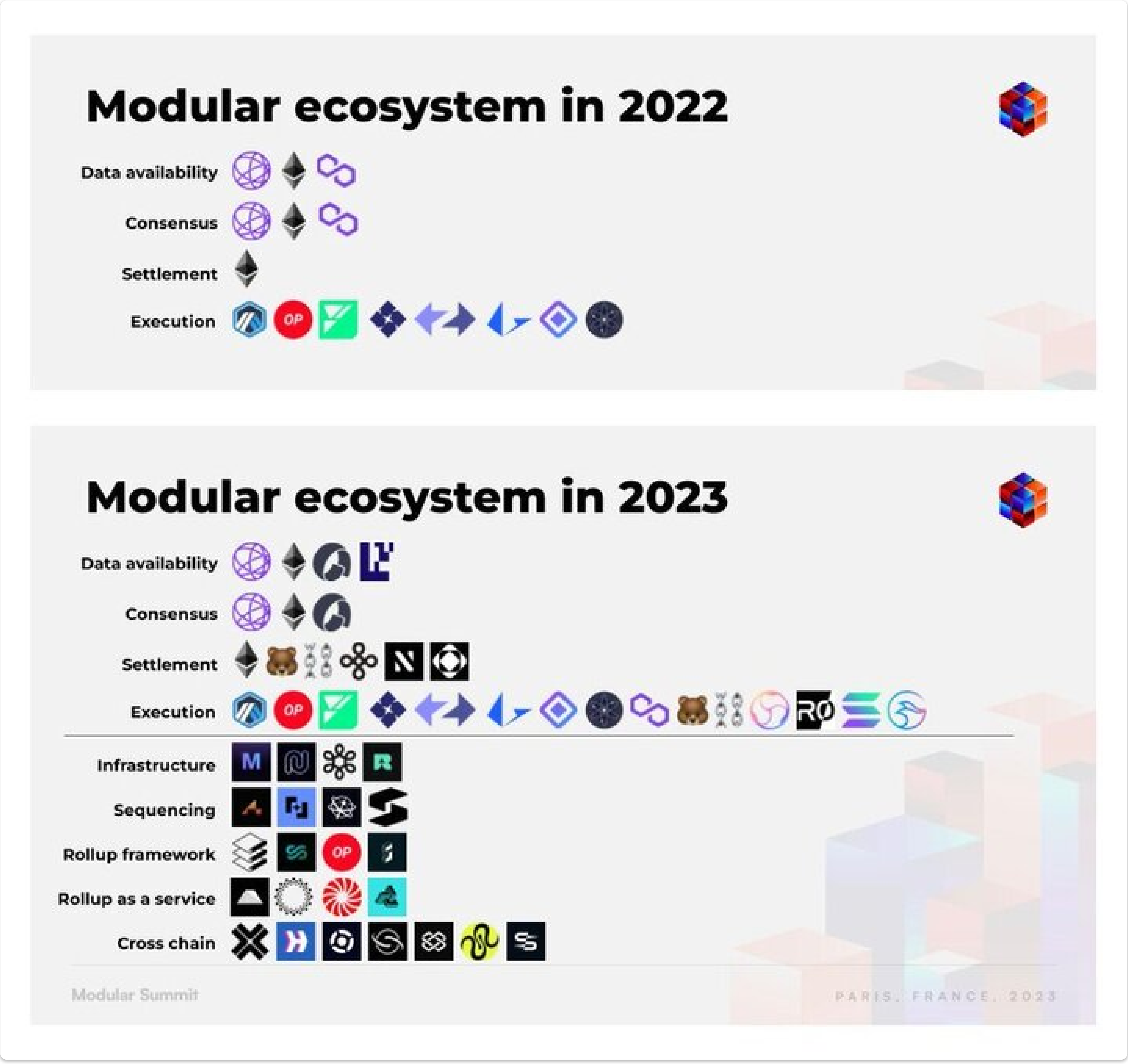
Lesson 16 - Governance etc.

Blockchain modularity update



Modular ecosystem in 2022

Data availability

Consensus

Settlement

Execution

Modular ecosystem in 2023

Data availability

Consensus

Settlement

Execution

Infrastructure

Sequencing

Rollup framework

Rollup as a service

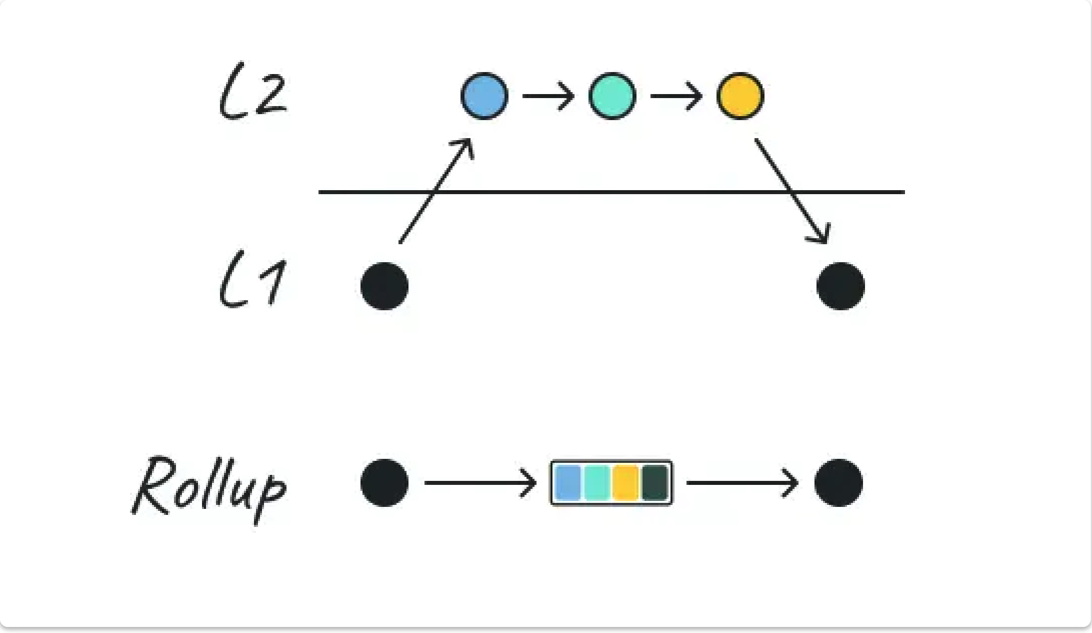
Cross chain

Modular Summit

PARIS, FRANCE, 2023

L2 Connectivity

In addition to ccip mentioned yesterday also see Mangata article



Interacting with Uniswap

Interaction uses the ISwapRouter interface

language-js

```
  struct ExactInputSingleParams {
      address tokenIn;
      address tokenOut;
      uint24 fee;
      address recipient;
      uint256 deadline;
      uint256 amountIn;
      uint256 amountOutMinimum;
      uint160 sqrtPriceLimitX96;
  }
```

The meaning of these fields is

- `tokenIn` The contract address of the inbound token
- `tokenOut` The contract address of the outbound token
- `fee` The fee tier of the pool, used to determine the correct pool contract in which to execute the swap
- `recipient` the destination address of the outbound token
- `deadline`: the unix time after which a swap will fail, to protect against long-pending transactions and wild swings in prices
- `amountOutMinimum`: we are setting to zero, but this is a significant risk in production. For a real deployment, this value should be calculated using our SDK or an onchain price oracle - this helps protect against getting an unusually bad price for a trade due to a front running sandwich or another type of price manipulation
- `sqrtPriceLimitX96`: We set this to zero - which makes this parameter inactive. In production, this value can be used to set the limit for the price the swap will push the pool to, which can help protect against price impact or for setting up logic in a variety of price-relevant mechanisms.

language-js

```
function exactInputSingle(
  struct ISwapRouter.ExactInputSingleParams params
) external returns (uint256 amountOut)
```

Simple Swaps

See Documentation

The `swapExactInputSingle` function is for performing *exact input* swaps, which swap a fixed amount of one token for a maximum possible amount of another token.
This function uses the `ExactInputSingleParams` struct and the `exactInputSingle` function from the ISwapRouter interface.

