系统理解 LSD：
Staking Restaking 和 AVS

主讲人：shawn 2024/05/08

大纲

1. 概念解释
2. 解读 ETH 2.0
3. Liquid Staking & Liquid Restaking
4. 解读 AVS

1. 概念解释

1) PoS（Proof of Stake, 权益证明）
2) LSD（Liquid Staking Derivatives, 流动性质押衍生品协议）
3) Staking / Restaking
4) AVS（Actively Validated Services， 主动验证服务）

概念解释

1. PoS（Proof of Stake, 权益证明）

是一种通过质押资产来分配记账权利的共识机制。

时间节点1: 2022年9月巴黎升级启动，以太坊正式从 PoW 转变为 PoS，完成了主网和信标链的合并。

时间节点2: 2023年4月上海升级允许网络质押者赎回 ETH 资产，标志 PoS 共识的技术路线发展成熟，以太坊网络完成 PoS 共识的转变。

概念解释

2. LSD（Liquid Staking Derivatives, 流动性质押衍生品协议）

是一套质押众筹，奖励共享的链上协议，充分降低了以太坊质押的用户进入门槛，大大提高了资金利用率。

背景1：进行 Validator 原生质押的资产量必须是 32 ETH 或其倍数，门槛相对较高。

背景2：在 2023 年 4 月上海升级前，用户质押的资产无法取出，资金的利用效率太低。

因此，LSDfi 赛道出现在大众眼前。LSD 普遍采用混合资金池的方式，用户可以将任意数量的 ETH 存放于 LSD 平台上，后者发放质押凭证（LST）。协议会将其聚合起来作为运行以太坊验证人节点的质押资产，这一特性有效的解决了散户资金不足的问题。其次，用户持有质押凭证（LST），不仅能获得以太坊共识层的出块奖励，还能随时换回 ETH。方便的解决了验证人节点的质押资产资金利用率太低的问题。

