Elements of DeFi

https://web3.princeton.edu/elements-of-defi/

Professor Pramod Viswanath

Princeton University

Lecture 18

Decentralized Autonomous Organization (DAO)

Last lecture: NFTs

- Fungible vs Non-fungible assets
- Non fungible assets in real world
- Tokenized Non Fungible assets: NFTs
- Use cases of NFTs:
  - Tokenizing RWA
  - Art
  - Games
  - Supply chain tracking
- Challenges

This Lecture: DAOs and Governance

- When are DAOs needed?
    - Examples of various use cases to gather funds, allocate capital
    - Run corporations and DeFi protocols
    - Are they truly decentralized today?
- DAO structure
    - Who can propose? Who can vote?
    - Different voting rules that are used
    - Downsides of different voting rules and insider trading
    - Attacks on DAOs : the Vampire attack
- DAO – Real World interaction
    - Legislation on DAOs

Governance

- What is governance?
    - Elections (permissionless), board meetings (permissioned)
    - Voting, Checks and balance, transparent procedures
- Ensuring enough participation
    - Enfranchisement
- Community driven vs Voter apathy
    - US elections (70% in previous presidential election)
    - K-pop (digitally native band)

DAO

- Decentralized Autonomous Organization
- Decentralized – Power to change some underlying service is vested in a community of users and not in the hands of a few
- Autonomous – Votes on proposals are translated to changes (such as releasing funds) automatically
- Organization – Underlying entity that focuses on some service to rendered e.g. Uniswap, MakerDAO

Types of decentralization

- Logical decentralization
  - Is the underlying data structure look more like a single monolithic object, or an amorphous swarm?
  - Simple heuristic is: if you cut the system in half, including both providers and users, will both halves continue to fully operate as independent units?
- Architectural decentralization
  - how many **physical computers** is a system made up of? How many of those computers can it tolerate breaking down at any single time?
- Political decentralization
  - how many **individuals or organizations** ultimately control the computers that the system is made up of?

When are DAOs needed?

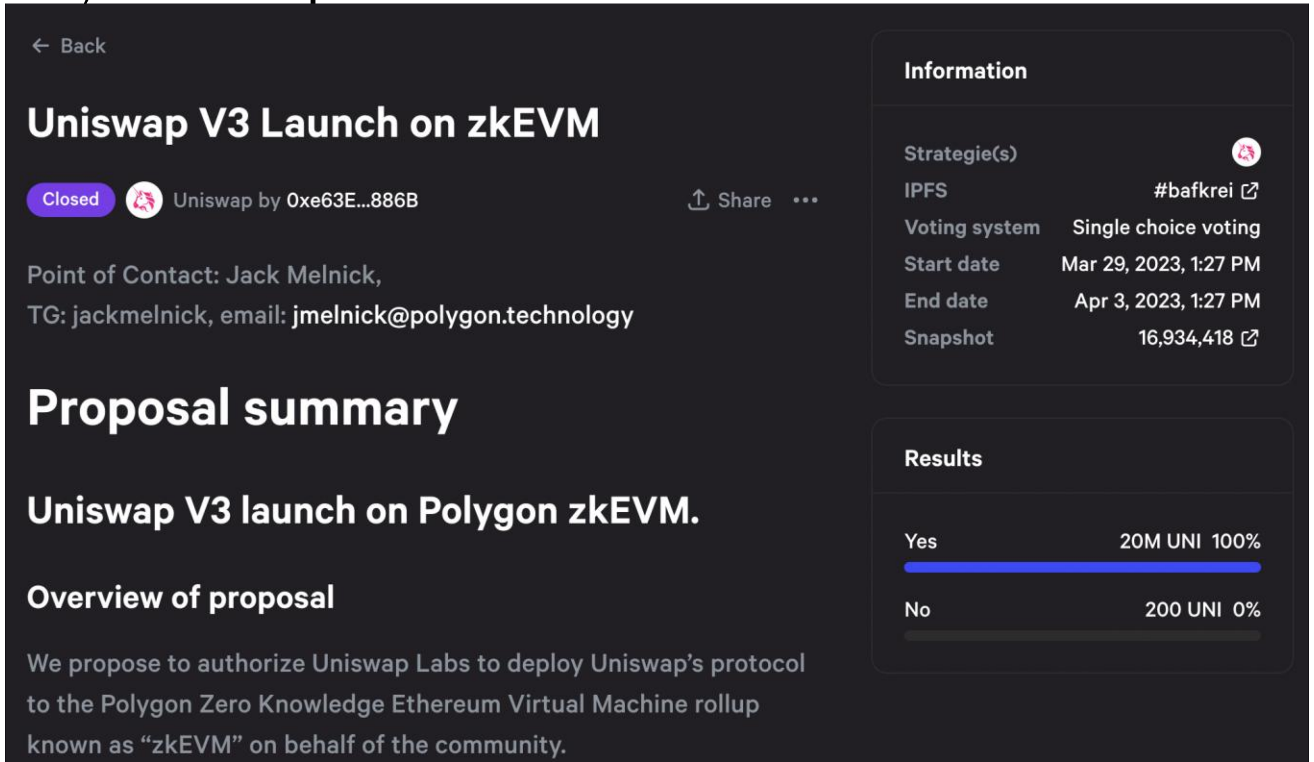
- Ideal DAO
  - When we need logical centralization…
  - But architectural + political decentralization

