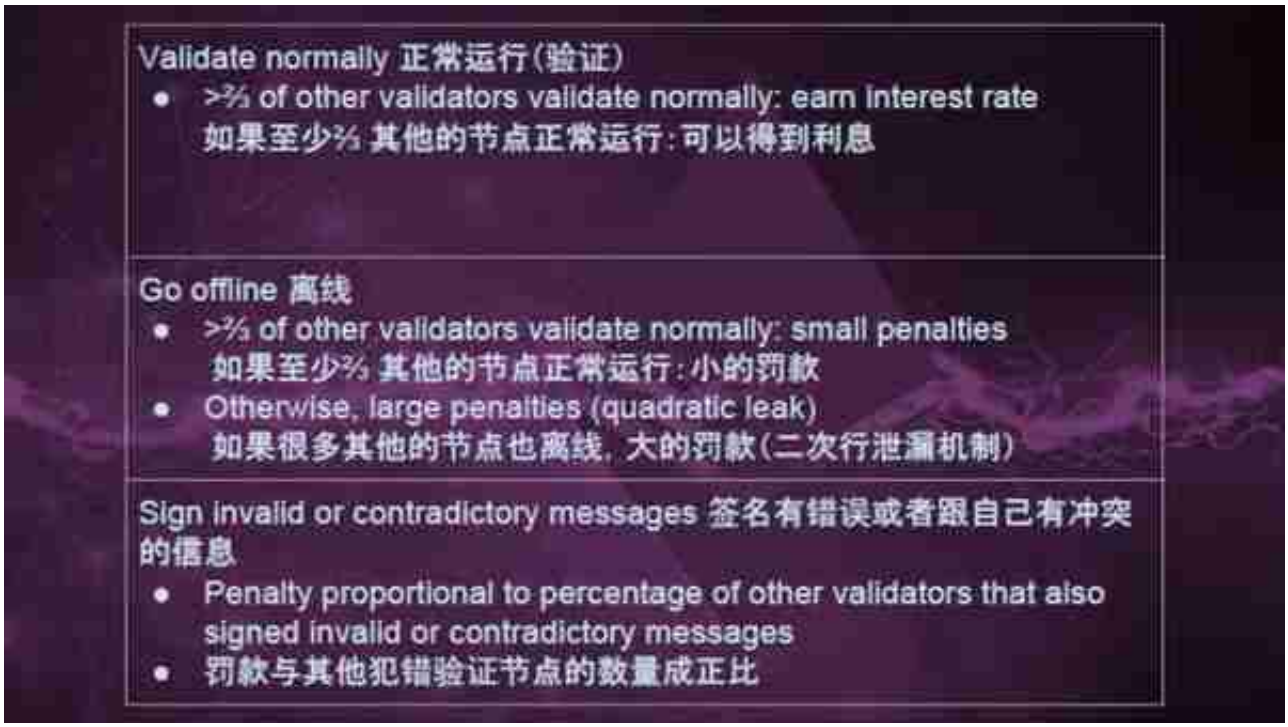
2018 年 6 月 3 日，“2018
以太坊技术及应用大会”在北京悠唐皇冠假日酒店举行，以太坊创始人 Vitalik Buterin 作为演讲嘉宾发表了“Casper
与分片技术最新进展”的主题演讲并向参会人员分享了如何成为 Casper PoS/分片协议的验证者。

此处，V
神详细介绍了分片提案以及主链和子链的责任分配。以太坊的分片提案包含约 100 个子链，每个子链都是跟主链连接的，账户和交易信息都存储在子链上。每隔一个小时左右，系统随机给各个验证节点分配一个分片。在此期间，该节点验证并帮助确认该分片上的区块。而跨分片互操作的主要方式则为交链（Cross-link）。主链不会追踪每个分片中的每个区块，只会追踪交链。

