PoS 共识机制及设计哲学

——区块链技术引卷之五

专题报告　　宏观研究

2019.04.04

通证通研究院
区块链研究报告

通证通 x FENBUSHI DIGITAL

分析师：宋双杰，CFA

Email:master117@bitall.cc

分析师：孙含儒

Email: sunhanru@bitall.cc

特别顾问

沈波

JX

Rin

更多研究请关注通证通公众号获取

通证通研究院　　FENBUSHI DIGITAL

请务必阅读最后特别声明与免责条款

导读：主网采用 PoS 共识的区块链项目从数量和市值规模上看，落后于采用 PoW 类共识的项目。为什么在已有成熟的项目的基础上，新的 PoS 项目进展仍然不及预期？PoS 共识是否有足够的优势能够让人们接受它并在区块链共识领域占有一席之地？“权益经济”（Staking Economy）是否是区块链未来新的发展方向？

摘要：

在基于 PoS 共识的区块链网络中，所有成为“验证者”的节点都能够获得生产（或者提议）区块的权利，其概率取决于其拥有的“权益”多少。相比工作量证明，PoS 共识的优势包括减少能源消耗、保障安全性、以及降低中心化风险。

早期的 PoS 共识面临着“无利害关系”危机，区块链容易分叉。“执剑人”机制通过加入对不诚实节点的惩罚措施解决以往 PoS 共识的无利害关系攻击。移动检查点和上下文感知机制能够预防针对 PoS 共识的“长程攻击”。

根据权益在共识经济模型中扮演的角色以及重要程度的不同，我们可以将 PoS 共识分为纯 PoS 共识、混合型 PoS 共识、DPoS 以及仅有权益的概念四种，一般只将前两种作为 PoS 共识讨论。PoS 代表的“权益经济”是一个与 PoW 共识不同的经济体系，一般采用通胀的经济模型，只有抵押通证参与网络共识过程才能获得利息收益。由于通胀的存在，“持币待涨”的守财奴策略不再适用于新型 PoS 共识，全体持有者都必须参与网络共识过程，在此需求基础上将有更多的金融应用场景出现。

我们还可以从经济角度分析 PoS 网络的安全性。在初始分配合理的情况下能够保证不低于工作量证明的"经济学"安全性。但 PoS 经济模式同样没能解决垄断与中心化的问题。

长远来看，以 PoS 共识为基础的区块链网络将发展到与 PoW 共识区块链同等的规模。

风险提示：中心化风险、技术进展不及预期、市场波动风险

目录

图表目录

2012 年，Scott Nadal 和 Sunny King 在一篇论文中提出 PoS 权益证明，作为对中本聪工作量证明的替代，首个将 PoS 概念融入到共识机制中的 Peercoin（点点币）于同年上线。随后的几年里，一些大型区块链项目例如 Ethereum、Cosmos 都提出了各自的 PoS 解决方案。但七年后的今天，主网采用 PoS 共识（这里不包括 DPoS、PoW+PoS 混合共识）的区块链项目从数量和市值规模上看，落后于采用 PoW 类共识的项目。为什么在已有成熟项目的基础上，新的 PoS 项目进展仍然不及预期？PoS 共识是否有足够的优势能够让人们接受它并在区块链共识领域占有一席之地？“权益经济”（Staking Economy）是否是区块链未来新的发展方向？

1 权益证明，一段简史

在基于 PoS 共识的区块链网络中，所有成为“验证者”的节点都能够获得生产（或者提议）区块的权利，其概率取决于其拥有的“权益”多少。这里的“权益”（Stake）可以是节点持有的通证数量，也可以是关于通证数量的一个函数。例如下面提到的 Peercoin 提出的“币龄”概念，节点持有通证的时间越长，累计的币龄也越多。相比工作量证明，PoS 共识的优势包括减少能源消耗、保障安全性、以及降低中心化风险。

