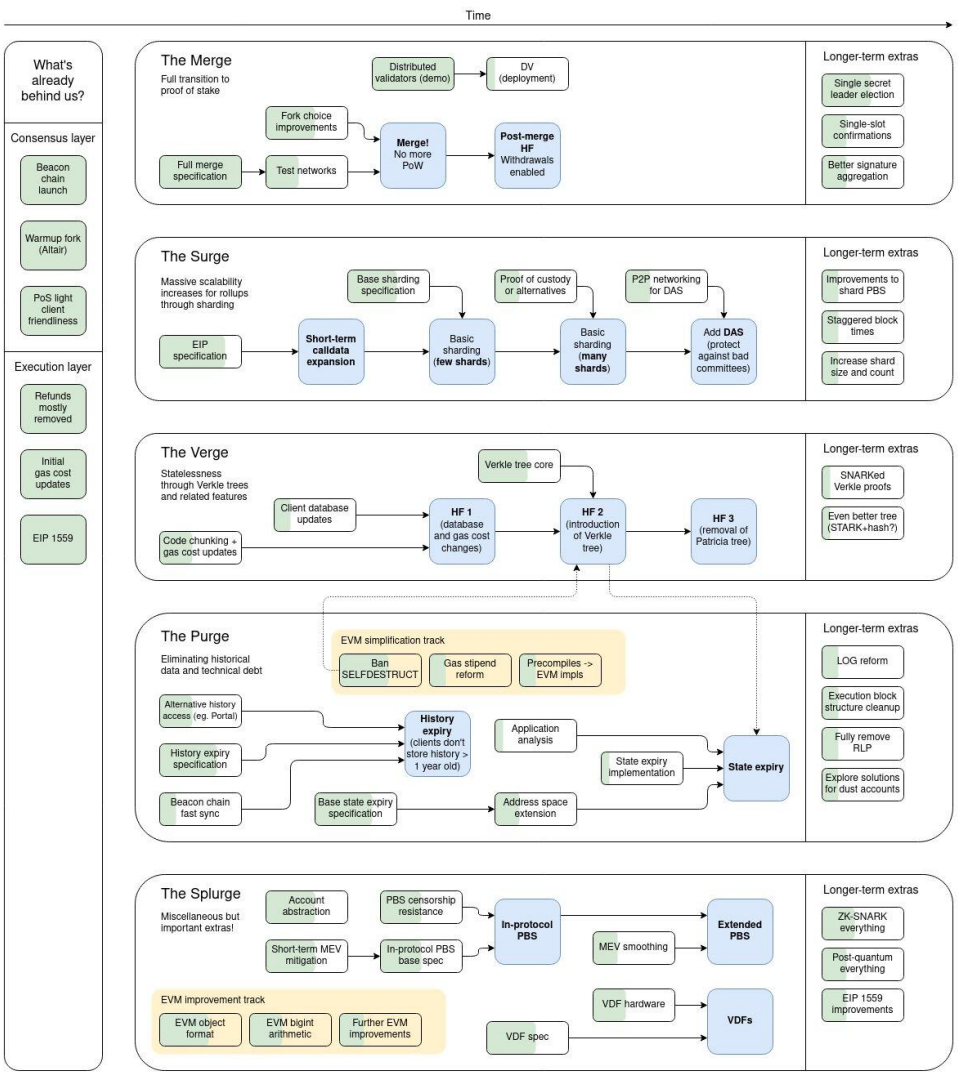
Everything a solo staker needs to know for the next phase of ethereum

Pol Lanski & Eduardo Antuña

Dappnode



Solo Stakers have a lot on their plates

"How the flop am I supposed to keep up with all of this?"

- A Solo Staker, upon seeing the Ethereum Roadmap

dappnode

Why? Solo Validators as the last bastion

MEV

DVT

Withdrawals

Proto-Danksharding EIP-4844

Validator Anonymity

Statelessness + PBS

Danksharding + DAS

dappnode

It is vital that we make staking easy because the alternative is an Existential Threat to Ethereum