概念解释

3. Staking / Restaking

是一种借助 LSD 平台的质押凭证，来参与到更多的网络/协议中，以获得收益，同时帮助更多的协议提升安全性的流动性创新行为

一句话概括

用户想参与以太质质押挖矿，拼团在LSD协议中做质押，协议发行质押凭证是 LST，把 LST 在 Restaking 平台再质押一次后得到 LRT

按照这种方式能无限层层嵌套下去吗？

概念解释

4. AVS（Actively Validated Services，主动验证服务）

借助Staking平台和Staking Slashing机制，衍生出的一套安全共享机制。

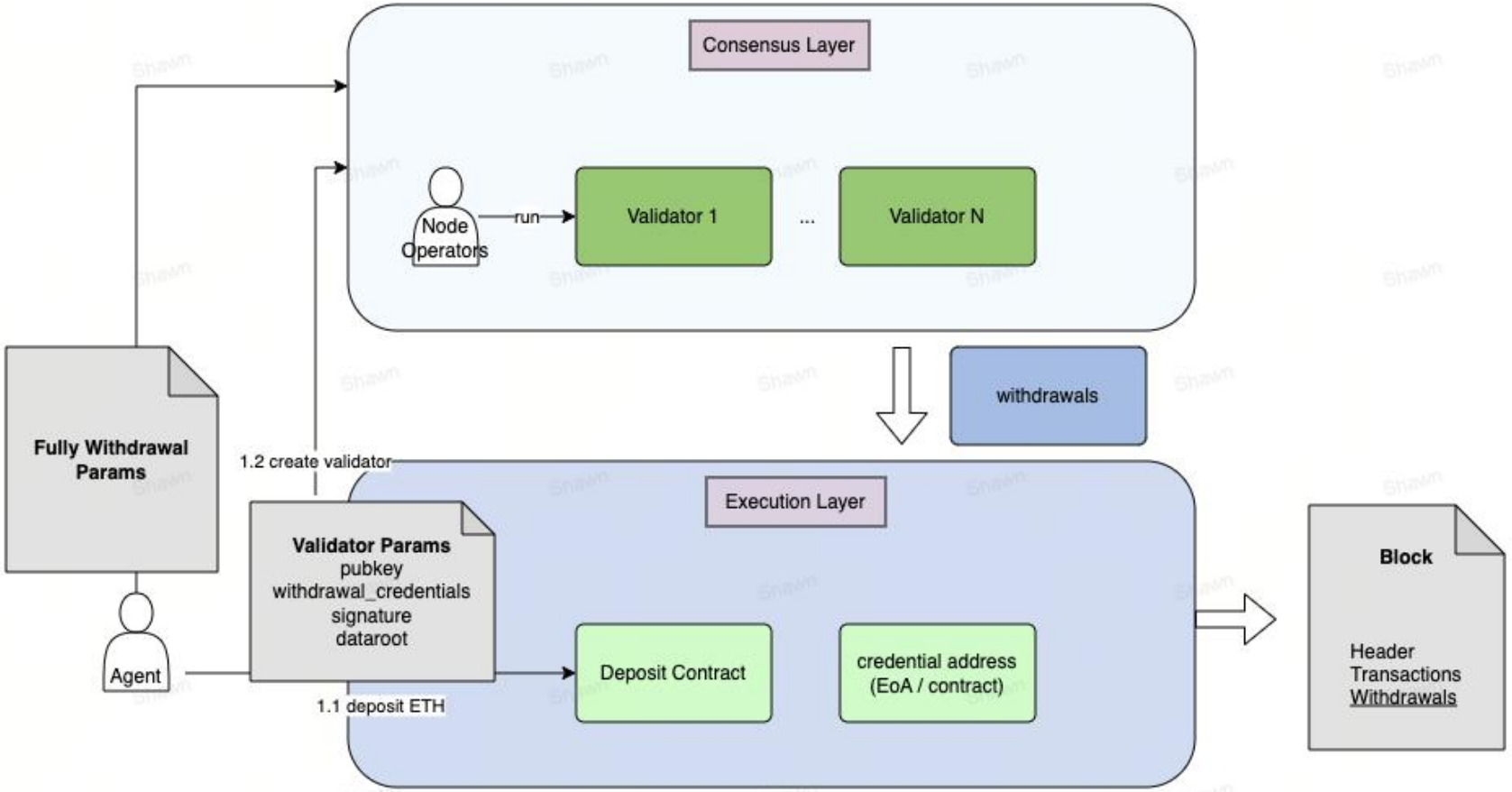
特别指出，所谓的安全共享，指的是流动性提供平台支撑运行以太坊网络验证人节点的同时，能够支撑更多项目方数据验证和共识节点运行的行为，例如 cosmos 架构中类似的 interchain security 安全共享方案。

2. 解读 ETH 2.0

1. 用户视角的ETH2.0 架构
2. 新增 Validator 的状态流转
3. Validator 生命周期
4. 社区资源

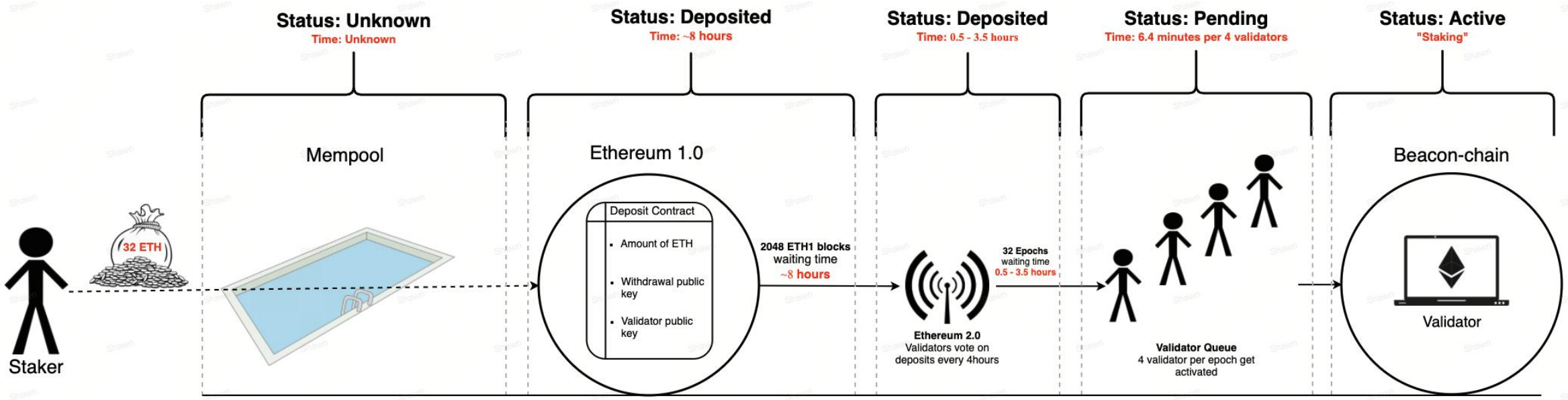
解读 ETH 2.0

1. 用户视角的ETH2.0 架构



解读 ETH 2.0

2. 新增 Validator 的状态流转



source: https://kb.beaconcha.in/ethereum-2.0-depositing

解读 ETH 2.0

Deposit Steps

1. Mempool - Status: Unknown

Every signed transaction visits the Mempool first, During this period, the transaction status is pending.