V 神表示：“如果一个节点能够处理N个交易，主链能够追踪 N
个分片，每个分片能够处理 N 个交易，系统则一共能够处理 N^2
个交易。所以该提案叫做二次性分片。”

此外，V神还介绍了作为验证节点应承担的责任。



这样的奖罚机制在设定了节点激励的同时，推动节点设置自己的安全保护机制，尽量不跟其他节点的安全保护同时失效。实现在去中心化的网络中，不同的节点在不同的时间上线或离线，确保不同节点不会在同一时间被黑。

对此，V 神给大家的提示是，不要选择一样的权益池、不要跟别人用一样的 VPS。

附以太坊创始人 Vitalik Buterin 演讲全文：

今天我和大家分享 Casper
Pos/分片的技术，尤其是作为验证者角度参与验证本身工作分享 Casper 技术。

Casper 有一个全新的算法，算法的分片是解决方案，我会具体跟大家阐述一下这两种技术的流程。大家如果参与到
Casper和分片，从节点角度来说要做什么？第一步是存款，Casper 是个验证系统，换句话说，为了加入，需要在权益当中有所存款，存款需要发送存款的交易，这是正常在以太坊上的交易。包括一个公钥，有 32 个以太币并且验证，首先规定你使用的公钥，用它做信息的签名。也要有一个取款地址，在验证的时候有相应的奖励措施。

这里大家要注意，签名公钥和取款地址并不意味着完全一致，这意味着两件事情，首先可以把签名 的权利分配给其他人，比如像我在全世界旅行，不可能一直带着电脑，就可以把这个key给你的朋友，让你的朋友为你签名验证，为你参与到算法。但你不会把所有资金托付给一个朋友，即便你的朋友能代替你做签名 ，但他也不能

把你的钱取出来，你的钱唯一可以进入的地址是之前提供的取款地址，这意味着你可以使用热钱包来签名 。我们刚才提到状态验证的机制，公钥是在一个在线的电脑上，但资金永远会留在冷钱包里，这个公钥是激活这部分资金，防止发给其他人，让你的资金留在自己的电脑上。这种情况下，作为验证者，就更加安全、有保障。

但是一旦你完成了取款交易之后，就进入了第二步：等待加入。这个可能需要一天的时间，这部分协议还没有完全被确定，但要等待这个协议把你加入了验证者的池。

第三步是参加验证机制，有了存款等待了一天时间加入这个机制，你现在已经进入了活跃验证者的池，你就是个验证者了，这是个好消息。作为验证者，在网络当中有两个关键功能，第一个是Casper的过程，来参与并且敲定主链，这意味着它可以确保主链上的区块，超过一定点之后，主链上的区块是不可逆转的。一旦完成之后，主链就被敲定了，你就完成了工作。第二个是验证分片上的区块，我们的系统中不会所有人都来做区块的验证，这些区块被可能分配到100甚至更多的分片中，交易也是分开的，有不同的验证者来验证不同的区块和交易。

这是验证者最主要的两个功能。Casper 这个工具的主要目的是一个敲定工具，是链上共识机制的一部分，用于区块的敲定，它可以给区块更多的安全性。

分片的提案看起来是这样子的，以太坊的分片提案包含 100 个子链，帐户交易信息都是储存在子链上的。主链完成一些工作，子链完成一些工作，主链负责生成随机数，随机选择哪个验证者进入哪个分片、谁可以创立一个分区，并且保持验证节点的追踪，如果你是一个验证者的话，它会一直追踪你验证节点的相关信息，比如你分配到什么分片、你现在的奖励和惩罚是什么，所有这些信息都是由主链完成的，除此之外，它可以追踪子链上的区块。

子链的责任比较简单，主要做交易处理，并且存储帐户状态、合约 状态，它可以存储绝大多数用户比较关注的信息，每个阶段是差不多1个小时左右，每个验证节点由系统随机分配一个分片，为了这个阶段或为了这个小时，验证节点的工作就是要验证，并且帮助确认这个区块是在这个分片之上的。在任何的时间点，如果验证节点被分配到某个特殊的分片上，比如我们一共有 100 个分片，有些人随机选择 1% 的验证节点，来确认任意一个分片上的区块。

