区块链共识机制研究与创新

作者：吕旭军 李尼 叶伟 LvXujun LiNi
YeWei

出版时间：2019 年 08 月

摘要：

良好的共识机制能够鼓励网络中善的节点打包正确的区块，避免恶的节点确认不合法的交易，篡改交易数据，从而保证主链的正确延续。目前不少主流公链就仍采用 PoW 来确保网络安全，但也有很多公链开始采用 PoS 来确保网络安全。相比工作量证明 PoW 共识依赖高能耗，PoS 共识则将公链的安全基础由耗费能源的算力转为纯粹的经济激励，这些持有权益的 PoS 节点通过随机的方式决定谁来产生区块并获得奖励，整个过程更加清洁环保；共识机制的升级转换将极大增加和提高整个网络的交易吞吐量 TPS 和安全性能。本报告中将以各个主流公链为例，着重介绍 PoS 共识机制的设计美学。

关键词： 去中心化共识机制 PoS

Abstract：

A good consensus mechanism can encourage honest nodes in the network to gather transactions and propose correct blocks，and prevent malicious nodes from confirming illegal transactions，tampering with transaction data. Thus the main chain can be well extended. Today，many popular public chains still use PoW to secure the network security，but many other public chains have begun to adopt PoS to secure the network security. In comparison of PoW that relies on high energy consumption，PoS turns the security foundation from the energy-consuming computer power to the pure economic incentives. Those PoS nodes will be chosen in a random way in order to determine which node is the block producer and receives the block reward. The whole process is more energy-saving and environmentally friendly. What's more，the upgrade of the consensus mechanism will greatly improve the Transactions Per Second （TPS） as well as the security in the whole network. In this article，we will focus on the design aesthetics of PoS mechanism according to the mainstream public chains.

Keywords： DecentralizationPoSConsensus Mechanism

一 从 PoW 到 PoS，共识机制的进化之路

（一）关于共识

共识，英文叫 Consensus，是指分布式网络中节点对某一事实达成一致意见的过程，主要囊括三个点。

第一，共识基于分布式网络，也就是通常理解的去中心化的 P2P 网络，区块链网络采用典型的分布式网络。

第二，共识的参与主体是节点。一个节点就是区块链网络中的一台计算机，这台计算机可以是实实在在看得见摸得着你的台式机、你的服务器，也可以是你花钱租赁的虚拟的云。

第三，共识的目的是对某一事情达成一致意见。区块链网络中最重要的事情就是对交易记账结果的确认。

（二）如何保证区块链网络达成正确的共识

这就需要设计一套良好的共识机制，就是保证这套共识机制能够激励善的节点打包正确的区块，避免恶的节点确认不合法的交易，篡改交易数据，从而保证主链的正确延续。像一部分主流网络就采用 PoW 来确保网络安全，一部分公链采用 PoS 来确保网络安全。

（三）PoW 如何保护区块链网络的安全

在 PoW 网络共识机制中，节点通过解决一个需要大量算力的数学难题来将交易打包成合法区块。某个节点解决了这道难题，这个节点就获得了网络的下一个打包出块权，因此该节点就能获得奖励。

但是解决这道数学难题是有门槛的，那就是节点需要耗费大量的算力和电力，这些高昂的成本会让节点只会打包正确的交易上链，而不会打包不合法的交易上链，对节点来讲，作恶成本是非常高的，从而保证了区块链网络的安全。

（四）PoS 如何确保区块链网络的安全

为了获得出块权和奖励，PoW 拼的是节点的计算机的算力，而 PoS 不需要节点有那么高的算力，因为 PoS 拼的是权益。在 PoS 共识机制中，节点通过质押一定数量的通证参与共识。节点被选中成为出块节点的概率与质押的通证数量呈正相关关系，而某一节点违反规则，则会受到相应的惩罚，这就是这套机制的魅力所在。

（五）从 PoW 共识向 PoS 共识全面升级，是共识机制发展的必然趋势

相比工作量证明 PoW 共识依赖高能耗，PoS 共识则将公链的安全基础由耗费能源的算力转为纯粹的经济激励，这些持有权益的 PoS 节点通过类似抽奖的方式决定谁来产生区块并获得奖励，整个过程更加清洁环保；这次共识机制的升级转换将极大增加和提高整个网络的交易吞吐量 TPS 和安全性能。

在当前区块链系统百家争鸣的形势下，安全高效的共识协议已经成为大家主要的研究方向之一，PoS、PoA、PoI 等众多共识模型被相继提出，而在众多共识模型中，经过谨慎的思考，万维链认为权益才是左右链上治理和发展的根本因素，因此研发了 PoS 星系共识协议，以替代原本高能耗的 PPoW（Permission Proof-of-Work），其迈出了完全去中心化的关键一步。目前整个行业中，拥有完整委托的 PoS 机制的项目屈指可数，星系共识就是其中之一。

二 关于 PoS 共识的整体架构与流程

（一）整体框架设计

对于共识协议的设计来讲，主要解决的就是两个核心问题：出块者选择（Leader Selection）和合法链选择（Chain Selection）。在传统的 PoW 中，出块者的选择是通过挖

矿进行的，借助的是哈希函数的随机性，矿工依赖自身的计算能力参与出块者竞争，而这里的公平性就体现为任何节点对哈希函数结果的不可预测性，任何节点都没有优势可言，只能通过简单粗暴的穷举运算来解决问题。合法链选择往往也采取最长链的规则，也就是让算力最大的分支成为主流。这样“挖矿+最长链”规则的框架设置就导致了大量的能源浪费，也是其他共识协议被提出的根本原因之一。那么当前主流的 PoS 协议又是通过怎样的框架设计来解决这一问题的呢？

经过长期的调研学习，我们以三种知名的共识协议来简单介绍 PoS 共识的主流框架。

Cardano 的 Ouroboros 是发表在美密会上的顶尖学术论文提到的协议，也是第一个被工业界采用的可被证明安全的 PoS 算法，其卓越的贡献就在于提出了可被证明安全的共识模型框架，并在其中设计了实用的算法模块。在其多个系列版本中，出块者选择也有不同的方式，由最初利用随机数的确定性选择到采用 VRF 算法的匿名选择，Ouroboros 逐渐将选择的过程隐私化、安全化，而有效链的选择一直采取最长链规则，也就是 Chain Based 方式，保证了链的安全性。所以 Ouroboros 的整体框架就是 VRF Selection+Chain Based 模式。

