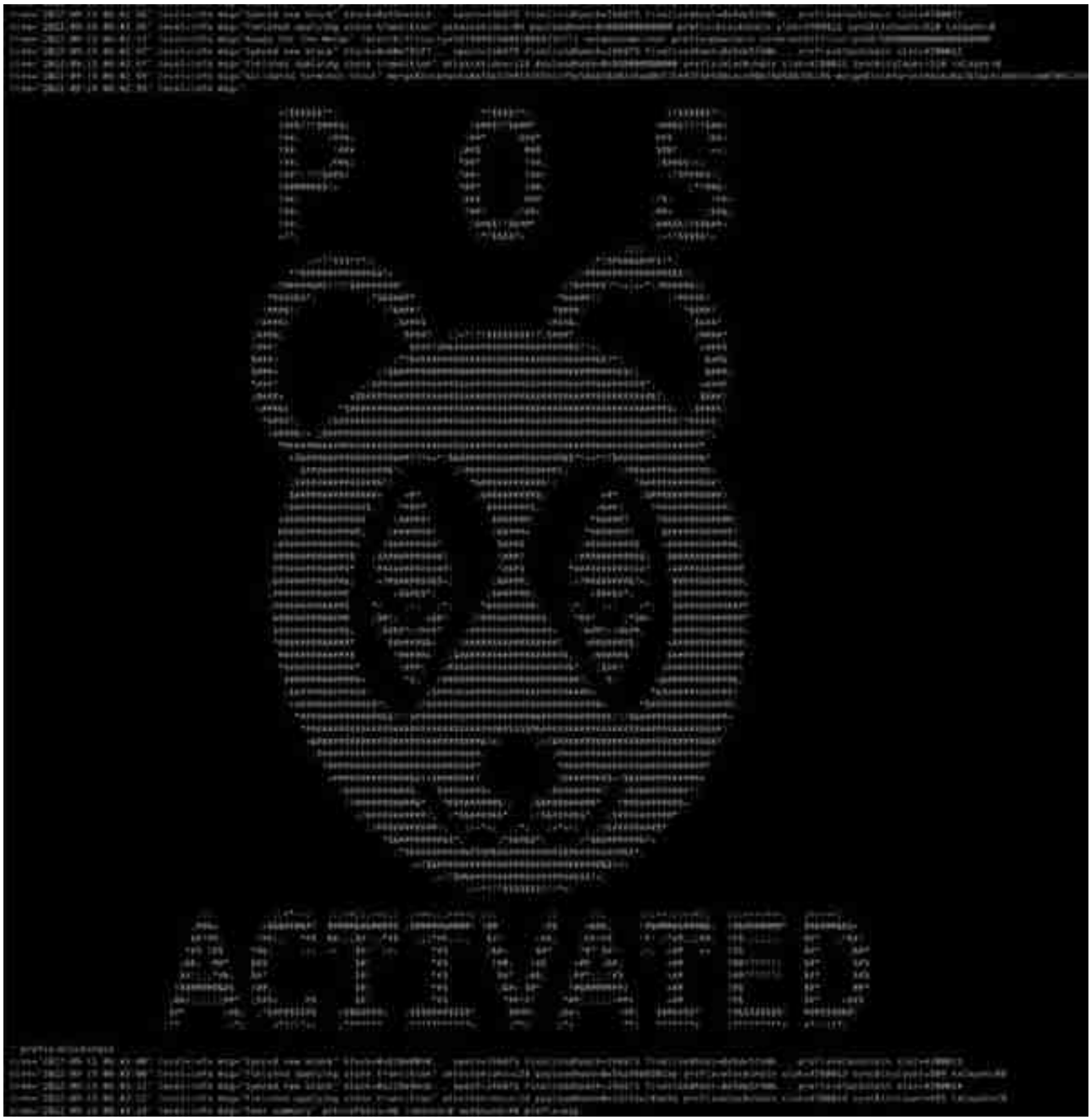

一：The Merge

1.1 背景

The
Merge是以太坊有史以来最大的技术升级，在2022年9月15日实现了Execution
Layer和Consensus
Layer的合并，其最大的变化是将以太坊的PoW共识切换为PoS共识。

图2：Vitalik对于合并后以太坊能源消耗的观点

1.2 合并带来的改变

- 代币增发：
  PoW时代的ETH代币增发停止，新的ETH仅通过PoS共识出块产生，以太坊的通胀率降低，当base fee超过15gwei的时候，以太坊甚至进入通缩。


Stake ETH
Liquid
Deposit as little as 0.01 ETH and receive the rETH liquid staking token. rETH accrues staking rewards over time.
Decentralised
A decentralised network of node operators earn rewards for rETH holders.
Non-custodial
Node operators do not handle funds. Any penalties incurred by node operators are taken from their earnings rather than rETH holders.
≈ 5.26% APR
Average Rewards
Stake

