

# I Experienced More than 10 DeFi Scams: On DeFi Users' Perception of Security Breaches and Countermeasures

Mingyi Liu, Jun Ho Huh, HyungSeok Han, Jaehyuk Lee, Jihae Ahn,  
Frank Li, Hyoungshick Kim, Taesoo Kim



# What is Decentralized Finance (DeFi)?

A financial ecosystem built on **blockchain** platforms like Ethereum.

Executed through smart contracts, provides a variety of **financial services**.

# DeFi Protocols

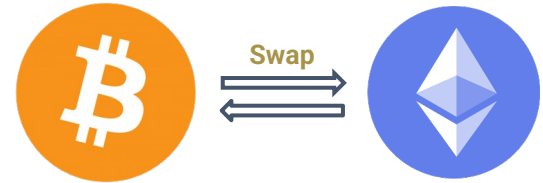
Jul 15, 2024

- Liquid Staking \$49.186b
- Lending \$47.549b
- Dexes \$20.427b
- Restaking \$17.609b
- Liquid Restaking \$12.595b
- CDP \$9.408b
- Yield \$8.012b
- Farm \$4.463b
- Derivatives \$3.948b
- Services \$2.397b
- Others \$12.206b



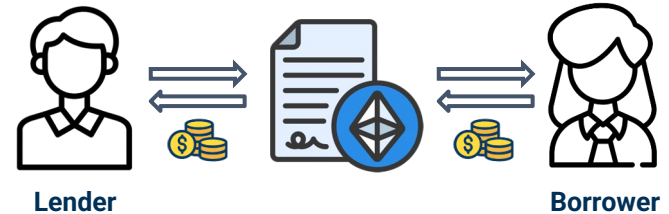
## Exchanges

(e.g., Uniswap, Curve)



## Lending

(e.g., AAVE, Compound)




## Liquid Staking

(e.g., Lido)




43 Protocol Categories,  
sorted by Total Value Locked  
(TVL)


Our lab member shared with us:


 6:52 PM Tuesday, May 28th ▾

<https://www.youtube.com/watch?v=ITchP7Wdlcs>



 **YouTube** | SpaceX

Elon Musk: SpaceX Starship IFT-4 Flight Test! Elon Musk gives update on Starship! ▾



 6:52 PM

LIVE!

  **2 replies** Last reply 2 months ago

What was this?

# DeFi Hacks & Scams

Transactions for address: 3EtrSPsMRgwEE9onLdmwAFqaH9j9rM

From	To	Value
SpaceX BTC Wall	90d8c6da81d1d688...	3 BTC
90d8c6da81d1d688...	SpaceX BTC Wall	0.269 BTC
SpaceX BTC Wall	6a2c90c584d9772...	8 BTC
6a2c90c584d9772...	SpaceX BTC Wall	0.782 BTC
SpaceX BTC Wall	c48e56b10ce74c33...	13 BTC
c48e56b10ce74c33...	SpaceX BTC Wall	1.257 BTC
SpaceX BTC Wall	cfc8fcd2d7ae7d...	8 BTC
cfc8fcd2d7ae7d...	SpaceX BTC Wall	4.750 BTC

More info on [ElonMuskFunding.org](https://www.ElonMuskFunding.org)

Scan this QR code for this BTC address to join:  
3EtrSPsMRgwEE9onLdmwAFqaH9j9rM

You just need to send 0.1 BTC to 20 BTC  
Confirmation required. We will immediately  
send you back 20 BTC to the address you sent it from.  
You can donate as little as 0.1 BTC to the address you sent it from.  
You can donate as little as 0.1 BTC to the address you sent it from.  
You can donate as little as 0.1 BTC to the address you sent it from.

**SCAM**

**SCAM**

NASA and SpaceX: Launch Falcon 9 rocket and Crew Dragon | Live

43,956 views • Streamed live 2 hours ago

3.4K 1.4K SHARE SAVE

Space X Live  
230K subscribers

SUBSCRIBE

# Incident Impacts

CeFi

Silicon Valley Bank bank run → **collapse**

- users withdrew \$42 billion in a single day



DeFi

Curve DEX has suffered multiple hacks → **survival**

- 08/2022: front-end exploit, **\$575K loss**
- 07/2023: smart contract exploit, **\$69M loss**
- the second largest DEX based on TVL

 **Curve DEX (CRV)**

Total Value Locked

> **\$2.21b**

# Research Questions

RQ1

Why do people **continue to use** DeFi despite numerous DeFi incidents being reported?