2. Deposit contract - Status: Deposited

Address: https://etherscan.io/address/0x00000000219ab540356cBB839Cbe05303d7705Fa#code

解读 ETH 2.0

Deposit Steps

3. Validator Queue - Status: Pending

The deposit is accessible now for the beacon-chain. Depending on the amount of total deposits, the validators have to wait in a queue.

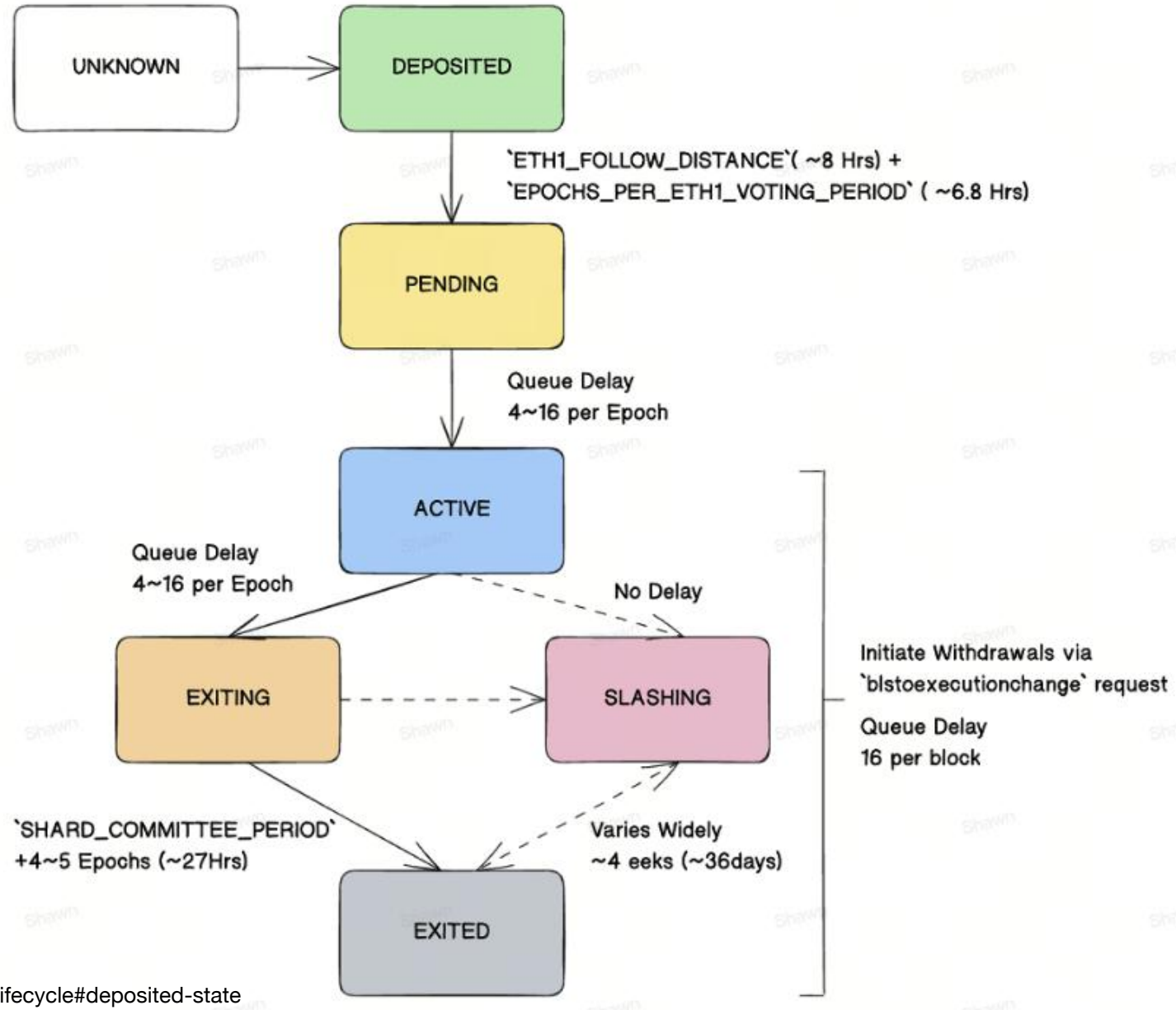
4. Staking - Status: Active

The validator is now actively staking. It is proposing blocks and signing attestations - ready to earn ETH!