Validator Centralization

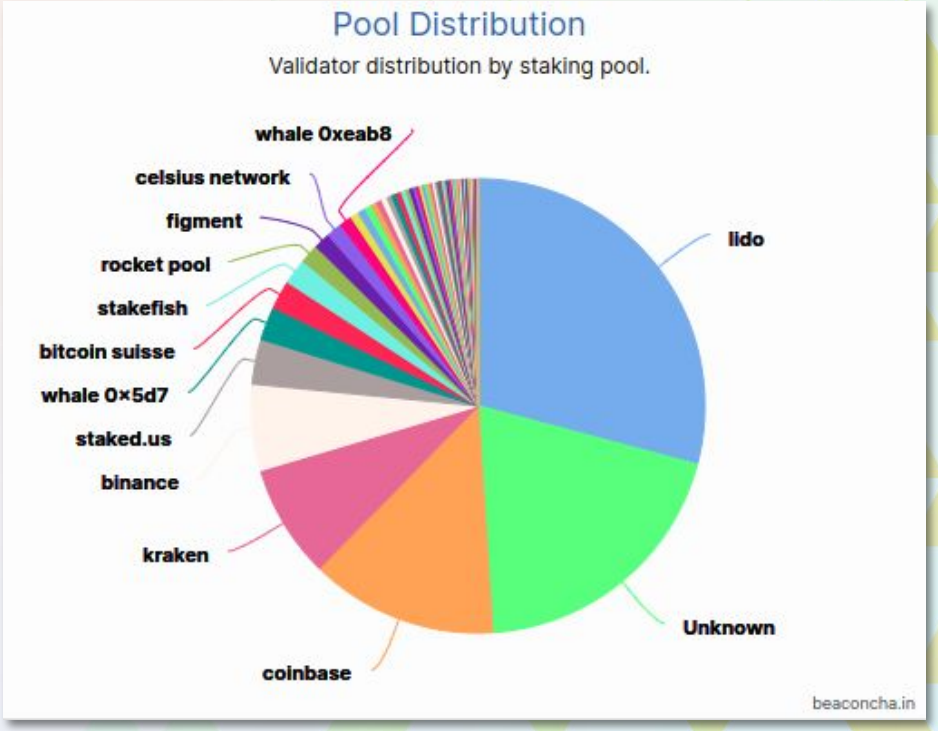
Lido - 29.15%

Coinbase - 13.35%

Kraken - 8.10%

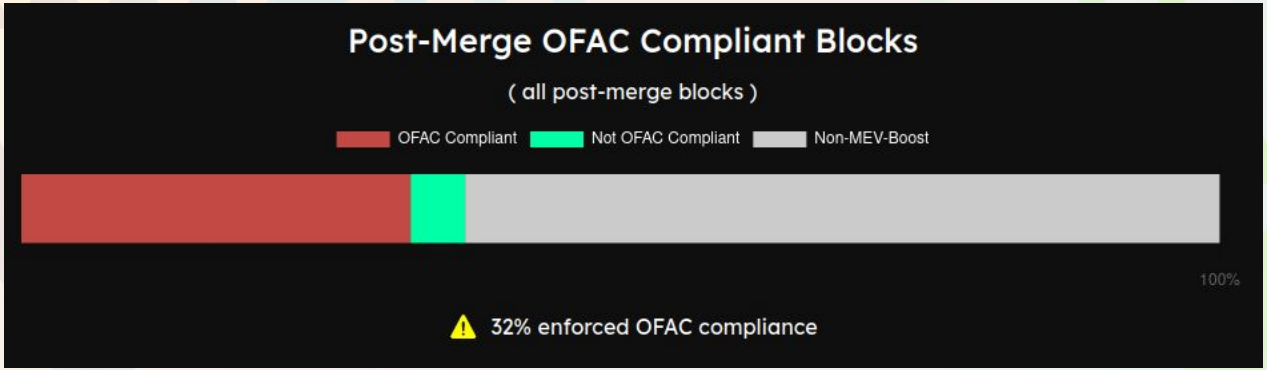
Binance - 6.12%

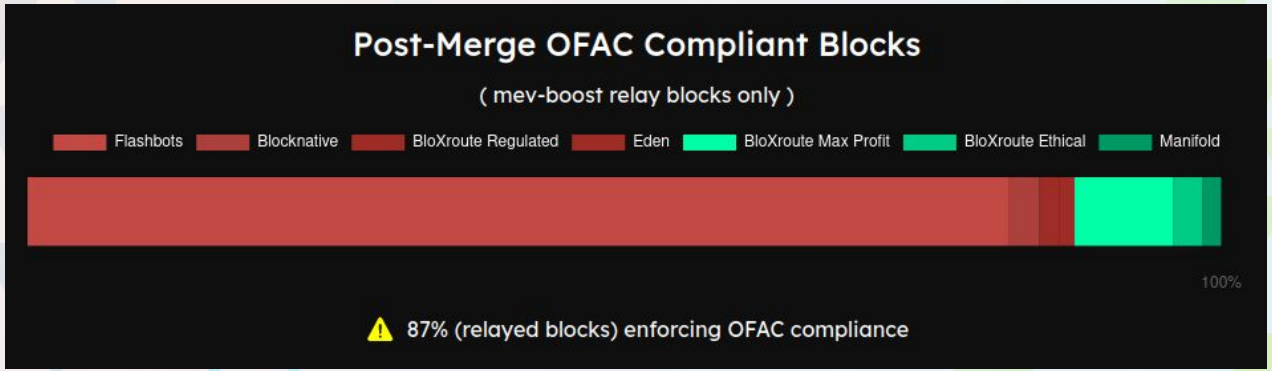
TOP 4 = 57.72%



dappnode

“Compliant” block production





dappnode

Dappnode wants to help

UI-based - No tech experience needed - no CLI

Auto-updates = 40h of DevOps work (16 Geth Releases, 20 Prysm Releases * 2h per releasing test = 72h of DevOps work saved per year (at 50$ Hour = 3200/year)

Web3signer - allows you to change Execution or Consensus Clients, securely, with the minimum safe downtime.

Community - Thousands of Node Runners like you sharing info and best practises

dappnode

Prater

Set up your Proof-of-Stake validator configuration for Ethereum and Ethereum-based chains. You will need to:
(1) Choose an Execution Layer client
(2) Choose a Consensus Layer client (+ validator)
(3) Install the web3signer, which will hold the validator keys and sign
(4) Optional; delegate block-building capacities through the MEV Boost network and potentially profit from MEV

The resulting testnet from the Prater and Göerli merge is the long-standing Ethereum testnet. Node operators can use it to test their node setups and app developers to test their stack

Execution Clients

Goerli Geth

Goerli is an Ethereum testnet merged with the Prater Beacon Chain

Goerli Erigon

Goerli Nethermind

Consensus Clients

Prysm Prater

Lighthouse Prater

Lighthouse Prater Beacon chain + validator

Fee recipient address

0x9758106Dc25403609105e10c11184bCAEc93B40e

Graffiti

validating_from_DAppNode

Checkpoint sync

https://checkpoint-sync-prater.dappnode.io

Teku Prater

Remote signer

Web3signer Prater

Remote signer + slashing protection database + User interface to import validator keystores

Mev Boost

Mev Boost Goerli

mev-boost allows proof-of-stake Ethereum prater consensus clients to outsource block construction

dappnode

The most important thing you need to know

YOU are the key for the future of Ethereum

Why? Solo Validators as the last bastion

MEV

DVT

Withdrawals

Proto-Danksharding EIP-4844

Validator Anonymity

Statelessness + PBS

Danksharding + DAS

dappnode

👹MEV👹: Maximal Extractable Value

✨The value is extracted from the users✨

👼: Arbitrage between DEXes

😈: Everything else

- Worse price execution on trades
- Gas wars, network congestion
- Chain reorgs
- Validators incentivized to attack themselves