- Increase transparency
  - Smart contract code that acts upon a vote being passed is public
  - Votes and mechanism are also public

- Decrease intermediaries
  - Do not need to trust any political entity to handle funds locked for some purpose

Examples

- Proposal Execution in DeFi protocols
    - Users who deposit liquidity in protocols get governance tokens
    - Governance tokens can be used to vote on changes to protocol
    - E.g. Curve, Uniswap



Uniswap V3 Launch on zkEVM

Point of Contact: Jack Melnick,
TG: jackmelnick, email: jmelnick@polygon.technology

Proposal summary

Uniswap V3 launch on Polygon zkEVM.

Overview of proposal

We propose to authorize Uniswap Labs to deploy Uniswap's protocol to the Polygon Zero Knowledge Ethereum Virtual Machine rollup known as "zkEVM" on behalf of the community.

Information

Strategie(s)	
IPFS	#bafkrei
Voting system	Single choice voting
Start date	Mar 29, 2023, 1:27 PM
End date	Apr 3, 2023, 1:27 PM
Snapshot	16,934,418

Results

Yes	20M UNI	100%
No	200 UNI	0%

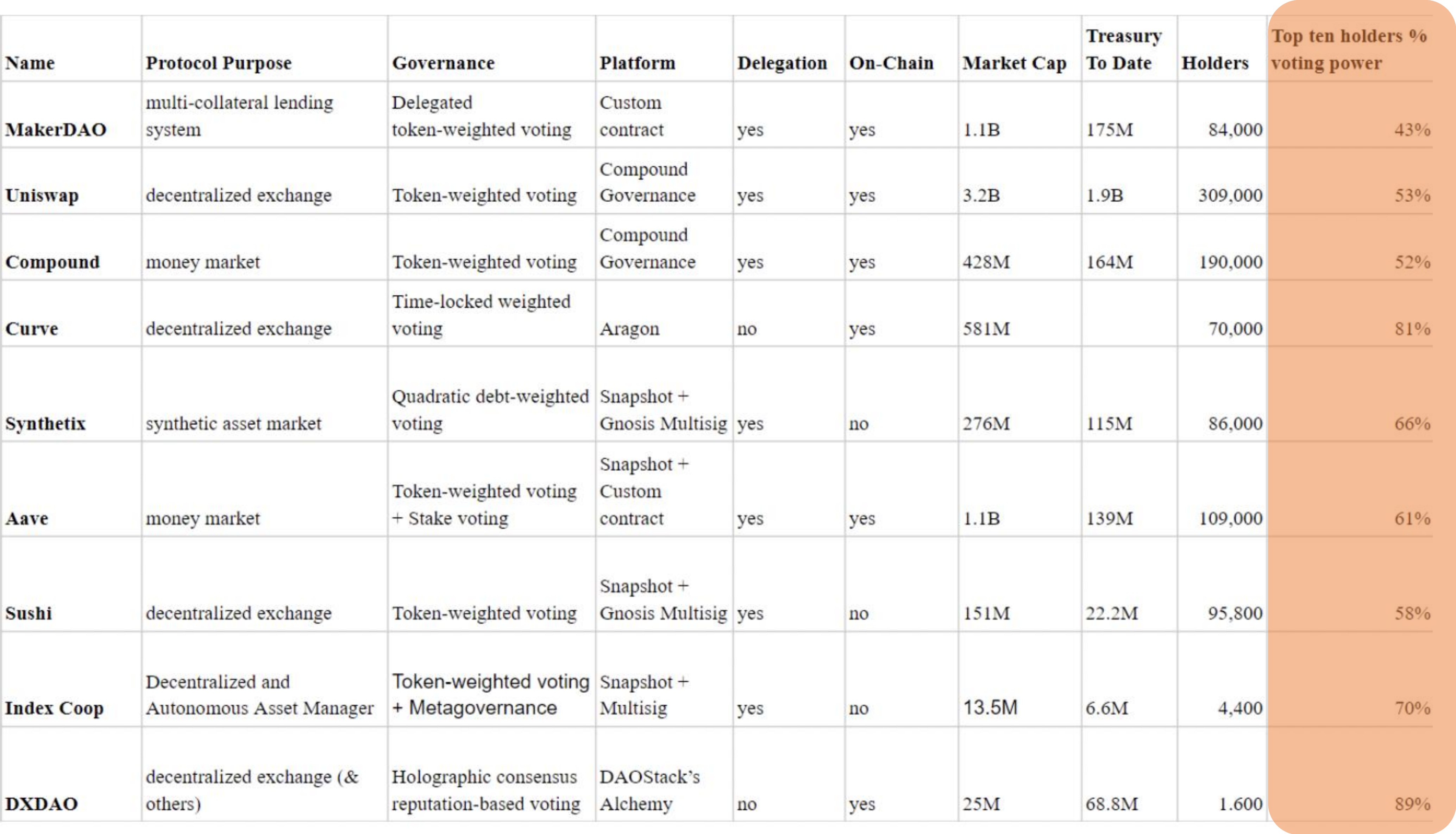
Examples

- Crowdfunding and Investment
  - Investors pool money into a contract, get governance tokens
  - Pool is used to buy real-world assets or build some product
  - Investors have voting rights over future proposals about those assets and products
  - E.g BitDAO, American CryptoFed DAO

Are DAOs really decentralized?

- DAO proposals usually discussed first on an informal forum – officially proposed only if they get enough attention – likes/views/comments – can be easily manipulated
- Move from informal forum to official proposals is often decided by a small council – protocol developers and “veterans” – council can censor arbitrarily
- Proposals are often too technical for most users
- Also have to trust developer teams to implement and audit any changes in a protocol