The Staker can get profit by staking until this time point. It may take monthes

解读 ETH 2.0

3. Validator 生命周期



source: https://docs.prylabs.network/docs/how-prysm-works/validator-lifecycle#deposited-state

解读 ETH 2.0

Validator lifecycle

1. DEPOSITED -> PENDING

- ETH1_FOLLOW_DISTANCE

The Ethereum 2.0 chain only considers transactions which have been in the deposit contract for at least 2048 Ethereum 1.0 blocks to ensure they never end up in a reorged block.

- EPOCHS_PER_ETH1_VOTING_PERIOD

In addition to the 2048 Ethereum 1.0 blocks, 64 Ethereum 2.0 Epochs *must be* awaited before the beacon-chain recognises the deposit. During these 64 Epochs, validators vote on newly received deposits.

2048 blocks = 2048 x 12 seconds = 24,576 seconds = 409.6 minutes = ~6.82 hours

64 Epochs = 64 x 6.4 minutes = 409.6 minutes = ~6.82 hours

解读 ETH 2.0

Validator lifecycle

2. PENDING -> ACTIVE

Validator Queue Exporter(Stake.fish): https://www.validatorqueue.com/?ref=blog.stake.fish

The beacon chain can process the deposits of 4 ~ 16(**The churn limit**) new validators per finalized epoch, the difference in the number is determined by the number of total active validators on the chain. Once a validator has reached the front of the queue, it is assigned an activation epoch after an additional 4~5 epochs (~31 minutes).

- Ethereum's churn limit equation

active validator set has size $|V|$, a maximum of $max(4, \frac{|V|}{65536})$ valdators can join per epoch

解读 ETH 2.0

Validator lifecycle

3. ACTIVE -> EXITING

Docs: https://docs.prylabs.network/docs/wallet/withdraw-validator

Validator Queue Exporter(Stake.fish): https://www.validatorqueue.com/?ref=blog.stake.fish

Validators that have been active and have a validator index (including validators that are slashed/exited) can initiate a **BLStoExecutionChange** request that changes its *withdrawal_credentials* which begins the withdrawal process.

Once the *withdrawal_credentials* are changed, withdrawals will automatically be processed at the rate of 16 per block. Fully exited validators will also be fully withdrawn once withdrawals are initiated.

- Withdrawal Types

The Capella/Shanghai Ethereum upgrade lets you withdraw your validator nodes' staked Ethereum in one of two ways:

1. **Partial (earnings) withdrawal**: This option lets you withdraw your earnings (that is, all value staked above 32 ETH) and continue validating.

2. **Full withdrawal**: This option lets you liquidate your entire stake and earnings, effectively liquidating your validator node(s) and exiting the network.

BLSExecutionChange：https://github.com/ethereum/consensus-specs/blob/dev/specs/capella/beacon-chain.md#blstoexecutionchange

解读 ETH 2.0

4. 社区资源

Consensus node dev docs

Docs: https://ethereum.org/en/developers/docs/nodes-and-clients/#consensus-clients