图4：Rocket Pool质押收益率

- Withdraw：
  合并以后质押的ETH并不能立即Withdraw，需要在上海升级以后才会放开Withdraw的限制，并且在提款的时候，用户并不能直接提取，为了避免大规模的提款，对于单次提款的数量和时间都有一定的限制，所以开放提款以后，并不会出现大量提款抛售的情况。具体的信息可以参考EIP-4895：Beacon chain push withdrawals as operations
- 数据结构的改变：Consensus Block里面会包含Execution Block的Hash值，同时Execution Block里面和PoW相关的参数不再生效。mixHash字段会记录以太坊原生的RANDAO随机数，供EVM调用，以太坊的开发者可以直接使用这个随机数到智能合约开发中。

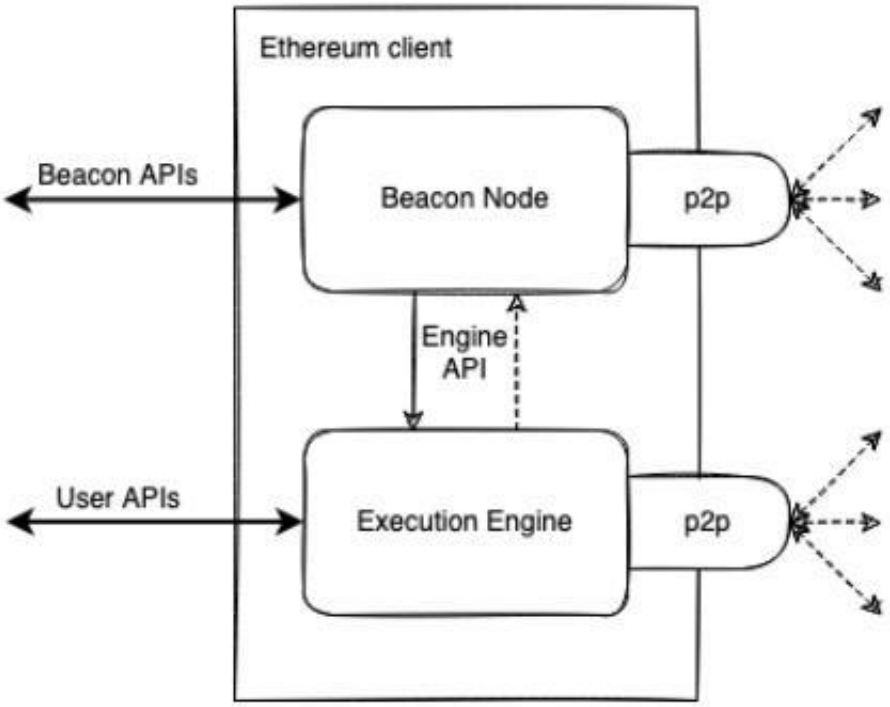

图6：合并后以太坊客户端

切换为PoS共识以后，以太坊的算法由Ethash转换为了Casper FFG（Gasper），相较之前的算法，Gasper更加节能，不需要再通过专门的矿机计算难度值，而是通过随机的方式来出块，让我们往下继续探索以太坊的共识算法和出块方式！

二：Gasper

目前信标链上面质押了13,830,378个ETH
，活跃验证者的数目为432,203个

（截至2022年9月23日），根据PBFT的特点，beacon chain的验证者数目很多，网络通信数据量大，简单的PBFT不再适用于以太坊网络，于是以太坊在网络结构上面采用PBFT的思想对网络架构进行了改进和设计，使用了Gasper算法。

Gasper为beacon chain协议中的终局性工具（finality gadget），用于确定哪些区块应被参与者认定为已经确定的、不可更改的，同时在分叉的时候用于确定哪个分叉链是主链。Gasper的终局性一般化了《Casper Friendly Finality Gadget（casper FFG）》论文中的概念。