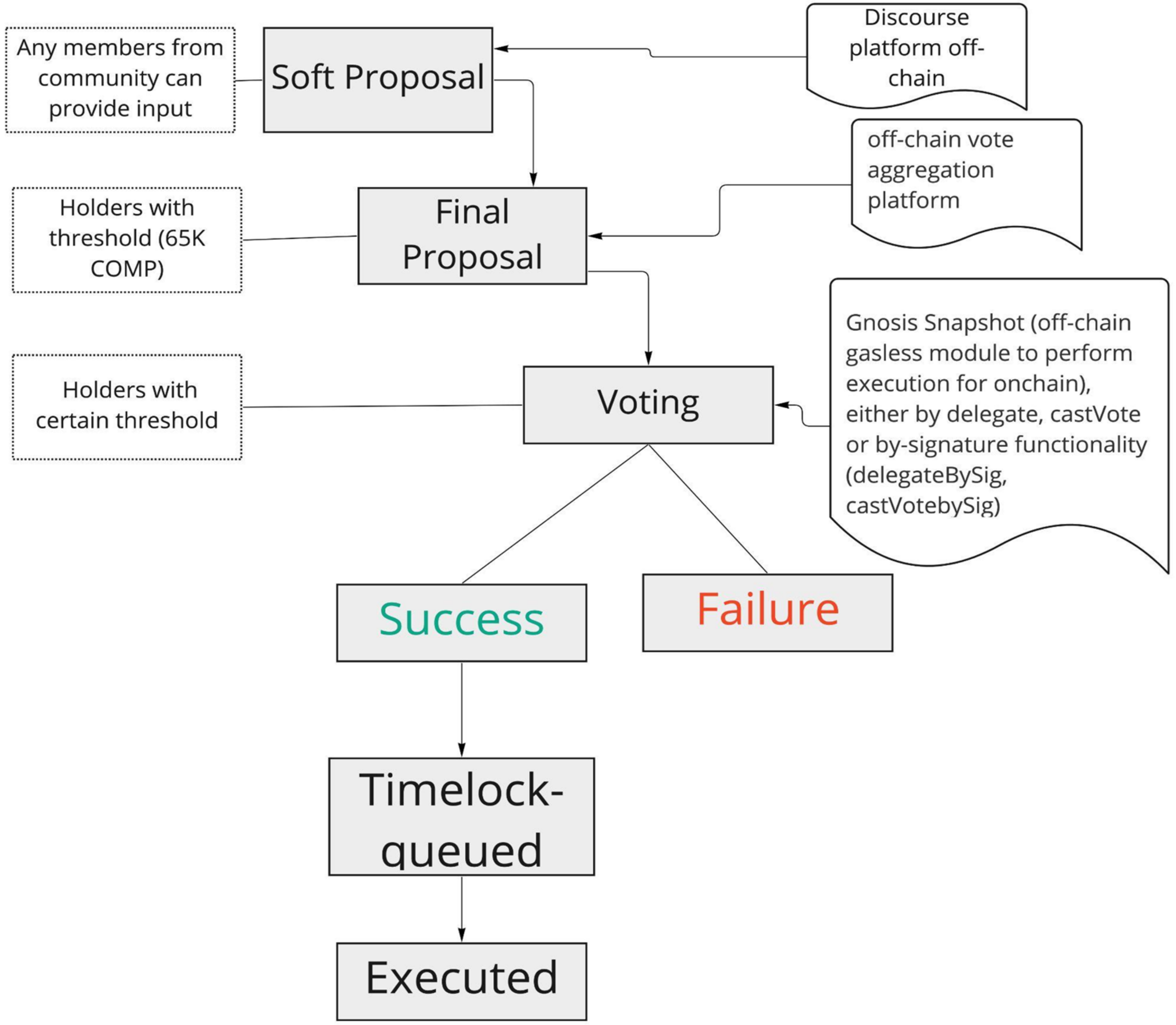
Are DAOs really decentralized?



Name	Protocol Purpose	Governance	Platform	Delegation	On-Chain	Market Cap	Treasury To Date	Holders	Top ten holders % voting power
MakerDAO	multi-collateral lending system	Delegated token-weighted voting	Custom contract	yes	yes	1.1B	175M	84,000	43%
Uniswap	decentralized exchange	Token-weighted voting	Compound Governance	yes	yes	3.2B	1.9B	309,000	53%
Compound	money market	Token-weighted voting	Compound Governance	yes	yes	428M	164M	190,000	52%
Curve	decentralized exchange	Time-locked weighted voting	Aragon	no	yes	581M		70,000	81%
Synthetix	synthetic asset market	Quadratic debt-weighted voting	Snapshot + Gnosis Multisig	yes	no	276M	115M	86,000	66%
Aave	money market	Token-weighted voting + Stake voting	Snapshot + Custom contract	yes	yes	1.1B	139M	109,000	61%
Sushi	decentralized exchange	Token-weighted voting	Snapshot + Gnosis Multisig	yes	no	151M	22.2M	95,800	58%
Index Coop	Decentralized and Autonomous Asset Manager	Token-weighted voting + Metagovernance	Snapshot + Multisig	yes	no	13.5M	6.6M	4,400	70%
DXDAO	decentralized exchange (& others)	Holographic consensus reputation-based voting	DAOStack's Alchemy	no	yes	25M	68.8M	1.600	89%