Beacon chain explorer

Mainnet: https://beaconcha.in/

Validator Queue Exporter

Stake.fish: https://www.validatorqueue.com/?ref=blog.stake.fish

4.4 Eth Beacon Node API

API Docs: https://ethereum.github.io/beacon-APIs/#/

Url: https://docs-demo.quiknode.pro/eth/v1/beacon/genesis

3. Liquid Staking & Liquid Restaking

1. Liquid Staking & LST
2. Liquid Restaking & LRT
3. LRT DApps

3. Liquid Staking & Liquid Restaking

Liquid Staking & LST

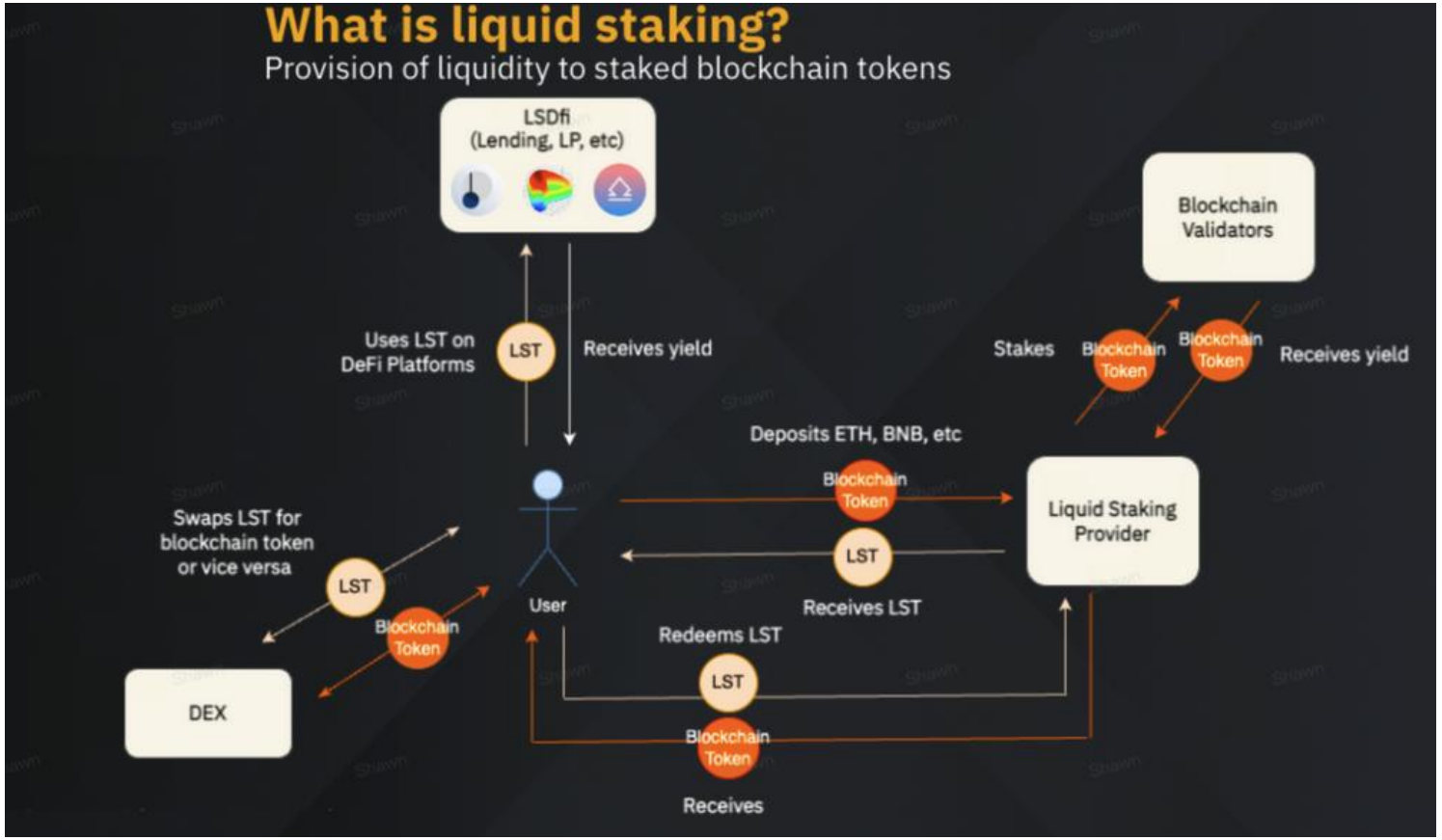


Figure4: Liquid Staking, Source: Binance Research

3. Liquid Staking & Liquid Restaking

Liquid Staking & LST

LST Asset Flows

Who controls the staked ETH?

- - The ETH stake principal is managed by LSD smart contracts. The Operator can initiate fund flows between LSD smart contracts, but requires Administrator signatures to modify destination smart contract addresses.
- - Staking involves two types of keys: validators keys and withdrawal keys. Validator keys are used for cryptographic signing of attestations, while withdrawal keys are used to set reward and withdrawal addresses. For Mantle LSD, the rewards and withdrawal address will be the LSD smart contract at the time of validator creation. This means the node operators (validators) do not have control over the staked ETH.

3. Liquid Staking & Liquid Restaking

Liquid Staking & LST

LST Token Model

- There are two main types of receipt token models: **Rebasing** and **Value Accumulating**.

The rebasing model maintains a loose 1:1 peg to ETH, while the value accumulating model is designed to increase the LST:ETH ratio over time, aligned with the weighted rewards APY.

- Our recommended token model for LST is the value accumulating model, following the standard ERC-20 format. This model provides maximum composability and technical familiarity across DeFi, omnichain, and centralized applications. See commentary on implementing rebasing tokens within applications: Lido Techdocs: stETH Booking Shares.

- It is worth noting that the current most widely adopted receipt token is Lido stETH, a rebasing token model.

