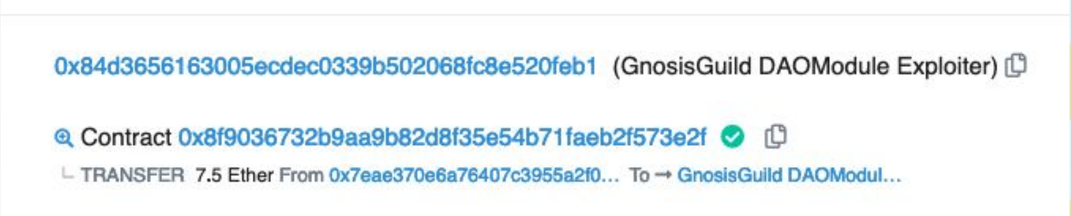
Resolved: 1 week ago

Last bond: 0.01 ETH

Final Answer

Yes

1 week ago



0x84d3656163005ecdec0339b502068fc8e520feb1 (GnosisGuild DAOModule Exploiter)

Contract 0x8f9036732b9aa9b82d8f35e54b71faeb2f573e2f ✓

└ TRANSFER 7.5 Ether From 0x7eae370e6a76407c3955a2f0... To → GnosisGuild DAOModul...

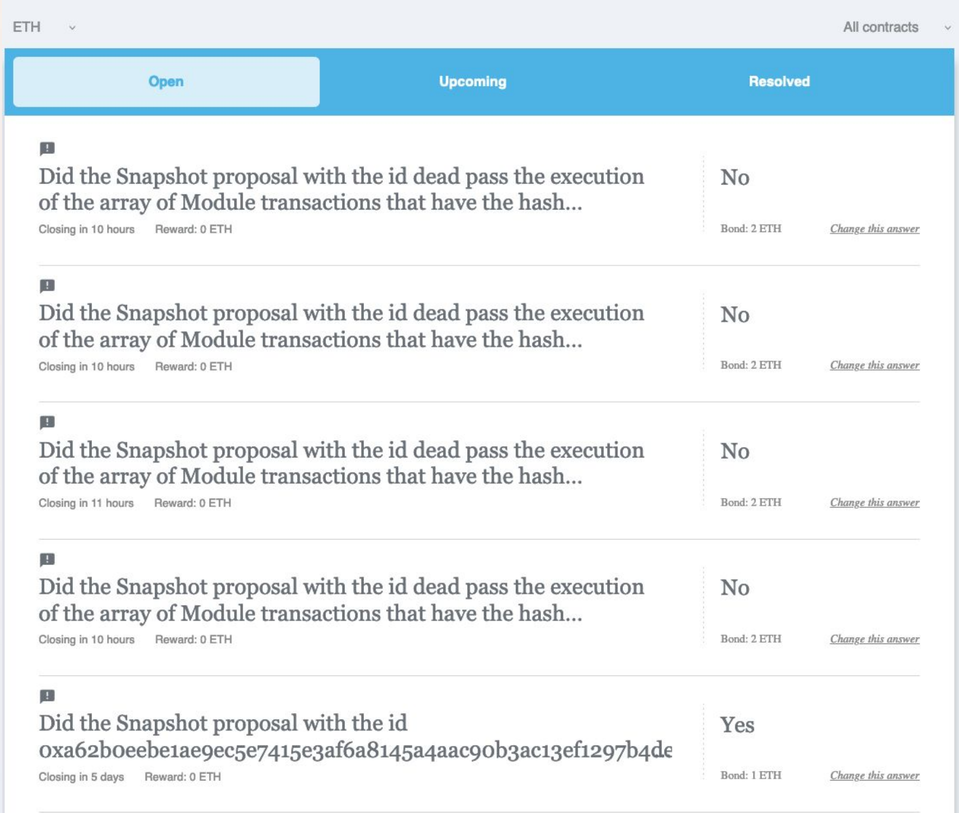
🎯 Attacks 2-7+

The attacker used the 7.5 ETH bond to place fraudulent answers in at least 6 other DAOs

They primarily targeted NFT collections including SZNS

🙌 The SZNS team had 7 day voting periods & 1 ETH minimum bonds so the attacker was limited in how many they could attempt

I was able to thwart the attack by overriding their answer, but if the attacker was more highly capitalized it would have been harder to defend



Did the Snapshot proposal with the id dead pass the execution of the array of Module transactions that have the hash...
Closing in 10 hours Reward: 0 ETH
No
Bond: 2 ETH

Did the Snapshot proposal with the id dead pass the execution of the array of Module transactions that have the hash...
Closing in 10 hours Reward: 0 ETH
No
Bond: 2 ETH

Did the Snapshot proposal with the id dead pass the execution of the array of Module transactions that have the hash...
Closing in 11 hours Reward: 0 ETH
No
Bond: 2 ETH

Did the Snapshot proposal with the id dead pass the execution of the array of Module transactions that have the hash...
Closing in 10 hours Reward: 0 ETH
No
Bond: 2 ETH

Did the Snapshot proposal with the id 0xa62b0eebe1ae9ec5e7415e3af6a8145a4aac90b3ac13ef1297b4de
Closing in 5 days Reward: 0 ETH
Yes
Bond: 1 ETH

$100Ms of DAO treasuries are at risk of inattention attacks

🔔 We need more **monitoring infrastructure** for DAO treasuries & governance tooling

📋 We need **configuration audits**, just as much as we need smart contract audits

Attacks like this are only going to start happening **more frequently**

Section 3

🦸‍♀️ Protecting you & your DAOs 🦸‍♂️

10 Steps to keep your DAO Safe:

1) Make a resiliency & continuity plan
2) Keep track of who has administrative controls over smart contracts (ideally 0 or limited multisigs)
3) Set up monitoring infrastructure
   a) Etherscan alerts, OpenZeppelin Sentry
4) Leverage automation tools to **pause** contracts if exploit conditions are detected
   a) OpenZeppelin Defender
5) Use simulation tools to check what proposals are going to change **before** you execute them
   a) Tenderly
6) Conduct regular configuration audits, especially focusing on new tools that can execute proposals
7) Minimize cross-chain communication
   a) It's *always* the bridges that get hacked
8) Implement spending limits & transaction guards on Safe treasuries
9) Use hardware wallets & never back up your seed phrase online (including password managers)
10) Use on-call shifts to track availability of multisig signers

Regularly **Audit** your DAO's tooling stack and set up robust **monitoring** infrastructure

Reach out to LOGOS DAO & isaac@logos.xyz

Composable governance tooling make DAOs **powerful** but requires **careful configuration**

Thank you!

Isaac Patka

Co-summoner, Logos DAO

isaac@logos.xyz

@isaacpatka