Rug Life

Using Blockchain Analytics to Detect Illicit Activity, Track Stolen Funds, and Stay Safe

Heidi Wilder

Coinbase

Special Investigations

PARANOIA IS KEY.

End of presentation. Jk.

Section 1

What do we define as illicit?

What do we define as illicit?

- Scammers?
- Dark markets?
- Thefts / hacks?
- Shrewd traders?
- OFAC'd entities?

Theft typologies

- Team / dev initiated (rug) → Token dumping
  (Un)limiting functions
  Cashing out of all proceeds
  Sometimes website 404s / socials down
- Third parties
  - Hacks → Same as above except website / socials aren’t down
  - Market manipulation? → Pool(s) / pairs usually manipulated to suppress the value of one token and pump up the value of another
- Third party service attacks → Service team relies on gets exploited
  Investor funds/asset loss

Section 2

Detection methods

Detection methods

- Protocols: set up alerts to monitor large flows of funds
- Alerting platforms: Blocknative (mempool monitoring,) Tenderly, Etherscan (ERC20 only)
- Follow auditors

...but once a tx is broadcast there’s no going back.

Detecting the “weird stuff” in advance

If you’re a dev…

- Constantly audit logs of your debits and credits
- Monitor for how users are transacting with your contract
- Monitor who's accessing your site's front/backend

If you’re an investor…

- Check the contracts you interact with!
- Revoke.cash is your friend (for now)
- Monitor socials and your wallet

