Lecture 9

—

Decentralised Autonomous Organisations

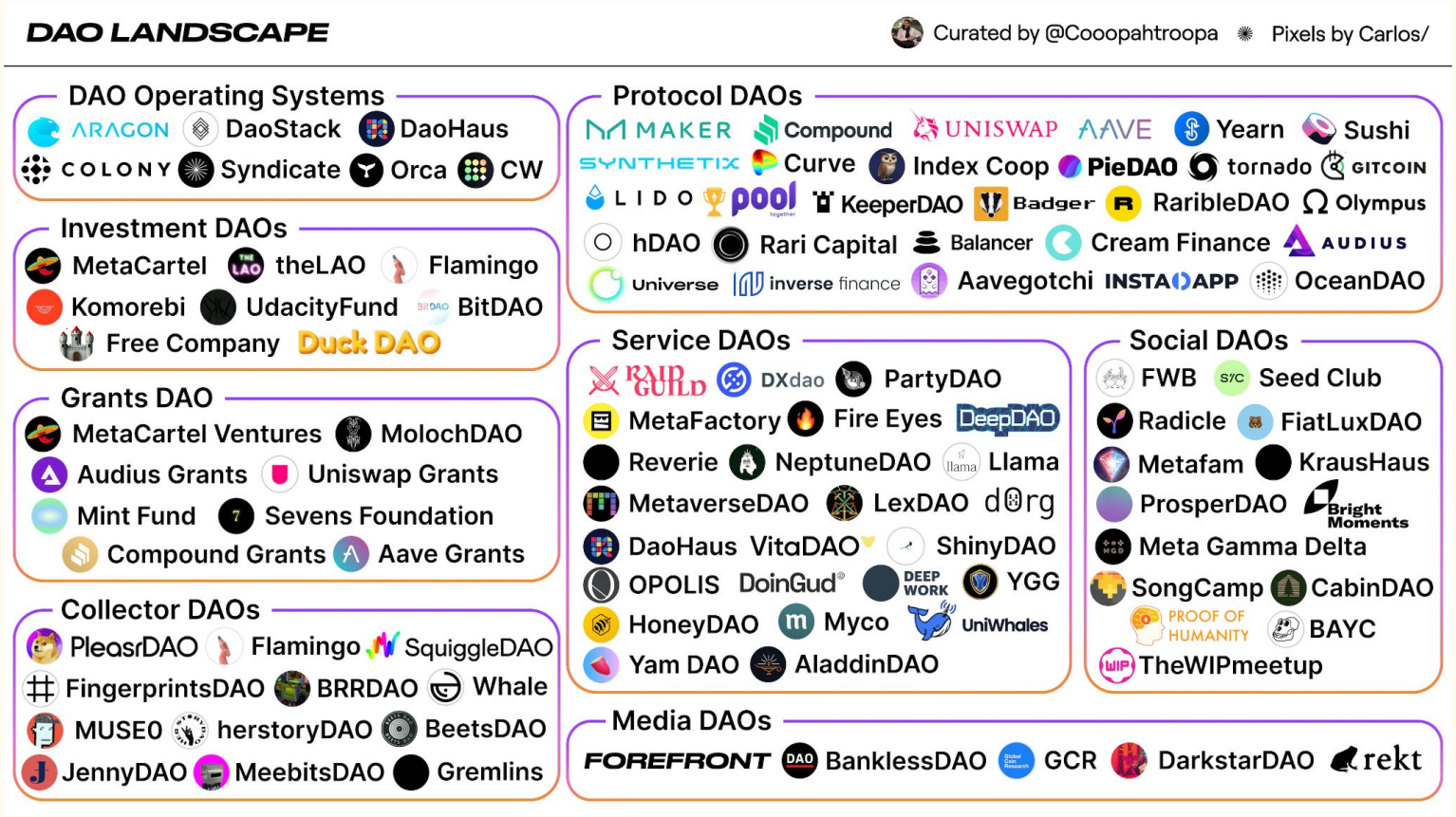
DAO - A definition

Decentralized - Everybody gets to voice their opinion. No hierarchy or authority.