RQ2

What **DeFi risks** are users concerned about, and how do they **mitigate** these risks?

RQ3

How do victims **respond** to DeFi incidents?

RQ4

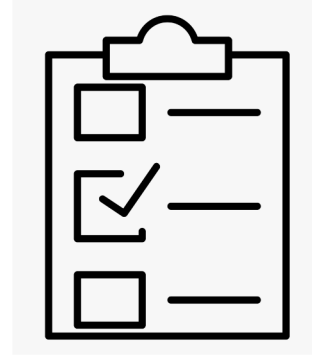
How do DeFi users **perceive regulation**?

# Methodology



Semi-structured **interview**  
with DeFi users  
( $N = 14$ )

1st study



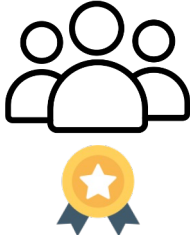
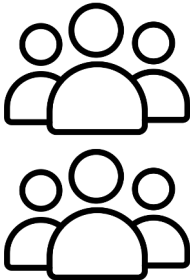
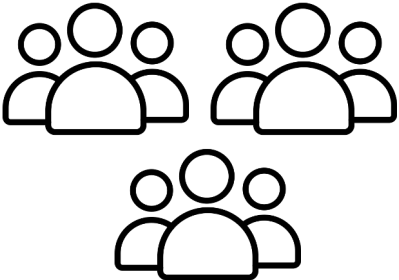
Large-scale online **survey**  
with DeFi users  
( $N = 493$ )

2nd study

**Real-world victims**



# Recruitment



Crypto users



U.S. residents

DeFi users  
*(self-reported)*

DeFi users  
*(validated)*

# Research Questions

RQ1

Why do people **continue to use** DeFi despite numerous DeFi incidents being reported?

RQ2

What **DeFi risks** are users concerned about, and how do they **mitigate** these risks?

RQ3

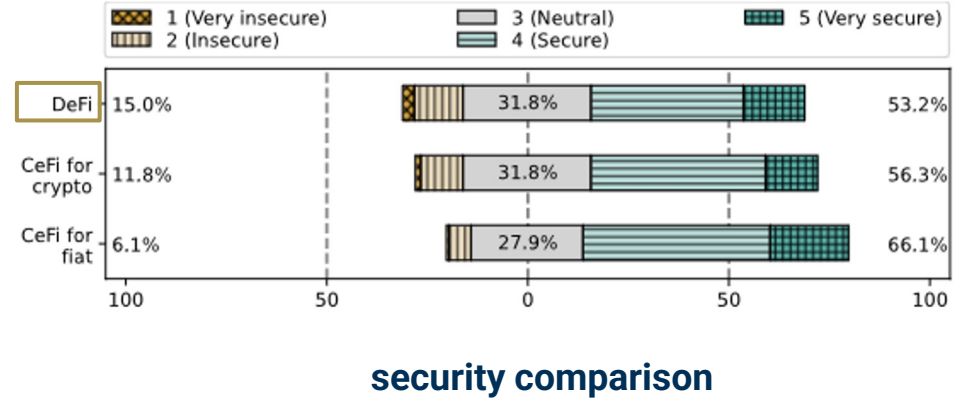
How do victims **respond** to DeFi incidents?

RQ4

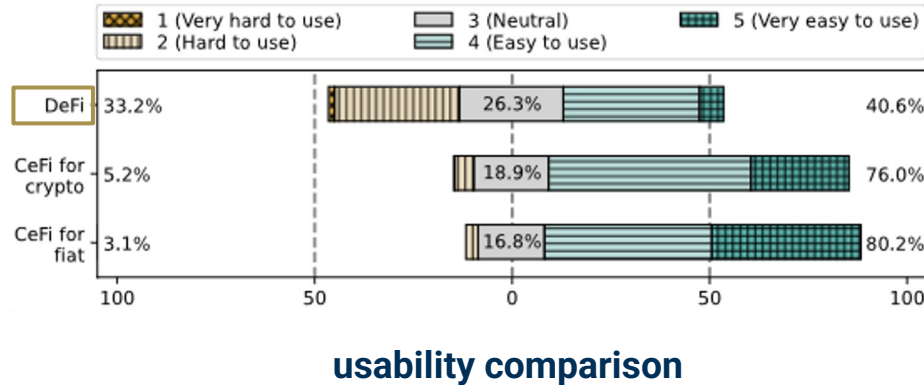
How do DeFi users **perceive regulation**?