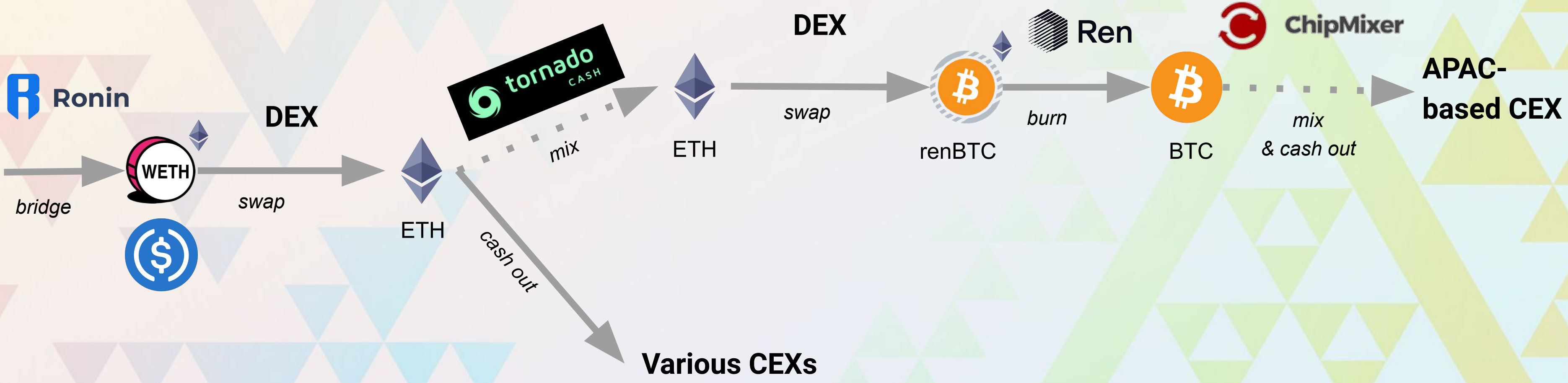
Section 3

Tracking funds

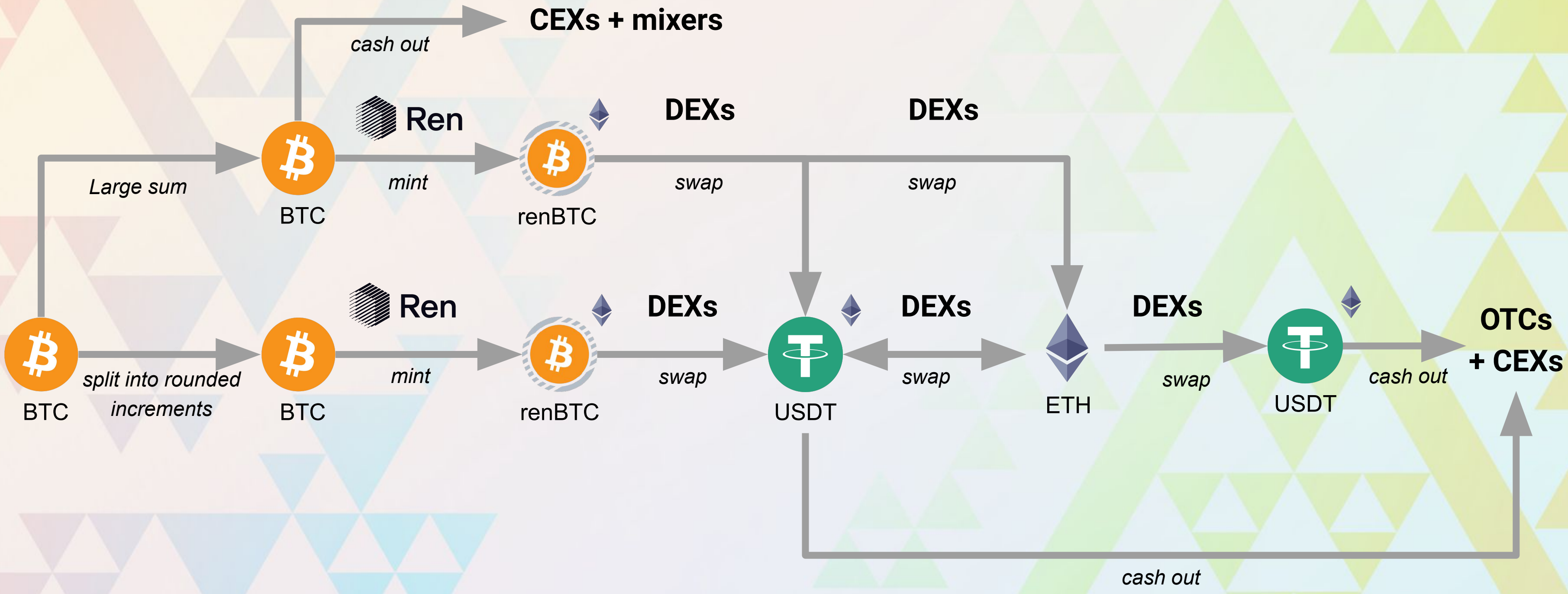
Tracking funds

- Etherscan
  - Learn how to read a block explorer
  - Blockchain analytics tools like Dune, Bloxy, graphing tools
- Leverage Twitter investigators (but not too much)
- File with IC3 - if you’re US based
  - Reach out to local LE equivalent in other countries
- If you're a part of the dev team:
  - *Communicate* with your community
- Story (nightmare) time:
    - Case study - Ronin theft

Case study - Ronin hack drive-by



Case study - Ronin hack drive-by



Case study takeaways…

- Trying to recoup stolen money is no joke
- It’s not only extremely costly and time consuming, but you likely won’t be able to recoup much
- Luckily, because the blockchain is transparent and immutable, we can track funds

Section 4

How to protect yourself

Protecting yourself

General stuff

- 2FA everywhere
- Use a cold wallet; multisig
- Don't download random offbrand software
- Don’t be impulsive

Blockchain stuff

- Check the contract you're planning to interact with, before you do
- Where did the team get funding from to set up their first contracts? Check on multiple networks
- Where is the team cashing out to
- Get audited from multiple outlets

Social Media

- Clamp down on socials; private your personal profiles
- Discord
  - Only let friends add you on Discord
  - Limit Discord bots; mod access