DAO: structure and mechanisms

Example of Governance Model: Compound Protocol



Any members from community can provide input

Soft Proposal

Discourse platform off-chain

Holders with threshold (65K COMP)

Final Proposal

off-chain vote aggregation platform

Holders with certain threshold

Voting

Gnosis Snapshot (off-chain gasless module to perform execution for onchain), either by delegate, castVote or by-signature functionality (delegateBySig, castVotebySig)

Success

Failure

Timelock-queued

Executed

Voting rules

DAOs need voting rules that combat the following problems:

- Voter apathy – most DAOs on –chain suffer from terrible participation rates
- Voting mechanism needs to be simple enough to hold voter attention
- Vote buying – since votes are public, can have smart contracts that pay locked bribes to voters if they vote a certain way
- Sybil attacks – many voting mechanisms have diminishing marginal voting power returns on stake to prevent vote buying – incentivizes sybil attacks

Quorum voting

- Tokens staked = votes
- Proposal passes if at least some minimum participation achieved and there is majority in favor
- Token hoarders get more power, especially if participation and quorum threshold is low
- Easy for token hoarders to bribe others as well

Conviction voting

- Gather votes continuously instead of one-shot
- Tokens staked longer = more voting power
- Change of opinion = voting power falls
- Vote buying costs more – need to ensure bribed users stake token for a longer time
- Voters can be dormant – only changes in voter distribution need to be expressed

Quadratic voting

- Fixed budget of tokens given to each user periodically (say 100 tokens)
- Voters use that budget on any proposal – voting power proportional to sqrt of tokens staked
- Makes bribing voters harder and decreases power of a single entity with a large stake
- But still prone to Sybil attacks

Holographic consensus

- Proposer runs a betting market on the possible outcomes of the proposal
- If proposal passes, users who bet on that outcome are rewarded, otherwise users who bet against are rewarded + proposer penalized
- Betters only bet on extreme proposals (obvious pass or obvious fails) and makes it easier for other voters to decide where to pay attention
- Increases voter engagement through betting rewards
- Rewards given out by protocol treasury

Attacks and abuse of power

- Privileged access to some DAO functionality can give rise to insider trading – indicates that not all of the power in the DAO is distributed equally