Autonomous - Able to take action and achieve goals without a stamp of approval

Organisation - A community working towards a common goal instead of paid labour

DAO landscape



The two pillars of DAOs

Governance Model

The management of voting and proposal lifecycle management. (Lecture 1 EIP process)

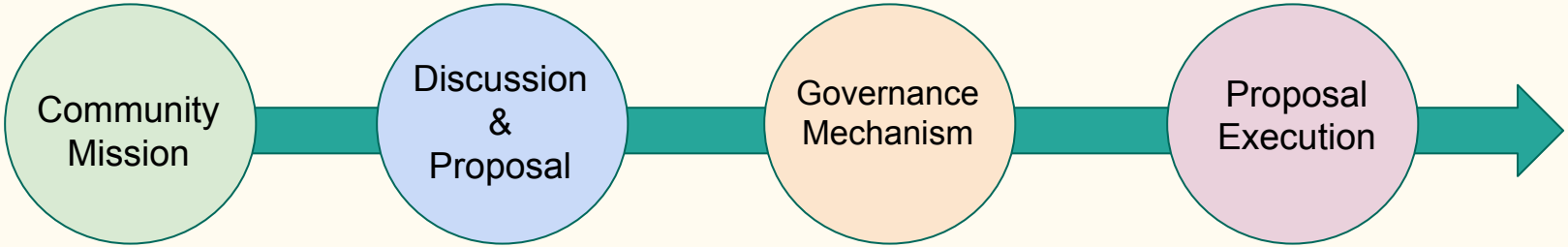
- Tools used to discuss and post proposals.
- Voting mechanisms to ensure fair representation and avoid token manipulation
- Timelocks and execution processes of passed proposals

Treasury Management

Managing funds and tokenomics of the DAO

- Manage asset portfolio and value volatility of the treasury
- Secure smart contract for treasuries
- Native-token tokenomics

DAO lifecycle and tooling



Define the purpose of your DAO and the target audience it serves.
.
Define the success metrics and ROI.

Token distribution and delegation

Have a place where people can freely exchange. A sense of community builds loyalty
.
Forum; Orbit; Community as a Service?

Onchain - history, transparency but gas fees
.
Offchain - fast, no gas, needs a separate onchain execution call

Eligibility, Token Power, Duration

Timelocks

Rage Quit (trade with treasury)

Who has power to execute?

Result feedback?

DAO treasuries

Valuation and Asset Portfolio of DAO treasuries

- Holding one token type - ok if multiple treasuries?
- Governance token separate from native/utility token?
- Perform yield earning activities with treasury?

Secure Storage and Execution

- Who owns the purse strings? A single person, an entity or a smart contract?
- Multisig Wallets
  - A wallet which requires a certain number of addresses to sign before execution.
  - Can be a specific number of signatures or a percentage out of the whole

Regulation - Legal & Fiscal

The US has made an attempt to recognise DAOs

- Wyoming became the first state to recognise DAOs on 1 July 2021. Legal definition here.
- Similar in status to LLC but with a certain % of governance done by Smart Contracts, membership based on token ownership and enforced dissolution if DAO does not pass any proposals in 1 year.
- A number of other US states have created similar legislation.