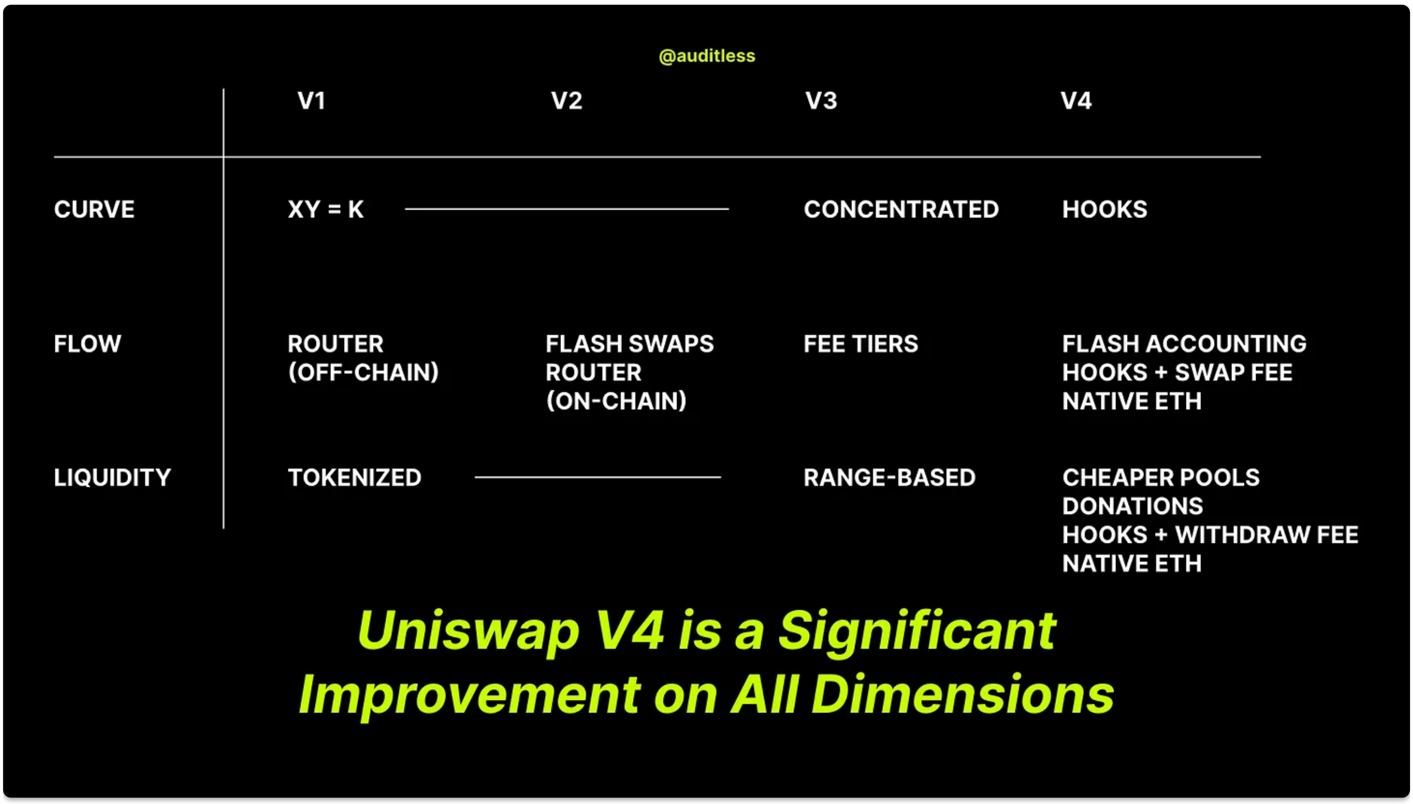
The `swapExactOutputSingle` function is for performing *exact output* swaps, which swap a minimum possible amount of one token for a fixed amount of another token.
This function uses the `ExactOutputSingleParams` struct and the `exactOutputSingle` function from the ISwapRouter]interface.

Fees

Uniswap v3 introduces multiple pools for each token pair, each with a different swapping fee. Liquidity providers may initially create pools at three fee levels: 0.05%, 0.30%, and 1%.

Uniswap V4

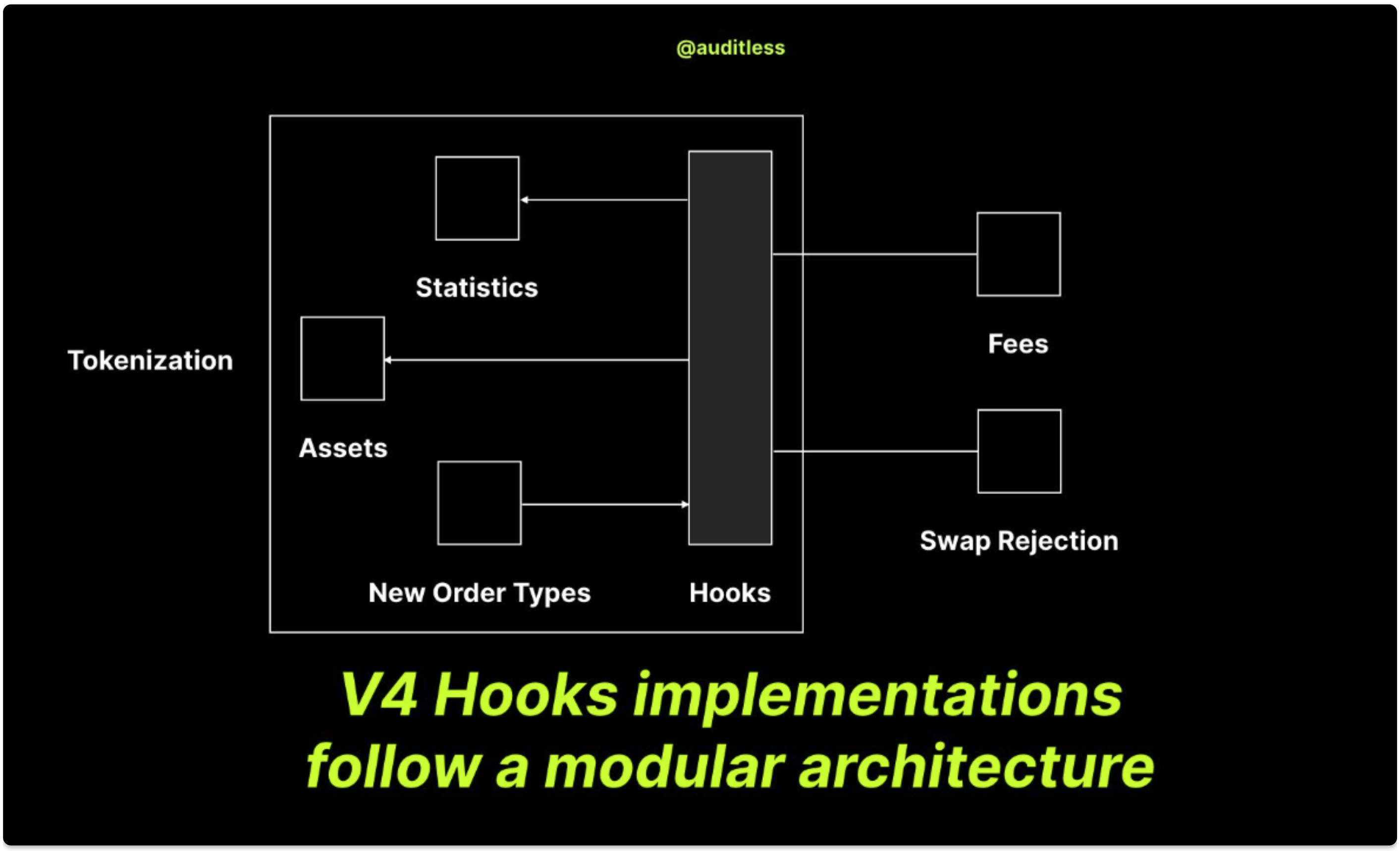
See article from @auditless



@auditless

	V1	V2	V3	V4
CURVE	XY = K		CONCENTRATED	HOOKS
FLOW	ROUTER (OFF-CHAIN)	FLASH SWAPS ROUTER (ON-CHAIN)	FEE TIERS	FLASH ACCOUNTING HOOKS + SWAP FEE NATIVE ETH
LIQUIDITY	TOKENIZED		RANGE-BASED	CHEAPER POOLS DONATIONS HOOKS + WITHDRAW FEE NATIVE ETH

Uniswap V4 is a Significant Improvement on All Dimensions

> Uniswap can now act as an aggregator of AMMs, by using hooks you can design a custom pool, and add the address of that pool via a hooks contract.
> This should lead to reduced development effort to build customised AMMs.
>
> See overview of hooks
>
> From that article
> Hooks mean you
> – Can modify how liquidity is presented to swappers
> – Can allocate idle liquidity elsewhere
> – Can accept custom order types
> – Can run computations in response to user actions
>
> 
>
>
> V4 Hooks implementations follow a modular architecture
>
> Tutorial for creating your own hooks

Governance

"The greatest challenge that new blockchains must solve isn't speed or scaling, it's governance"

- Kai Sedgwick - Why Governance is the Greatest Problem for Blockchains To Solve

We are concerned with how blockchain protocols develop and can adapt to circumstances, rather than how blockchains are used in say administrative settings.