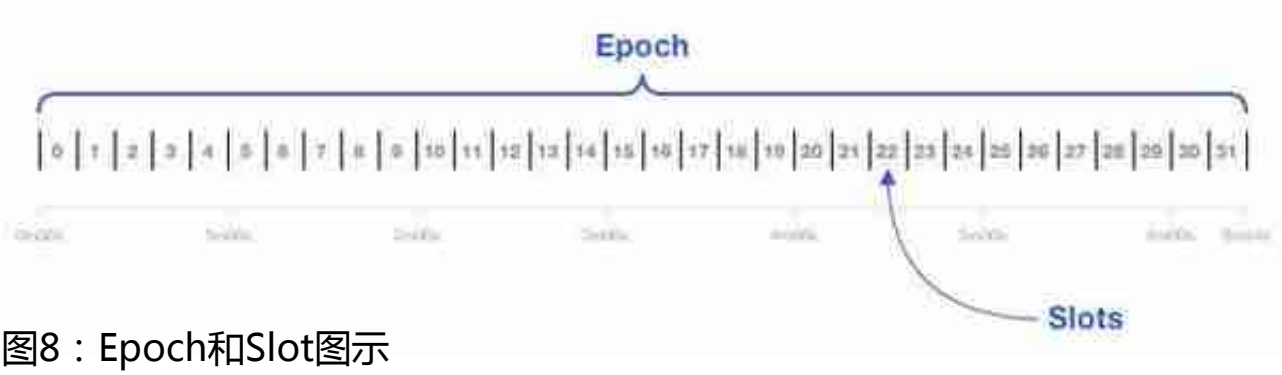

图8：Epoch和Slot图示

- Slot（时隙）：
  合并以后一个Slot就是一个区块，有一个committee负责在12S的时间内生成该Slot。
- Epoch：
  每32个Slot组成一个Epoch，一个Epoch的时间为384S，即6.4Min。
- Committee（验证者委员会）：
  每个验证者委员会最低会分配128个Validator，验证者会对自己负责的Slot进行Attestation操作，并且在委员会中有一个Validator会被随机选为Proposer，进行出块。
- Attestation（投票签名）：
  每一个Slot对应的committee里面的Validator都需要对上一个Epoch进行投票签名，确保自己认可了上一个Epoch里面的交易。
- Validator（验证者）：由于以太坊The Merge以后共识算法切换为了POS，原来的矿工被Validator取代，Validator通过质押32ETH资产成为Validator，负责参与各个Epoch内slot的出块和签名工作。
- Proposer（提议者）：
  Proposer来自committee中的Validator，通过RANDAO产生的随机数选出，被选用于Slot区块的打包。
- Beacon chain（信标链）：用于替代PoW共识的PoS区块链，beacon chain node被用来挂载Data
  Blobs的交易类型，为Rollup提供更多的存储空间。

2.2 流程

Epoch开始的时候，通过RANDAO为每一个Slot（时隙）分配一个Committee（验证者委员会）对上一个Epoch进行Attestation（签名投票）。