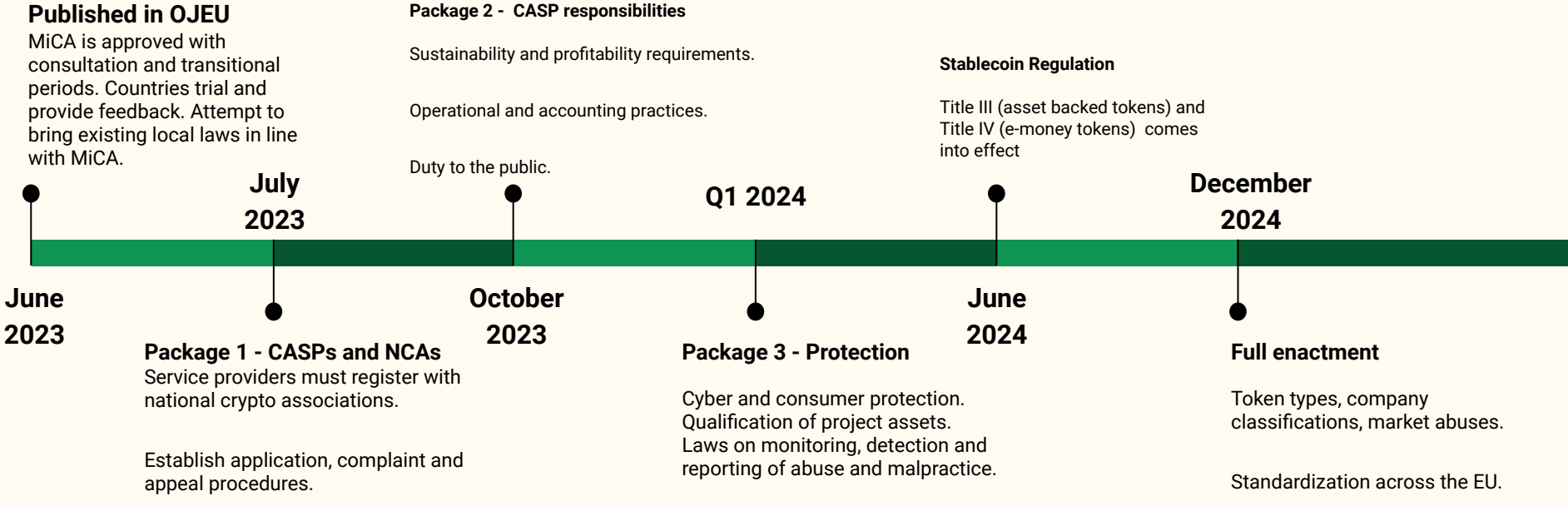
The EU is still undecided and highly fragmented

- Germany - Crypto vested for more than 1 year is tax free!
- France - very complex - categorized by mining, trading and corporate gains. Tax Law.
- Non official status in the EU. Most registered as an "association". Provides basic legal protection for private individuals.
- MakerDAO - are they truly a DAO?
    - Has a stablecoin, do not rely on donations
    - Has a treasury worth $1.2Billion
    - Pays salaries to its core employees
    - Has income statements with revenue and expenses....

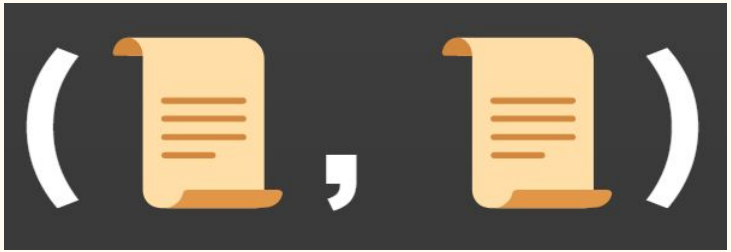

THAT JUST SOUNDS LIKE
A COMPANY WITH EXTRA STEPS

MiCA - Markets in Crypto Assets

Standardizing EU wide regulation on crypto assets and companies. Full text.

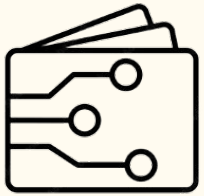


ConstitutionDAO - An example



A DAO that lived for 7 days, existing fo the sole purpose of purchasing an original copy of the US Constitution

Community was solely managed through Discord. The mission was simply: Putting the Constitution in People's hands



Created a Multisig Wallet. 7/13 Signatures required. Community distrust due to anonymity. Signers volunteered identity.

Created the $PEOPLE token. Exchange ETH for $PEOPLE. Voting rights to what to do after Constitution was purchased.

ConstitutionDAO - Result

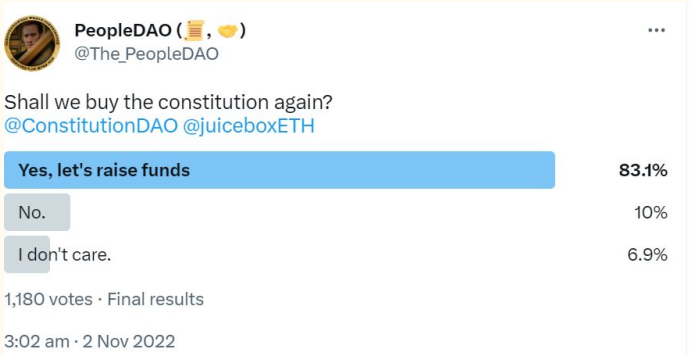
Sotheby's

Raised $47Mil in 7 days. Gained confidence from Sotheby to participate.
Result: Failed to win auction

Full refunds were given on Juicebox at a hard pegged rate of 1ETH : 1Mil PEOPLE.

