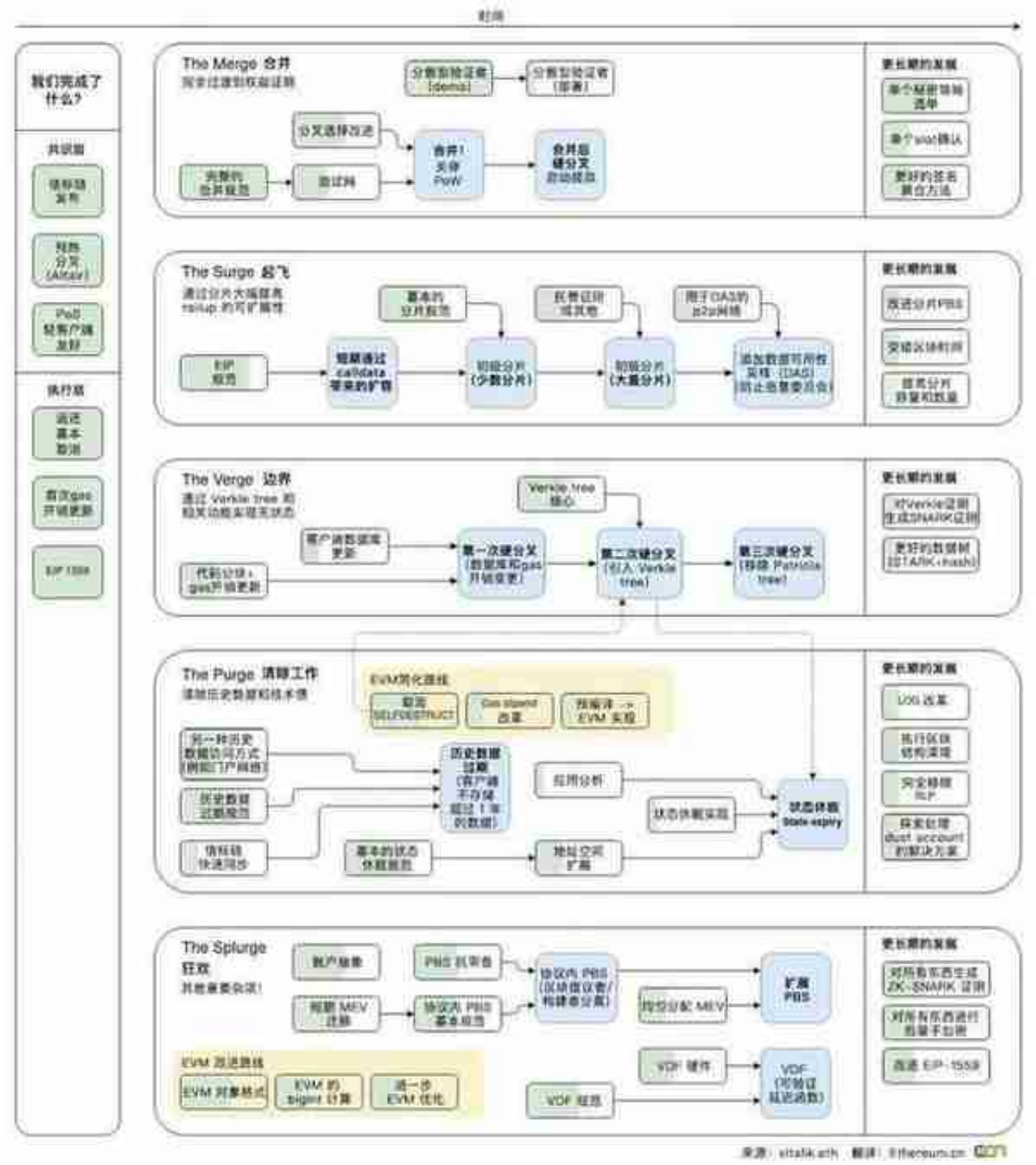

以太坊协议开发路线图

关于以太坊的 PoS 设计，有一些有趣的东西经常被忽视：二次方惩罚。单个验证者节点宕机、出问题或直接攻击网络并不会受到很严重的惩罚。而如果一千个验证者同时这样做则会受到更严重的惩罚。