为当前Epoch的32个Slot分配多个Aggregator将committee对上一个Epoch的Attestation聚合以后记录进Slot区块里。

RANDAO通过生成随机数确定Proposer负责出块。

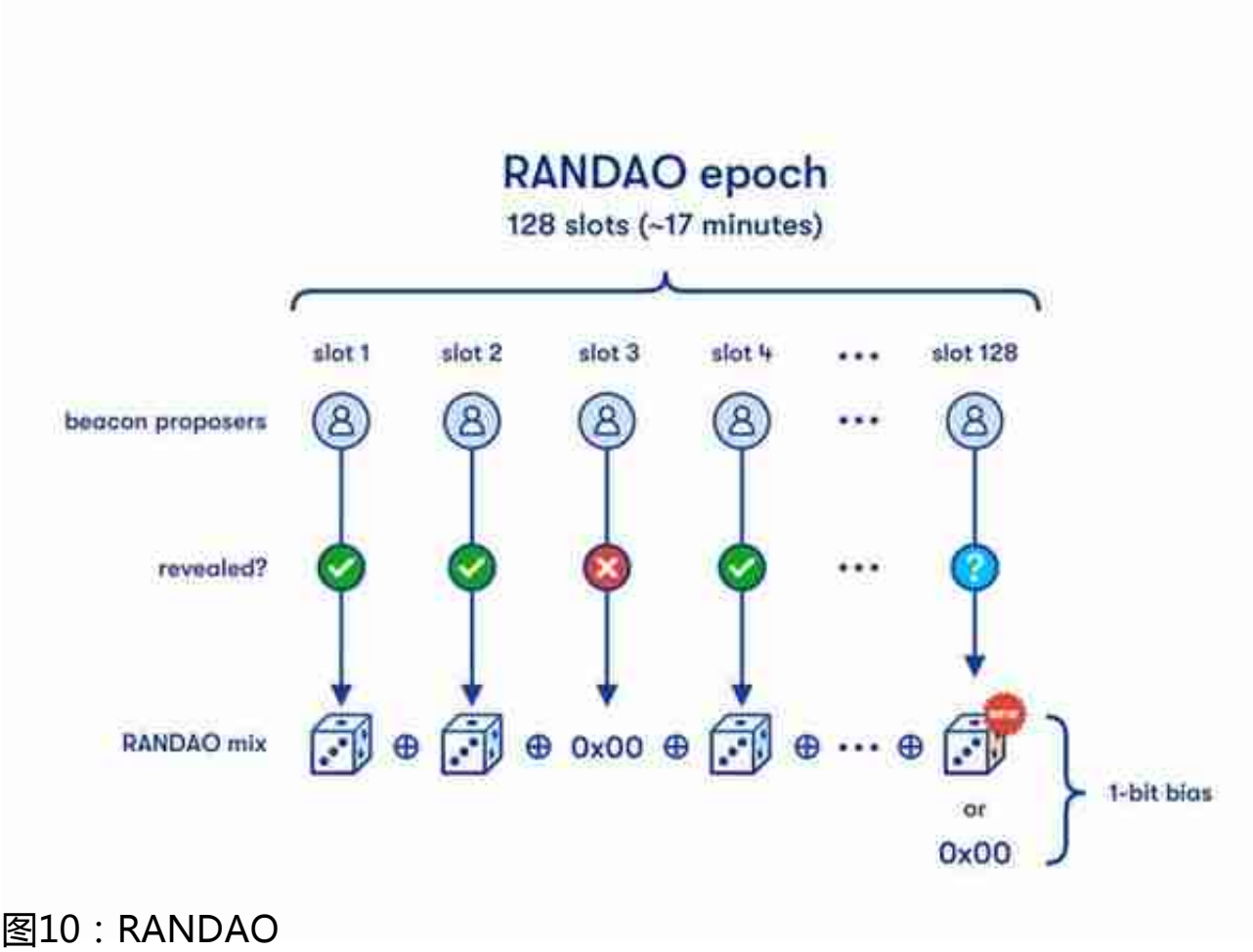

图10：RANDAO

2.4 Latest Message Driven GHOST（LMD-GHOST，由最新消息驱动的GHOST）

在以太坊新的POS共识机制中使用LMD-GHOST作为分叉选择规则，当发生分叉的时候，GHOST会选择获得更多消息支持的子树。其背后的理念是在计算链头时，只考虑每个验证者最近的投票，而不是过去产生的任何投票，以此降低运行GHOST所需的计算量。

想要深入学习的可以查阅：https://eprint.iacr.org/2013/881.pdf

2.5 随之而来的问题

- 通信与验证成本增加：
  是不是验证者越多越好呢？其实不然，虽然验证者的数量增多有利于数据可用性采样（DAS）和去中心化，但是验证者增多意味着单个Slot的验证者也会变多，在收集各个验证者签名的时候就会增加Aggregator和验证者之间的通信负担，除此之外，聚合签名的验证成本也会增大，这无形中会增加验证者节点的负担。
- 长程攻击：
  长程攻击是指某个验证者在Withdraw质押在信标链上的ETH后，他可以利用旧私钥在某个曾经签署过的区块进行恶意分叉，因为此时其在链上已无任何质押资产，然后迅速产生空块至目前的区块高度，对网络进行攻击。这也是未来可能出现的攻击方式。以太坊在设计的时候是对Pre-Epoch的checkpoint（检查点）进行投票，其设计思路也就是将初始状态不断往前推进，避免可能出现的攻击。

三：以太坊质押挖矿

3.1 Staking

质押门槛：验证者为了履行职责参与共识出块需要质押32ETH作为保证金资产。

验证者的职责：在协议规定的时间生产区块和attestation。

3.1.1 Staking方式

- Solo Staking：solo staking的方式是由想要自己出资32个ETH做验证者的质押人自己在云服务器上运行验证者节点，除了选择在云服务器上面运行节点，也可以选择在自己家中摆放服务器设备运行以太坊节点，区别在于云服务之上运行节点更加稳定，在参与网络共识的时候可以避免和减少因为停电和网络原因造成的怠工惩罚，而在家自己搭建节点的优势在于硬件和网络服务的成本低于云服务器，这里质押人可以自行选择采用哪种托管方案。
- Staking
  Pool：
  由于32个ETH对于普通人来说是一笔不菲的资金，寻常小资金的质押者想

要参与网络共识却没办法自己运行节点，于是出现了质押池解决方案，其中以许可型的半去中心化质押解决方案Lido为主要项目，其吸收了较大的资金体量，成为赛道内的头部解决方案，其次还有去中心化程度更高一些的解决方案如Rocket Pool和Swell等，在现有的质押池解决方案之上，还产生了Unamano这样的聚合解决方案来帮助和发展以太坊Staking领域。

- 在节点运营方面，Lido选择指定部分专业的运营商来运行网络节点，这也是其相对中心化的一点，运营商掌握签名私钥，用户的资产部分信赖Lido和运营商，至于提款私钥，2021年7月之前，提款地址是一个6/11的多签地址，多签私钥由行业内OG保管，2021年7月之后，提款地址指向一个可升级的合约地址，该合约由DAO进行管理。Rocket Pool在节点方面选择更加去中心化，任何人只需要提供16个ETH和相应的软硬件设备就可以作为运营商运行节点，虽然降低了运营商门槛，但是Rocket Pool引入$RPL质押来降低运营商作恶的风险。
- Staking Pool的方案使得普通的用户可以将小额的ETH存入合约来获得以太坊的挖矿奖励，同时返还生息代币如stETH和rETH来释放质押资产的流动性，进一步增强了以太坊的去中心化程度和资金使用效率，是社区最为看好的方向。
- CEX，中心化托管机构：除了Solo Staking和Staking Pool,中心化的交易所和一众资管机构都是以太坊质押的主要参与者，例如Coinbase和币安等也都推出了自己的质押服务，通过吸收小额的ETH来参与低风险的以太坊质押挖矿。三种方案在去中心化程度和安全性方面都各有优劣，这取决于质押者的信任对象，但是无可置疑的是，三种方案都捕获到了相应的资金和用户，共同维护着以太坊的安全和去中心化。