3. Liquid Staking & Liquid Restaking

Liquid Restaking & LRT

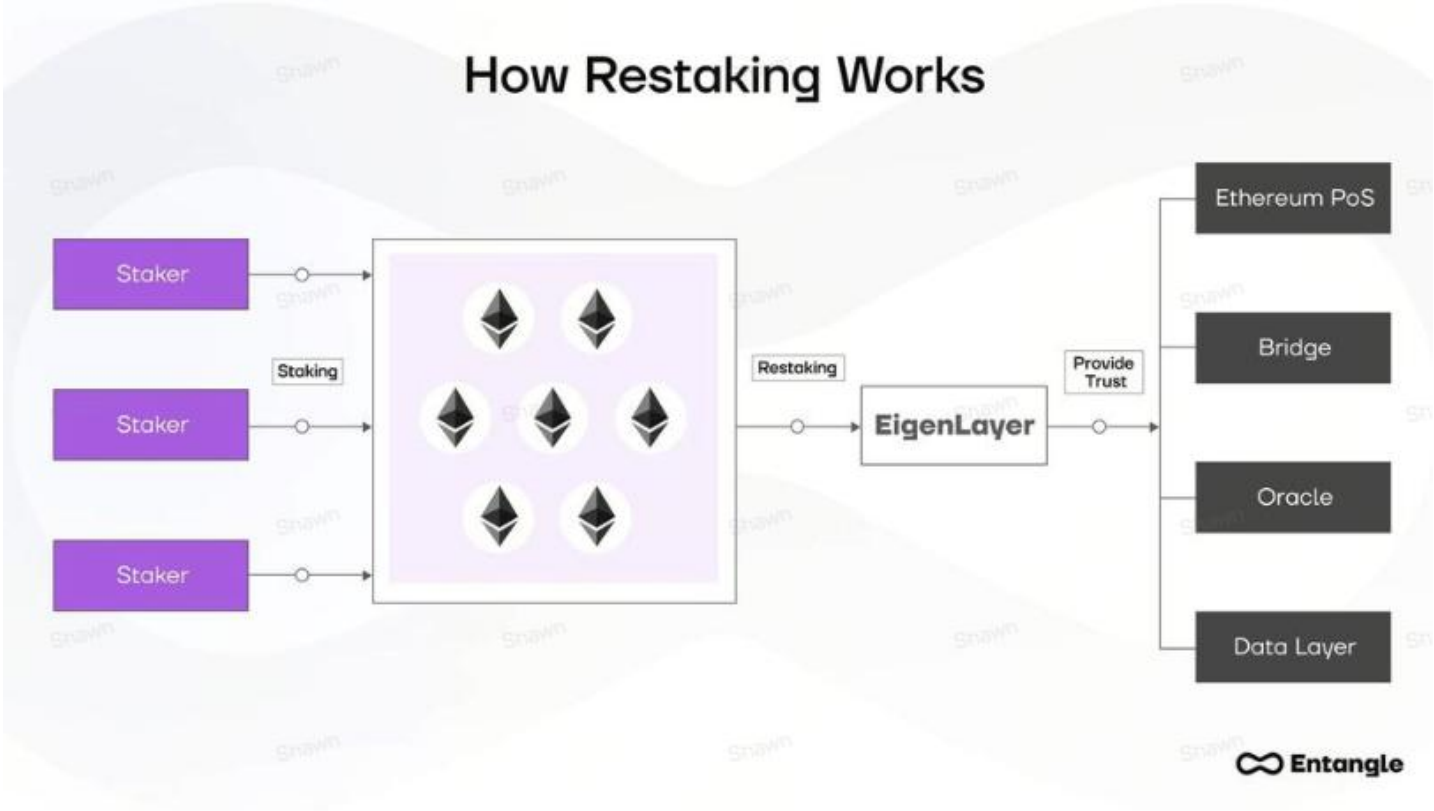


Figure5: Liquid Staking, Source: Entangle

3. Liquid Staking & Liquid Restaking

Liquid Restaking & LRT

Advantages

- 1. Increased safety. That’ s a chance to increase economic security due to implementing new AVS with existing Ethereum validators;
- 2. Capital efficiency. Boosting the financial value of all networks involved;
- 3. Balancing costs. The costs of improving Ethereum security are balanced by being shared among several AVS;
- 4. Stronger security. Increasing costs of potential hacks as the system becomes more global and stronger.

3. Liquid Staking & Liquid Restaking

Liquid Restaking & LRT

Major drawbacks

1. Single point of failure. If EigenLayer is attacked with a substantial amount of staked ETH, the main network would be at great risk.

2. Centralization risks. If many stakers are responsible for one application's security and are subject to penalties, this could have negative consequences for Ethereum.