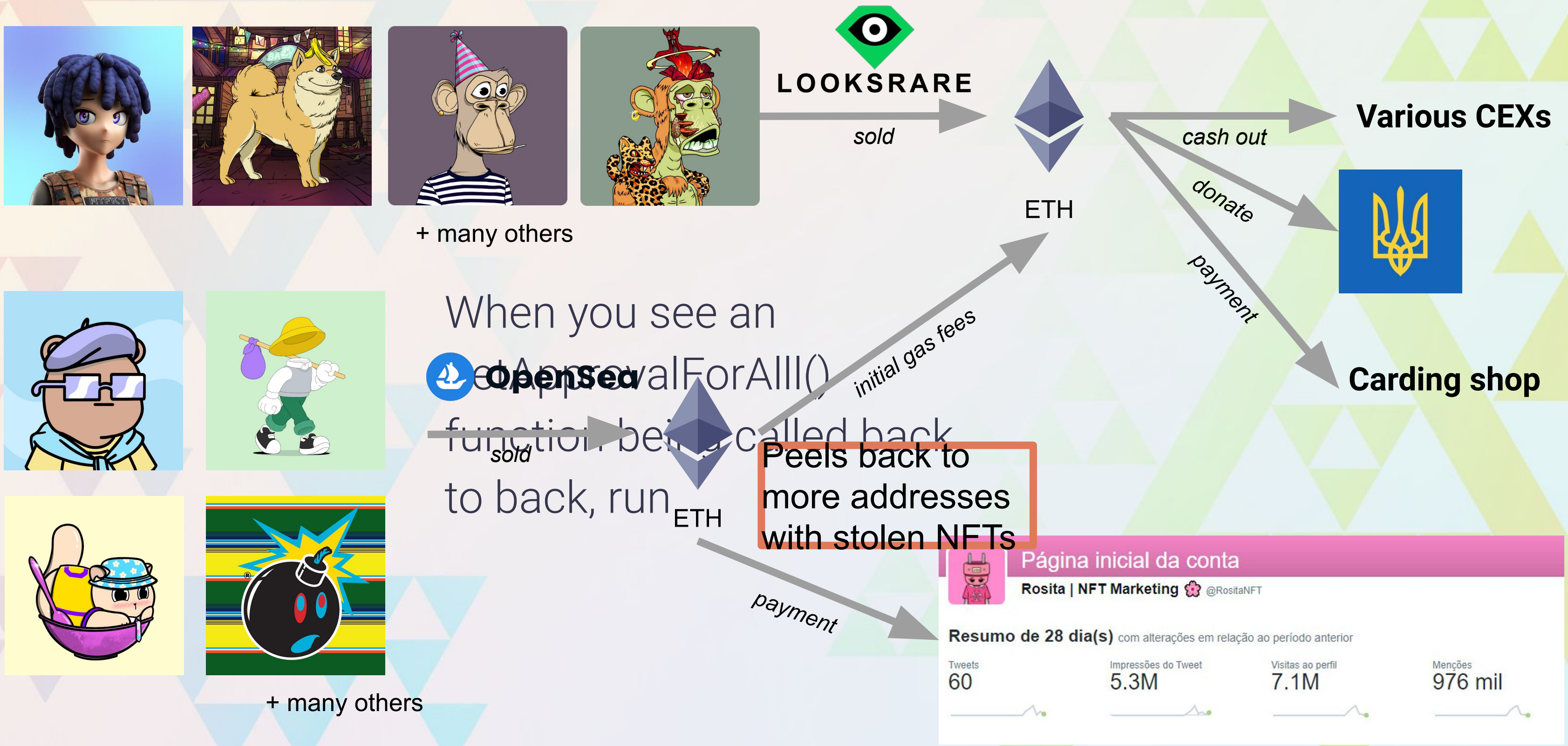
Emails

- Limit ability to open emails (Don’t open random email attachments!)
- Verify email domains

Basic DD

- If you’re a dev...surround yourself with a team you can trust
- If you’re an investor, do some DD on the team.
  - Who are they? How long have their socials been up for?
  - Are their followers all bots? Is the discord full of bots/paid advertisers? How do you know?
  - Where are they cashing in/out of - CEX-wise?
- If you’re an investor, who’s interacted with the contract? Are team members/others given advantages?