纵观 PoS 历史，可以将 PoS 的发展大致划分为三个阶段。

第一阶段是以 Peercoin 为代表的 PoW+PoS 混合共识。但是这类早期的共识混合共识仍然需要参与区块生产的节点进行一定量的哈希值计算，即以类似工作量的方式生产区块，只不过各节点计算出合法区块的概率与节点持有的权益相关，即根据权益选择生产者，并且采用基于权益的激励方式。Peercoin 并没有完全实现“降低能耗”的目标。

第二阶段是以 Nextcoin 为代表的纯 PoS 共识。这类 PoS 共识机制不需要节点或只需进行少量的哈希值计算，而采用分布式的、可验证的随机数生成函数来选择区块生产者，激励方式仍然与节点持有的权益相关。这类 PoS 共识相比工作量证明耗费更少的能源，但 PoS 共识仍然有一个危害网络安全的隐患没有彻底解决——Nothing at Stake 攻击（无利害攻击）。

第三阶段是以以太坊 Casper 为代表的新型 PoS 共识。这类共识或是将 PoS 作为区块链共识的一部分，例如以 PoW 的方式生产区块，每间隔一定数量的区块以 PoS 方式确认共识的最终性；或是以 PoS 的方式生产区块，使用 BFT 类算法进行区块验证。这类共识不以实现共识过程的算法为划分依据，它们的共同点是实行“权益经济”，节点能够通过参与网络共识，根据拥有权益的比例获取区块奖励。不同于早期的 PoS，这类共识通过加入对不诚实节点的经济惩罚解决了“无利害关系”问题，增强了 PoS 共识的安全性。

除此之外，以 BitShares、EOS 为代表的“委托授权”类（Delegated PoS）共识也被公众熟知。但这类共识中，权益仅仅体现在投票选举“共识节点”上，而与经济模型、奖惩制度无关，因此一般不作为 PoS 共识讨论。

根据区块链生产的过程可以将 PoS 共识分为以下两类：

基于“链”的 PoS（Chain-based Proof of Stake）。类似 BTC PoW 生产区块的原理，算法每隔一定的时间内根据节点持有的权益

随机选择一个节点负责生产区块，这个区块必须附加在一个合法区块链的末端，当分叉产生时，通过共识算法规定的规则选择一条链作为共识链。

“拜占庭”类 PoS（BFT-style Proof of Stake）。算法每隔一定的时间内根据节点持有的权益随机选择节点提议一个区块，但这个区块是否合法、能被附加到共识链之后需要得到一定比例的验证者投票确认。

2 权益证明的安全“执剑人”

与 PoW 共识中算力竞争这样通过引入稀缺的外部资源，并以通证对算力的付出予以奖励来保证区块链网络的安全性的模式不同，PoS 希望依托区块链经济体系内生力量来解决安全性问题。PoS 共识选择按“权益”分配区块记账权与激励，并通过一系列创新性的解决方案保证区块链网络的安全性，并在此基础上开创了区块链世界独特的“权益经济”。

2.1 区块链世界的“公地悲剧”

早期的 PoS 共识面临着容易分叉的危机。哈丁教授在《公共地悲剧》（Tragedy of the commons）一文中描述了这样一个故事：一些牧羊人在一片公共的草原上放牧，由于草原的资源是有限的，因此当羊群数量超过草原能承载的最大数量后，羊群的总产值会下降。考虑一个简单的由两名牧羊人构成的模型，假设草原合理的放牧量为两只，两名牧羊人各有一只羊，此时每只羊的产值为 1 个单位，每增加一只羊，羊群的总产值会有所下降。

图表1：公地悲剧

羊的数量	每只羊的产值	总产值
2	1	2
3	0.6	1.8
4	0.4	1.6

资料来源：通证通研究院

每个牧羊人面临两个选择：增加一只羊或是维持现状。如果牧羊人是理性的，那增加一只羊将是最优策略，然而当两名牧羊人都选择增加一只羊时，草原的总产值下降了。“公地悲剧”给人们的启示是，个体对公共资源无节制的开发利用会导致整体利益的受损。