3.1.2 风险与隐患

是否合并以后真的就万事大吉？我觉得未必，从下图的数据我们可以窥探一下解除信标链提款限制以后的局面。

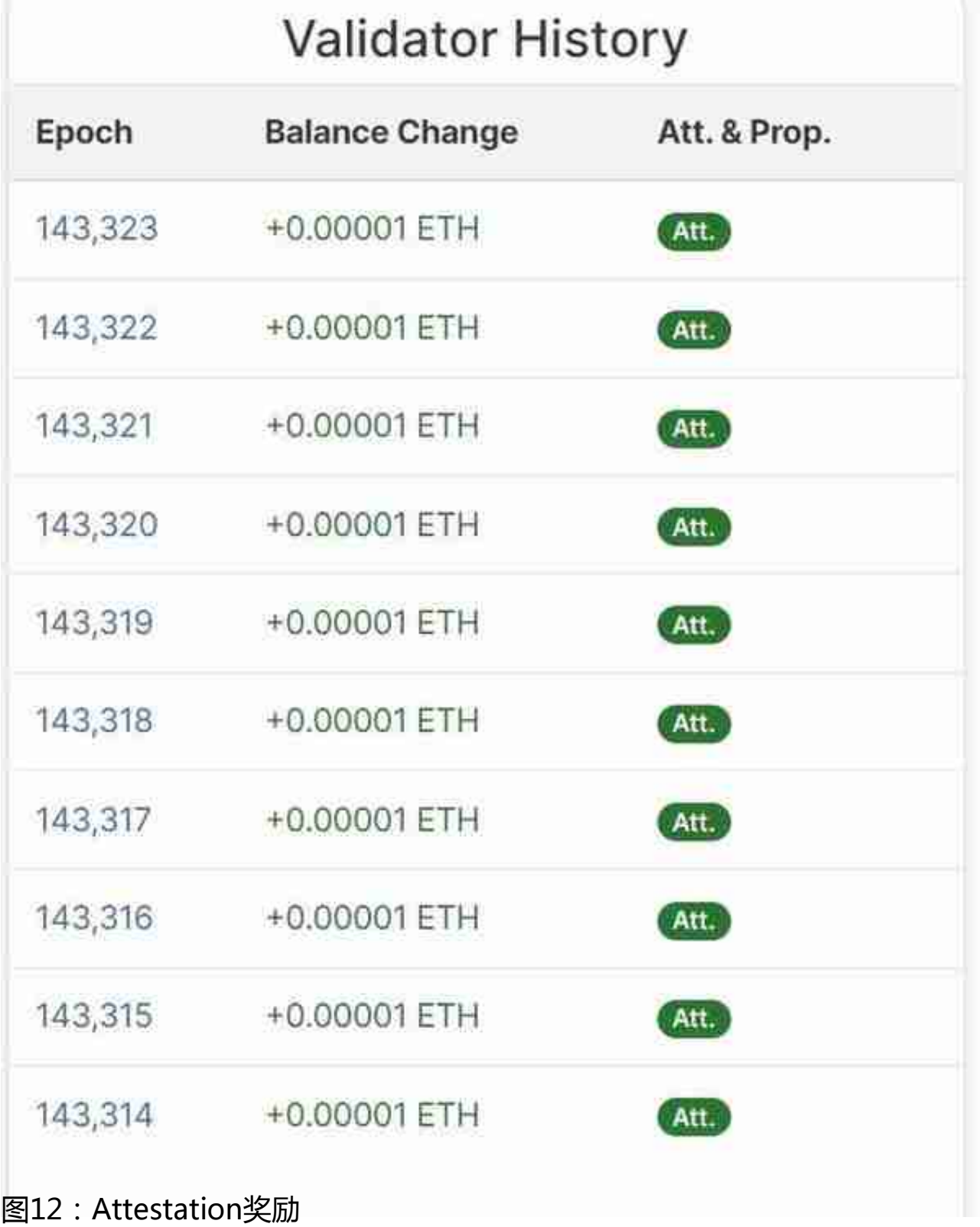

图12：Attestation奖励

- 出块奖励：
  每一个Slot会有一个Validator作为proposer来打包区块，被选为proposer的Validator可以获得出块奖励。（概率低，奖励多）

图14：合并后MEV情况

3.1.4 惩罚类型

- 怠工惩罚：
  未能按照共识预期产生出块：未在预期时间对区块进行Attestation。
- 恶意行为导致slash（罚没）：
  在单个Slot内生产两个区块或者进行两次Attestation；违反Casper FFG共识规则提议错误区块。

3.2 私钥类型

- 签名私钥：
  签名私钥用于验证者在履行职责时的消息签署，包括attesting和proposing blocks，每6.4min，即每个Epoch，该密钥将被使用一次。
- 提款私钥：
  提取质押资产和出块奖励时使用的密钥，需要离线存储，在上海分叉以后，可用提款私钥提取质押的ETH和奖励。

3.3 ETH2质押风险

- 私钥被盗：ETH2的签名/提款私钥被盗。

- 单点故障/验证者的有效性：
  目前，验证人以单一的机器或节点存在并履行其职责。协议严格的规则禁止常见的冗余形式，如在多个节点上运行同一个验证人，这样做可能会导致验证人被
  “惩罚”（slashed）。如果使用质押服务，密钥位于一个云服务器上（如AWS）。如果任何组件出了问题，验证人就会停止验证，从而受到惩罚。