也就是说，如果你是一个运营着数千个验证者节点的大型机构，为了你自己的利益

着想，你最好将它们分散开来，避免使用云托管，并使用不同的客户端等等。当然，资产还是集中化的，但至少故障点是分散的，这有利于网络的整体健康状况。

一些大型的挖矿实体依赖于某个中心位置以摊销成本，当局可以根据能源使用情况监测到具体位置，并且可以关停它们。在全世界范围内转移挖矿设备是很难的，但是质押仅依赖于私钥/公钥和消费级的计算机。

PoS 实际上是让「有钱的更有钱」

是的。不幸的是，我们生活在一个财富极度不平等的世界。区块链并不能解决这个问题。

这对 PoW 来说也是如此。谁有钱就可以购买更多的矿机，赚更多的钱。除了挖矿，投资回报率也会受规模经济效应影响：集中化的挖矿业有大笔资金以一定的折扣率购买硬件，并搬到电费便宜的地方运作。个人矿工在现实中根本无法与其竞争。而在 PoS 中，无论他们的质押金额是 10 美元还是 1000
万美元，每个人都能按比例获得相同的收益率。

"这些大型挖矿业可能是中心化的没错，但他们没有理由攻击网络，因为他们在基础设施上投了数百万美元……」。所以你的意思是，你对大型中心化运营者的存在没有意见，只要他们在网络中占有某种程度大的份额吗？

这是你存款的被动利息？凭空印钞票？这不就像中央银行增发法币一样吗

你得延伸来说才能得出这样的观点，但我已经看到人们这样做了
(笑)。这些观点通常从「PoS 并不是什么新鲜事」开始。

验证者还是有在进行一些「工作」的：创建区块和验证其他区块。只是这些工作完全由实际有用的工作组成 (区块链需要达成共识)，而不是一遍又一遍地计算哈希值，直到其中一个满足任意的要求。

这并不是真的「凭空印出的免费钱」，质押资产中仍然涉及成本，只是与能源账单相比，它们更抽象、更不直观而已。

机会成本——如果另一项投资能给你带来更高的收益率，为什么还要质押？

流动性差——从你存款的那一刻起，你的资金就被锁定了，排队等待你的验证者激活，然后当你提款时，又要排队才能提出。

固有风险——质押仍然是一个相当新的东西，过程中可能会出问题。可能会出现一个关键错误，网络可能会受到攻击，你的质押硬件可能会损坏等等。

波动性——毕竟它仍然是一种不稳定的资产，如果你是那种以本国法币计价的投资者，那么当资产一夜之间可能下跌 30%，而收益率可能只有 5%
时，这并没有很吸引人 (不过，一旦资产翻倍了，5% 的收益率是非常不错的，将 100% 的收益变成 110%)。

维护成本——你仍然需要维护你的验证者节点并保证其安全性，确保 100%
的正常运行时间，更新软件，等等。

这里有个有趣的地方：质押者越多，个人获得的质押奖励就越低。这基本上意味着，上文所罗列的所有成本将由市场本身来定价。原因很简单：如果质押收益率太低，获得的奖励不够维护成本，那么人们就会退出质押并投资于其他地方。质押的人少了，收益率重新回升。同样，如果收益率太高，也会吸引更多的资本加入，收益率又降落下来。

至于通胀情况：假设市场整体来说，理想收益率是 5%，其中 3% 来自 Token
增发。这样算下来，每年大约有 3000 万枚 ETH 质押、增发 90 万
ETH。在总供应量为 1.2 亿枚 ETH 的情况下，通货膨胀率为 0.75%。只要 gas 费至少有 23 gwei，通胀率就低于 EIP159 的带来的 ETH
销毁率。(这点我再强调也不为过：以太坊很快就会成为一种有收益的通缩资产)

「算数不错，但没有供应上限，而且他们总是改变货币政策」

多年来，目标一直是 "在确保网络安全下，实现最低可行发行量"，相比于设定一个任意的供应上限，以太坊优先考虑网络的安全性。

至于货币政策的改变，没有一个更新是提高通胀率的。从第一天起，低通胀率 (尤其是通缩) 就是社区的目标。

一旦 EIP-1559 的销毁率与发行率相匹配，就会出现一个作为有效供应上限的平衡点——再次由市场力量对以太坊区块空间估值来决定。

所以，不存在一个「以太坊中央银行」这样的东西任意调整通胀/通缩率并向亲信印钱。市场本身决定通胀/通缩情况，没有一个实体可以像中央银行控制法定货币的通货膨胀率那样控制它。