It is useful to think of governance in the following areas

- Consensus
  Who is involved and how do they come to consensus ?
- Information
  How does relevant information reach the participants ?
- Incentives
  How are the incentives aligned to ensure
  > - Correct Behaviour
  > - There is a sufficient level of participation
- Procedures
  In a decentralised system how are
  > - Proposals made
  > - Votes submitted
  > - Consensus reached

On Chain

Explicit on-chain governance is typically touted as having several major advantages.

- First, unlike the highly conservative philosophy espoused by Bitcoin, it can evolve rapidly and accept needed technical improvements.
- Second, by creating an explicit decentralized framework, it avoids the perceived pitfalls of informal governance, which is viewed to either be too

unstable and prone to chain splits, or prone to becoming too de-facto centralized

Off Chain

The mechanism to change the protocol are external to the system

The process is often

- ad hoc
- may be poorly specified
- communication and coordination can be problematic

Developers may have a key role in deciding and implementing changes to the protocol

Bitcoin

Actors :

- Miners
- Developers
- Users (Exchanges / Wallets)

Governance mainly off chain through improvement proposals
A high degree of coordination is needed, done via mailing lists

Results of the nature of Bitcoin Governance :
“This results in a self-reinforcing cycle of more power becoming concentrated in a small group of early core developers, slower technological advancement, and conservatism. Developers are at risk of being bribed since they have a lot of power but weak economic incentives. “

“Similarly, asymmetries in ability to coordinate give miners disproportionate power. Communication amongst miners is easier because they are a small and concentrated group. Since mining is a business with economies of scale, we’d expect a continued trend towards natural monopoly in mining and even greater coordination advantage. “

From : article**

Bitcoin Cash hash wars in late 2018.

“Jihan (Bitmain’s CEO) does have a lot of control for now, and much of that is simply due to mining centralization. As Bitmain is so vertically integrated, from selling ASICs, to operating mining farms, to running mining pools, he can prevent network upgrade and attempt to hijack the Bitcoin brand with things like Bitcoin Cash”

- Samson Mow (CSO of Blockstream - http://fortune.com/2017/08/25/bitcoin-mining/)

Ethereum

- Similar to Bitcoin
- Ethereum founder Vitalik Buterin seen as a “benevolent dictator”
- Some on chain governance over system parameters, e.g. Miners can vote on gas price.
  See article

Tezos

‘Self Amending Ledger’

- Proof of Stake Consensus
- Governance Process
- Code updates are open to anyone
- On chain vote pushes change to test network
- Confirming vote pushes change to the live network
- Contributions are rewarded with tokens
- Power moves away from miners and developers
- Allows delegated democracy

paper 1
abstract

Tezos white paper

- A blockchain protocol can be decomposed into three distinct protocols:
- The network protocol discovers blocks and broadcasts transactions.
- The transaction protocol specifies what makes a transaction valid.
- The consensus protocol forms consensus around a unique chain.

- Tezos implements a generic network shell. This shell is agnostic to the transaction protocol and to the consensus protocol.
- There is the ability to replace the current protocol by one on the test network
- Amendments are adopted over election cycles lasting 131 072 blocks each. Given the a one minute block interval, this is about three calendar months.
- The election cycle is itself divided in four quarters of 32 768 blocks.

**

Terzos implemented their first on chain governance in May 2019

There was a series of stages

Proposal Stage (gas limit)

```
  Athens A: 71% (102 bakers)


Athens B: 29% (68 bakers)
```

Exploration Period

Yay/Nay/Pass vote:

```
  Yay: 57.86% (178 bakers)


Nay: .02% (3 bakers)


Pass: 42.12% (13 bakers)
```

Testing Period

Promotion period

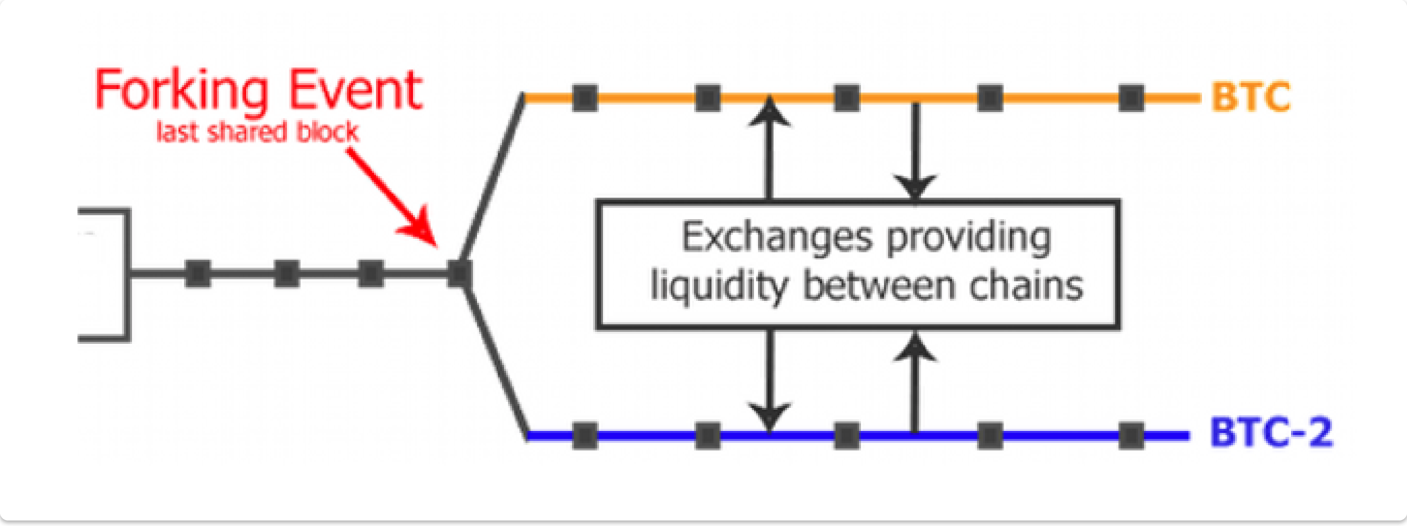
```
  Yay: 64.94% (200 bakers)


Nay: .07% (3 bakers)


Pass: 34.98% (12 bakers)
```

When all else fails : Exit Strategies

- Hard and Soft Forks
- Software Forks



See https://fork.lol/

Governance Tokens

Governance is non trivial , as seen on Ethereum and Bitcoin
Various attempts at governance have been tried with on chain / off chain or hybrid models

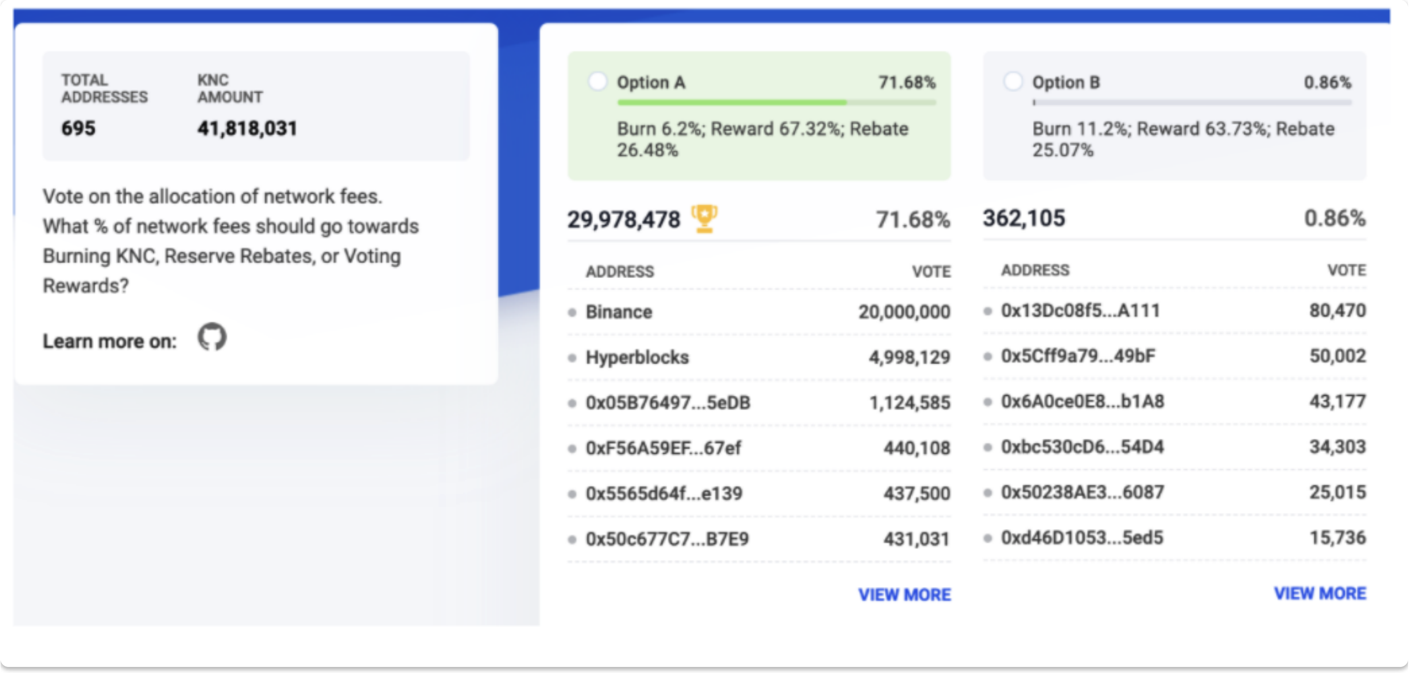
Incentives are (needed) given for participants in the governance process

Many DeFi projects issue governance tokens, though with a different purpose.

