以太坊协议技术升级前景解析（1）：The Merge

撰文：Ebunker

今年 10 月份以来，以太坊联合创始人 Vitalik Buterin 发布了一系列关于以太坊协议未来可能性的文章，内容涵盖了以太坊发展路线图的六个部分：The Merge、The Surge、The Scourge、The Verge、The Purge 和 The Splurge。本文将解读路线图的第一部分（The Merge），探讨 PoS 权益证明还有哪些技术设计可以改进，以及实现这些改进的途径。

Vitalik 认为，「合并」是指以太坊协议自推出以来历史上最重要的事件：从 PoW 工作量证明到 PoS 权益证明的过渡。如今，以太坊成为一个稳定运行的 PoS 系统已经接近两年了，这种权益证明在稳定性、性能和避免中心化风险方面表现非常出色。然而，权益证明仍有一些重要领域需要改进。

以太坊 2023 年的路线图将其分为几部分：改进技术特性（例如稳定性、性能和对较小验证者的可访问性），以及经济变化以应对中心化风险。根据 Vitalik 的说法，本文并不是对权益证明进行改进的详尽清单，而更多的是正在积极考虑的想法。

#### 合并的主要目标如下：

1.单时隙确定性（SSF）：通常以太坊区块大约需要 15 分钟才能最终确定。 然而，可以通过提高以太坊的共识机制验证区块的效率，大幅减少最终确定所需的时间。 区块可以在同一时隙内提议并最终确定，无需等待 15分钟。

2.以最快速度确认和完成交易，同时保持去中心化

3.提高单独质押者的质押可行性

4.提高稳健性

5.提高以太坊对 51% 攻击的抵抗和恢复的能力（包括最终性逆转、最终性阻止和审查）

## 单时隙确定性和质押民主化

目前，需要 2–3 个 epoch（约 15 分钟）才能完成一个区块，并且需要 32 ETH 才能成为质押者。这最初是为了在三个目标之间取得平衡而做出的妥协：

使参与质押的验证者数量最大化（使质押所需 ETH 最小化）；

使最终性时间最小化；

使运行节点开销最小化。

这三个目标是相互冲突的：为了实现经济最终性（即攻击者需要销毁大量 ETH 才能恢复最终确定的区块），每次最终确定时，每个验证者都需要签署两条消息。因此，如果验证者数量很多，要么需要很长时间来处理所有签名，要么需要非常强大的节点来同时处理所有签名。



这一切都取决于以太坊的一个关键目标：确保即使成功的攻击也会给攻击者带来高昂的成本。这就是「经济最终性」一词的含义。

也有反例，不具备「经济最终性」的区块链（例如 Algorand）的做法是通过随机选择一个委员会来最终确定每个时隙来解决这个问题。但该方法的问题在于，如果攻击者确实控制了 51% 的验证者，攻击成本极低：只有委员会中的部分节点会被检测为参与攻击并受到惩罚。这意味着攻击者可以多次反复攻击该链。

因此，如果以太坊想要实现经济最终性，那么基于委员会的简单方法是行不通的，而是需要全套验证者的参与。

理想情况下，以太坊希望在保留经济最终性的同时在两个方面改善现状：

1.在一个时隙（slot）内终结区块（理想情况下，保持甚至减少当前 12 秒的长度），而非 15 分钟

2.允许验证者用 1 ETH 进行质押（从 32 ETH 降至 1ETH）

第一点可以确保所有以太坊用户都能从通过最终性机制实现的更高级别的安全保障中受益。如今，大多数用户都无法享受这种保障，因为他们不愿意等待 15 分钟；而通过单时隙确定性机制，用户几乎可以在交易确认后立即看到交易最终确定。其次，如果用户和应用程序不必担心链回滚的可能性，那么它就简化了协议和周围的基础设施。

第二点是为了支持单独质押者。根据多次的民意调查，阻止单独质押的主要因素是 32 ETH 的最低限额。将最低限额降低到 1 ETH 将解决这个问题。

目前存在一个挑战：更快的确定性和更民主化的质押目标都与最小化开销的目标相冲突。事实上，这个事实就是以太坊一开始不采用单时隙确定性的原因。然而，最近的研究提出了一些解决这个问题的可能方法。

工作原理：

单时隙确定性涉及使用在一个 slot 内最终确定区块的共识算法。这本身并不是一个难以实现的目标，许多算法（例如 Tendermint 共识）已经实现了这一点。

以太坊独有的一个理想属性是（即 inactivity leaks）：即使超过 1/3 的验证者离线，该属性也允许区块链继续运行并最终恢复。



## 单时隙确定性提案

对于如何使单时隙确定性在验证者数量非常高的情况下发挥作用，而不会导致极高的节点运营商开销这个问题，有几种领先的解决方案：

选项一是暴力破解，实现更好的签名聚合协议，可能会使用 ZK-SNARKs，这将使处理单时隙中数百万个验证者的签名成为可能。例如，Horn 是为了设计更好的聚合协议而提出的提案之一。