图表2：公地悲剧中的博弈

另一名牧羊人 / 自己的决策	增加一只羊	维持现状
增加一只羊	0.8	1.2
维持现状	0.6	1.0

资料来源：通证通研究院

早期的 PoS 共识同样面临着类似的难题，即"理性分叉"。在以"链"为基础的区块链网络中，当节点发现同样高度的两个区块，即网络出现分叉时，节点面临两个选择：一、根据共识规则，选择其中的一个节点作为主链，在此基础上生产新区块；二、在两条分叉链上同时生产新区块。

区块链作为一种无形的技术，承载的生态是其价值重要的一部分。在“公地悲剧”的例子中，被滥用的草原资源是有限的，虽然区块链生态仍在飞速发展中，但无限制分叉势必会造成区块链开发人员、社区、生态系统的割裂，分叉链之间的竞争相对没有分叉来说会降低它们的总体价值。

在 PoW 共识区块链中，这样的选择其实是不成立的。因为节点拥有的算力是固定的，如果节点分配一部分的算力在分叉链上挖矿，那么首先要承担该分叉链最终不具有任何价值的风险，节点会损失因为在分叉链上挖矿而在主链上减少的收益。如果该分叉链具有一定的价值，那么其他理性的节点会迅速将算力切换到分叉链上，达到两条链上单位算力收益的平衡。如果节点的算力占全网算力的比例没有变化，那么它并不能因此获取超额收益。一个理性节点的选择是在最有可能成为主链的链上继续挖矿。

图表3：PoW 共识下节点面对分叉的博弈

自己 \ 其他节点	挖分叉链	不挖分叉链
挖分叉链	分叉链存活的概率增加，网络总价值降低	分叉链存活的概率低，损失主链收益
不挖分叉链	主链总算力降低，可能带来收益增加，算力可以随时切换到分叉链	维持原状

资料来源：通证通研究院

而 PoS 共识下，分叉链在分叉高度之前的区块与原链完全相同，因此节点在分叉链上也拥有相同数量的通证。从而有相应的权益能够在分叉链上继续生产区块，两条链上的挖矿互不影响，因此理性的节点会默许分叉链的存在。

图表4：PoS 共识下节点面对分叉的博弈

自己 \ 其他节点	挖分叉链	不挖分叉链
挖分叉链	获得两条链上的利息收入，网络总价值降低	获得主链以及分叉链上的利息收入
不挖分叉链	仅能获得主链上的利息收入	维持原状

资料来源：通证通研究院

有一种观点认为，通证的持有者如果可以预见到这种分裂带来的危害，会为了维护自己的利益而拒绝在分叉链上生产区块的行为。但事实上，群体中的大部分个体都是短视的，如果没有其他的规则加以限制，很少有节点会放弃分叉链上的权益。这又被称为“无利害攻击”（Nothing-at-Stake）。

2.2 “执剑人”机制

以太坊 Casper 共识应用了“执剑人”（Slashers）机制，通过加入惩罚措施，解决以往 PoS 共识的公共地悲剧。该协议的核心内容是，参与区块生产的节点（被称为验证者）需要抵押一定的保证金，并规定一系列的惩罚条件。当发现节点采取了惩罚条件中列出的行动之后，将没收节点抵押的保证金。会被惩罚的行为通常包括同时在两条链上生产区块、没有在最新高度上生产区块等恶意行为。对

可能表现出恶意的节点进行经济制裁（Slashing），改变了节点在可能出现分叉链时挖与不挖两种选择的预期收益，只要节点挖分叉链，或者做出其他攻击行为的收益小于其抵押的保证金，那么理性节点的选择将是遵守规则，做一个诚实的节点，从而化解了公共地问题。

科幻小说《三体》中也存在“执剑人”这一身份，执剑人是引力波广播系统开关的控制者，一旦三体舰队对地球发动攻击，包含三体星系坐标的引力波广播将被发送，三体星系和太阳系会因"黑暗森林"法则灭亡，因此执剑人是地球制约三体舰队的关键力量。新一代 PoS 共识中的“执剑人”机制也是制约潜在攻击者的利器，通过规定合理的惩罚条件与抵押金额，能够有效增强共识机制抵御各类网络攻击的能力。