四：分布式验证者技术（DVT）

在质押层面，虽然我们有去中心化的质押解决方案来降低质押门槛和提高质押服务的去中心化，但是在Validator层面，依然存在着单点风险，现在单个验证者运行着网络的多个客户端，如果因为网络原因或者是断电等物理因素会造成怠工惩罚，slot也无法收集到有效的签名，我们无法通过冗余的方式在多个地方运行同一个验证者节点，因为这会造成签名的混乱，会被认为是对网络的攻击，但是我们可以将签名私钥拆分
，通过DVT技术来降低单点故障的风险，在实施升级的时候，也为节点提供了升级空间，并不会因为网络升级导
致节点的大面积掉线，具体分析，请让我们往下探究！

4.1 概念

- operator：运行一个（或多个）节点的个人或实体。
- operator
  node：
  指的是一个硬件和软件，执行以太坊验证者的任务。这些任务可以由节点单独完成，也可以与其他使用DVT工具的节点联合完成。
- 分布式验证者技术：
  分布式验证者技术是一种将单个以太坊验证者的工作分配给一组分散节点的技术。相比验证者客户端在单台机器上运行，分布式验证者技术能够提供更加安全和去中心化的服务。

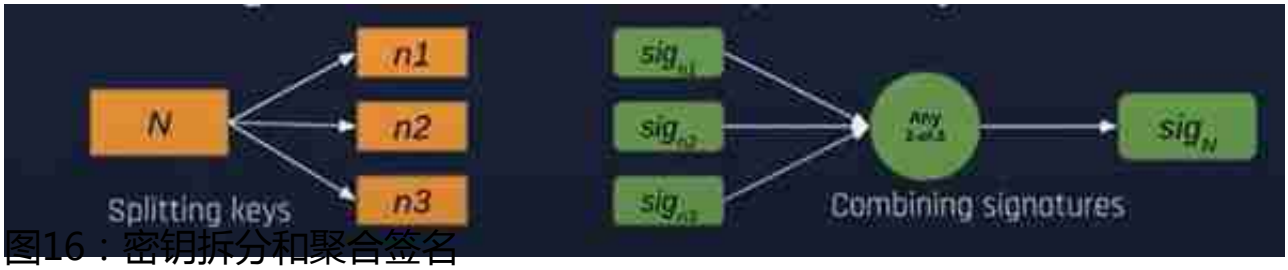

图16：密钥拆分和聚合签名

- 节点宕机

1. Crash Faults：
2. 原因：因为停电，断网，硬件故障，软件错误导致的崩溃；
3. 防范措施：通过在多个地方运行同一个节点的冗余备份方案来防范节点掉线；
4. Byzantine Faults：
5. 原因：由软件bugs，网络攻击导致；
6. 防范措施：多个参与节点通过共识决定，单个节点无法做出决定。

4.4 总体架构

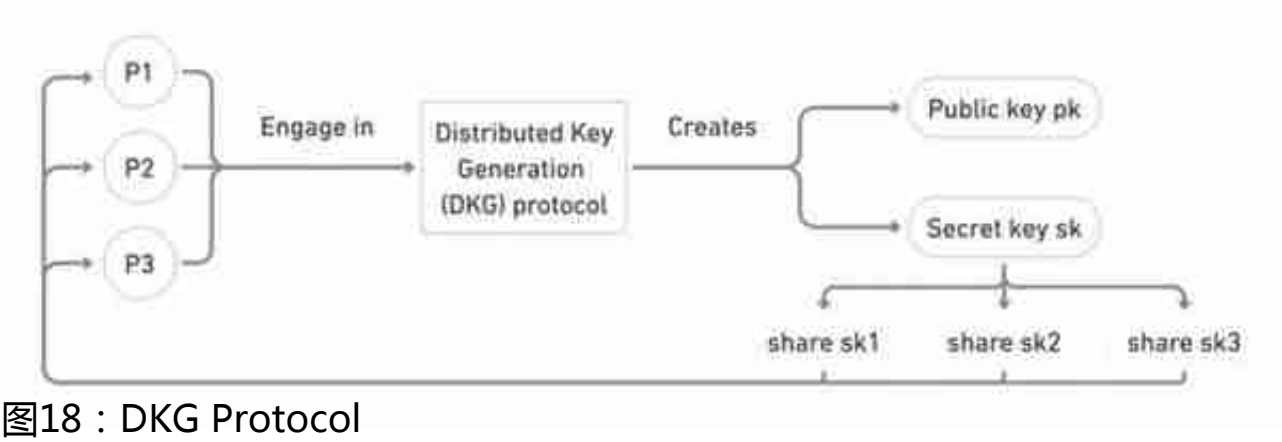

图18：DKG Protocol

4.6 Threshold Signature Schemes (TSS)（阈值签名方案）

当验证者对区块达成一致需要签名时，采用BLS阈值签名方案来实现签名。其允许N个验证者共同签名数据，并且在t+1（0

五：从主流项目看DVT

5.1 SSV

表面上看，SSV提供了稳健的、去中心化的进入以太坊质押（Staking）生态系统的途径。再深入一点，SSV是一个复杂的、配有共识层的多签钱包，SSV在信标链节点和验证者客户端之间充当缓冲器的作用。