dappnode

👹MEV👹: A Bug, not a feature

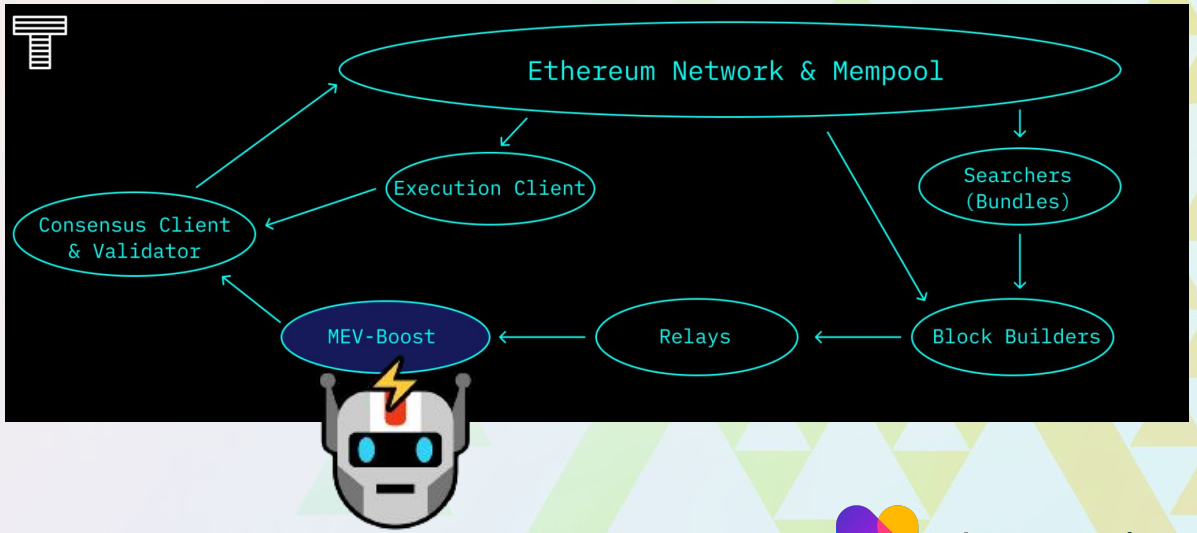
HUGE implications on the design of Ethereum

- PBS was designed to mitigate MEV, but now it’s necessary to implement Danksharding.
- MEV consequences mitigation strategies:
  - single-slot finality,
  - single secret leader election (Validator Anonimity)
- Democratize what cannot be mitigated
  - MEV-Boost
  - PBS
    - **MEV smoothing**

dappnode

MEV: What do you need to know

- MEV is a **centralizing force**
- As a Solo Staker, You CANNOT access MEV opportunities if you don't use **MEV Boost**



- In the future, PBS provides the same separation of powers, allows for easier builder decentralization, and removes the need for proposers to trust anyone.
  - MEV smoothing

dappnode

Why? Solo Validators as the last bastion

MEV

DVT

Withdrawals

Proto-Danksharding EIP-4844

Validator Anonymity

Statelessness + PBS

Danksharding + DAS

dappnode

DVT: Distributed Validator Technology

Now: 1 validator key = 1 validator client.

“Whoever runs the machine has access to the key”

DVT: Split the validator key so it can be distributed over many validator clients

✅ Allows for high availability

✅ Different trust assumptions - you can distribute shares with small or no collateral requirements

✅ Those running nodes can monetize them ON TOP of their validator - Everyone wants decentralized nodes!

dappnode

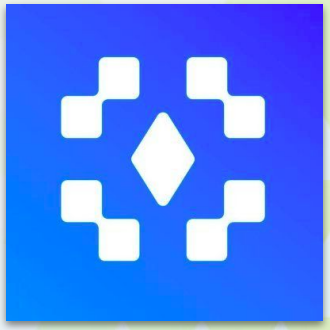
DVT: What you need to know

🚀 You will be able to monetize your machine and setup by leveraging other protocols on top of it.

👐 People will be able to participate in validation with less than 32 ETH

SSV.network

obol.tech



divalabs.org

dappnode

Why? Solo Validators as the last bastion

MEV

DVT

Withdrawals

Proto-Danksharding EIP-4844

Validator Anonymity

Statelessness + PBS

Danksharding + DAS

dappnode

Withdrawals!

- New “system level operation”
  - No gas cost
  - No EVM execution
- Increase the balance of the Withdrawal address
- Limited amount of withdrawals per block

Withdrawals: what you need to know

It means that you can get your money if you want to

What's going to happen when withdrawals are enabled?

Possibilities:

1. Distribution doesn't change significantly
2. There is a flow from Staking Services to Solo Staking
3. There is a flow from Solo Stakers to Staking Services

dappnode

Why? Solo Validators as the last bastion

MEV

DVT

Withdrawals

Proto-Danksharding EIP-4844

Validator Anonymity

Statelessness + PBS

Danksharding + DAS

dappnode

Proto-Danksharding: A Rollup-centric future

- A Rollup Centric Roadmap (Vitalik Oct'20)

The Long Term

In addition to these short-term concerns, a rollup-centric roadmap could also imply a re-envisioning of **eth2's long-term future: as a single high-security execution shard that everyone processes, plus a scalable data availability layer**.

