Part 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

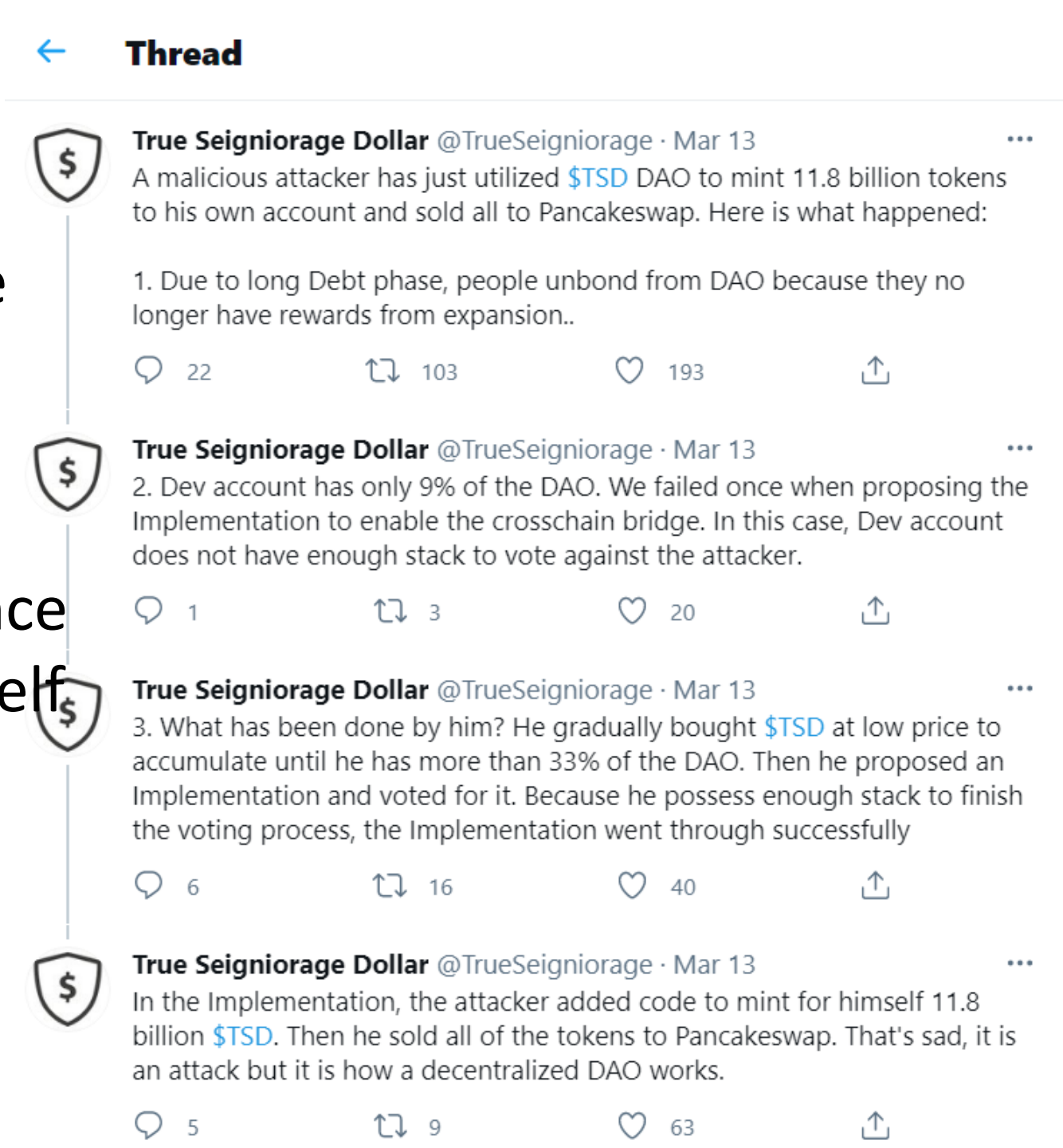
51% (or less)

- 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

True Seigniorage Dollar (TSD) Price Chart

Risks: Governance risk: Delegation

Andreessen Horowitz

Open Sourcing Our Token Delegate Program - Andreessen Horowitz

Over the last year we've worked with dozens of delegates across a number of leading protocols. Here are some of the best practices that we've identified.

