澎湃新闻记者 王蕙蓉

世界第二大加密货币以太币(ETH)背后的区块链网络以太坊，预计在9月中旬“合并”。此举将带来什么影响？

当地时间8月12日，以太坊联合创始人Vitalik Buterin发布推文称，此次在加密领域被称为“合并”的区块链软件升级，预计发生于9月15日左右，尽管具体日期取决于哈希率。

以太坊联合创始人Vitalik Buterin发布的推文

有外媒报道称，本周以太坊的开发人员将敲定具体合并时间。

从工作量证明过渡到权益证明

合并意味着，以太坊将通过两个区块链的合并，将共识机制从工作量证明(PoW)过渡到权益证明(PoS)。早在2013年，Vitalik Buterin发布以太坊白皮书，就提及其愿景是让以太坊成为一个节能的权益证明网络。

目前人们使用的以太坊区块链被称为“主网”，区别于各种仅供开发人员使用的“测试网”区块链。2020年12月，以太坊开发者创建了一个名为信标链(beacon chain)的新网络。信标链本质上是新的以太坊。

信标链是一种权益证明区块链，自18个月前创建以来一直在运行。验证器向信标链中添加区块，但这些区块不包含任何数据或交易。合并需要将存放在以太坊主网的数据传输到信标链，使信标链成为以太坊网络上的主要区块链。在合并的准备阶段，以太坊开发人员始终在对这一新区块链进行压力测试，通过各种以太坊测试网运行数据和交易。

“以太坊最初使用工作量证明算法，需要成千上万的挖矿硬件设备持续运行，以支撑和保护网络。”中国移动通信联合会元宇宙产业委员会执行主任、中国通信工业协会区块链专委会共同主席、火大教育校长于佳宁向澎湃新闻(www.thepaper.com)记者分析道，“相对于工作量证明
来说，
权益证明算法在一定程度减少了数学运算带来的资源消耗，性能也得到了相应的提升，但依然是基于哈希运算竞争获取记账权的方式。”

于佳宁提及，本次合并是以太坊“主网”与采用权益证明的信标链网络的合并。当以太坊合并后，网络的共识机制会正式从PoW转换到PoS，带来一个实质性的转换

。以太坊网络将从工作量证明的约束中解脱出来，网络将更加快速、出块更快、更加有效、对新用户来说更加易用、减少维持以太坊网络运营的电力支出以节约能源等等。

“以前的PoW挖矿方式网络效率很低，大约平均每秒处理十几笔交易。由于以太坊的主要目标是运行智能合约，智能合约的运行中需要大量的网络确认，所以对于网络的效率要求很高。而每秒十几笔的效率远远不能满足系统的要求。”一位虚拟货币观察人士向澎湃新闻 (www.thepaper.com)表示，“特别每笔网络确认，都需要付出一定的Gas费用。而这个费用的数量是竞价决定的，出价越高，发出的请求就会被优先确认，而出价低的请求只能慢慢等待。所以在去年市场比较火热的时候，一笔合约确认的Gas费高达几十甚至上百美元。这个大大阻碍了以太坊应用的推广。所以变成PoS模式以后，增加了网络确认的效率，也会降低以太坊网络使用的成本。”

以太坊合并为何迟未“落地”

权益证明(PoS)共识算法其实就是想要参与记账的网络成员可以通过质押(Staking)以太币来参与，每次验证交易时按照比例奖给节点一定的提成，比例根据节点拥有的资产数量而定，拥有越多相关资产，持有时间越长，得到记账权的机会就大。“PoS的核心就在于Staking。这对于行业的先行者具有先发性优势，类似于早期低成本获得以太币的‘巨鲸’们，就很容易在新的以太坊区块链上获得更多的奖励，致使出现强者恒强，大者恒大的马太效应。”于佳宁说道。

于佳宁预测，未来随着以太坊PoS共识的达成，会涌现出越来越多的Staking服务商，而服务商的可靠性，以及它们存储以太币的安全性并不能被有效把控。加密市场中平台失窃、倒闭甚至卷款跑路的现象屡见不鲜，尽管Staking领域是未来一个非常有潜力的赛道，但在可预见的未来里势必会出现来自服务商的风险。