DeFi Governance Tokens

Holding the token gives the holder the right to vote on aspects of the protocol, typically economic settings, inclusion of assets

The tokens may have a yield



TOTAL ADDRESSES	KNC AMOUNT
695	41,818,031

Vote on the allocation of network fees. What % of network fees should go towards Burning KNC, Reserve Rebates, or Voting Rewards?

Learn more on:

○ Option A 71.68%

Burn 6.2%; Reward 67.32%; Rebate 26.48%

29,978,478 🏆 71.68%

ADDRESS	VOTE
Binance	20,000,000
Hyperblocks	4,998,129
0x05B76497...5eDB	1,124,585
0xF56A59EF...67ef	440,108
0x5565d64f...e139	437,500
0x50c677C7...B7E9	431,031

VIEW MORE

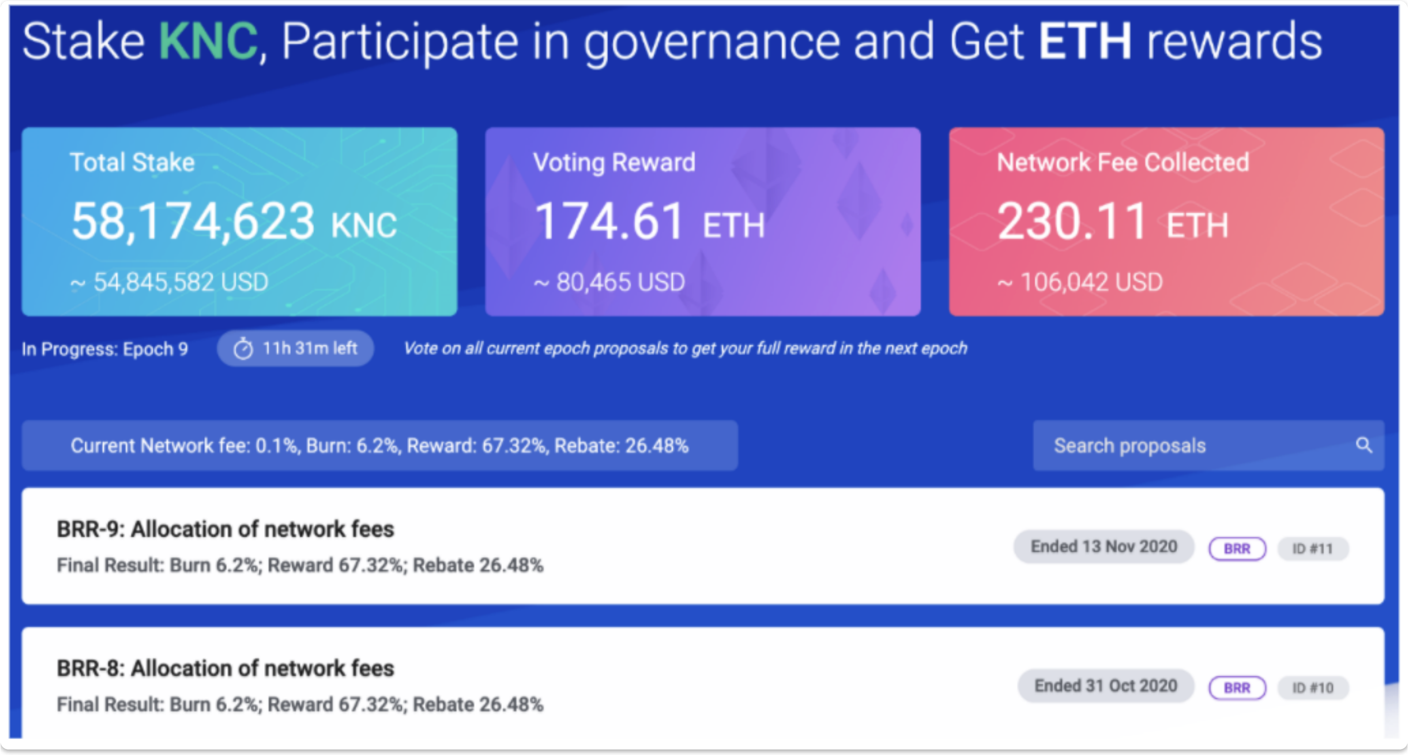
○ Option B 0.86%

Burn 11.2%; Reward 63.73%; Rebate 25.07%

362,105 0.86%

ADDRESS	VOTE
0x13Dc08f5...A111	80,470
0x5Cff9a79...49bF	50,002
0x6A0ce0E8...b1A8	43,177
0xbc530cD6...54D4	34,303
0x50238AE3...6087	25,015
0xd46D1053...5ed5	15,736

VIEW MORE



Stake KNC, Participate in governance and Get ETH rewards

Total Stake	Voting Reward	Network Fee Collected
58,174,623 KNC	174.61 ETH	230.11 ETH
~ 54,845,582 USD	~ 80,465 USD	~ 106,042 USD

In Progress: Epoch 9 11h 31m left *Vote on all current epoch proposals to get your full reward in the next epoch*

Current Network fee: 0.1%, Burn: 6.2%, Reward: 67.32%, Rebate: 26.48%

Search proposals

BRR-9: Allocation of network fees
Final Result: Burn 6.2%; Reward 67.32%; Rebate 26.48%
Ended 13 Nov 2020 BRR ID #11

BRR-8: Allocation of network fees
Final Result: Burn 6.2%; Reward 67.32%; Rebate 26.48%
Ended 31 Oct 2020 BRR ID #10

DeFi and Governance

See article

Compound developers turned over the operation and ownership of the network to the community.
The Compound Governance DAO gave the community members control of the protocol's reserve assets that are generated via fees from borrowers. These cash flows were at the time the highest revenues ever generated by an on-chain protocol.

Their mechanism is now

"Screenshot 2022-03-22 at 16.40.50.png" is not created yet. Click to create.

The Compound protocol is governed and upgraded by COMP token-holders, using three distinct components; the COMP token, governance module (Governor Bravo), and Timelock. Together, these contracts allow the community to propose, vote, and implement changes through the administrative functions of a cToken or the Comptroller. Proposals can modify system parameters, support new markets, or add entirely new functionality to the protocol.

COMP token-holders can delegate their voting rights to themselves, or an address of their choice. Addresses delegated at least 65,000 COMP can create governance proposals; any address can lock 100 COMP to create an Autonomous Proposal, which becomes a governance proposal after being delegated 65,000 COMP.

When a governance proposal is created, it enters a 2 day review period, after which voting weights are recorded and voting begins. Voting lasts for 3 days; if a majority, and at least 400,000 votes are cast for the proposal, it is queued in the Timelock, and can be implemented 2 days later. In total, any change to the protocol takes at least one week.

Governance token Value

Protocols may try to claim to their token has no value

Yield Finance
“In further efforts to give up this protocol (mostly because we are lazy and don’t want to do it), we have released YFI, a completely valueless 0 supply token. We re-iterate, it has 0 financial value. There is no pre-mine, there is no sale, no you cannot buy it, no, it won’t be on Uniswap, no, there won’t be an auction. We don’t have any of it.”

Within a week it was worth $3000 and was giving returns of 35,000%

YFI demonstrated that the promise of governance alone could bootstrap network adoption. The fair-launch model, and its use of initial token distribution to target the ideal future users, has since become prevalent.