An example of being impulsive…



When you see an setApprovalForAll() function being called back to back, run

Peels back to more addresses with stolen NFTs

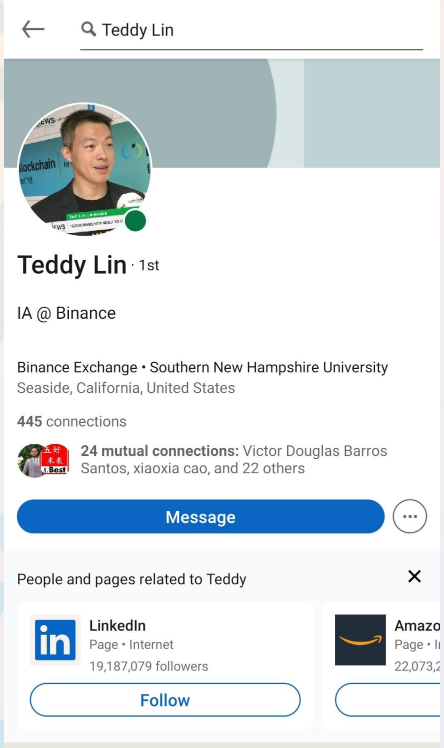
Página inicial da conta

Rosita | NFT Marketing 🌸 @RositaNFT

Resumo de 28 dia(s) com alterações em relação ao período anterior

Tweets	Impressões do Tweet	Visitas ao perfil	Menções
60	5.3M	7.1M	976 mil

An example of social engineering…



Teddy Lin

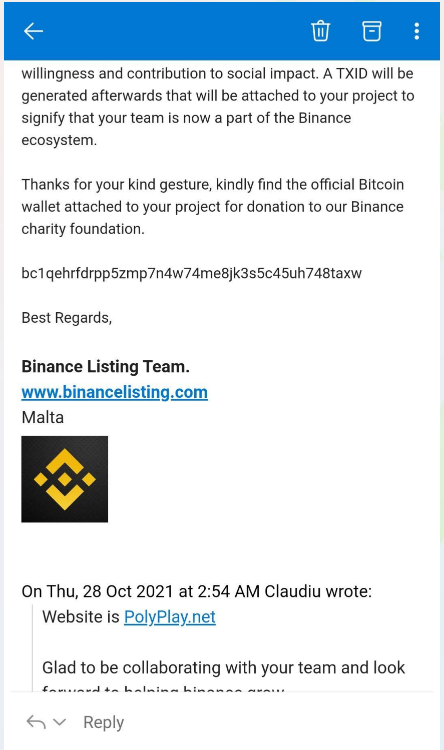
Teddy Lin · 1st

IA @ Binance

Binance Exchange • Southern New Hampshire University
Seaside, California, United States

445 connections

24 mutual connections: Victor Douglas Barros Santos, xiaoxia cao, and 22 others



willingness and contribution to social impact. A TXID will be generated afterwards that will be attached to your project to signify that your team is now a part of the Binance ecosystem.

Thanks for your kind gesture, kindly find the official Bitcoin wallet attached to your project for donation to our Binance charity foundation.