Varying strategies - get ETH back, hodl PEOPLE tokens for round 2.

In the end, no voting was ever done on the DAO since they failed to purchase the Constitution. However in December 2022… Round 2 starting on Twitter!



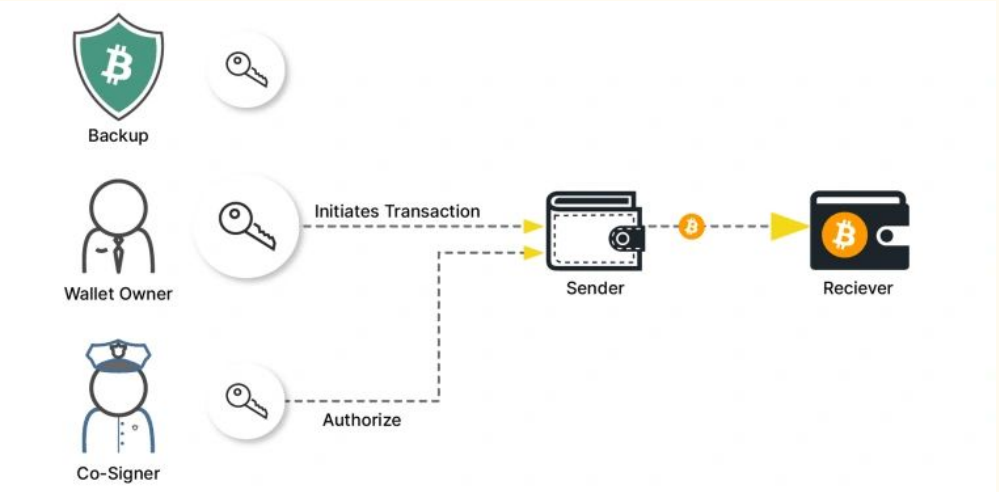
Voting Power

Multisig wallets - signing power

- n-of-m scheme where transactions are executed upon reaching required n.
- Nice code examples: https://solidity-by-example.org/app/multi-sig-wallet/

Do you trust your collaborators?

- Harmony hack - $100M - Server holding private key compromised
- Parity - library self-destructed, contract ownership seized
- Axie DAO - lent their keys out



Token Based Voting

1. Have a token contract
    a. ERC20 - quantity of fungible tokens
    b. ERC721 - NFT holders go on allowlist
    c. ERC5805 - vote and delegation tracking through NFT-like metadata
2. Decide the weight of each token
3. Check the token balance of each account in contract
4. Greatest token weight wins.

Pros

- Voters are financially invested
- Don't need to KYC wallet addresses and prevent sybil attacks