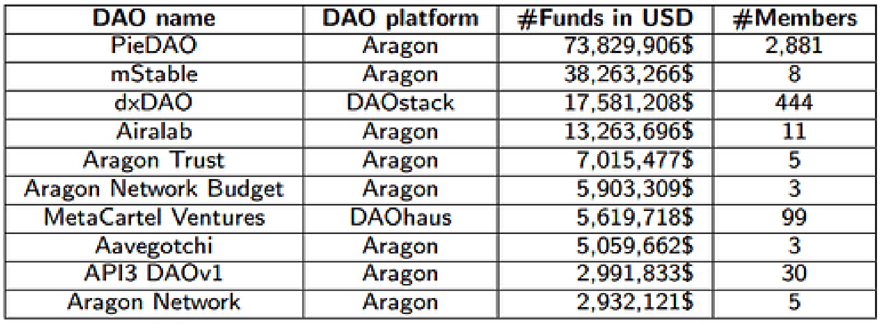
NFT DAOs

Some DAOs use their DAO governance token to manage their treasury, perform asset sales (including proceeds from fractionalization), and for asset curation. DAO tokenholders have the right to vote on these issues and in many cases, the outcomes of these votes are directly executed on-chain algorithmically using DeFi protocols such as Fractional or Uniswap.

Gaming DAOs

Unlike in traditional gamer guilds play-to-earn mechanics found within games like Axie Infinity can encourage cooperative strategies and revenue sharing amongst participants. These mechanics make them more like DeFi DAOs — participation in the network earns rewards while also boosting the network's prospects — but to this point the governance of the networks are less tied to pure financial metrics and more tied to game performance and social metrics.

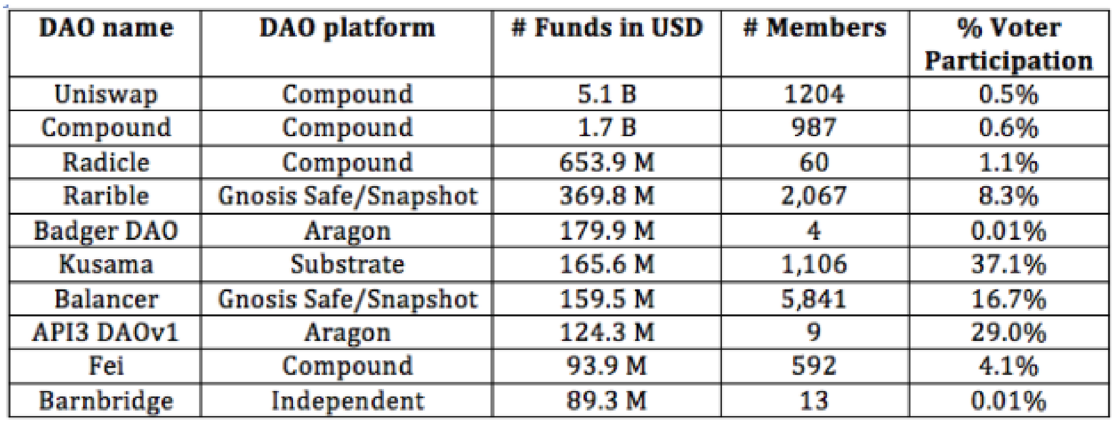
See also survey of DAOs



DAO name	DAO platform	#Funds in USD	#Members
PieDAO	Aragon	73,829,906$	2,881
mStable	Aragon	38,263,266$	8
dxDAO	DAOstack	17,581,208$	444
Airalab	Aragon	13,263,696$	11
Aragon Trust	Aragon	7,015,477$	5
Aragon Network Budget	Aragon	5,903,309$	3
MetaCartel Ventures	DAOhaus	5,619,718$	99
Aavegotchi	Aragon	5,059,662$	3
API3 DAOv1	Aragon	2,991,833$	30
Aragon Network	Aragon	2,932,121$	5

Table 5: Top 10 DAOs by a total of cryptocurrencies in USD, as of 1st December2020.

(Faqir-Rhazoui Y., et al., 2021)



DAO name	DAO platform	# Funds in USD	# Members	% Voter Participation
Uniswap	Compound	5.1 B	1204	0.5%
Compound	Compound	1.7 B	987	0.6%
Radicle	Compound	653.9 M	60	1.1%
Rarible	Gnosis Safe/Snapshot	369.8 M	2,067	8.3%
Badger DAO	Aragon	179.9 M	4	0.01%
Kusama	Substrate	165.6 M	1,106	37.1%
Balancer	Gnosis Safe/Snapshot	159.5 M	5,841	16.7%
API3 DAOv1	Aragon	124.3 M	9	29.0%
Fei	Compound	93.9 M	592	4.1%
Barnbridge	Independent	89.3 M	13	0.01%

(Retrieved August 2021)

Open Zeppelin Governance Contracts

Meta governance

See article.
It is commonly defined as holding one DAO's token in order to influence decisions in another DAO(s). The benefits of metagovernance are clear - DAO2DAO relationships are positive-sum incentive-alignment mechanisms that

> amplify the voices of individuals.
> According to the article there has been a change over time
>
> 1. Token holders believing they can participate in all governance decisions
> 2. Token holders realizing they can’t participate in all governance decisions
> 3. Token holders delegating to individuals with perceived specialized expertise and bandwidth
> 4. Token holders and individual delegates realizing delegate models have been constructed ineffectively
>
> While the trend of governance delegation to individuals had all the best of intentions, it is clear that it has fallen short of expectations. The combination of the time-commitment and depth required for participation, misaligned incentives and accountability mechanisms, and legal complexity has made it impossible for governance delegation to fulfill its promise.
>
> Because of this underperformance, it is clear that the rising prevalence of metagovernance committees is the next logical experiment to drive meaningful progress within DAOs.
> Metagovernance committees are better positioned to create aligned incentives with stakeholders and have structures suited to provide scaled governance impact.

Optimistic Governance

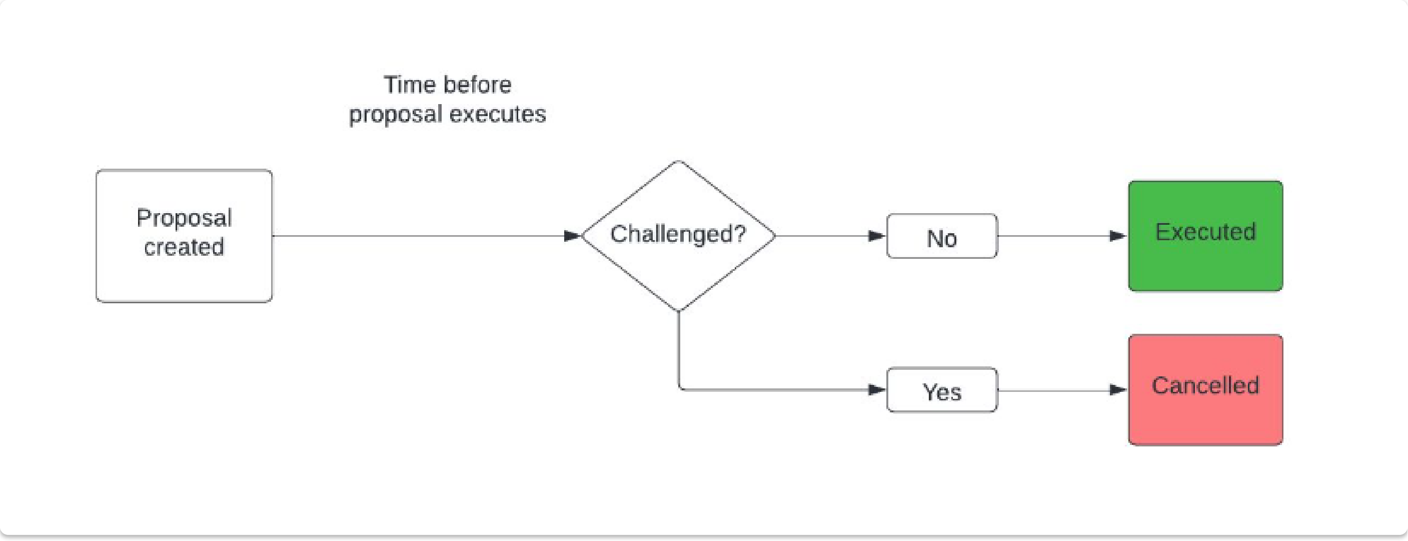
Based on a talk from Tom Waite from Fei / Tribe DAO

Models of Governance in DeFi

- Direct Democracy - token holders vote in a DAO
- Delegated Democracy - others vote on your behalf
- Multisig Governance - High context individuals make the decisions
- Optimistic Governance - Assent is assumed, but the community can veto

With Direct Democracy there is a trade off between building consensus and deadlines for a decision.