选项二是 Orbit 委员会，这是一种新机制，允许随机选取的中型委员会来负责链的最终确定性，但是需要保留攻击成本特性。Orbit 利用验证者存款规模中预先存在的异质性，获得尽可能大的经济最终性，同时仍将给予小型验证者与其匹配的角色。

如下图所示，在从范围 x=0（Algorand 委员会，没有经济最终确定性）到 x=1（以太坊的现状）之间 — — Orbit SSF开辟了中间地带：

1.其中作恶成本仍然很高，用以确保极其安全；

2.但与此同时，仅需中等规模的随机验证者样本参与每个时隙，减轻节点负担。



选项三是双层质押，一种有两类质押者的机制，一类质押者有较高的存款要求，另一类质押者有较低的存款要求。只有存款要求较高的层级会直接参与到提供经济最终性的过程中。至于低层级存款应有哪些权责，已有各类提案提出，包括：

将权益委托质押给更高级的权益持有者的权利；

随机抽取低层级质押者来证明并最终确定每个区块；

生成纳入列表的权利等。

对于以太坊的安全体验和质押中心化属性而言，每一种解决方案都有其优缺点和需要权衡的地方：暴力破解虽然可以解决问题，但需要在很短的时间内聚合大量签名，技术难度极高；Orbit 委员会需要验证其安全性和特性，并进行正式化和实施；双层质押机制则面临着中心化风险，风险在很大程度上取决于低质押层获得的具体权利。

除了单时隙确定性，单一秘密领袖选举也是以太坊权益证明系统中的一个重要问题。如今，哪个验证者将提出下一个区块是可以提前知道的，这会产生一个安全漏洞，攻击者可以监视网络，确定哪些验证者对应哪些 IP 地址，并在验证者即将提出区块时对其发起 DoS攻击。

解决这个问题的最佳方法是隐藏哪个验证者将生成下一个区块的信息，至少在区块实际生成之前要隐藏这些信息。

## 单一秘密领袖选举

目前，哪个验证者将提出下一个区块是可以提前知道的，这会产生一个安全漏洞：攻击者可以监视网络，确定哪些验证者对应哪些 IP 地址，并在验证者即将提出区块时对其发起 DoS攻击。

单一秘密领袖选举协议通过使用一些加密技术为每个验证者创建一个「盲」验证者 ID ，然后让许多提议者有机会对盲 ID 池进行改组和重新盲化，从而解决这个问题。



然而，实现一个足够简单的单一秘密领袖选举协议并非易事。

以太坊协议的简易性至关重要，不希望进一步增加其复杂性。使用环签名的简化 SSLE （Simplified SSLE using ring signatures）仅用了数百行规范代码，并在复杂的加密中引入了新的假设。

如何实现足够有效的抗量子 SSLE 也是一个问题。最终可能会出现这样的情况：只有当我们出于其他原因大胆尝试并在 L1 的以太坊协议中引入执行通用零知识证明的机制时，SSLE 的「边际额外复杂性」才会下降到足够低的水平。

另外，更快的交易确认也是以太坊权益证明系统需要解决的问题之一。

进一步缩短以太坊的交易确认时间（从 12 秒缩短到 4 秒）是有价值的。这样做将显著改善 L1 和基于 rollups 的用户体验，同时使 DeFi 协议更加高效。它还将使 L2 更去中心化，因为它将允许大量 L2 应用程序在 rollups 上运作，从而减少 L2 构建自己的基于委员会的去中心化排序的需求。

大致有两种技术：减少时隙（slot）时间，降至 8 秒或 4 秒；允许提议者在单时隙期间发布预确认。然而，目前还不清楚缩短时隙时间的可行性。

即使在今天，世界上许多地区的质押者也很难以足够快的速度获得证明。4 秒 slot 时间的尝试有验证者集中心化的风险，而且由于延迟，在少数具备地理优越性的地区之外成为验证者是不切实际的。

提议者预确认方法的弱点在于，它可以大大改善平均情况下的纳入时间，但不能改善最坏情况。此外，还有一个待解决的问题，即如何激励预确认。



面对未来可能的量子计算威胁，以太坊需要积极开发抗量子攻击替代方案。当前依赖于椭圆曲线的每个以太坊协议部分都需要有一些基于哈希或其他抗量子的替代方案。这证明了在围绕权益证明设计的性能假设中的保守主义是合理的，也是更积极地开发抗量子攻击替代方案的原因。

## 小结

以太坊权益证明系统在技术演进的道路上充满挑战。由于以太坊单独质押门槛较高， 以 Lido 为首的质押服务供应商们已成为以太坊节点质押的首选，双层质押方案也具有一定程度的中心化风险。为了应对这些挑战，单时隙最终确定性及质押民主化、单一秘密领袖选举、更快的交易确认以及抗量子攻击替代方案的开发，都是以太坊需要处理的重要问题。

Vitalik 对「The Merge」升级进行了全面的思考，并提出了尽可能多的技术解决组合方案，对以太坊 PoS 权益证明技术的设计潜力，以及当下潜在可行的技术升级路径进行了讨论。

在技术升级的过程中，以太坊仍然在努力不断探索和创新，在不同的技术方案之间进行权衡和选择，以找到最适合的发展路径，实现更高的安全性、性能和去中心化程度。