Cons

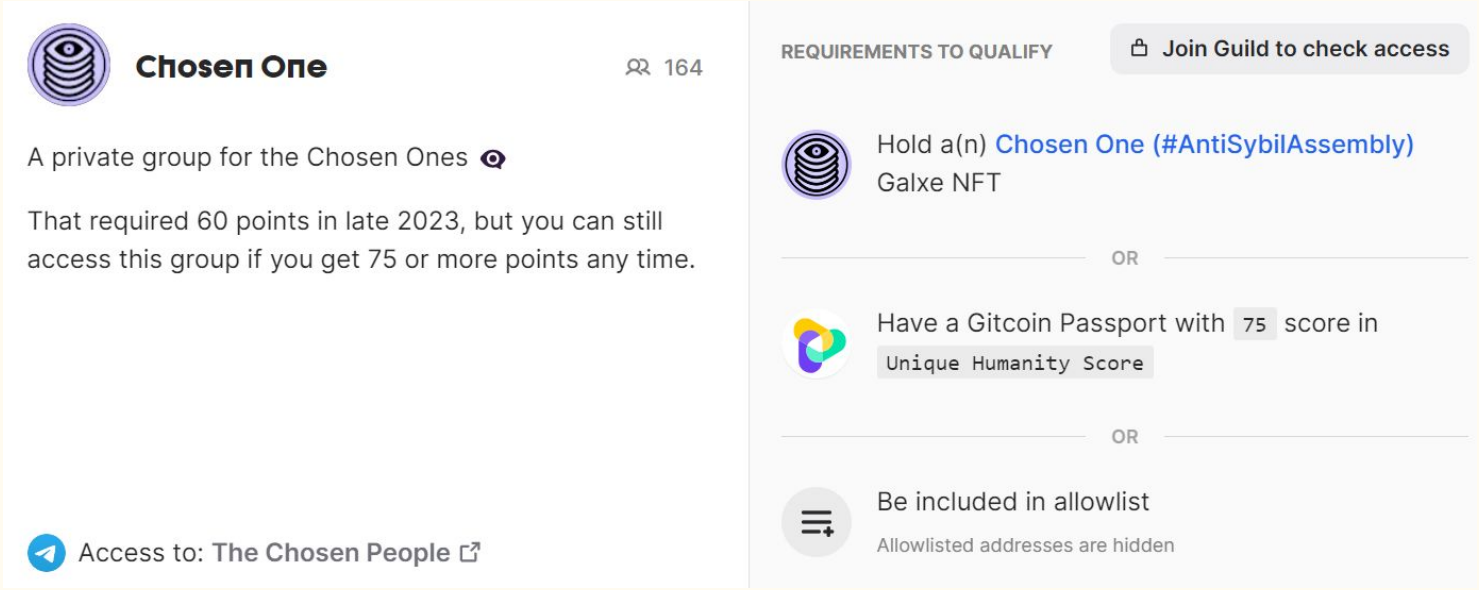
- Flash loan for voting tokens
- Usually whales, ie. investors, hold majority - plutocracy
- Token trading / double counting

Who are the voters?

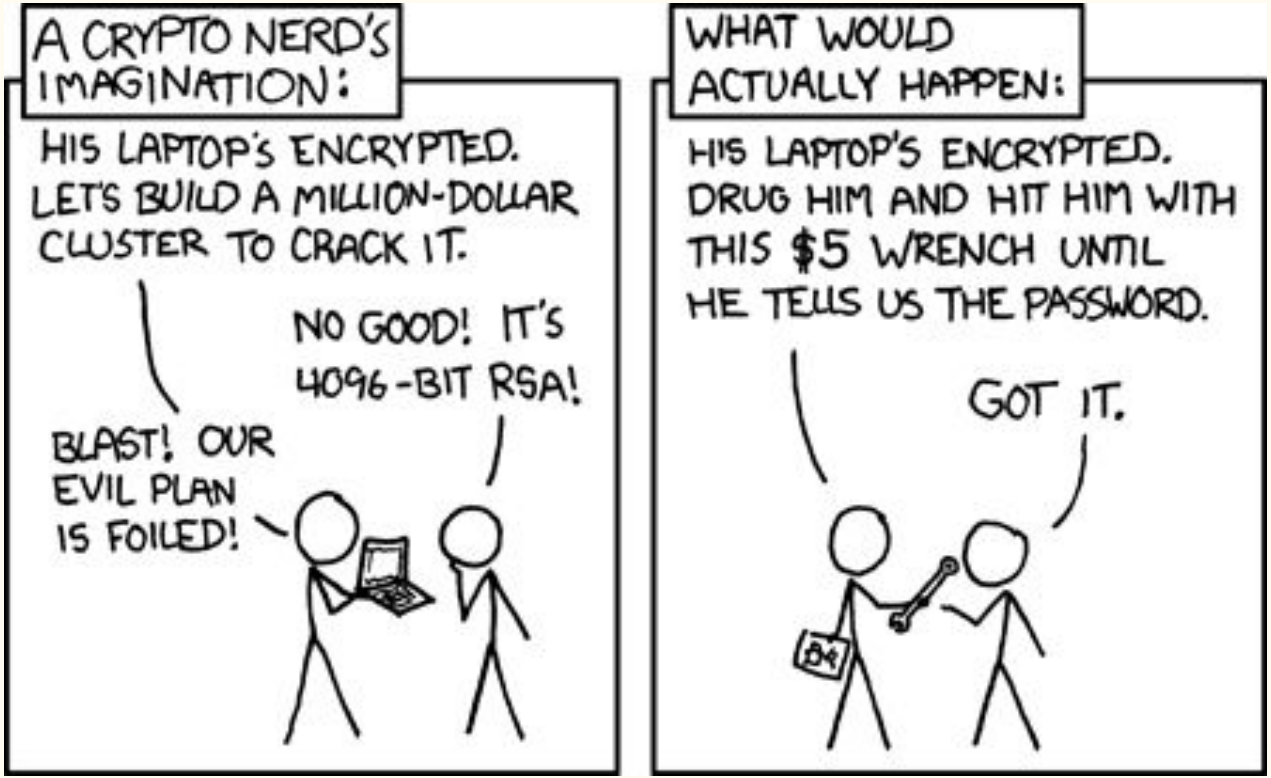
Can identity be associated to wallet addresses? - Social Engineering