值得注意的是，由于权益证明相关技术的复杂性，以及日益庞大的资金风险，以太坊合并已被多次推迟。该合并是“以太坊2.0”的一部分，也是为了重塑其区块链基础的一系列升级。

于佳宁指出，合并遇到的主要困难就是在利益分歧以及过渡的技术等。“共识机制变化最主要影响的就是原先受益的矿工，尽管Vitalik Buterin也在鼓励支持工作量证明算法的矿工转向以太坊经典，但很显然矿工的收益依旧会受到很大的损失。或许也是在这样的利益分歧下，以太坊的合并迟迟没有落地。”

上述虚拟货币观察人士也提出了相同观点：“以太坊合并的困难一个是重新构建了一个新的底层逻辑，这个新的底层需要市场适应和接受。另外现在在以太坊网络上

有很多应用合约和资产，避免技术上出错也是很重要的一点。这里面还会涉及到大量矿工的利益，矿工和以太坊开发团队也会有一定的博弈。所以，以太坊的合并最近两年一直在不断推迟，现在这次应该是最接近正式合并的一次。”

于佳宁认为，合并期间会涉及到一系列技术上的问题，甚至说一旦出现此前尚未被发现的漏洞，就极有可能造成网络运行的混乱，造成大量资金和应用的损害。因而在合并之前，以太坊的开发者们必须慎之又慎，考虑到各种微小的可能性，才能使得合并的成功实施。

加密货币分析公司德尔福数字分析师Jon Charbonneau表示，以太坊的开发人员非常小心，以确保在合并时不同的客户端验证器可以一起工作。但以太坊“客户端”(可以读取以太坊数据和挖掘区块的软件)可能会出现一些bug，甚至需要数月时间来修复。

加密货币耗能惊人，转向权益证明有望降低能耗？

加密货币的反对者通常认为，像比特币和以太币这样的加密货币是无用的，而且会消耗大量电力。

假设有人想挖掘加密货币，就需要一台功能强大的计算机，即一台“采矿钻机”来运行软件。这台“采矿钻机”将与世界各地成千上万的“矿工”竞争，通过运算解开复杂的加密谜题。如果解开了加密谜题，那么就赢得了“验证”区块的权利，就可向区块链中添加新数据。比特币“矿工”每验证一个区块可以获得6.25个比特币，以太坊“矿工”则可以获得2个以太币以及Gas交易费用。

为了在竞争中获得更多机会，人们通常会利用很多台计算机。“工作量证明”共识机制是比特币和以太坊区块链运行的方式，允许区块链在分散的同时保障安全。

“这就是所谓的西比尔抵抗机制，” Charbonneau解释道，每个区块链都需要使用一种稀缺资源，而这种资源是无法垄断的。对于工作量证明型区块链来说，这种资源就是运行“采矿”操作所需的电力。

以太坊由世界各地的数十万台计算机组成，如果要“垄断”以太坊，即意味着需要控制其中51%的算力，但这样做将耗资数十亿美元。因此，“工作量证明”共识机制保护了比特币和以太坊区块链在过去没有被黑客攻破过。

但弊端也是显而易见的。随着加密谜题变得越来越复杂，越来越多的“矿工”争相解决，能源消耗随之飙升。

据外媒CNET报道，比特币每年消耗约150太瓦时，超过了阿根廷4500万人的一年用电量；以太坊每年消耗约62太瓦时，接近瑞士900万人的一年用电量。

如果以太坊将两个区块链合并，从工作量证明成功过渡到权益证明，加密谜题将不再是其网络系统的一部分。以太坊基金会表示，由此以太坊的电力支出预计将下降99.65%。

“以太坊转向PoS，在一定程度上确实减少了加密资产存在的弊端，主要就体现在能源消耗方面。”于佳宁分析称，目前全球能源系统陷入动荡，能源供应紧缩已经严重短缺，并导致电力和燃料价格飙升。