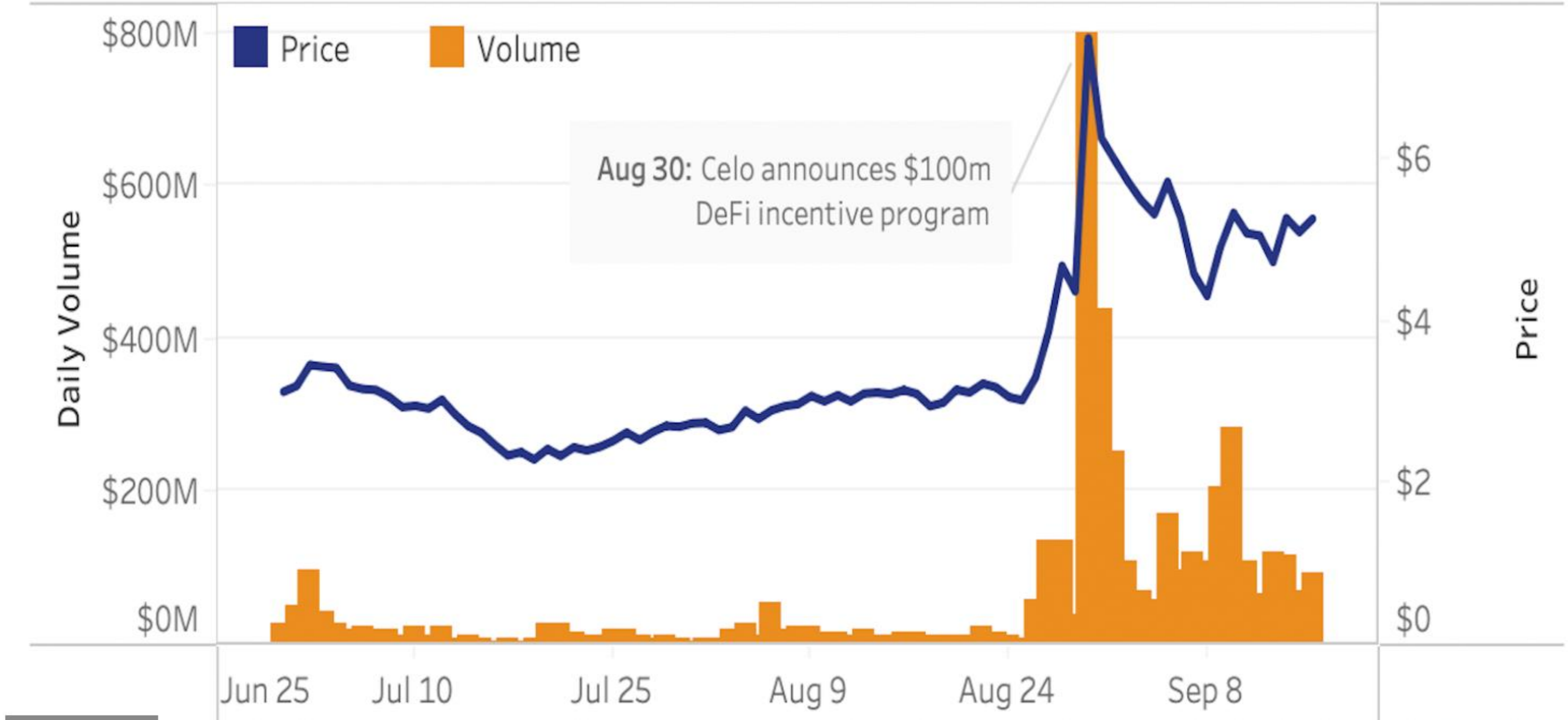
- DAO with low participation can be subject to hostile takeover attacks

- Because protocol code is public, any other copy can be made (with more lucrative joining incentives) and same governance token used – this draws users/voters from the former protocol

Insider trading in DAOs

- Evidence of insider trading has been observed in the run up to the announcement of incentive schemes
- E.g. Celo, Algorand, Avalanche

Celo token price, volume



Hostile takeovers

- DAOs with large treasuries and liquidity in AMMs incentivize governance takeovers
- Made easier with low participation rates

- E.g. 1
  - In Feb 2022, Build finance was attacked by an entity hoarding large number of governance tokens.
  - Proposal that was passed minted more governance tokens, which were sold on Uniswap to drain the liquidity from all pools containing that token - $500k worth of cryptocurrency

Hostile takeovers

- If governance proposals and their execution is allowed in the same block, it leads to easier passing of malicious proposals

- E.g. 2
  - In Apr 2022, Beanstalk was attacked by an entity who put up two malicious proposals to send treasury funds to their own account
  - The proposals were approved and executed in the same block since the flash loan enabled the entity to give enough votes to pass the minimum threshold

Vampire attacks

- Transparency of DAOs and underlying blockchains imply that anyone can copy your code
- If the copied DAO gives out more lucrative rewards for joining and uses the same governance token to stake – leads to draining of governance power in the older DAO
- E.g.
  - Aug 2020 : Sushiswap sucked around $1.8B in liquidity from Uniswap in just 11 days, by simply copying their code
  - Feb 2022 : LooksRare NFT platform did a similar attack on OpenSea, getting over $300M of volume in a month vs OpenSea's $100M

Legislation on DAOs

1. Vermont, Wyoming, and Tennessee:
   1. Have introduced new legislation for DAOs.
   2. Allows limited liability without corporate structure.
2. Criticisms:
   1. Imposes restrictions and mandates decisions at the incorporation stage.
   2. Legislations lack understanding of the technology.
3. Examples of restrictions:
   1. Identifying public keys of all associated smart contracts.
   2. Smart contracts must be capable of amendment.
   3. Tennessee: Majority of interests required for a valid vote – not possible with low participation
4. Conclusion:
   1. Need to bridge the gap between legislators and field experts

LECTURE ENDS