Algorand 是由图灵奖得主、MIT 教授 Sivio Micali 提出的 PoS 共识协议，其突出贡献在于设计了 BFT 的升级协议 BA*协议，利用投票的方式解决了区块合法性的选择，在出块者和验证者的选择上，Algorand 也采用了 VRF 算法，保证了随机性和匿名性，经过 BA*协议的运行，保证每一个高度的区块都是被确认的，即使最终是空区块，也是经过投票认证的。所以 Algorand 的整体框架就是 VRF+BA*投票模式。

Casper 是以太坊当前研究开发的 PoS 共识协议，秉持实用性的特点，Casper 采用了投注式共识，完成保证金质押的验证者可以投注自己相信会被确认的区块，在投注规则的限制下保证了最终胜出区块的唯一性，而胜出的验证人也将得到收益。Casper 将帮助其由 PoW 转型为 PoS，也是大家十分期待的共识协议。所以 Casper 的整体框架就是验证人+投注的模式。

简单介绍了几种主流 PoS 共识协议之后，我们回归到星系共识，经过深入的思考研究，星系共识坚持学术派的发展路线，借鉴了 Ouroboros 可证明安全的模型框架，全新设计更加高效安全的随机数生成算法，并创新性设计 Unique Leader Selection 算法以替代 VRF 算法，用于出块者选择，保证了合法出块者的唯一性，大大降低了自然分叉概率，所以星系共识的整体框架就是 ULS+Chain Based，在保证安全性的前提下极大地提升了实用性。

（二）共识中的角色分类

1.两种星体

在星系共识之中，所有在智能合约中参与质押的用户都将成为整个星系中的一个节点，而这些节点由于能力的大小被分为两种星体：恒星（star）和行星（planet）。

为区分两种星体，这里就不得不说星系共识中的委托机制，为了给仅持有少量通证或权益较小的用户提供参与共识的机会，在星系共识中，我们设计了完整的委托机制。委托机制的实现基于三重 ECDSA 委托签名算法，对当前的区块链系统有着天然的兼容性，通过委托机制，持有少量通证的用户可以将自身权益委托给代理节点，由代理节点参与共识的运行，同时由于签名消息空间的限制，代理节点只能代为出块，无法进行其他操作，保证了用户权益的安全性。

了解了委托机制，就可以介绍两种星体了。在星系共识中，恒星节点是可以接受委托的共识节点，其自身持有一定量的权益，而且其自身权益值将影响其接受委托的权益上限；行星节点是不可以接受委托的共识节点，其参与共识完全依赖自身持有的权益值。虽然两种星体的能力大小有区别，但在参与共识的过程中是相同的，并不做区分。如何成为恒星节点，一方面需要更多的权益质押，另一方面也取决于节点的信誉程度，最终方法后续将有详细说明。

2.两类星群

星系共识之中，参与节点由于任务分工被划分为两个星群：RNP 星群和 EL 星群。这两个星群主要解决了共识中的两个关键问题。

RNP 星群是在所有星系共识节点中按照自身持有权益比例选择出来的，负责构建链上随机数的群体。RNP 星群中的节点通过 DKG1、DKG2、SIGN 三个阶段的工作完成随机数的更新，保证了链上随机数的安全性。正如上面介绍的主流 PoS 框架，如何维护一个公平的随机数是保证协议安全的重中之重，RNP 星群负责这一关键性工作，其每一轮产生的随机数将作为星群构建、出块者选择和其他随机源应用的重要种子，以维持共识的健康运转。

EL 星群是在所有星系共识节点中按照自身持有权益比例选择出来的，负责收集交易、打包出块的群体。EL 星群需要完成两个周期的工作，第一个周期通过 SMA1、SMA2 两个阶段完成秘密信息序列（secret message array）的协商，完成 EL 星群内部秘密数据的共享；第二个周期通过秘密信息序列和链上随机数确定出块权归属，并在自身负责出块的时间段内打包区块并广播，完成链的生长发展，其作用毋庸置疑，是保证共识安全运行的基础。

3.运行流程

首先我们介绍两个时间上的概念：slot 和 epoch。对 Ouroboros 了解的读者对这两个概念应该并不陌生，slot 是一个区块的生成时间，即每个 slot 内产生一个新的区块；而 epoch 是由大量连续 slot 构成的时间周期，是协议完整运行的一个循环。下面分四个步骤讲述协议运行流程。

（1）构建星系

这是协议运行的准备阶段，在这一阶段，所有想要参与星系共识的节点通过在共识智能合约中质押一定量的通证成为星系节点，质押时会选择锁定时间，这一时间将影响节点

的权益值，锁定时间越长，权益值则相应越高，同时权益值随着锁定时间的流逝也将呈增长趋势，这一设计很好地模拟了币龄的概念，确保了权益设计的合理性和节点参与的公平性。经过这一阶段的准备，星系中就出现了大量的节点，这些节点将正式运转星系共识。

（2）组建星群

在每次协议运行周期（epoch）的起始，星系中会出现两大星群，即 RNP 星群和 EL 星群，这两大星群的选择是基于节点持有权益值的比例，利用链上随机数进行的随机选择过程，类似于 Follow-the-satoshi，这里我们使用 Follow-the-stake-ratio，保证了星系节点参与组建星群的公平性，权益占比越高，被选入星群的概率越大，参与共识进而获得收益的可能性就越大，这也是 PoS 共识的核心思想之一。

（3）RNP 星群运转

RNP 星群被选择组建之后，星群中的节点完成 DKG1、DKG2 和 SIGN 三个阶段的工作：在 DKG1 阶段，各节点提出自身对随机数碎片选择的承诺，保证了碎片选择的不可更改性；在 DKG2 阶段，各节点将自身选择的随机数碎片通过门限秘密分享的方式分享给星群中的其他节点；最终在 SIGN 阶段，各节点公布自身收集的随机数碎片数据，完成随机数的生成，更新链上随机数数据。而整个过程由于门限秘密分享的特点，保证了只要在线节点数超过门限值就将顺利完成随机数的更新，确保了随机数生成的可靠性，同时只要星群中至少一个节点在随机数碎片的选择上是随机的，那么最终随机数结果就是随机的，保证了随机数生成的安全性。