Voting history is fully transparent, an identity doxx would be bad.

Currently using allowlist contracts, Token ownerships, but ZK Proofs allow for full masking of identity!



A hacker's POV on hacking wallets



Voting Strategies

Perceived image matters

https://archive.devcon.org/resources/6/2022-statistics-on-makerdao-voter-delegation.pdf

Challenges discourage voting

Name	Number of proposals	Total votes	Members	Average participation rate per proposal
MoonDAO	25	6338	8800	2.88%
Gnosis	40	20510	18200	2.82%
Badger DAO	13	3297	10100	2.51%
Silo	3	251	4500	1.86%
Ribbon	11	1081	5700	1.72%
Gitcoin	29	10187	26600	1.32%
Botto	8	332	3300	1.26%
Aave	64	121354	151200	1.25%
Balancer	91	15583	13700	1.25%
Merit Circle	13	1165	7800	1.15%

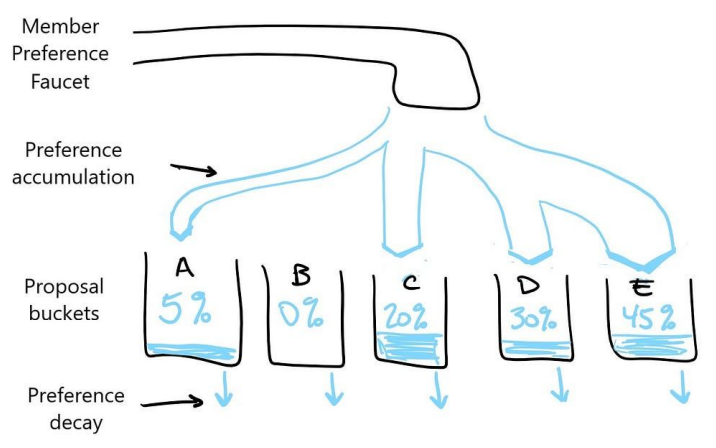
Token (power) delegation

- Mostly investors hold the greatest voting power.
  - Are they delegating to parties with similar beliefs. Is this real power sharing?
  - Delegates have their own incentives and motivations as well. Bribery?
- Investors generally have more financial expertise.
  - Some DAOs lock important decisions for core members only
- Recognized vs Shadow Delegates
  - Delegating to arbitrary players?
- Token Delegation contract / extension
  - Cannot delegate if already voted
  - Who pays gas fees?
  - Prevent further delegation / double voting
  - auto undelegate functionality, lockups

Total delegates	115
Recognized delegates	23
Shadow delegates	92
Total MKR delegated	142,669
Percent of MKR delegated	14.59%
Total Delegators	227

Conviction voting

- Intensity of certainty
- Delegation is still a small percentage of the voting power
- Vote buying and trading
  - Get a flash loan to vote
  - Sell your voting power for important proposals
- Voter sentiment manipulation
  - Write a few "thought leadership" pieces on social media
  - Last minute bait and switch
- Continuous vs Discrete conviction