To see why this is the case, consider the following:

- Today, Ethereum has ~15 TPS.
- If everyone moves to rollups, we will soon have ~3000 TPS.
- Once phase 1 comes along and rollups move to eth2 sharded chains for their data storage, we go up to a theoretical max of ~100000 TPS.
- Eventually, phase 2 will come along, bringing eth2 sharded chains with native computations, which give us… ~1000-5000 TPS.

It seems very plausible to me that when phase 2 finally comes, essentially no one will care about it. Everyone will have already adapted to a rollup-centric world whether we like it or not, and by that point it will be easier to continue down that path than to try to bring everyone back to the base chain for no clear benefit and a 20-100x reduction in scalability.

This implies a "phase 1.5 and done 269 **" approach to eth2, where the base layer retrenches and focuses on doing a few things well - namely, consensus and data availability**.

Proto-Danksharding: A Rollup-centric future

- Instead of providing more space for transactions, provide more space for **blobs of data**, which the Ethereum protocol itself does not attempt to interpret

- Verifying a blob simply requires **checking that the blob is available** - that it can be downloaded from the network

- The data space in these blobs is expected to be used by **layer-2 rollup** protocols that support high-throughput transactions

dappnode

Proto-Danksharding: What you need to know

- The Beacon Chain will need to store this new “blobs” of data that are going to be used mostly by rollups.
- This data will be stored in your Beacon Chain nodes for about a month
- Your Consensus Layer Node will become bigger, but it will not grow indefinitely

dappnode

Why? Solo Validators as the last bastion

MEV

DVT

Withdrawals

Proto-Danksharding EIP-4844 + PBS?

Validator Anonymity

Statelessness

Danksharding + DAS

dappnode

Single Secret Leader Election

- The Beacon Chain publishes the validator list, easy to deanonymize them and map their IP addresses.
- More sophisticated validators can use tricks to better hide themselves, but small-time validators will be particularly susceptible to getting doxxed and subsequently DDOSd. This can be quite **easily exploited for MEV.**
- SSLE protects validators as only the proposer knows when their turn is up

dappnode

Validator Anonymity: What you need to know

- Because the list of proposers of the new epoch are known, validators can be targeted to be offline at the time of their block production
- SSLE protects validators as only the proposer knows when their turn is up
- Validator IPs could still be found, unless we use some sort of mixnet or privacy solution like **HOPR**

dappnode

Why? Solo Validators as the last bastion

MEV

DVT

Withdrawals

Proto-Danksharding EIP-4844

Validator Anonymity

Statelessness + PBS

Danksharding + DAS

dappnode

Statelessness

- Validation is **stateful.** Pre-state root, process all transactions and check if pre-state root matches
- “**Statelessness**” meaning state isn’t required to validate a block, but it is required to build the block
- It allows validators to take a look at a block and know if it’s valid or not, in isolation
- Weak statelessness gives the **builders** a bit more work, and **validators** far less work
- Builders will start including the pieces of state affected by transactions in a given block, and they’ll **prove** they correctly accessed that state with **witnesses**

PBS: Proposer Builder Separation

- Started as an MEV mitigation strategy
- Becomes important because then we can start making scalability tradeoffs by giving builders more computational work without compromising the decentralization of the validation.
- Proto-danksharding and Statelessness put more burden to the block builder
    - **PBS is a way of using fancy tools while building blocks without requiring Solo Stakers to have huge machines.**

dappnode

Statelessness + PBS: What you need to know

- **Hard-drive** requirement for holding state **disappears**
- **Bandwidth** requirements will **increase** a bit (witness data and proof)
- … but it won't increase a lot because we migrate from patricia-merkle trees to **Verkle-trees**, proofs are more efficient
  - It's a constant size proof regardless of the width of the tree
- When the requirements to build and validate become too high, PBS will kick in
  - PBS will also make MEV boost redundant and embedded in the protocol.