bc1qehrfdrpp5zmp7n4w74me8jk3s5c45uh748taxw

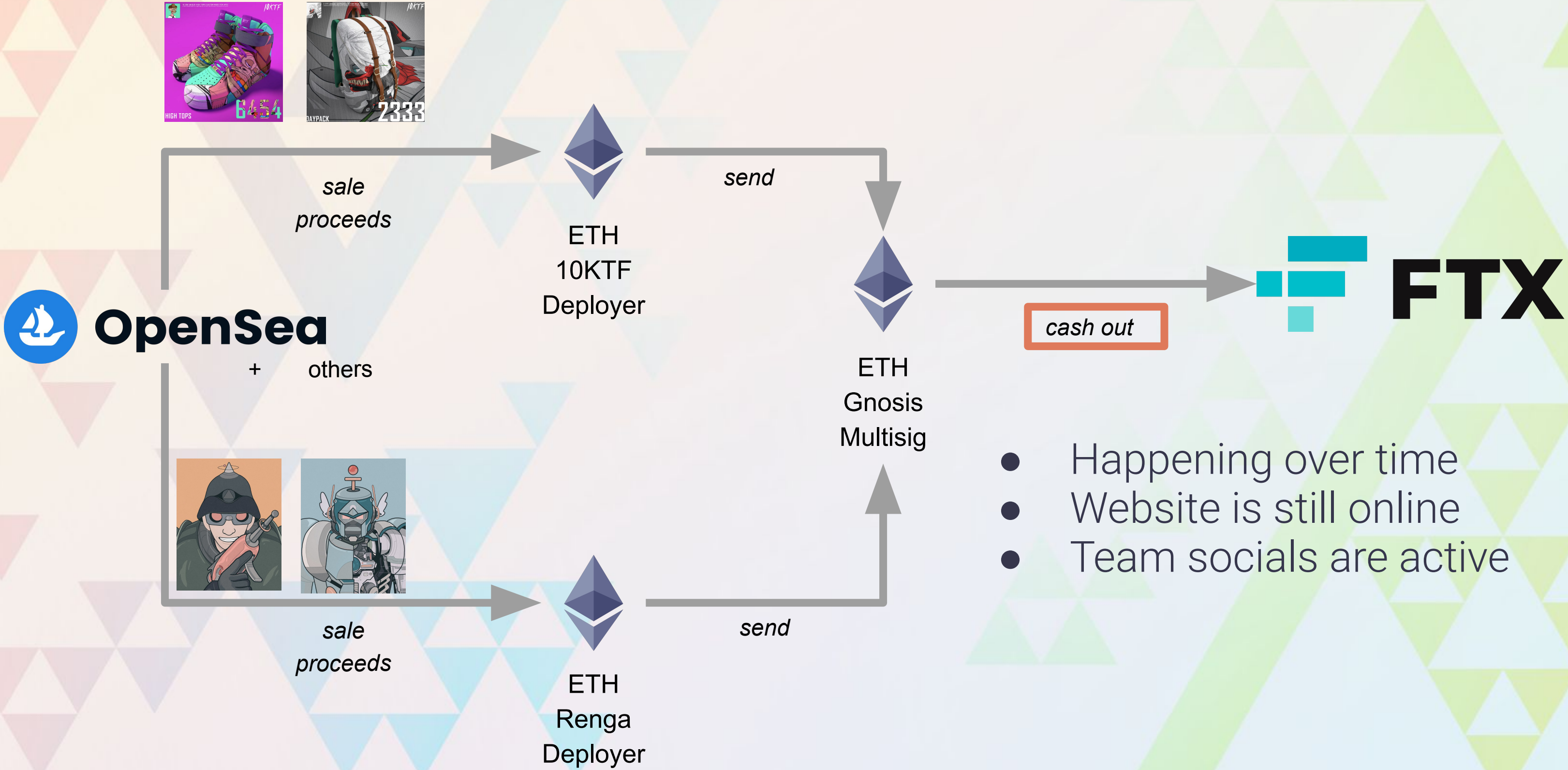
Best Regards,

Binance Listing Team.
www.binancelisting.com
Malta

On Thu, 28 Oct 2021 at 2:54 AM Claudiu wrote:

> Website is PolyPlay.net
>
> Glad to be collaborating with your team and look forward to helping binance grow