（4）EL 星群运转

EL 星群被选择组建后，将参与两个周期的工作。在第一个周期中，EL 星群节点参与 SMA1 和 SMA2 两个阶段的工作：在 SMA1 阶段，各节点提出自身秘密信息的承诺数据，保证了秘密信息的不可更改性；在 SMA2 阶段，各节点将自己的秘密信息加密共享给其他节点，完成秘密信息序列（Secret Message Array）的生成。在第二个周期起始时，EL 星群中的节点会依据 RNP 星群产生的随机数进行排序，这一排序在整个周期中有效，同时依据秘密信息序列执行出块者选择算法，确定整个周期内各时间段的出块权归属，这一过程是在 EL 星群内部秘密执行的，其他节点无法获知结果，而 EL 星群中节点就依据出块权的归属完成整个周期内新区块的生成，当新区块被提出时，EL 星群中的节点要添加自身合法性的凭证，这一凭证可被全网验证，确保了链的正常安全发展。

三 关于共识的随机数生成算法

（一）随机数对于区块链系统的重要作用

在正式谈随机数的作用之前，我们需要了解一个概念，那就是“熵”（Entropy）。熵对于物理学领域的朋友一定不会陌生，它是体系混乱程度的度量。在 1948 年，香农（Claude Elwood Shannon）提出了信息熵的概念，以描述信源的不确信度。简而言之，熵就是不确定性的度量。

那么熵和区块链系统有何关系呢？可以说，熵对于区块链系统是至关重要的，是整个系统运行的安全保障。以中本聪设计的比特币系统为例，它采取 PoW 共识算法，矿工进行大量哈希计算去争夺出块权，任何高度区块的出块者的身份都无法提前预测，这就是熵在该系统中的体现。试想如果熵为 0，即每个区块的出块者都是事先确定的或者人为可控，那么必然会出现合谋、分叉等攻击。因此任何区块链系统都需要一种安全有效的方式为系统引入熵。基于 PoW 共识的区块链系统由于挖矿的随机性，以天然的方式为系统引入了熵，然而对于 PoS 和 DPoS 共识的区块链系统，就需要单独设计一种方式去引入熵，那就是随机数生成算法。可以说随机数生成算法是设计共识机制的主要挑战之一，也是衡量共识机制优劣的重要标准之一。

（二）随机数生成算法优劣的衡量标准

既然随机数生成算法这么重要，那么一个优秀的随机数生成算法应该具备哪些因素？就安全和实用角度而言，它应当满足以下六大性质：去中心化（Distributed）、不可预测（Unpredictable）、无偏性（Unbiased）、均匀分布（Uniformity）、保证输出（Guaranteed Output Delivery）、公开可验证（Publicly Verifiable）。

以上六大性质对于随机数生成算法至关重要，违背其中任意一个都可能会导致严重的安全漏洞。据区块链安全公司 PeckShield 披露，EOS 上有超过 8 个竞猜项目遭受黑客攻击并且其获利几百万美元，严重威胁到了 EOS 正常生态秩序，而大部分攻击成功的原因与随机数生成漏洞有关。我们以 EOS.WIN 项目为例，剖析其随机数算法漏洞根源。

EOS.WIN 支持的一个游戏是猜数字，即用户输入某个数字并压大或者压小，然后系统随机生成一个数字，如果用户压对大小，则视为中奖并获取收益。显然如果能够控制系统随机生成的数字，就可以左右游戏的结果。而决定 EOS.WIN 系统随机数生成的因素为交易哈希 ID、成交区块高度、成交区块前缀、全局开奖序号。其中成交区块高度、成交区块前缀虽然是未来某区块信息，但是在实施过程系统指定使用当前同步到的最新块信息，因而是确定的；同时，交易哈希 ID 能够通过交易内 action 结合块信息预先计算。于是随机数的生成仅依赖全局开奖序号了。攻击者利用不断制造错误交易，造成交易状态回滚，控制全局开奖序号，从而控制随机数的生成，直到中奖。显而易见，EOS.WIN 的随机数生成算法不满足上述的第二个性质（不可预测）和第三个性质（无偏性），因此存在漏洞，最终被攻击者有效攻击。

（三）星系共识随机数生成算法

星系共识中的 RNP 星群借助承诺、零知识证明、门限秘密分享、门限签名、椭圆曲线序对等多种密码学手段，确立了安全高效的随机数生成算法，为整个共识过程安全提供了数据基础。为了能够形象地介绍随机数生成算法的设计初衷以及精妙之处，我们将其类比为一个简单的游戏：

纸牌游戏

Alice 和 Bob 玩纸牌游戏，两人分别秘密选一张扑克牌放在桌面下方，选定之后，同时将纸牌亮在桌面上。如果两张纸牌的点数和为偶数，则 Alice 获胜；否则，Bob 获胜。

这个游戏看似简单，但是在区块链上公平地进行并不容易，要通过多种手段防止 Alice 或者 Bob 作弊。我们接下来一步一步分析。

问题 1：Alice 和 Bob 选定之后就不能再更换扑克牌，否则就可以根据对方扑克牌的点数决定自己的扑克牌点数，从而获胜。例如，Alice 如果可以更换扑克牌，那么只要保证自己所选扑克牌的点数和 Bob 的扑克牌点数具有相同奇偶性，那么点数和总为偶数，Alice 便可以获胜。

星系共识通过使用“承诺”（Commitment）的方式来保证不会发生以上作弊行为。“承诺”是一种密码学工具，能够保证在不暴露原始数据的基础上，将其进行“证据留存”，它和明文是一一对应的，任何人都可以验证二者的对应关系是否成立。

结合我们的例子形象地理解就是，Alice 和 Bob 将自己选定的扑克牌撕一个小角下来，放在桌面上，这个小角不会暴露扑克牌的点数，而且只与撕坏的另一部分才能够拼接为一张完整的扑克牌。在星系共识协议中，这是 DKG1 阶段：每个 RNP 节点计算其所选数据的承诺并发送到链上进行存证（见图 1）。