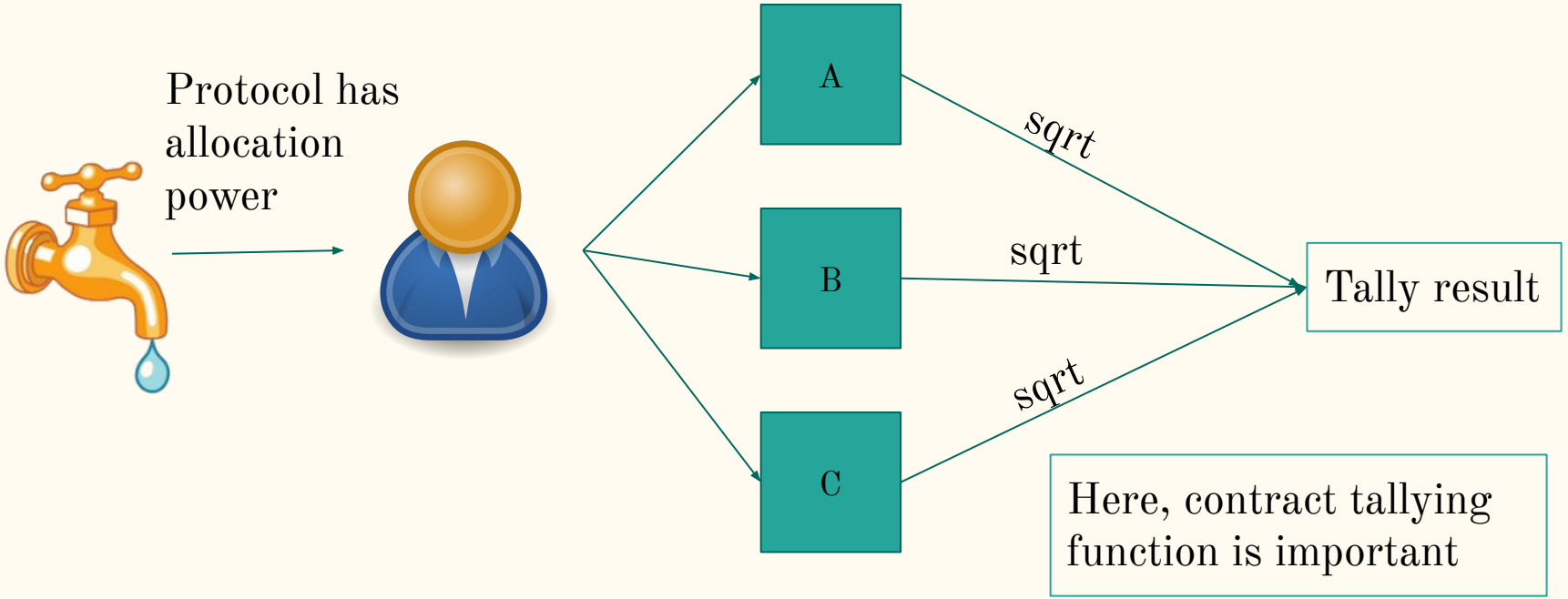


Contract specifics

1. Tokens can maintain delegation
2. Half life decay function
3. Time tracking very important!
   a. Unix time - started 1970
   b. weeks/days/hours/minutes/now

Quadratic Voting

A reflection of the intensity of desire



Proposal Execution

Onchain, Offchain, Hybrid

Proposal execution

Onchain Execution

- Fair, automatic execution after locking period
  - No need to trust an executor or errors in execution
  - Used for high profile changes
- Many token standards and extensions supporting vote counting methods.
- Custom defined quorum mechanism.
- Proposals are queued and time locked for some time after passing and before execution

```
const tx2 = await governanceContract.execute(
    [tokenAddress],
    [0],
    [transferCalldata],
    descriptionHash
);
```

Offchain Execution

Tally votes and an executor executes the action described in the proposal
- Do you trust the executor?
- Did the executor make a mistake?

Hybrid Execution

Proposal voting is onchain but robust discussions and developer meetings offchain in discussion forums.

Rage Quitting

If you do not agree with important proposals? DAO management paying themselves a comfortable salary out of the treasury?

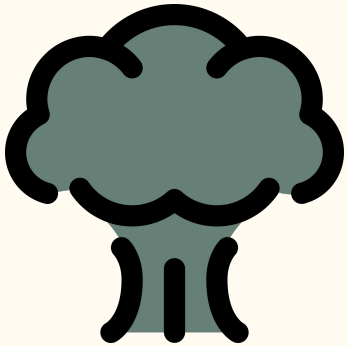
Trade in your governance tokens for a part of the treasury.

Can be manipulated! Deliberately make bad decision, exit before effects take place. Therefore, rage quitting has the following conditions:

- Voted "yes" on active proposal: cannot withdraw until a certain time after implementation.