Optimistic Governance



Tribe DAO

See docs

There are 4 layers

1. Tribe DAO

- The highest level entity and has ultimate control over managing the protocol.

2. Optimistic governance pods

- These are working groups of community members and protocol experts sitting on a Gnosis safe connected to a timelock. They are able to optimistically govern specific parts of the protocol.

- Specifically, there is a top level Tribal Council pod that oversees other pods and is able to run the protocol on an operational day to day basis. Other pods will be created in the future to manage different aspects of the protocol

3. Nope DAO

- A sub-DAO with a low quorum that is specifically able to veto governance pod proposals.

4. Guardian

- An emergency multisig operated by the Core teams which can take limited safety and security actions in the event of a protocol emergency.

Tribe DAO

The Tribe DAO has ultimate control over the Tribe ecosystem. It has the highest level access control roles, including:

- Arbitrarily moving PCV
- Minting FEI
- Creating and granting new access roles

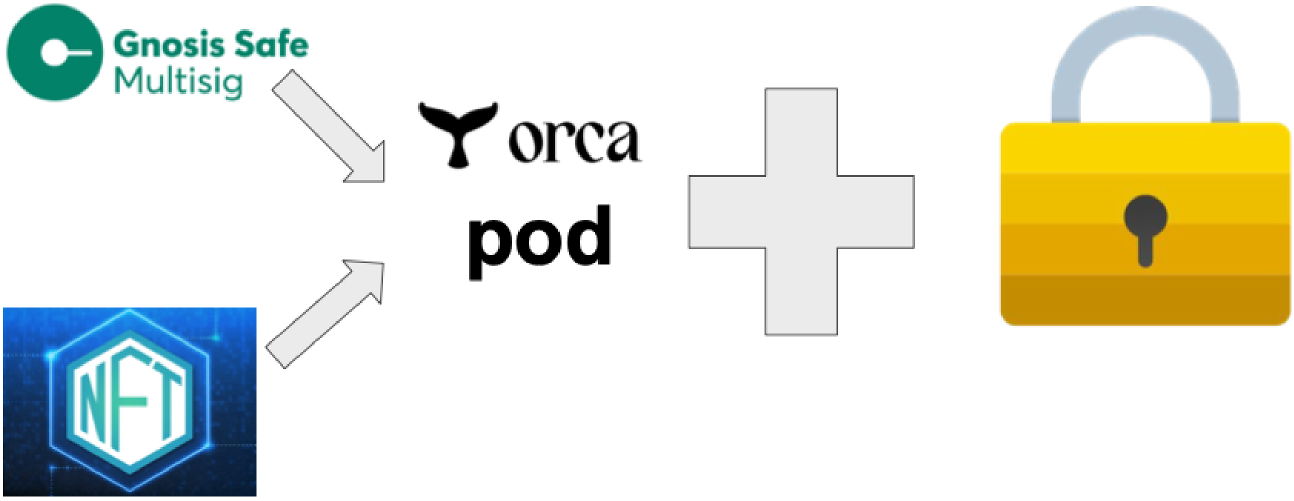
The Tribe DAO is controlled by Tribe token holders and in order to perform an action it requires a proposal to be created and passed. The proposal threshold is 2.5M TRIBE, with quorum being 25M TRIBE.

- Voting period: 2 days
- Timelock period: 1 day

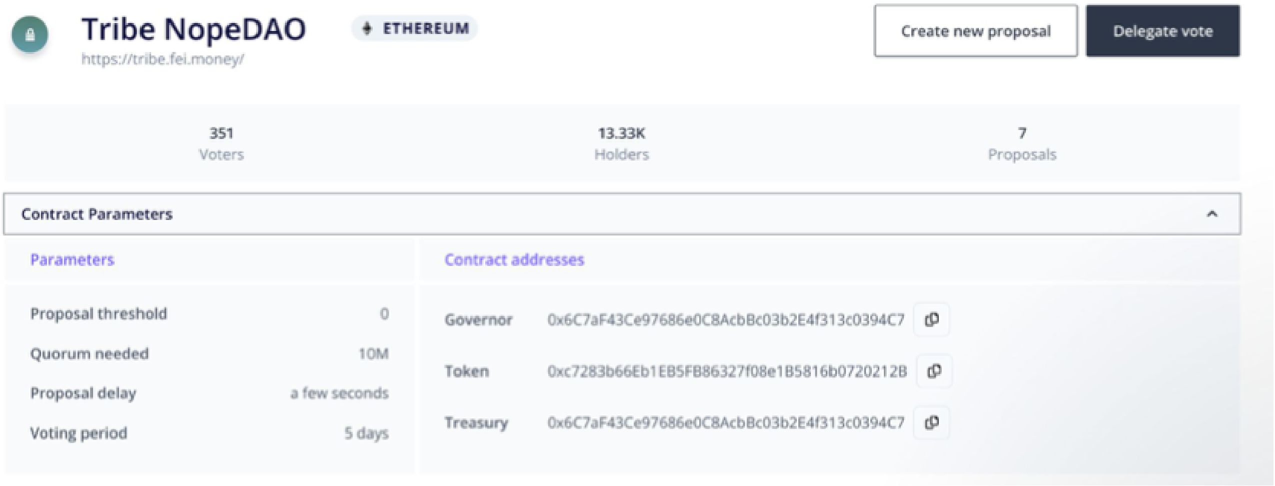
Optimistic Governance Pods

The governance pods are the core of the optimistic governance process within the Tribe ecosystem. They are the primary way in which the protocol is managed on an operational, day to day basis. Most proposals do not require a full expensive DAO vote, and instead they can be approved in an optimistic fashion via a pod.

Optimistic pods: Built as an Orca pod (Gnosis safe with an NFT membership wrapper) + timelock



Veto: Built as a sub DAO, whose only role is the veto


Tribe NopeDAO

https://tribe.fei.money/

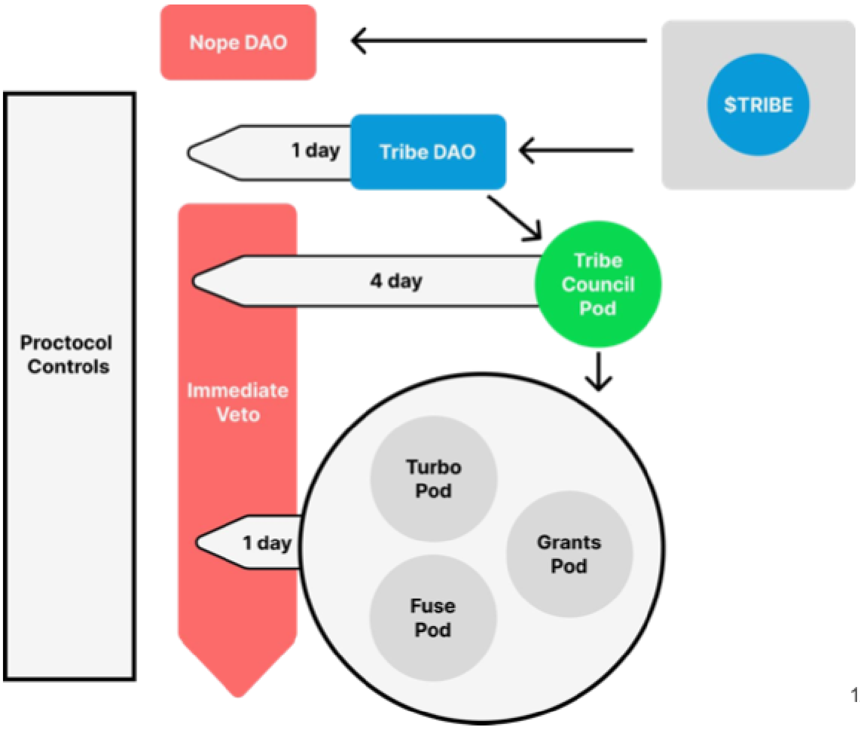
351	13.33K	7
Voters	Holders	Proposals

Contract Parameters

Parameters	
Proposal threshold	0
Quorum needed	10M
Proposal delay	a few seconds
Voting period	5 days

Contract addresses	
Governor	0x6C7aF43Ce97686e0C8AcbBc03b2E4f313c0394C7
Token	0xc7283b66Eb1EB5FB86327f08e1B5816b0720212B
Treasury	0x6C7aF43Ce97686e0C8AcbBc03b2E4f313c0394C7

Putting it together...