国际能源署执行董事法提赫·比罗尔在7月全球能源论坛上表示，世界从未见过如此重大的能源危机，全球性的能源供应紧张局面可能还会进一步恶化。“PoW共识机制虽然有其特有的优势，但在目前这个能源危机的背景下，其庞大的耗电量势必会引起各国相关部门的重视。尽管未来整个行业会向风能、太阳能、水电等清洁能源转型，清洁能源成为行业的主导能源，针对当下而言，转型PoS未尝不是一个选择。”于佳宁说道。

“矿工”将何去何从

以太坊从PoW到PoS的转型升级，意味着相关的“矿工”也需要转型。

“以太坊合并后其实还是有‘矿工’这个角色的，只是方式发生了变化。”上述虚拟货币观察人士解释道，“严格地说，矿工应该叫打包节点。矿工起到的作用是记账，然后把账本广播到整个网络。”

他表示，区块链最核心的是无中介和网络的安全性，其中就涉及到记账权的问题。区块链通过让全网所有人平等参与来解决安全性问题。他举例道，比如A给B转账100元，这时候网络中有一个人抢到了这个记账权，他就记录下来，然后告诉全网的人，A给B转了100元。为了奖励这个记账的人，系统就会给他分配固定数额的代币，比如比特币或者以太币。由于有了激励，大家都愿意来记账，于是就开始争夺记账权，比的就是谁的计算速度快，这个过程就俗称“挖矿”。

他指出，由于网络中有非常多的节点，大家都同步存储了账本，即使一部分节点被毁掉，另外一部分节点也保留了账本，所以整个网络很难毁掉，具有安全性。但这种安全性是冗余带来的，势必也会影响效率。而PoS就是把共识的机制做了改变，但记账节点这个角色还是存在的。PoS把纯粹的从拼算力争夺记账权，变成了质押代币的模式。“PoW就好比是全民投票，一人一票，每个节点都可以投票。而PoS有点类似公司董事会的角色。有人往系统里质押代币，才有权确认记账。激励的方

式也从原来的拼算力拿奖励，变成了质押激励。所以，以太坊从PoW转向PoS以后，传统那种靠拼算力争夺记账权的矿工不需要了，但网络确认节点这个角色依旧存在，只是激励方式从挖矿奖励变成了质押奖励。”

以太坊合并后的应用与监管走向

上述虚拟货币观察人士表示，以太坊从PoW到PoS，对于应用者来说，最大的改变就是网络效率提高，使用成本会下降。“至于是否会减少弊端，这个无法下结论。作为一个基础设施，以太坊从PoW转到PoS只能说是牺牲一部分安全性来换取网络效率的提升。”

该观察人士认为，从去中心化和公平分发的角度来说，PoW模式肯定优于PoS模式，去中心化在区块链世界里代表的就是网络的安全性。网络越安全，就代表网络中的冗余会越多，自然效率就要低下。但由于以太坊是一个智能合约平台，其存在的主要价值是有人大量使用，因此网络效率的提升也是重要的考虑因素。“至于相关的监管审查来说，以太坊的机制是PoW还是PoS并没什么区别，毕竟这些只是内部的技术方案。监管上首先要确认的是以太坊究竟是商品还是证券，有了定性才能套用相关法规的监管。正式定性前，只能是一种模糊和大概的监管。”

于佳宁也表示，以太坊合并仅仅是以太坊网络自身的重大升级，对于监管机构而言，以太坊采取什么共识机制并不是其考虑的重点。早期美国证券交易委员会(SEC)就曾表示，由于足够的去中心化，因此比特币和以太坊并不属于证券。而在这之外的数字资产，都会通过豪威测试(Howey Test)判定是否构成证券发行进行监管，在各国监管模式中尤具代表性，也成为了部分国家对辖区内数字资产定义的一个标准。“目前来看，以太坊转型PoS并不会令监管机构调整其态度，但如果发展到后期，以太坊网络的中心化程度有所变化，也不排除包括SEC在内的监管部门调整相关的监管审查。”

责任编辑：王杰

校对：张艳