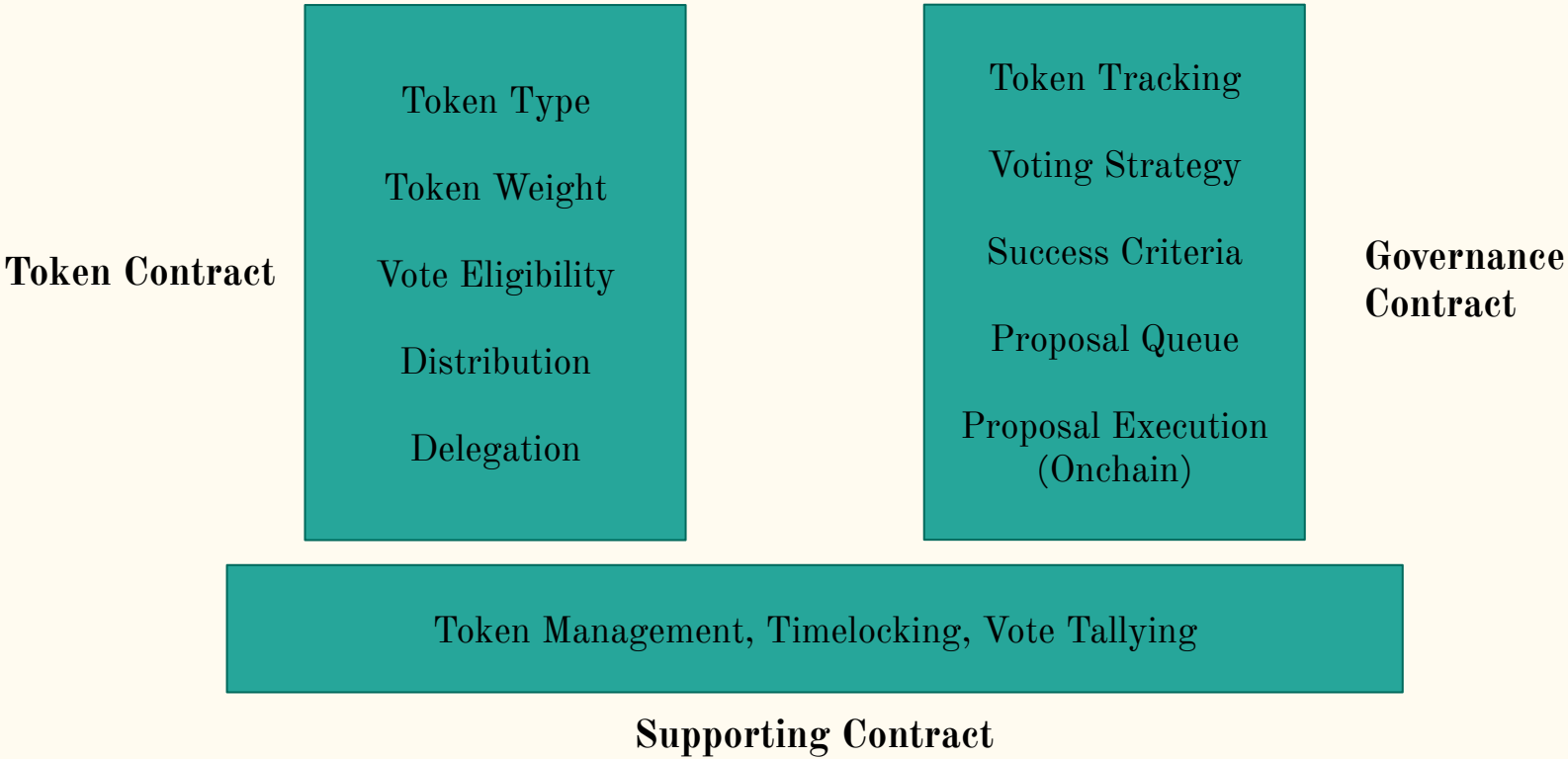
- Voted "no" or "abstain": can withdraw during grace period

Strangely attracts very loyal and passionate members?



Putting it all together

DAO Technical Architecture



Homework 5 - All together now

https://github.com/Dauphine-Digital-Economics/Class-DAO