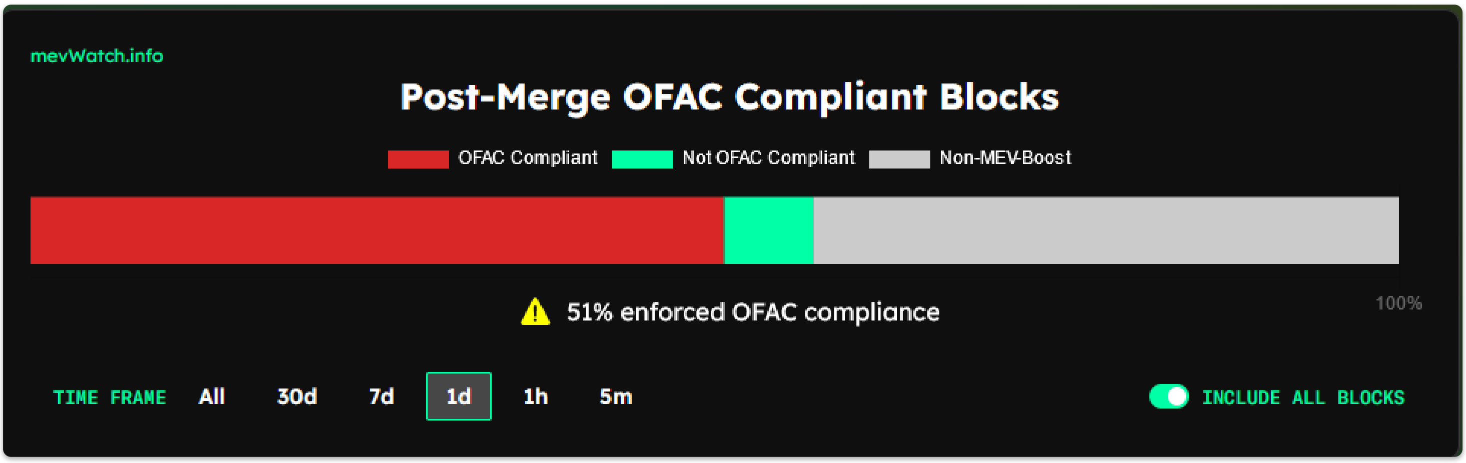


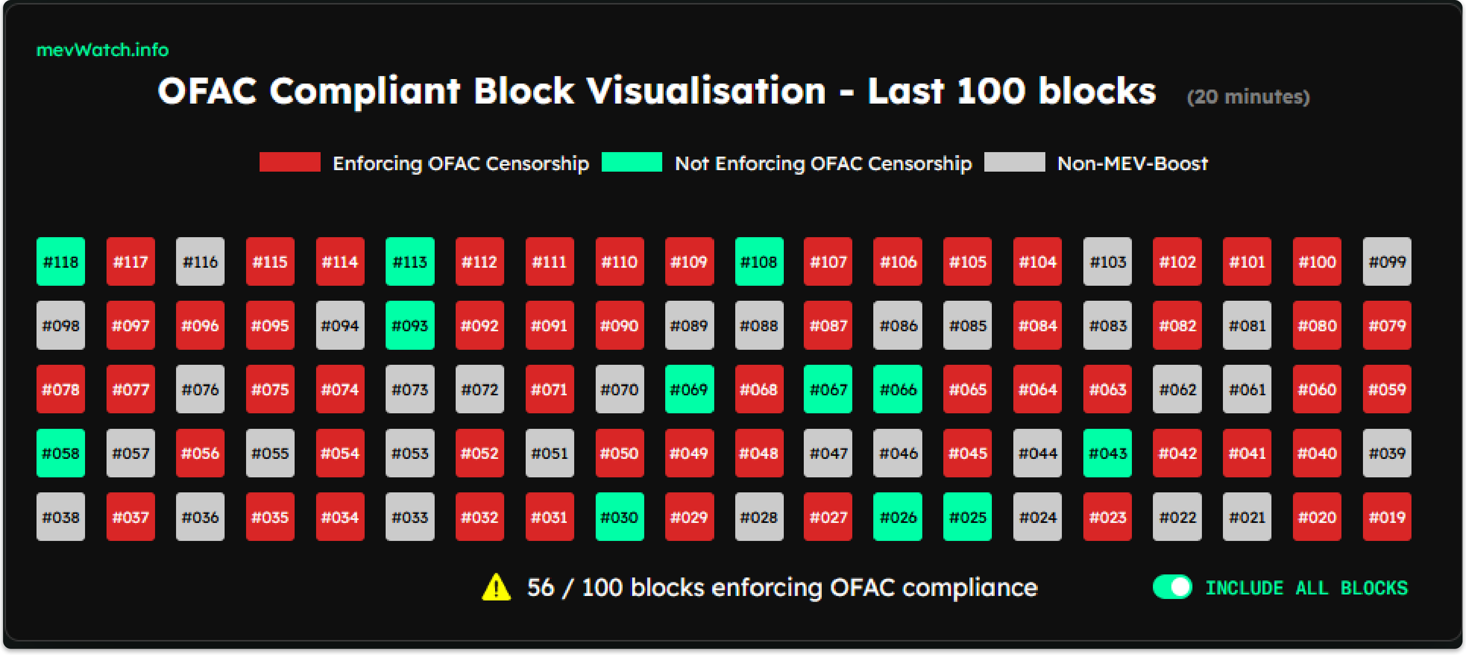
OFAC / Censorship / Tornado Cash

August 2022
Tornado cash (custodial mixing software), their website URLs and some Ethereum contract addresses were put on the OFAC sanctions list, if you send funds to those addresses you may be in violation of sanction laws.

Github removes the repo
Front ends start to implement wallet screening to prevent access to those contracts.
Later we see that flashbots were also censoring transactions.
Mining pools such as Ethermine start to reject transactions going to Tornado Cash

Post Merge we have single companies in regulated jurisdictions producing many blocks.
In an epoch of 32 blocks, typically
Coinbase makes 6
Binance makes 1
Kraken makes 3





mevWatch.info

OFAC Compliant Block Visualisation - Last 100 blocks (20 minutes)

🟥 Enforcing OFAC Censorship 🟩 Not Enforcing OFAC Censorship ⬜ Non-MEV-Boost

🟩 #118	🟥 #117	⬜ #116	🟥 #115	🟥 #114	🟩 #113	🟥 #112	🟥 #111	🟥 #110	🟥 #109	🟩 #108	🟥 #107	🟥 #106	🟥 #105	🟥 #104	⬜ #103	🟥 #102	🟥 #101	🟥 #100	⬜ #099
⬜ #098	🟥 #097	🟥 #096	🟥 #095	⬜ #094	🟩 #093	🟥 #092	🟥 #091	🟥 #090	⬜ #089	⬜ #088	🟥 #087	⬜ #086	⬜ #085	🟥 #084	⬜ #083	🟥 #082	⬜ #081	🟥 #080	🟥 #079
🟥 #078	🟥 #077	⬜ #076	🟥 #075	🟥 #074	⬜ #073	⬜ #072	🟥 #071	⬜ #070	🟩 #069	🟥 #068	🟩 #067	🟩 #066	🟥 #065	🟥 #064	🟥 #063	⬜ #062	⬜ #061	🟥 #060	🟥 #059
🟩 #058	⬜ #057	🟥 #056	⬜ #055	🟥 #054	⬜ #053	🟥 #052	⬜ #051	🟥 #050	🟥 #049	🟥 #048	⬜ #047	⬜ #046	🟥 #045	⬜ #044	🟩 #043	🟥 #042	🟥 #041	🟥 #040	⬜ #039
⬜ #038	🟥 #037	⬜ #036	🟥 #035	🟥 #034	⬜ #033	🟥 #032	🟥 #031	🟩 #030	🟥 #029	⬜ #028	🟥 #027	🟩 #026	🟩 #025	⬜ #024	🟥 #023	⬜ #022	⬜ #021	🟥 #020	🟥 #019

⚠ 56 / 100 blocks enforcing OFAC compliance

INCLUDE ALL BLOCKS

There are currently seven major mev-boost relays including Flashbots, BloXroute Max Profit, BloXroute Ethical, BloXroute Regulated, BlockNative, Manifold and Eden. Of the 7 available major relays only 3 do not censor according to OFAC compliance requirements.

Note that MEV boost exists to allow any validator to get the benefits of flashbots, the motivation is that this would prevent a validator whose is good at extracting MEV from attracting large number of delegations. This is preserving validator level decentralisation.

In PoS we have a mechanism whereby we can target validators individually if we think they are for example censoring transactions. This would involve the community initiating a user activated soft fork to slash that validators funds.