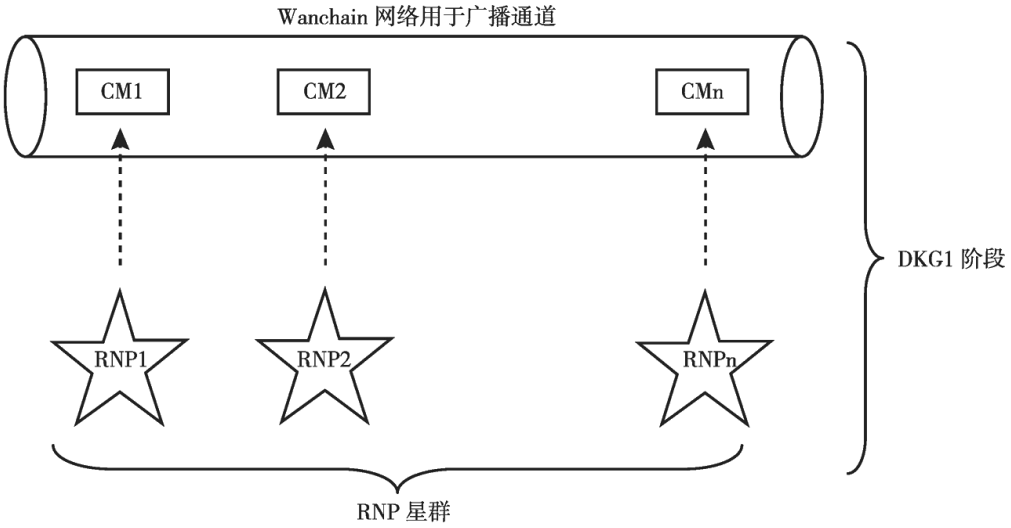

图 1 DKG1 阶段示意

问题 2：Alice 和 Bob 在选好扑克牌之后，在正式亮牌之前要对自己的扑克牌保密，不能让对方看到；同时在亮牌时要证明这张牌确实是之前选定的牌，而不是新选的另一张牌。

星系共识通过公钥加密算法加密原始数据，之后将加密结果发送到链上，保证了数据的机密性；同时使用零知识证明保证链上的加密数据与承诺完全匹配。结合我们的例子形象地理解就是，Alice 和 Bob 将被撕过角的牌从桌下取出，扣在桌面上，并且二者都验证扣在桌面上的牌与之前放在桌上的小角能够拼接为一张完整的牌。在星系共识协议中，这是 DKG2 阶段：每个 RNP 节点将在其给其他节点的数据进行对方公钥加密之后将其发送

到链上，同时发送到链上的还有 DLEQ-Proof，以用于证明加密内容与承诺 CM 是匹配的。这个阶段之后，所有节点都可以从链上获取其他节点发送的数据，并且在本地解密为明文（见图 2）。

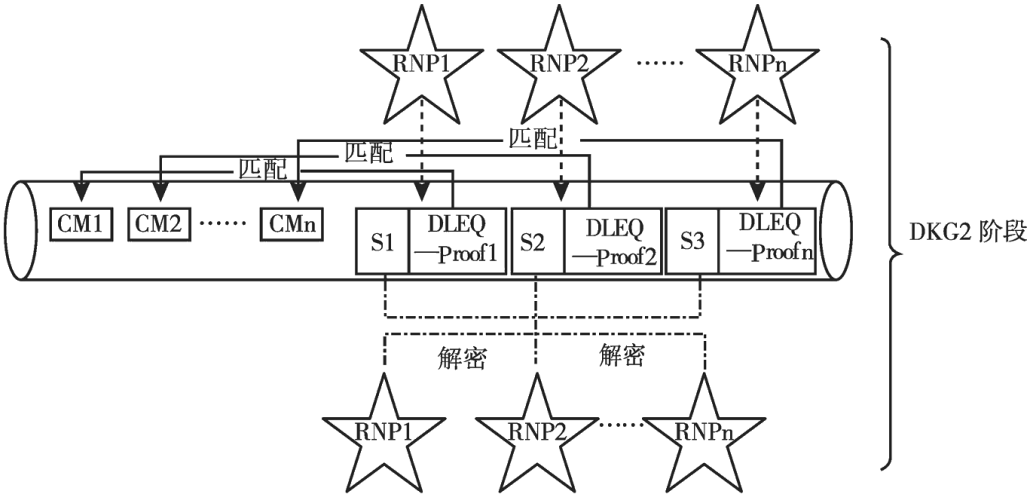

图 2 DKG2 阶段示意

问题 3：开牌之后，需要计算两张扑克牌的点数。我们保证 Alice 和 Bob 都要计算出同一正确结果。这个问题看似很荒唐，但是非常重要。因为某位玩家可能会装疯卖傻，故意计算错数字，从而降低游戏进行的效率。

问题 4：此时，无论是 Alice 还是 Bob 都不能够终止游戏，也就是说，一旦游戏开始，就一定要正常结束，不能因为某一玩家拒绝配合游戏规则而导致游戏流产。

星系共识通过使用分布式密钥生成的算法解决了问题 3，即所有 RNP 节点通过交互生成一个共同的组密钥（Group Secret Key），这个组密钥不会完整出现，而是分割为密钥碎片，每一个 RNP 节点掌握一个密钥碎片。之后，RNP 节点能够合成组密钥签名，而签名的哈希值即为最终输出的随机数。由于组密钥是公共确定的，因此组密钥签名也是唯一固定的。结合我们的例子形象地理解就是，Alice 和 Bob 会计算得到共同的点数。

星系共识通过门限签名的方式解决了问题 4，即只要超过门限值数量的 RNP 节点参与计算，就能够合成组密钥签名。个别 RNP 节点拒绝参与计算并不会影响结果的生成。结合我们的例子形象地理解就是，即使 Alice 不想亮牌，Bob 也有能力将两张牌亮出，从而完成游戏。