5.1.1 配置的主要组成部分

- Distributed Key Generation：

operator通过运行SSV程序计算生成了一个共享的公私钥集。每个operator只拥有私钥的单一部分，确保没有一个运营商可以影响或控制整个私钥做出单方面的决定。

- Shamir Secret Sharing：
  这个机制被用于使用预先定义的KeyShares阈值重构验证者密钥，单个的KeyShared不能被用于签署消息。SSV能够利用BLS技术聚合签名，创建验证者的完整密钥签名。通过结合Shamir和BLS，验证者的签名私钥被切片共享，并在需要签名时聚合重组。
- Multi-Party Computation：将安全的多方计算（MPC）应用于secret sharing，允许SSV的KeyShares安全地分布在operators之间，以及执行验证者职责的分散计算，而无需在单个设备上重建验证者密钥。
- Istanbul Byzantine Fault Tolerance Consensus：
  将这一切联系起来的是SSV的共识层，基于伊斯坦布尔拜占庭容错（IBFT）算法。该算法随机选择一个验证者节点（KeyShare），负责区块提议并与其他参与者分享信息。一旦预定的KeyShares阈值认为该区块是有效的，它就被添加到链上。因此，即使一些operators（达到阈值）有问题或目前不在线，也可以达成共识。

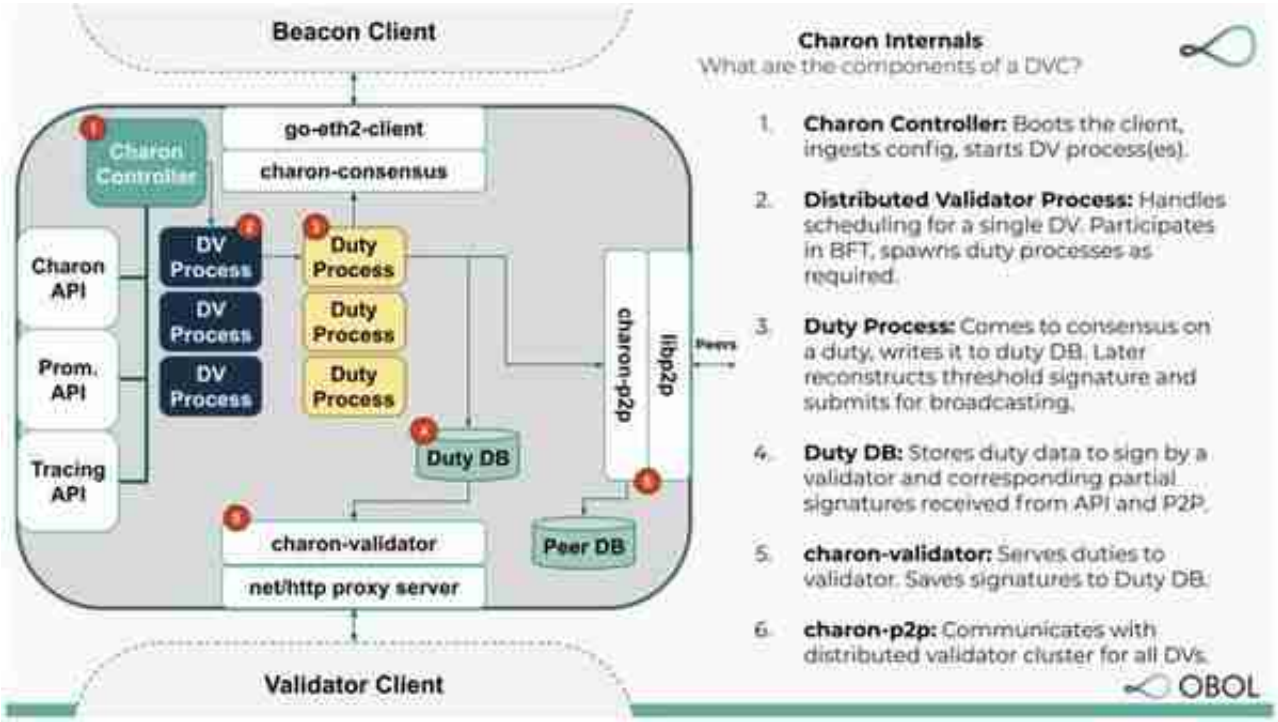

图20：Charon内部架构

- Obol Managers：一组用于形成分布式验证器的可靠智能合约

- Obol
  Testnets：
  一组正在进行的公共激励测试网，使任何规模的运营商都可以在为Obol主网网络服务之前测试他们的部署。

5.2.2 关键概念：

- Distributed
  Validator：
  分布式验证器是运行在多个节点/机器上的以太坊权益证明验证器。使用分布式验证器技术 (DVT) 可以实现此功能。分布式验证者技术避免了单点故障的问题，如果DVT集群中
- Distributed Validator
  Node：
  分布式验证器节点是operator需要配置和运行以履行分布式验证器operator职责的一组客户端。operator可以在同一硬件上运行冗余的执行和共识客户端，运行执行层中继器（如mev-boost），其他检测服务，以确保最佳的性能。在上述例子中，客户端堆栈包括Geth，Lighthouse，Charon和Teku。