# DeFi is more secure than CeFi? – seems not

“ Because [of] the amount of hacks... it sounds like it would be very **difficult to secure** [DeFi]. ”



# DeFi is easier to use than CeFi? – seems not, either



“ I had a **lot of trouble** at first figuring out what type of crypto I needed for gas fees. I was also shocked at how **expensive ETH fees** were. ”

# DeFi Love Points

Rank  
**2**

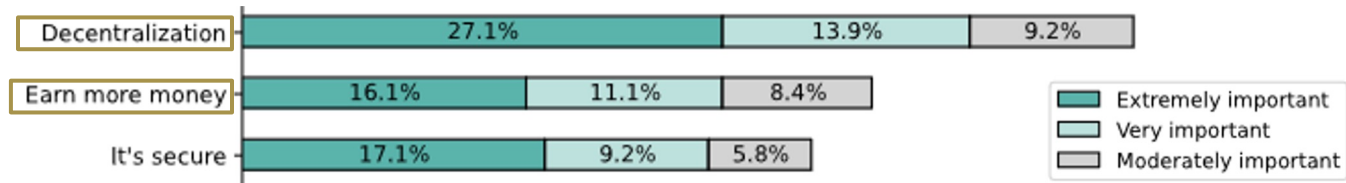
“ There are a lot of opportunities to have a **twenty percent APY** income. ”

Rank  
**1**

“ **Decentralized** [service] is always more safe than centralized [service]. ”



**misconception**



# Research Questions

RQ1

Why do people **continue to use** DeFi despite numerous DeFi incidents being reported?

RQ2

What **DeFi risks** are users concerned about, and how do they **mitigate** these risks?

RQ3

How do victims **respond** to DeFi incidents?

RQ4

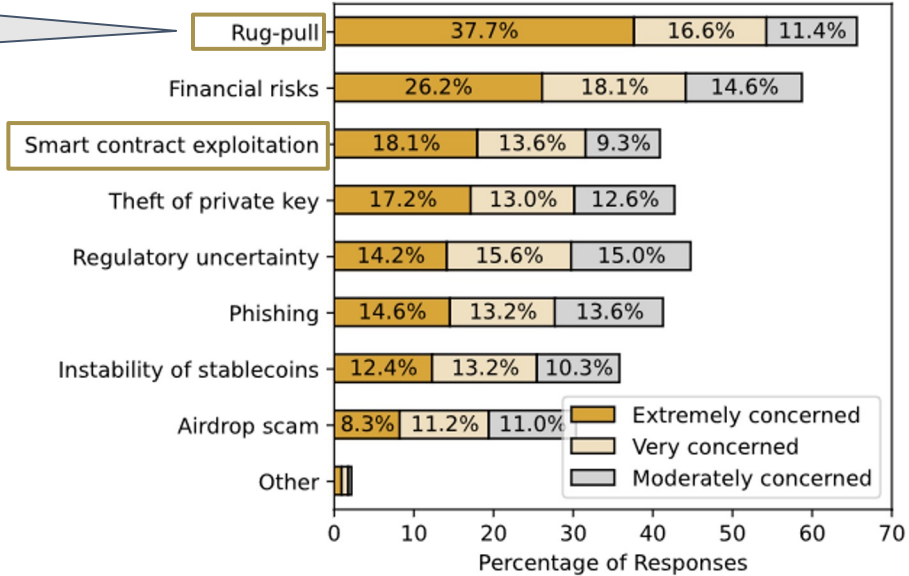
How do DeFi users **perceive regulation**?