以上过程对应星系共识协议中的 SIGN 阶段，在这一阶段中 RNP 节点合作生成组密钥签名并计算得到输出的随机数。

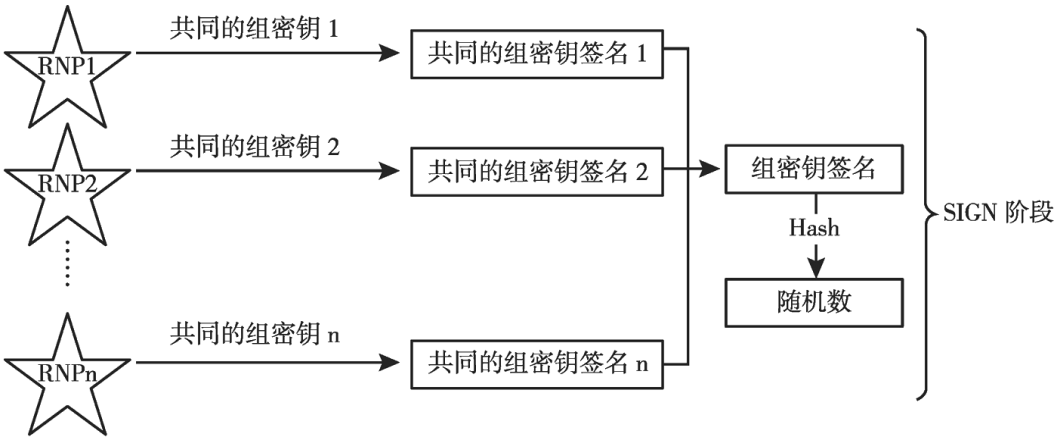

图 3 SIGN 阶段示意

现在我们把上述过程梳理一下：①Alice 和 Bob 扑克牌的点数之和是由二者共同决定的；②每一局游戏的点数和都是独立的，不存在相互依赖的关系，因此历史游戏数据没有预测作用；③Alice 和 Bob 都无法先知道对方的扑克牌点数，因此没有后发优势去左右点数之和；④Alice 和 Bob 可以选择任何一张扑克牌，因此点数分布是均匀的；⑤Alice 和 Bob 都无法中断游戏；⑥任何第三方都可以对游戏过程进行审计，因为所有数据都在链上存证。

由以上分析可知，星系共识的随机数算法满足前文提到的六大性质，是安全高效的随机数生成算法。

四 共识之合理出块者选择

（一）合理出块者选择的重要意义

在区块链共识协议中要解决的两个核心问题是出块者选择和合法链选择，无论在哪种共识协议中，合理的出块者选择都是重中之重，我们设计随机数生成算法时引入熵的一个关键作用就是要将其用于出块者选择。

合理的出块者选择对保证链的安全性和活性至关重要，一个好的出块者选择算法是共识健康运行的基石。我们先说说出块者选择对链安全性的意义，链的发展延长本质上就是块的不断接续，而完成打包提出区块的就是这些出块者。其一方面决定哪些交易写入区块进而上链确认，另一方面也通过选择接入的父区块决定链的发展走向。在网络中共识节点善恶并存的环境下，一个好的出块者选择算法就是要保证诚实节点能够获得更多的出块权，进而主导链的发展。当然，由于不同的共识协议在不同的安全假设之下，出块者选择算法的设计也是不同的。

1.工作量证明（PoW）的安全假设：50%以上算力

在这一安全假设下，PoW 采用哈希运算的方式进行出块者选择，即节点通过大量哈希运算来寻找解决难题的随机数据，也就是挖矿，在这一过程中，由于哈希函数运行结果的

不可预测性，任何节点在哈希运算上不存在优势，是纯粹算力的竞争，而 50%以上安全算力就保证了出块者中大部分是诚实节点，进而保证了链的安全性。

2.类 BFT 协议的安全假设：2/3 以上节点安全

在这一安全假设下，类 BFT 协议通常采用轮流坐庄或概率选择的方式进行出块者选择，无论采用哪种方式，都必然能够保证诚实节点获得多数出块权，同时要求共识网络中节点必须对提议的区块进行投票，只有获得了 2/3 以上投票的区块才算最终合法区块，进而保证了链的安全性。

3.权益证明（PoS）的安全假设：50%以上权益安全

在这一安全假设下，PoS 协议通过依据节点权益持有量比例随机选取出块者，而这一选择的关键就在于安全性，保证了随机源的安全就保证了在大量出块者选择过程中诚实节点能够获得多数出块权，进而主导链的发展，保证链的安全性。

上面介绍了常见共识协议在不同安全假设下出块者选择的设计方法，当然也有特殊的混合模式，这里不进行详细论述。由上可见，合理的出块者选择对保证链的安全极其重要，可以用一个简单的反向例子来直观理解，如果在 PoW 挖矿中，某个恶意节点找到了挖矿的窍门进而获得了半数以上的出块权，那么其就可以任意地重构链来实现双花等攻击，任何一笔交易都将不再可信，这将是对 PoW 生态系统的毁灭性打击。

我们再来简单说说出块者选择对保证链活性的重要意义。简而言之，就是链可以持续稳定地发展延长，有效合法的交易经过一段时间可以得到确认。出块者本就担负着链发展建设的重任，很显然其就是保证链活性的主体，有很多共识模型（如 Snow White）对于保证链活性都有深入的研究和探索。总体来说，保证链活性，需要解决两个问题：一是保证出块者活性，被选中的出块者要活跃积极地参与共识过程，而不能处于离线或者休眠状态，进而导致大量区块缺失，影响链的正常发展；二是保证节点间数据一致性，诚实节点必然能够接收到有效合法交易，并诚实地将其打包进入区块上链确认。加上上面对安全性的论述就能保证链的活性。而出块者的活性就要由出块者选择来保证，这一选择是一个广义的概念，并不一定狭义地体现在具体选择算法之中，而是在整体的设计理念里加以考虑，Wanchain 的星系共识中对此进行了着重思考，并通过权益概念的全新定义、委托机制的设计和奖惩机制的刺激妥善解决，后续将具体解释。