Yesterday at 6:00 PM (169 kB)

Over the last year we've built a delegation program around these exact principles. We've used it to delegate well over half of our voting power in protocols like Compound, Uniswap and Celo to a broad network of qualified delegates. These include: leading non-profits like Kiva and Mercy Corps; global businesses like Deutsche Telekom; crypto startups like Gauntlet, Argent, and Dharma; university organizations like Stanford Blockchain Club and Blockchain at Columbia; and up-and-coming community leaders like Getty Hill.

https://a16z.com/2021/08/26/open-sourcing-our-token-delegate-program/

Part IV:

DeFi Risks and Opportunities

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

(ii) DNS Attack

Risks: DNS attack

DNS

- Hacker takes over domain name service and tricks user into giving private key
- This type of attack is not special to DeFi – it is a common cyber threat
- However, it contains special lessons for those active in the DeFi space

Risks: DNS attack

coindesk

March 15, 2021

DeFi Projects Cream Finance, PancakeSwap Hit With 'DNS Hijacks'

The hijacker appears to be asking users to input the 12-word seed phrase unique to each crypto wallet in order to steal funds.

Risks: DNS attack

PancakeSwap #BSC @PancakeSwap · 23h

This is now confirmed.

DO NOT go to the Pancakeswap site until we confirm it is all clear.

NEVER EVER input your seed phrase or private keys on a website.

We are working on recovery now.

Sorry for the trouble.

Cream Finance
@CreamdotFinance

Our DNS has been compromised by a third party; some users are seeing requests for seed phrase on app.cream.finance. DO NOT enter your seed phrase.

We will never ask you to submit any private key or seed phrases.

9:10 AM · Mar 15, 2021

873 706 Copy link to Tweet

Mar 15, 2021 at 11:00 a.m. EDT ▪ Updated Mar 15, 2021 at 1:30 p.m. EDT

Update (March 15, 17:30 UTC): *PancakeSwap says it has regained access to the DNS. Cream is still working to resolve the issue.*

Part IV:

DeFi Risks and Opportunities

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

(iii) Oracle Attack

Risks: Oracle risk

What is oracle risk?

- Oracles are one of the last unsolved problems in DeFi and are required by most DeFi protocols in order to function correctly.
- Fundamentally, oracles aim to answer the simple question: How can off-chain data be securely reported on chain?
- Without oracles, blockchains are completely self-encapsulated and have no knowledge of the outside world other than the transactions added to the native blockchain.

Risks: Oracle risk

What is oracle risk?

- Many DeFi protocols require access to secure, tamper-resistant asset prices to ensure that routine actions, such as liquidations and prediction market resolutions, function correctly.
- Protocol reliance on these data feeds introduces *oracle risk*.
- If an oracle's *Cost of Corruption* is ever less than an attacker's potential *Profit from Corruption*, the oracle is extremely vulnerable to attack.

Risks: Oracle risk

Types: Shelling-point oracle

- This oracle relies on the owners of a fixed-supply token to vote on the outcome of an event or report the price of an asset.
- Examples of this type of oracle include Augur and UMA.
- While Schelling-point oracles preserve the decentralization components of protocols that rely on them, they suffer from slow times to resolution.

Risks: Oracle risk

Types: API oracle

- These oracles are centralized entities that respond asynchronously to requests for data or prices.
- Examples include Provable, Oraclize, and Chainlink. All systems relying on API-based oracles, must trust the data provider to respond accurately to all queries.

Risks: Oracle risk

Types: Application-specific oracle service

- This type of oracle is used by Maker and Compound.
- Its design differs based on the requirements of the protocol it was developed for.
- For example, Compound relies on a single data provider that the Compound team controls to provide all on-chain price data to the Compound oracle.

Risks: Oracle risk

Highest risk

- Oracles, as they exist today, represent the highest risk to DeFi protocols that rely on them.
- All on-chain oracles are vulnerable to front-running, and millions of dollars have been lost due to arbitrageurs.
- Additionally, oracle services, including Chainlink and Maker, have suffered crippling outages with catastrophic downstream effects.
- Until oracles are blockchain native, hardened, and proven resilient, they represent the largest systemic threat to DeFi today.

Part IV:

DeFi Risks and Opportunities

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

(iv) DEX Risk

Risks: DEX risk

What is DEX risk?