There was a poll of how to react
Options :
X) Consider the censorship an attack on Ethereum and burn their stake via social consensus
Y) Tolerate the censorship

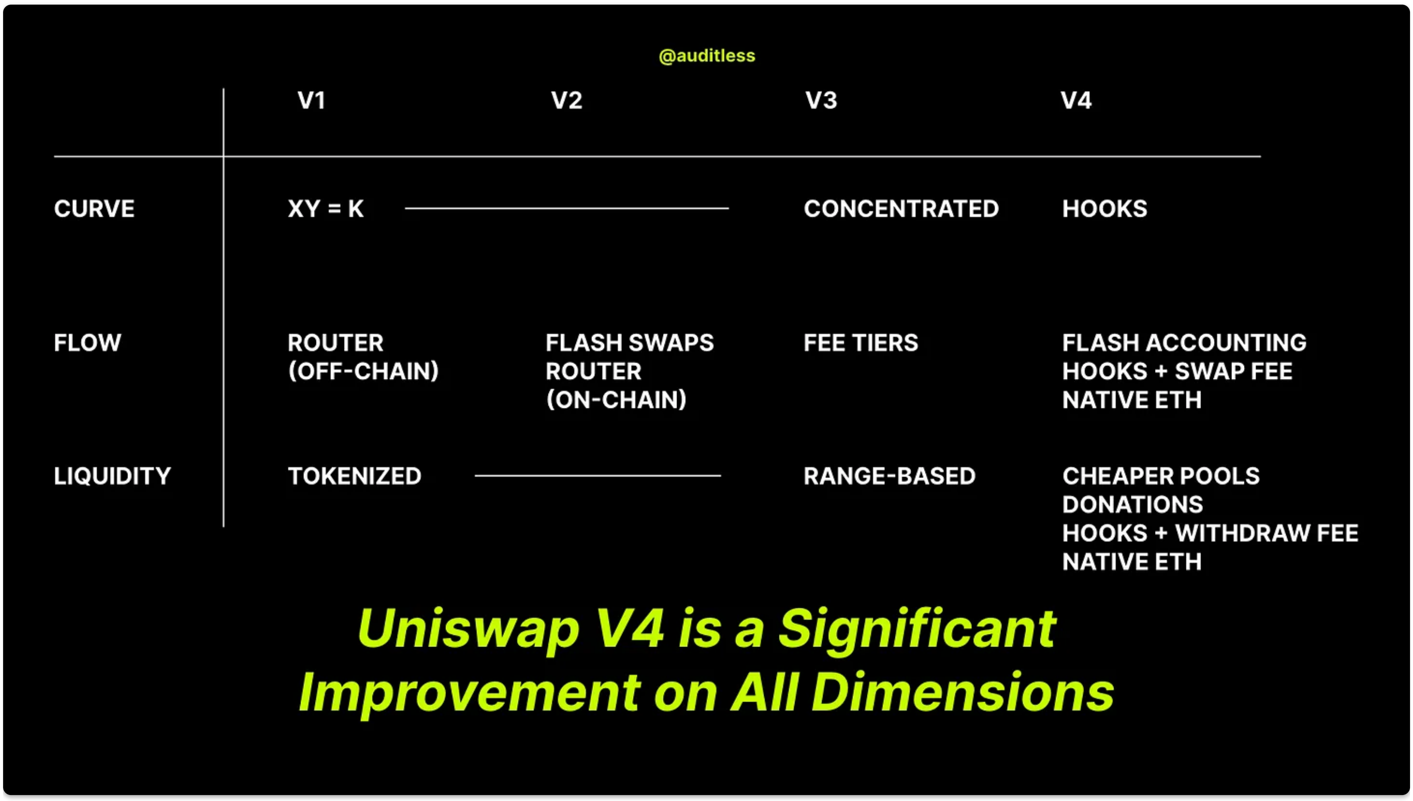
Vitalik tweeted that he voted for X

But there are technical solutions possible to reduce the reliance on these relays without allowing centralisation.

Social Slashing Video
Commentary on Tornado Cash Regulation by Coin Center
EFF - Kurt Opsahl Devcon video

Uniswap V4

See article from @auditless



@auditless

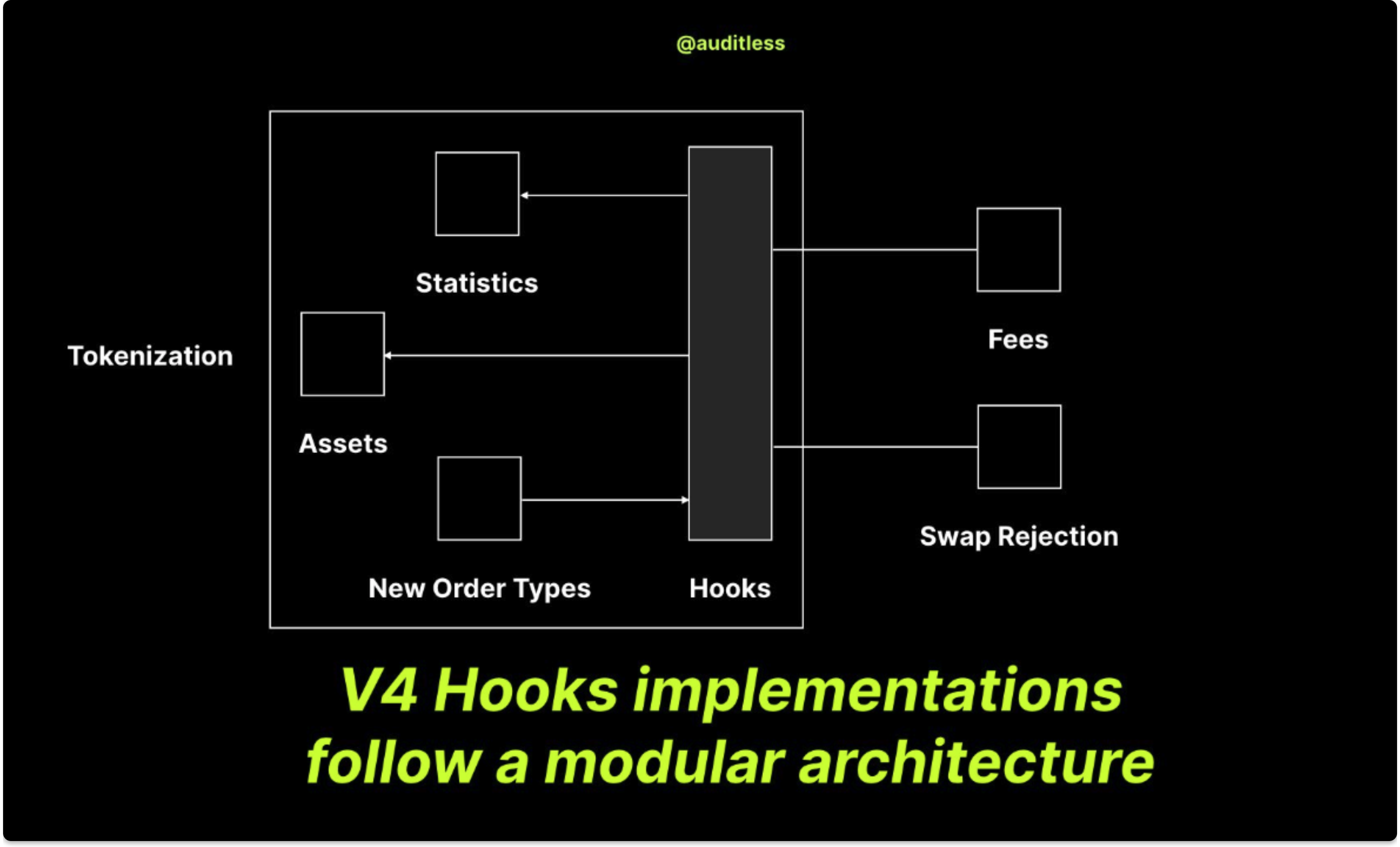
	V1	V2	V3	V4
CURVE	XY = K		CONCENTRATED	HOOKS
FLOW	ROUTER (OFF-CHAIN)	FLASH SWAPS ROUTER (ON-CHAIN)	FEE TIERS	FLASH ACCOUNTING HOOKS + SWAP FEE NATIVE ETH
LIQUIDITY	TOKENIZED		RANGE-BASED	CHEAPER POOLS DONATIONS HOOKS + WITHDRAW FEE NATIVE ETH

Uniswap V4 is a Significant Improvement on All Dimensions

Uniswap can now act as an aggregator of AMMs, by using hooks you can design a custom pool, and add the address of that pool via a hooks contract.
This should lead to reduced development effort to build customised AMMs.

See overview of hooks

From that article
Hooks mean you
– Can modify how liquidity is presented to swappers
– Can allocate idle liquidity elsewhere
– Can accept custom order types
– Can run computations in response to user actions



V4 Hooks implementations follow a modular architecture

Tutorial for creating your own hooks