（二）出块者选择算法需要考虑的几个问题

上面介绍了出块者选择算法的重要性，那在设计一个出块者选择算法时应该重点考虑哪些问题呢，或者哪些性质才是评定一个出块者选择算法好坏的衡量标准呢？

1.公平性

出块权是依据共识节点资质均衡分配的。例如 PoW 中算力越高，获得出块权的机会越大，而 PoS 中权益持有量越大，获得出块权的机会越大。这是一个很自然合理的性质，但它的外延很广，出块者选择就像博彩，想实现真正的公平性也需要规避很多问题，我们以

一个例子来说明：假设 A 和 B 是两个共识节点，通过掷骰子的方式决定谁是出块者，点数为奇数则 A 获得出块权，为偶数则 B 获得出块权，公平条件下，骰子被“上帝”掷出，A 和 B 的机会各一半，而如果 A 获得了掷骰子的权利，那么公平性就被打破了，其可以多次试验甚至直接摆出奇数点数来霸占出块权，进而独自决定链的发展甚至肆意进行攻击，这是十分可怕的。

2.可验证性

出块权的合法性是可以被公开验证的。例如 PoW 中区块头哈希值小于难度值可以被全网运算验证。这条性质是显而易见的必然要求，区块链作为去中心化的系统，其运行必然是接受全网监督认可的，区块的合法性验证是基本要求之一，而区块的合法性中除了交易合法性和结构合法性外，出块者的合法性也是必须被验证的一点。

3.匿名性

出块者通过匿名方式隐私参与共识。这条性质并不是必然要求，之所以提出是因为匿名性可以应对共识中可能出现的安全风险，如腐蚀攻击。具体来说，如果出块者在其出块权归属时间之间被全网所知，那么恶意节点有可能通过贿赂等方式将其腐蚀，把原本的诚实节点变成恶意节点，进而进行攻击，甚至直接进行网络攻击导致出块者掉线，这就增强了恶意节点的攻击能力或削减了诚实节点获得的出块权，所以实现匿名性对于共识协议来说也是一个需要考虑的问题，很多项目（如 Dfinity、Algorand）大多采用 VRF 算法来实现匿名性，但 VRF 算法也存在其自身的缺陷和弊端，现在也有项目（如 Ouroboros Crypsinous）提出使用零知识证明进行匿名共识，但还没有具体实现。

（三）常见的出块者选择算法

1.算力竞争

算力竞争的方式是区块链系统里最早使用的出块者选择算法，最典型的就是比特币系统，是比较简单粗暴又直接有效的方式。共识节点打包交易后，通过不断调整区块头中的随机数来反复运算区块头的哈希值，当哈希值小于当前区块要求的难度值时就形成了符合要求的合法区块，此时就获得了出块权，成为一名合法的出块者，也就是完成了整个挖矿过程。这种方式的好处就是对于所有参与节点都是公平的，任何节点不会在哈希运算上取得优势，只要总体算力超过一半是安全的，那么链就是安全的。同时，这种方式在同一区块高度可能存在多个合法区块和合法出块者，会出现短暂分叉，这也是系统需要等待确认时间的原因。目前来看这种出块者选择算法是共识协议中去中心化程度最高的，当然随着技术的发展和研究的深入，挖矿也从最初的 CPU 挖矿逐步发展到 GPU、ASIC 挖矿，算力增长迅速，很多项目为抵抗芯片挖矿通过增加存储要求设计了新的共识协议，如 Zcash 的 Equihash。

2.Verifiable Random Function（VRF）

VRF 用于出块者选择算法是为了解决匿名性而提出的，具体方式是先设置一个合理的阈值，节点利用自身的私钥对某一随机数据进行运算（如签名），得到的结果小于设置的

阈值则为合法出块者，获得出块权。这一过程中由于私钥运算只能通过节点自身进行，保证了其他节点不能获知出块权归属，而计算结果如签名结果可以被公开验证，确保了出块权合法性可以被验证，形成了完整的出块者选择过程。显然，这种方式是概率性的，若想某一区块高度可以有尽量多的合法出块者，就需要尽量提高阈值；反之想某一区块高度可以有尽量少的合法出块者，就需要尽量降低阈值，这对阈值的设置就有极高的要求，同时对私钥运算结果的分布也有较好的预期，这往往是很难做到的，就容易出现某一区块高度有大量合法出块者而形成密集分叉，某一区块高度没有合法出块者而形成空白，所以 VRF 算法虽然解决了匿名性问题，但在具体使用中仍然存在难以避免的问题。

3.Follow-the-satoshi

Follow-the-satoshi 是 PoS 中常见的一种出块者选择算法，具体方式是将所有的代币进行排序编号，通过一个随机源产生一个随机数，这个随机数落到了哪个代币的编号上，那么这枚代币的持有者就是合法的出块者，获得了出块权。这种方式显然是唯一确定性的，难点就在于如何找到一个安全的随机源来产生真随机数。Cardano 项目当前就采用了 Follow-the-satoshi 的方式进行出块者选择，其随机数的生成使用了多方计算、门限秘密分享等多种密码学技术，保证了随机源的安全性，但在出块者选择的匿名性上还没有实现。但就随机数生成而言，另一种方式就是使用链上的某段历史数据的哈希值，其中以 Algorand 为代表，将之前某个区块的数据和当前区块高度进行混合运算哈希值作为随机数，算是一个较好的伪随机源，但仍有被刻意控制的风险。

（四）Galaxy ULS 算法原理流程

兜兜转转介绍了这么多，最后还是要回到我们的主题，Wanchain 星系共识的出块者选择算法——ULS 算法，ULS 代表的是唯一出块者选择，ULS 算法在设计之初就考虑到了公平性、可验证性和匿名性，采用了秘密分享、零知识证明等多种密码学手段，实现了固定时间窗口内的唯一合法出块者的匿名选择，在保证链安全性的基础上，尽量降低短分叉概率，提升共识效率，下面我们就形象化地介绍星系共识 ULS 算法的整体原理流程。