- The DEX landscape on Ethereum consists of two dominant types, Automated Market Makers (AMMs) and order-book exchanges.
- Both types of DEXs vary in architecture and have differing risk profiles.

Risks: DEX risk

AMM DEX

- AMMs, however, are the most popular DEX to date, because they allow users to trustlessly and securely exchange assets, while removing traditional counterparty risk.
- By storing exchange liquidity in a trustless smart contract, AMMs give users instant access to quotes on an exchange pair.

Risks: DEX risk

CFMM DEX

- Uniswap is the best-known example of an AMM, also known as a Constant-Function Market Maker (CFMM).
- Uniswap relies on the product of two assets to determine an exchange price.
- The amount of liquidity in the pool determines the slippage when assets are exchanged during a transaction.

Risks: DEX risk

CFMM DEX

- CFMMs such as Uniswap optimize for user experience and convenience, but sacrifice absolute returns. CFMM liquidity providers (LPs) earn yield by depositing assets into a pool, because the pool takes a fee for every trade (LPs benefit from high trading volume).
- This allows the pool to attract liquidity, but exposes LPs to smart contract risk and impermanent loss.

Risks: DEX risk

CFMM DEX

- Impermanent loss occurs when two assets in a pool have uncorrelated returns and high volatilities.
- These properties allow arbitrageurs to profit from the asset volatilities and price differences, reducing the temporary returns for LPs and exposing them to risk if an asset moves sharply in price.
- Some AMMs, such as Cap, are able to reduce impermanent loss by using an oracle to determine exchange prices and dynamically adjusting a pricing curve to prevent arbitrageurs from exploiting LPs, but impermanent loss remains a large problem with most AMMs used today.

Risks: DEX risk

On-chain order-book DEX

- On-chain order-book DEXs have a different but prevalent set of risks.
- These exchanges suffer from the scalability issues inherited from the underlying blockchain they run atop of, and are often vulnerable to front running by sophisticated arbitrage bots.
- Order-book DEXs also often have large spreads due to the presence of low-sophistication market makers.
- Order-book DEXs are often forced to rely on a single market maker for each asset pair.

Risks: DEX risk

Off-chain order-book DEX

- Several decentralized exchanges use an entirely off-chain order book, retaining the benefits of a noncustodial DEX, while circumventing the market making and scaling problems posed by on-chain order-book DEXs.
- These exchanges function by settling all position entries and exits on chain, while maintaining a limit-order book entirely off chain.
- This allows the DEX to avoid the scaling and UX issues faced by on-chain order-book DEXs, but also presents a separate set of problems around regulatory compliance.

Part IV:

DeFi Risks and Opportunities

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

(v) Custodial Risk

Risks: Custodial risk

What is custodial risk?

- Cryptocurrency ownership is guaranteed by the possession of a **private key** – a **long random number** that cannot be guessed. For Bitcoin and Ethereum, the private keys are 256 bits or 64 hexadecimal characters.
- Private keys are used via a **digital signature algorithm** to sign transactions. Hence, you need your private key to **"spend"**.
- Custodial risk is **when you lose your private key**.
- Both **individual users and institutions** (corporations, endowments, etc.) are subject to custodial risk.

Risks: Custodial risk

Types of Custodianship

- Self-Custody: Build our own solution
  - In-house or commercial solutions that store crypto assets
  - Solely responsible for assets and not insured against unexpected events
- Partial Custody: Your own wallet + external solution
  - Includes 2-FA and multi-signature solutions (e.g., BitGo)
  - Aligns with needs of retail and high net-worth clients
- Third-party Custody: Hire a managed solution
  - Fully maintained by service provider(s)
  - Aligns with needs of institutions, needed by regulatory bodies

Risks: Custodial risk

Retail Users

- Retail users have a choice between custodial and non-custodial wallets
  - Non-Custodial Wallet (Self-Custody) : User has full control of keys
    - E.g., Hardware wallet, Web wallet (MetaMask – keys stored in browser), Desktop wallet (Electrum – stored on machine), Mobile Paper wallet
  - Custodial Wallet (Third Party Custody): 3rd party holds access to private keys
    - E.g., Coinbase, Binance
    - Users are subject to KYC/AML regulation

Risks: Custodial risk

The New York Times

Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes

Bitcoin owners are getting rich because the cryptocurrency has soared. But what happens when you can't tap that wealth because you forgot the password to your digital wallet?