# Concerned Risk

an exit scam, the team suddenly disappears



exploit of the vulnerability in smart contracts



# Risk Mitigation



**Low** adoption of **effective technical measures**

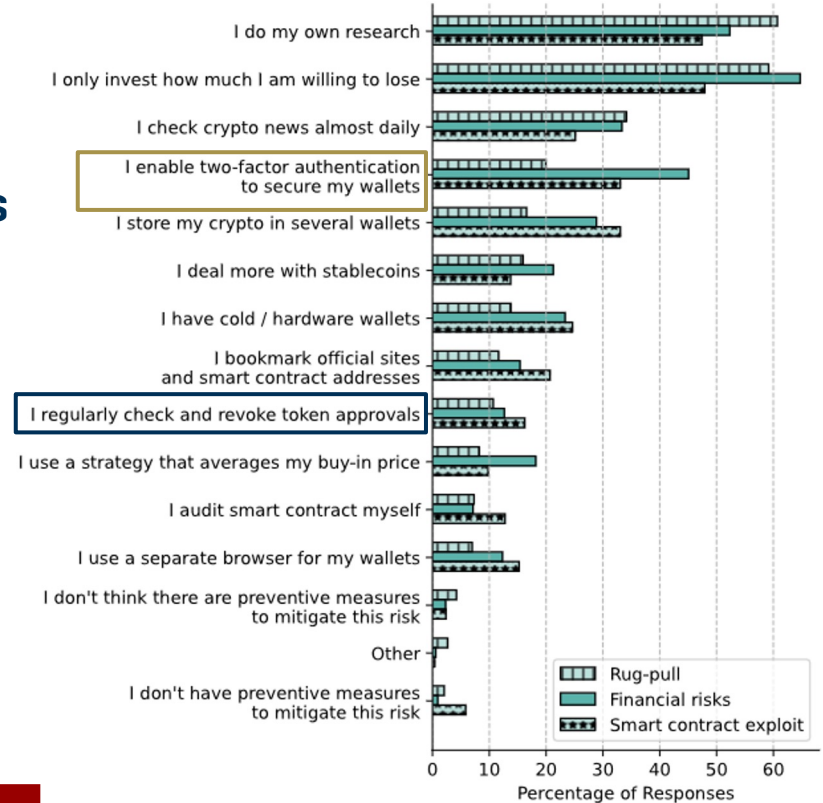
- e.g., revoke token approvals regularly

grant dApps access to a user's wallet

“ *Two-factor authentication has been one of the best solutions for keeping wallets safe.* ”