3. Risks for profitability. The protocols use Ethereum to ensure their security. However, stakers on EigenLayer may select the highest returns to maximize their profits, which could lead to a race to raise capital between protocols.

4. Fines. Protocols can change conditions, reducing penalties to attract more capital and thereby undermining their own security.

3. Liquid Staking & Liquid Restaking

LRT DApps

There are two ways users can interact with LST and LRT.

- Direct Staking and Redemptions: Users can directly deposit into and redeem from the Staking Contract. As of June 10, 2023, there is a delay of 40+ days for Beaconchain activations (staking) and 2 days for withdrawals (redemption). For more details, please visit: https://www.validatorqueue.com/. The protocol may have to implement delays on withdrawals to prevent a griefer from staking and immediately withdrawing, causing the protocol to exit validators to the detriment of all mETH holders.

- Trading for mETH on Secondary Markets: Users have the option to convert between ETH and mETH directly on applications such as DEX and CEX. The exchange rate on these markets is determined by price discovery and slippage. In theory, the exchange rate should follow the exchange rate for direct staking and redemptions due to market makers and arbitrage opportunities.

4. 解读 AVS

1. AVS 中的主要角色
2. Staking Slashing 机制
3. Liquid Staking & Liquid Restaking
4. 对生态的影响和启发

4. 解读 AVS

AVS 中的主要角色

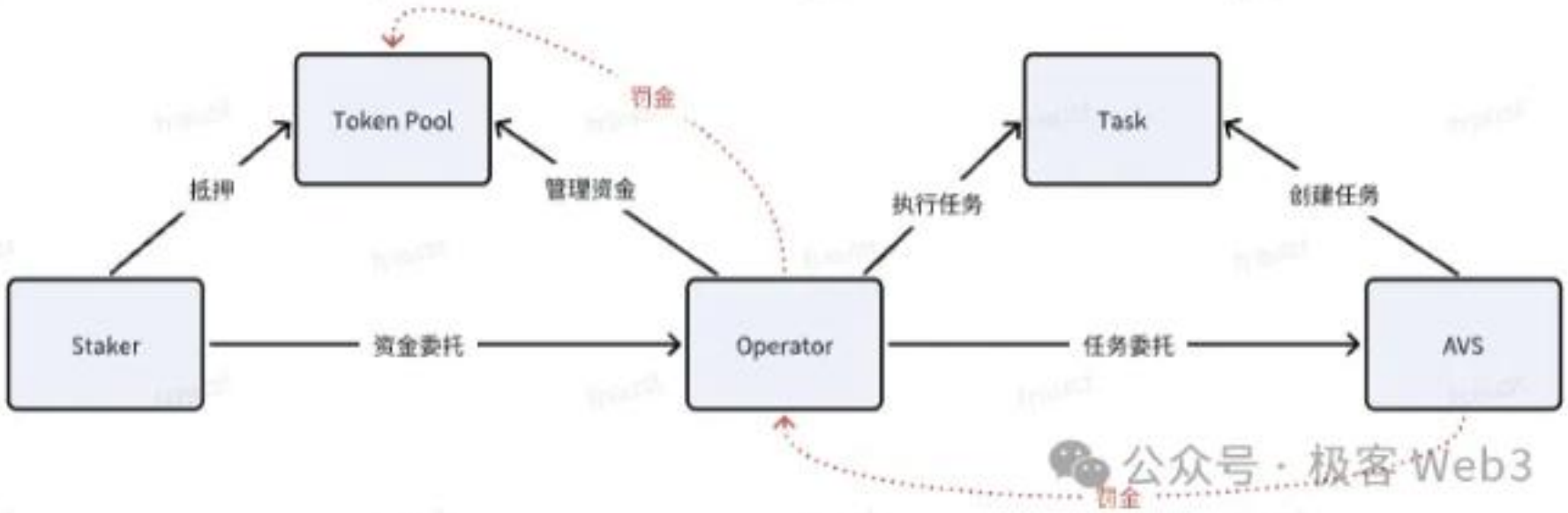
- 安全的出借方——Staker (质押者)。Staker质押资金以提供安全性
- 安全的中介方——Operator (节点运营商)。负责帮助 Staker 管理资金的同时，帮助 AVS 执行任务。
- 安全的接收方—— 预言机等去中心化服务。