2.3 新的问题——“长程攻击”

基于链的 PoS 共识在如何确定共识的最终性上更加复杂。PoS 抛弃了“以累计工作量最大的链作为主链”的概念，在节点可以自由加入或退出的 PoS 网络中，抵押金的变动是动态的，验证者需要获取最新的其他验证者信息，才能判断哪些区块是真正有效的。不同于 PoW 网络判断区块是否有效仅仅依赖几个客观的信息：交易合法性、区块头哈希是否满足要求，判断主链采用确定的最长链原则，PoS 还需要考虑“长程攻击”的可能性。

“长程攻击”是 PoS 共识中威胁最大的攻击形式，当一个节点收回了他的抵押金时，虽然它不再拥有验证以后的区块的权利，但是仍然可以对收回抵押之前的区块进行验证，并且由于它不再会收到没收押金惩罚，因此攻击者能够通过贿赂这些节点，收集足够的"幽灵"抵押金（这些抵押金已经被收回了），重新构造一条足够长的攻击链，尝试替换这些节点在作为验证者期间曾经验证过的区块。

一种解决策略是**移动检查点**。即每隔一定的区块间隔设置检查点，只有检查点之后的区块可能会被重组。检查点的间隔一般少于要求的最短抵押金抵押时间，从而保证有充足可能性的区块都是由还有缴纳了抵押金的节点验证的。

另一种解决策略是**“上下文感知交易”**（Context-Aware transactions）。在构造一笔交易时，在交易中记录前一个或前几个区块的哈希值，这样就能将一笔交易和特定的区块分支联系起来，在分叉链上伪造交易就变得困难。

3 权益经济——PoS 共识的经济理念

3.1 PoS 共识种类

图表5：PoS 类共识机制划分

	“纯粹”PoS	混合型 PoS	DPoS	仅有权益的概念
权益对共识的重要性	决定因素	重要因素	次要因素	几乎无影响
权益的功能	选择验证者并生产区块、分配经济激励等	确认网络的最终性、分配经济激励	选举超级节点	作为次要通证存在、社区治理投票权等
例子	Cosmos、Tezos、Cardano、Casper CBC	Casper FFG、Decred	EOS	NEO（GAS）交易所平台通证（投票上币、分红）

资料来源：通证通研究院

根据权益（Stake）在共识经济模型扮演的角色不同，我们可以将 PoS 再细分为以上几类。

在后两种共识机制中，权益在共识过程中没有起到决定性作用，因此一般不将其作为 PoS 共识讨论。它们与前两种 PoS 共识的区别在于**网络的经济激励是否按照拥有的权益多少进行分配**。有些 PoS 共识虽然也是通过投票选举出有限数量的验证者参与共识过程，但这种选举是通过智能合约将通证"委托"给验证者实现的。验证者对委托的通证不具有使用权，并且验证者获得的区块奖励按通证数量分配给其所有者。而 DPoS 共识中，区块奖励仅分配给超级节点以及一定数量的候选人节点。

纯粹 PoS 和混合型 PoS 共识的区别在于选择验证人的过程是否与其持有的权益相关，对应 PoW 共识中选择区块生产者的概率与其算力相关。混合型 PoS 共识一般通过 PoS 为区块链提供"最终性"检验，而区块的生产、验证者的选择通过其他方式完成。如果节点取得记账权的概率与它持有的权益相关，那么可以认为此类共识是纯粹的 PoS 共识。

这样定义的纯粹 PoS 并不是说不能包含其他的共识算法，事实上大部分 PoS 共识都使用 BFT 类算法完成对区块的投票。例如，Tendermint 的基础算法是 PoS+pBFT，Proof of Activity 的基础算法是 PoS+PoW，Casper FFG 的基础算法是 PoW+PoS+BFT，PoS 未来的发展趋势也将是混合型共识。

3.2 全体持有人参与共识的网络

PoS 共识可以概括为：权益持有者将通证投给他们认为合法的