EL 星群节点是运行 ULS 算法的主体，那我们就从 EL 星群的来源说起，在 PoS 协议中，话语权由权益持有量决定，而我们将这一对应关系在 EL 星群的选择过程中进行实现。基于 Wanchain 共识合约中当前 Committee 的质押状态，可计算每个节点的权益值和其权益比例，利用 Random Beacon 提供的随机数，运用 Follow-the-stake-ratio 算法，类似于 Follow-the-satoshi 的过程，形象地说，就是 Committee 中节点按照其权益比例划分了一块钟表的表盘，每个节点拥有一段与其权益占比相同的时间窗格，然后随机数就是拨动时间指针的上帝之手，指针落到哪个时间窗格，此窗格的拥有者就被选入 EL 星群，每轮选择独立进行，某一节点有可能被多次选入，所以最后 EL 星群有可能是一个多重集，选出的 EL 星群将肩负起运行 ULS 算法的责任（见图 4）。

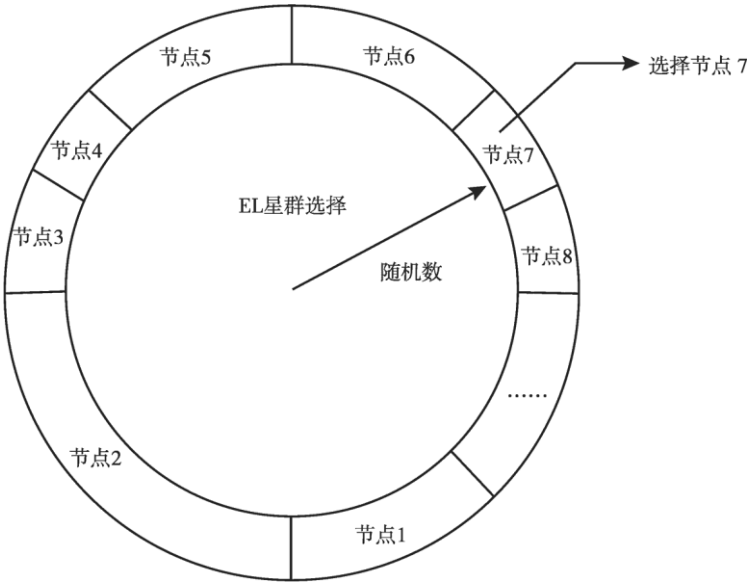

图 4 EL 星群选择示意

（1）秘密消息序列（Secret Message Array）生成

EL 星群被选择组建之后，需要先进行一次链上的通信协商，这一过程是为了在星群内部生成一个秘密消息序列，以用于后续出块权分配，是我们实现匿名性的关键一步。为保证秘密消息序列不会被某些恶意节点控制，进而影响到后续算法运行，我们将这一过程拆分成两个阶段，也就是 SMA1 和 SMA2。在 SMA1 阶段，星群中每个节点选择一个随机数，将其利用自身公钥加密后发送到链上，完成对随机数选择的承诺，保证任何节点选定的随机数在后续阶段不可更改。在 SMA2 阶段，星群中每个节点将自己选择的随机数用所有节点（包括自身）的公钥加密发送到链上，同时提供协调性证明（DLEQ-Proof），这里对照在 SMA1 阶段利用自身公钥加密的数据就可确保随机数并未更改，同时协调性证明保证了所有公钥加密的都是同一个随机数。这一阶段完成后，所有 EL 星群节点都可以自行解密，得到随机数据序列，也就是我们的秘密消息序列，准备运行出块权分配算法（见图 5）。

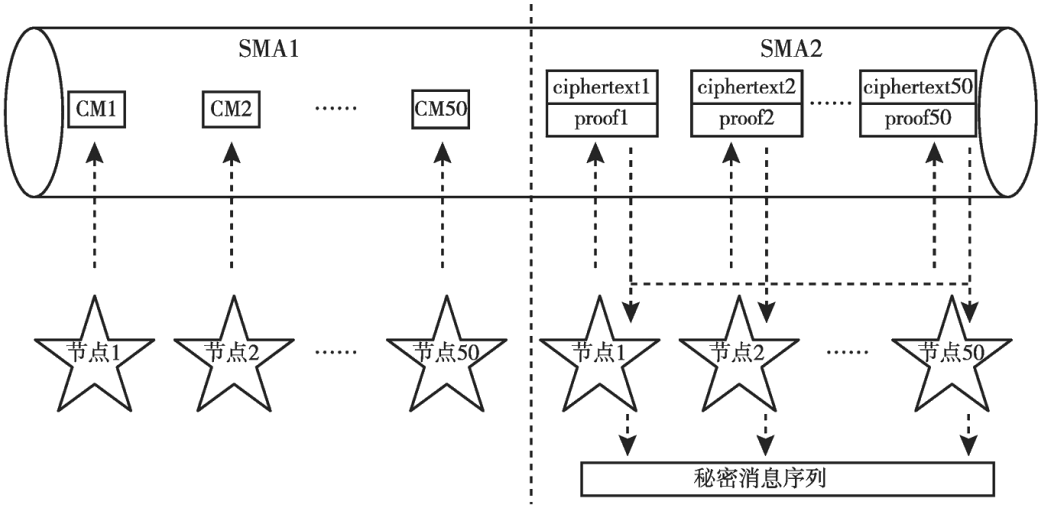

图 5 秘密消息序列示意

（2）EL 星群节点排序

秘密消息序列生成后，随机数进行更新，新产生的随机数将作为种子对 EL 星群节点进行排序，具体方式就是将星群节点公钥与随机数接续进行哈希运算，基于运算结果进行升序排列，这一排序结果将用于后续出块权分配。显然，排序是在秘密消息序列后基于新随机数进行的，任何节点无法影响，完全是随机的排序结果（见图 6）。