source: https://mp.weixin.qq.com/s/b6QpeiiMAsejDPY3h_FhHg

4. 解读 AVS

AVS 中的主要角色

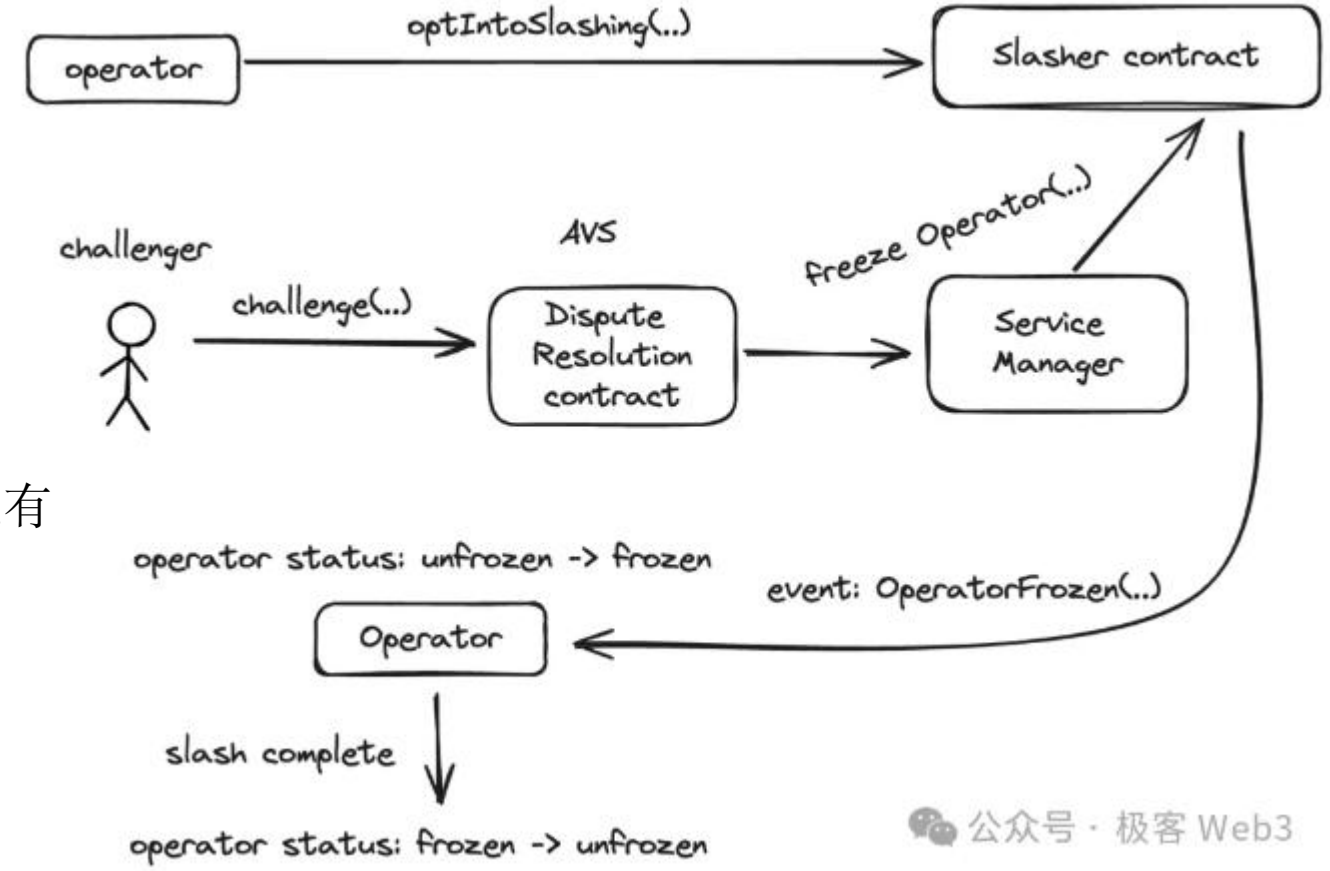
质押的交互流程如下图所示。



4. 解读 AVS

Staking Slashing 机制

在 Staker、Operator 和 AVS 中，只有 Operator 会成为罚没的直接对象。



4. 解读 AVS

对生态的影响和启发

Defi、CeFi 潜在的应用包括：

- 抵押品市场：LST / LRT 等有价资产可以在抵押品平台中进行杠杆行为，并且是多倍杠杆。
- LST 流动性池子：可以将多个 LST（收据代币）汇集在一起，创建一个共同的收据代币。目标是集中其他分散的流动性，可能导致应用程序更好地采用共同的收据代币。但是，需要注意的是，共同的收据代币共享其基础组件的累积风险。

丰富了生态的同时也带来了更高的系统性风险

- 多重杠杆
- 连续套娃

感谢支持!