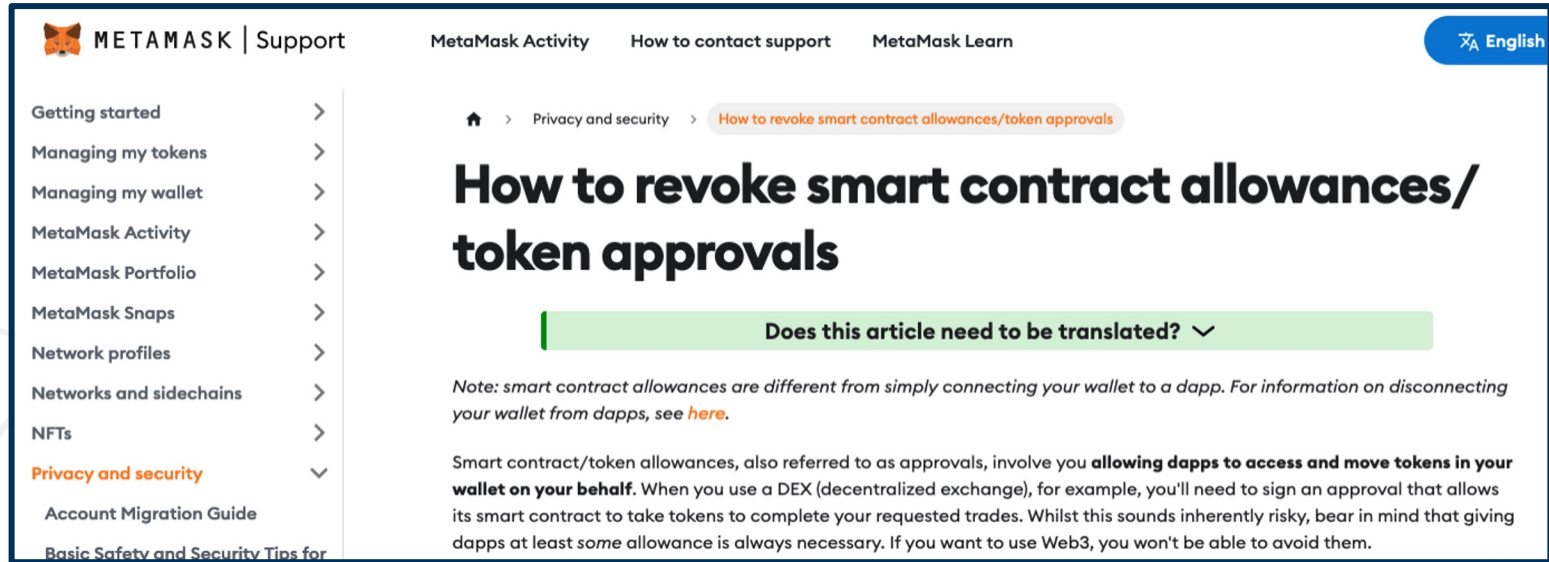
**misconception**





# Recommendation: Increase Adoption of Security Practices

- Implement a **reminder feature** that regularly prompts users to review their current token approvals



The screenshot shows the MetaMask Support website. The header includes the MetaMask logo and 'Support' text, along with navigation links for 'MetaMask Activity', 'How to contact support', and 'MetaMask Learn'. A language selector for 'English' is in the top right. A left sidebar lists various support topics, with 'Privacy and security' expanded to show sub-topics like 'Account Migration Guide' and 'Basic Safety and Security Tips for...'. The main content area features a breadcrumb trail: 'Home > Privacy and security > How to revoke smart contract allowances/token approvals'. The article title is 'How to revoke smart contract allowances/token approvals'. Below the title is a green button that says 'Does this article need to be translated?'. A note follows: 'Note: smart contract allowances are different from simply connecting your wallet to a dapp. For information on disconnecting your wallet from dapps, see [here](#).' The main text explains that smart contract/token allowances, also called approvals, allow dapps to access and move tokens on the user's behalf. It notes that while this is risky, some allowance is necessary for using Web3.

MetaMask's educational material

# Overconfidence in 2FA

Rug-pull

Smart contract exploit

62%

65%

to mitigate  
**technically...**

were using 2FA

57%

49%

were using 2FA **only**

# Recommendation: Correct Misconceptions

- Suggest **clarifying** the covered threats in the **2FA** settings of custodial wallets



Coinbase's current 2FA interface

# Incident Impact on Risk Mitigation

- **Integral practices** were **not** sufficiently adopted by **victims**
  - timely check and revoke token approvals
  - use hardware wallets
- The **misconception about 2FA** was **also prevalent** among the **victims**

# Research Questions

RQ1

Why do people **continue to use** DeFi despite numerous DeFi incidents being reported?

RQ2

What **DeFi risks** are users concerned about, and how do they **mitigate** these risks?

RQ3

How do victims **respond** to DeFi incidents?

RQ4

How do DeFi users **perceive regulation**?

# Response Actions

after a scam...

*disconnected wallet  
from every site* **27%**

*revoked every token  
approval on wallet* **20%**

**Good**

**26%** *did nothing but  
moved on*

**16%** *invested more in  
other DeFi services*

**Good?**

# Perception Changes



“ *My belief in cryptocurrency has grown stronger after [experiencing] that [DeFi scam] because I made good money from it...  
**An opportunity to make money is something I believe in.*** ”

“ *I just felt like I was the victim of my own circumstance... Not doing enough research before diving into it... **it was my fault basically.*** ”

> **50%** of victims did not change their belief...

# # of Incidents Encountered

Hack

1.8

Scam

4.7

some victims reported experiencing **> 10** scams...





- Users' strong financial motivations seem to outweigh security priorities and concerns.
- Experience and education may be insufficient to help users employ better security practices.

Link to paper:



# Thank you!

## Q & A

Mingyi Liu <[mingyiliu@gatech.edu](mailto:mingyiliu@gatech.edu)>



**SAMSUNG**



SUNGKYUNKWAN UNIVERSITY