这个是系统的可扩展性，我们假设一个计算机可以来处理 N 个交易，主链这个时候就可以来追踪N 个分片，每个分片本身都能够处理 N 个交易。系统可以处理的是 2 倍 N 的交易，所以它叫“2 次性分片”，如果你电脑的计算能力是翻一番，这时主链可以来追踪 2 倍的分片，系统能处理的交易是之前的4倍。

接下来看 Cross-links，交联是彼此间沟通的方式，并且是主链追踪分片的方式，主链不会追踪每个分片中的每个区块，只会追踪交联。每个交联大概是 100 个左右为这个分片分配节点的签名 ，并且在主链上确认这个分片节点的区块。

这个验证节点有以下职责，首先，作为验证节点工作，做主链验证，并且验证主链上的每个区块，主链包括副联、交易以及对验证节点的奖励和罚款 。会验证两个节点的区块，时间更久做区块的生成。我们也可以经常在不同的分片中来回交换，做区块的确认，还有分片和主链之间的交联。作为验证节点，它必须要在分片上做区块的生成，主链区块的生成，并且确认分片上的区块已经交联。这些都是大家作为验证节点的主要责任，也是大家在一个分片系统当中主要的工作。

在线正常运行的状况发出了应该发出的信息，所有都是正常的，这种情况下会发现其他的三分之二节点正常，就可以拿到利息，如果没有的话就拿不到利息。如果大部分其他节点都在线，会有一些小小的惩罚。第三种情况是最差的情况了，如果你有这个签名，这个争鸣是错误或者有冲突，你可能是在线的，但签名 的信息是不正确的。

当我说到你签的这个信息不对，我可以更深入的讲一下，但是现在我先不讲它为什么这样，但我只知道这个情况发生了。这种情况是你要攻击网络，或者你被黑了，如果有这样的情况发生，你会有一些惩罚，而这个惩罚是按比例的，这个比例是按照其他的在线签名的验证节点的比例做到的，也就是说你的罚款与其他犯错节点的罚款数量是成正比的。

另外，如果你是无辜的，有这种情况出现是因为你被黑了，或者电脑有问题，或者数据有问题，这时你受的惩罚就会比较小。如果真的有攻击发生，需要非常多的验证节点，这时你的罚款 就会非常大。攻击系统的成本非常高，如果你作为个人的验证节点出现了问题，成本 是没有那么高的，是公正的。

这个机制希望激励大家做验证节点，也希望大家去设置时，能够更好的保护自己的机制，不要和其他的验证节点同时有不成功的感觉。比如你是一个高度去中心化的网络，不同的节点会在不同时间上线或离线，不同的节点会在不同的时间被黑。如果是一个去中心化网络，大家都有同样的权益池，所有人都用不一样的权益池，如果权益池被黑了的话，假设我们非常集中，所有人都会有非常高的罚款 。

但是这就是说明要告诉大家的，不要跟大家用一样的权益池、不要跟别人用一样的 VPS，如果你所有的节点都在这上面，就避免跟其他人撞车，一旦被黑了的话大家都赔很多钱，如果只有你一个人被黑的话也会损失 很大，所以大家不要跟其他人使用同样的系统，也不要跟其他人使用同样的客户端。这个机制是希望大家更好的去进行配置自己，不让网络同时有非常高的风险。

现在假设大家已经拿到自己的奖励了，你希望能够把这个以太币提出来，该怎么做？

私钥或提款地址其中的一个都可以触发取款过程，一旦触发了取款过程，验证节点会在大概 7 天左右关闭，你一旦退出了之后就要等待 4 个月，4 个月之后就可以提取太币了。