An example of an actual dev team cash out



OpenSea + others

sale proceeds

ETH 10KTF Deployer

send

ETH Gnosis Multisig

cash out

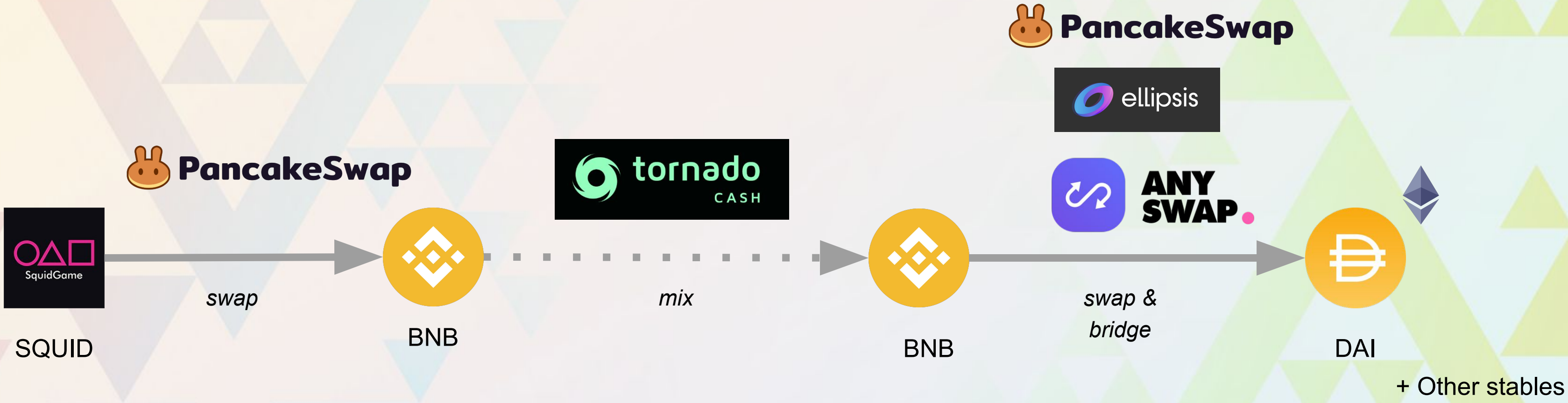
sale proceeds

ETH Renga Deployer

send

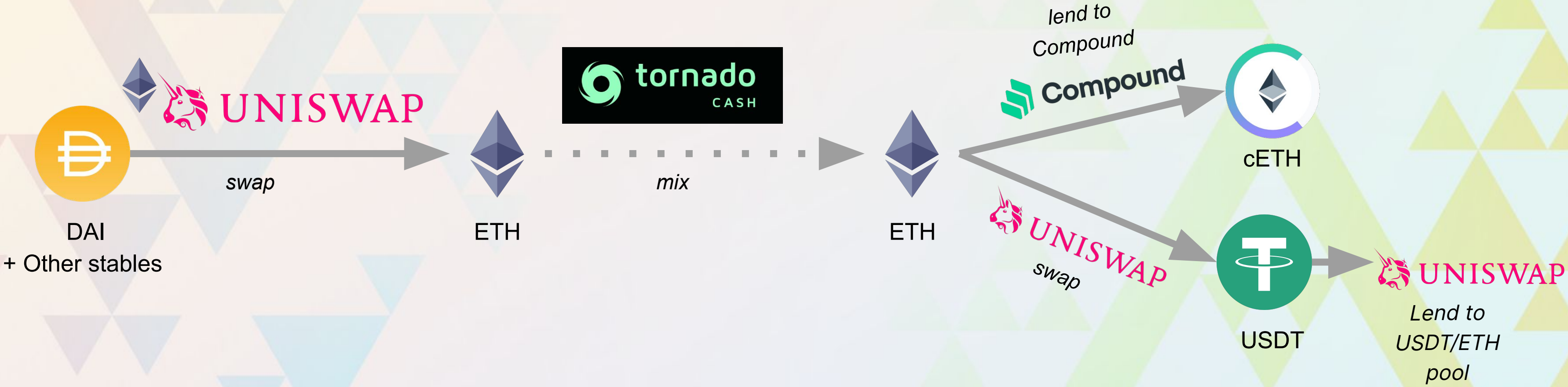
- Happening over time
- Website is still online
- Team socials are active

An example of a “dev team” “cash out” aka rug



- Website 404
- Socials deleted

An example of a “dev team” “cash out” aka rug



Predictions

- We expect hacks/scams/etc to continue (even in a bear market)
- Defi protocols, especially those with large pools (TVL) will continue to be perceived as honeypots
- Threat actors will mainly sit on funds, possibly earn yield and cash out in the next bull market (if they can)

Takeaways

- Be paranoid!
- Protect yourself BEFORE something happens.
    - Once a tx is on the blockchain, it’s too late.):
- DYOR
- Learn how to read a block explorer and set up monitoring

Thank you!

Heidi Wilder

Coinbase

Special Investigations

heidi.wilder@coinbase.com