Stefan Thomas, a German-born programmer living in San Francisco, has two guesses left to figure out a password that is worth, as of this week, about $220 million.

https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html

Risks: Custodial risk

MINIMIZE RISKS ASSOCIATED WITH LOST OR STOLEN DRIVES

Self-defending IronKey Basic drives are hardened to stand up to malware or mischief, so confidential data stays where it belongs. And after 10 failed consecutive password attempts, the device will either self-destruct or reset (if previously enabled) back to its default state.

https://www.ironkey.com/en-US/encrypted-storage-drives/250-basic.html

Risks: Custodial risk

Exchange Hacks

- Several exchanges have been hacked, highlighting the security risk of cryptocurrencies
  - Mt. Gox (2011-2014) - 850k Bitcoin
  - Bitfloor (2012) - 24k Bitcoin
  - Bittfinex (2016) - 120k Bitcoin
  - Coincheck (2018) - 523 million NEM (Worth $500 million at the time)
  - Binance (2019) - 7k Bitcoin
- Stolen cryptocurrency is often not completely recovered

Risks: Custodial risk

Delegating custody

- If you delegate the ownership of your private keys, say to an exchange, there is risk the exchange will be hacked and the keys stolen.
- Exchanges keep most of the private keys in “cold storage” (either on a drive not connected to the Internet or hard copy in a physical vault)
- Some exchanges, like Coinbase, are insured. However, the insurance is only as good as the health of the insurer.

Risks: Custodial risk

Infrastructure by Custodians

- Wallet
  - Hot – Internet-connected solutions; fast and frictionless
  - Cold - Air-gapped or internet-isolated solutions; slower but very secure
- Storage Mechanism
  - Software – Digital platforms storing data on the internet or a network segment
  - Hardware – Specially built electronic devices storing data (e.g., Hardware Security Modules)
- Access Protocols
  - Multi Party Computation – Single signature computed by a distributed set of users
  - Multi-Sig – Uses multiple signatures from distinct private keys to secure a wallet

Risks: Custodial risk

Example of Infrastructure - Splitting keys

- Companies like BitGo offer multi-signature solutions
- Three keys:
  - Owner has two keys and BitGo holds one.
  - 2 of 3 keys can be used for a transaction
  - A hack of BitGo's key is useless because a single key cannot spend
- If a user loses one key, there is a backup

Risks: Custodial risk

Concerns around custodianship

- Latency vs Speed
  - Trading at low latency = having fast access to funds
  - But this raises questions around security and proper verification
- New Coins
  - Custodians don't support all newly invented coins for compliance
  - Some coins are offered in some countries and not in others
- Staking
  - Transaction validation on a PoS chain, can be done independently or through a custodian
  - Choose custodian wallet for staking based on proper care and due-diligence

Risks: Custodial risk

Top Custodians

- Coinbase Trust
- Bitgo
- Fidelity Digital Assets
- Bakkt Warehouse
- Kingdom Trust
- Several Banks looking into developing solutions – ING, BBVA, Northern Trust

Institutions looking into Crypto

- Facebook
- Visa
- PayPal
- Mastercard
- Goldman Sachs
- IBM

https://medium.com/blockchain4all/leading-us-based-crypto-custodian-providers-for-institutional-clients-3ba9b8683c6d#:~:text=Who%20are%20the%20leading%20crypto,the%20world's%20largest%20crypto%20custodian.
https://finance.yahoo.com/u/yahoo-finance/watchlists/top-crypto-bets/

Risks: Custodial risk

Regulatory Environment

- In the past, a lack of custody solutions has been a main reason why hedge and mutual funds could not invest in crypto
- Legal and regulatory environments for custodians and institutions have not been clearly defined
  - Custody Rule of Investment Adviser Act of 1940 – Institution with $150 million AUM needs a licensed custodian
- Federally charted banks are allowed to provide crypto custodial services

https://www.coindesk.com/sec-qualified-custodian-statement
https://www2.deloitte.com/us/en/pages/audit/articles/cryptocurrency-custody-regulations-from-occ-deloitte-us.html