巨鲸拥有足够多的资金控制和改变规则，并罚没诚实的验证者

不存在这样的风险，以太坊没有任何形式的链上治理，就是因为这个。协议的更新是社区共同努力的结果 (Layer 0)，你不需要质押任何资产来报告一些不好的注意并参与这个过程。

这方面完全与 PoW 一样：即便你拥有 99% 的算力，你也不能在没有私钥的情况下进行无效的交易，窃取他人的资产或者改变协议规则。除了重组区块之外，无法真的做什么。1% 的诚实节点将拒绝任何不遵守规则的区块，那么作恶者就会在一条无效/无用的链上挖矿。PoS 共识下也是如此，现在只是把「算力/挖矿」换成「质押权重/质押」(不同的是，重组区块的作恶者被发现了会被罚没掉所有质押资产，然而区块链不能完全摧毁挖矿的设备)。

简单地说，链上涉及到大量的 ETH。目前已超过 1000 万 ETH，而且是在合并之前。按照目前的价格，大约是 300 亿美元。「质押的 ETH 数量」和「ETH 的价值」预计都会上升，所以攻击变得越来越不可能，因为发起一次攻击的经济成本太高。而且如果攻击者来自以太坊之外，首先要获得这么多 ETH 是很荒谬的 (你在哪里买到 1000 万枚 ETH 来达到 51% 的质押占比？又或者 2000 万？)

32 枚 ETH 太多了，一般人没那么多钱

我同意这是一个很大的问题。这里有一些降低质押门槛的提议 (更好的签名聚合或设定活跃验证者上限和轮值机制)，但它们目前的优先级别似乎并不高，更重要的是确保基础层可以很安全。

之所以需要那么高的 ETH 质押数量，是因为这个数值需要刚好满足一个技术点。简而言之，需要低到一个点让大家可以参与，并有足够的验证者来保证区块链的安全；但又要足够高，以免有太多的验证者，使区块链的开销过大。并且每个验证者节点的质押数量相同，这样每个验证者在分布式随机过程中决定谁生产区块时拥有完全相同的权重，减少了很多复杂性。

从技术角度来看，得出 32 个 ETH 这个门槛涉及大量的数学计算，当时 32 个 ETH 价值约 7000 美元。早期于 2017 年的数学推算甚至建议最低超过 1000 ETH。

值得庆幸的是，就像 PoW 中矿池，PoS 也有质押池以允许质押小数额的 ETH。这并不一定与「不是你的私钥，不是你的 Token 」的口号相悖，这要感谢像 RocketPool、Secret Shared Validators "秘密共享验证者" (尚未推出) 这样的方案，它们利用智能合约来实现无需许可、去中心化和非托管。而且由于上面提到的二次方惩罚，我相信从长远来看，去中心化质押会由于中心化质押方案。我推荐大家阅读 superphiz 的质押指南以获取更多信息。如果你重视去中心化，通过交易

平台参与质押是非常糟糕的。

与上文相关，我们最好将 Rocket Pool 这样的方案看作是基础质押的一种更高层次的抽象，而不只是一个「质押池」。我在这里写了更多相关细节，供感兴趣的人参考。

PoS 还未被证明是否行得通，但我们知道 PoW 是有效的

这论点实际上完全合理，显然我们没法真的反驳这个说法。只有时间会告诉我们。我只是认为，在以太坊正在切换为 PoS，并且一直以来都决定切换的背景下，这个论点是不相关的。如果你不相信它，就不要参与/投资它。我个人相信一个长期可持续的 PoS 以太坊。

这些都是我们人生中伟大的加密货币实验的一部分。要么它只是昙花一现，并且最终以失败告终以至于最后无人知晓，这将是一个遗憾；又或者我们将成功地创造出能够长存于人类文明的强大网络。为了实现这一目标，优先考虑去中心化是关键。我主要在比特币和以太坊中看到去中心化这种东西，尽管它们的理念大不相同。这就是为什么长期来说，我很乐意地看到这两者最终会如何发展。