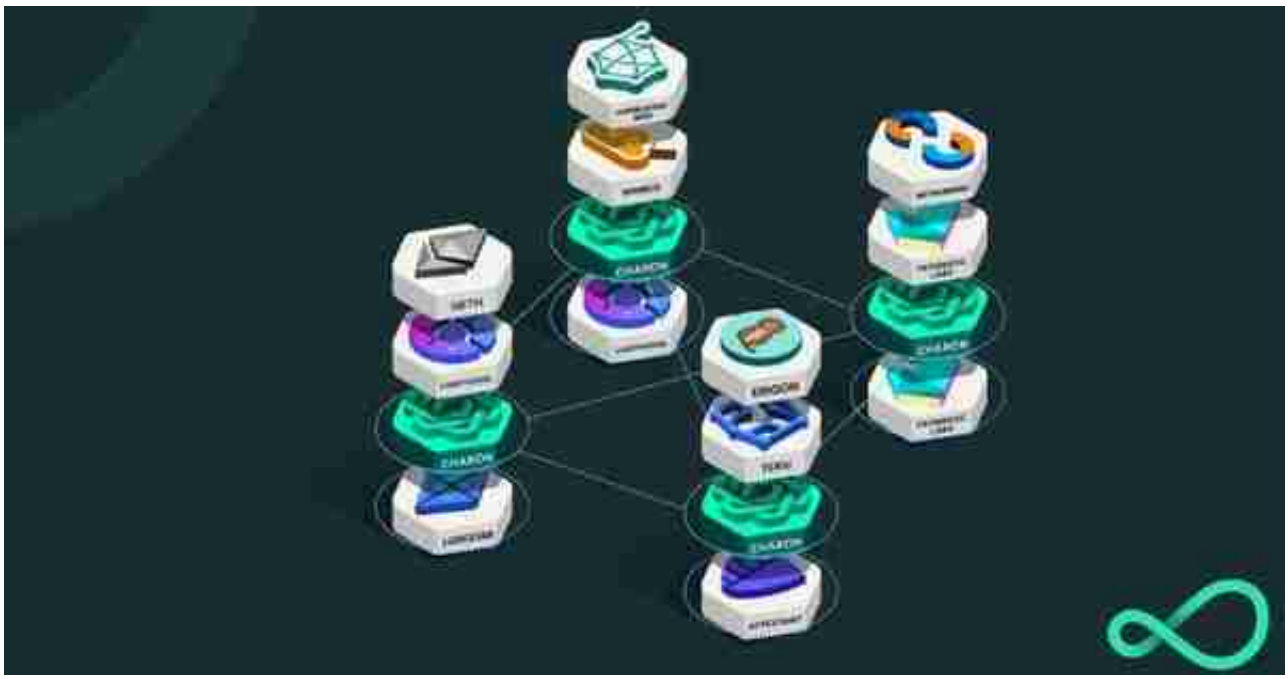

图22：Obol的DVT网络拓扑

- Distributed Validator Key：Distributed Validator
  Key是一组BLS私钥，它们共同作为参与权益证明共识的阈值密钥。

- Distributed Validator Key Share：分布式验证者私钥的一份私钥。
- Distributed Validator Key Generation Ceremony：
  为了在分布式验证器中实现容错，各个私钥份额需要一起生成。与其让受信任的经销商产生私钥，将其分割并分发，不如让分布式验证器集群中的每个操作员参与所谓的分布式密钥生成仪式，这样做的好处是在任何时候都不会构建完整的私钥。分布式验证器密钥生成仪式是DKG仪式的一种类型。仪式产生签名的验证器存放和退出数据，以及所有的验证器密钥份额和它们相关的元数据。

六：总结与展望

6.1 总结

行文通篇，从The Merge开始叙述，讲述合并以后以太坊采用的Casper FFG算法，熟悉了合并以后区块的产生方式以及新的一些技术概念，随后讲到了以太坊新的挖矿方式以及目前存在的Staking方案，了解到验证者存在的单点故障问题，随后又深入到DVT技术，并通过两个项目的案例简述DVT如何解决了这个问题，整篇文章按照去中心化的思路叙述，为读者了解以太坊的共识算法和去中心化发展方向提供了一定的参考。

6.2 展望

以太坊在The Merge以后，将会逐步实现Danksharding，首先通过EIP-4488降低calldata的gas花销，从16gwei降低到3gwei，为rollup的提速扩容进行强有力的支持，之后一步是在Proto-danksharding中引入Blobs的交易类型，使得以太坊能够为rollup提供更多的存储空间，降低D/A的成本，并逐渐实现Danksharding。

要实现Danksharding中描述的数据可用性采样（DAS）、区块提议者/构建者分离（PBS）等设想，必须要确保以太坊网络的节点足够多，足够去中心化，数据可用性采样才能实施，也就是说要确保扩容和低成本的D/A，以太坊的去中心化是最为重要的一环，因为去中心化的质押方案和DVT等技术对以太坊后续的发展至关重要。

责编：Lynn