Why? Solo Validators as the last bastion

MEV

DVT

Withdrawals

Proto-Danksharding EIP-4844

Validator Anonymity

Statelessness + PBS

Danksharding + DAS

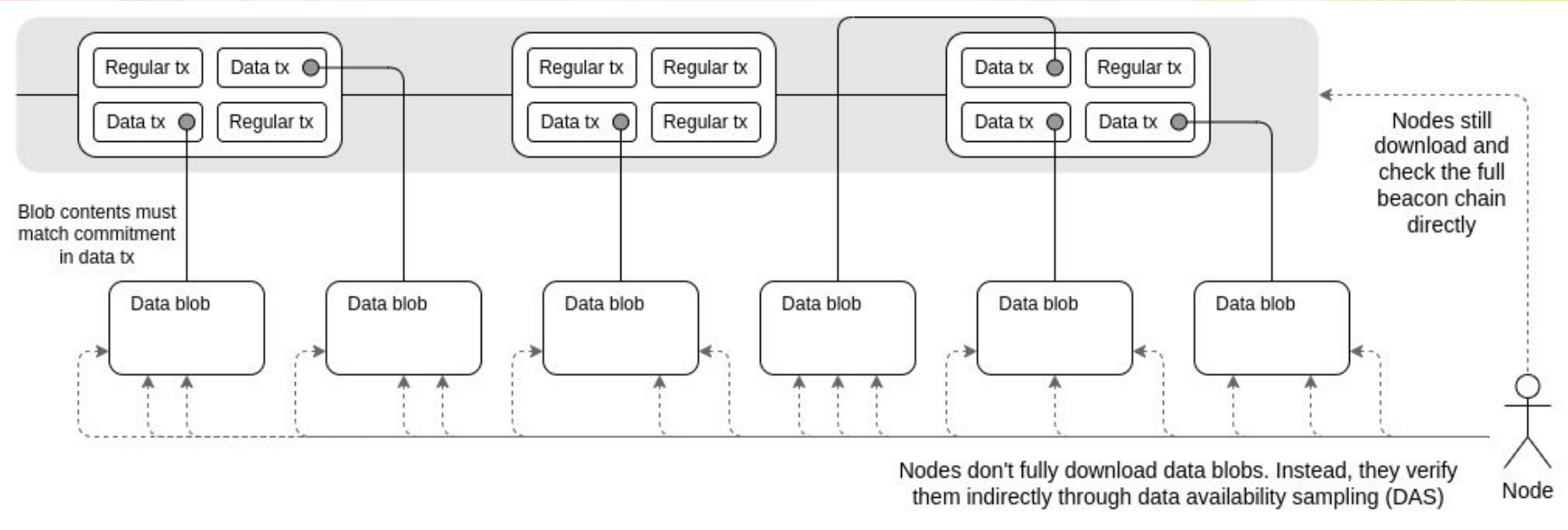
dappnode

Danksharding

- **The merged fee market:** instead of there being a fixed number of shards that each have distinct blocks and distinct block proposers, in Danksharding **there is only one proposer that chooses all transactions and all data that go into that slot** - no distinct shards.
- The concept of shard is that **only** the **block builder needs to process the entire block** all other **validators** and users can **verify** the blocks very efficiently **through data availability sampling** (DAS)

dappnode

DAS - Data Availability Sampling



dappnode

What does it all mean for solo stakers?

1. **We don’t know**. It’s too far, and there are many moving pieces.
2. Is there going to be History Expire and State expiry?
3. The idea is that we are going to make some parts more complicated so Solo Stakers can still hold the ultimate power of validation, and hence, the security of the network.

dappnode

Why? Solo Validators as the last bastion

A bug, not a feature. Centralizing force vs. Censorship resistance

MEV

Leverage your setup to earn extra rewards

DVT

Take your deposit out!

Withdrawals

Proto-Danksharding EIP-4844 + PBS?

Your CL will grow with new "Blobs" of Data.

Validator Anonymity

SSLE will save us from MEV extractors

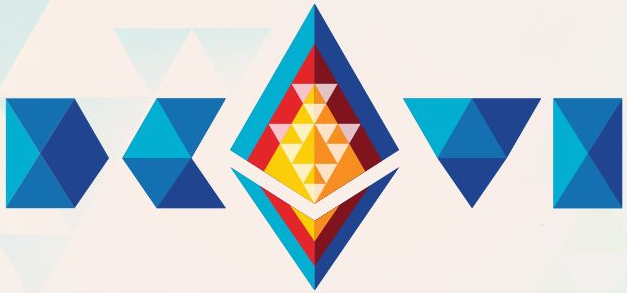
Statelessness

Less hard drive requirements but more bandwidth

Danksharding + DAS

Hard to know as of now

dappnode



Thank you!

Pol Lanski - Edu Antuña

Dappnode

@Dappnode
@Pol_Lanski
@eduadiez