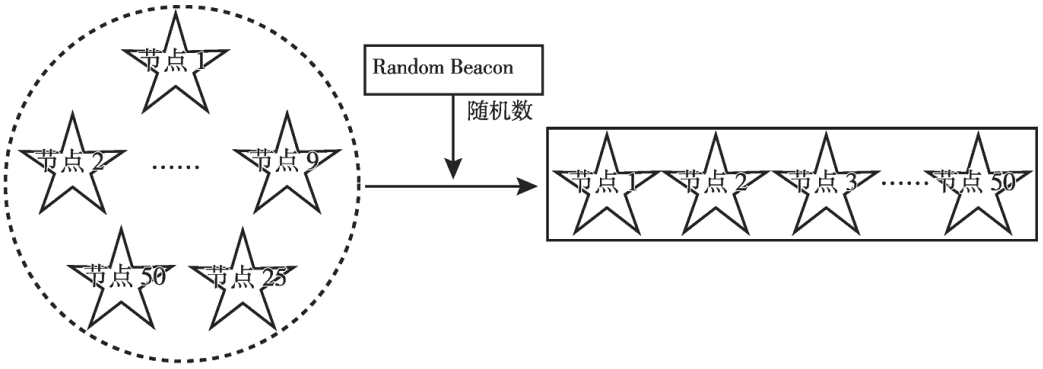

图 6 EL 星群节点排序示意

（3）出块权分配

在上述三项工作完成后，就可以为 EL 星群节点进行出块权分配。在之前的解读中我们说过，一组 EL 星群负责一个 epoch 内区块的生成，那么这个 epoch 内每个 slot 的出块权如何决定呢？首先将当前随机数和 epoch 编号、slot 编号进行哈希运算，运算结果取 EL 星群节点数量的模结果，如哈希值是 2019，目前 EL 星群节点数量 50，取模结果就是 19，那么 EL 星群节点排序中的第 19 位即被选为合法出块者，获得出块权。这一选择过程是等概率进行的，结合 EL 星群节点选择时的按权益比例进行，确保了出块者选择是按权益持有量合理进行的，确保了公平性；合法出块者在提出区块时需要提供合法性凭证，这一凭证可被公开验证，确保出块合法性的可验证性；合法出块者选择中使用了秘密消息序列，而这一消息序列只在 EL 星群内部共享，其他节点不可知，就保证了选择过程的匿名性（见图 7）。由此可见，ULS 算法是全面考虑了公平性、可验证性和匿名性的创新性设计，将对保证链的安全性和活性起到积极作用。

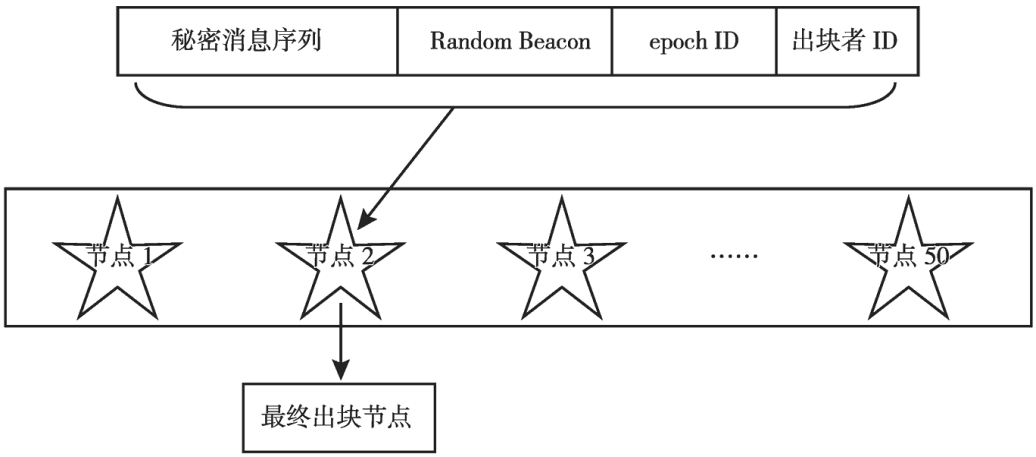

图 7 出块权分配示意

五 共识机制之委托机制

随机数生成算法以及出块者选择算法这两个算法在确定了共识参与者之后使共识过程能够安全稳定的进行。那么，如何才能够让所有的权益持有者参与到共识过程中呢？

（一）星系共识委托机制设计背景

当前区块链业界已经有了众多 PoS 共识机制，它们或由严谨细致的学院派提出，或由拥有丰富从业经验的产业界提出，但是都普遍缺乏实用性，体现在如下几点。

1.实际参与门槛较高

一方面，PoS 共识协议虽不同于 PoW 对算力的高依赖性，但是也要求参与者节点有较好的计算能力和网络带宽，能够及时地完成协议内容，因此 PoS 参与者需要投入一定的硬件资源；另一方面，PoS 的收益分配原则是“权益越大，收益越大”。二者相结合的结果就是参与 PoS 有较高门槛，即只有拥有较高权益的节点才会有足够的动力去参与 PoS，拥有较小权益的节点则由于参与 PoS 的成本高于预期收益而被“拒之门外”。这个“门槛”虽不在 PoS 理论设计中，但是现实存在的。

2.中心化风险

由于参与门槛较高，只有较大权益拥有者可以参与到 PoS 共识过程中，从而获取共识收益。而获取的共识收益会拉大共识参与者和非参与者之间的权益差距，陷入“富者愈富，穷者愈穷”的恶性循环，最终可能导致共识中心化的风险。

3.违背基础安全假设的风险

几乎所有 PoS 共识机制的安全基础为诚实大多数假设（Honest Majority Assumption），即诚实节点占参与共识协议权益的大多数。这个假设对于整个区块链网络是成立的，但是如果共识参与门槛很高，只能吸纳一小部分权益参与到共识过程中，那么具体到 PoS 共识协议中这一假设就未必成立了。这本质上是一个取样问题，当样本量较小时，并不一定具有整体的统计特征。

因此，如何设计一种机制能够降低 PoS 参与门槛，尽可能吸纳更多的权益参与到共识过程中，对整个共识的实用性和安全性都具有重要意义。

（二）星系共识委托机制的意义

星系共识在设计之初就充分考虑了协议的实用性。这个实用性不仅体现在减少共识过程中需要的计算和存储资源，还保证共识的参与者能够顺畅地参与到整个过程中。星系共识具有完整的委托机制，拥有较大权益的节点可以直接参与到共识过程中，而拥有较小权益的节点可以通过委托机制参与到共识过程中。完整的委托机制降低了 PoS 共识参与的门槛，提高了星系共识的实用性，与其他 PoS 共识协议相比具有明显优势。

（三）星系共识委托机制的理论基础——委托签名（Proxy Signature）

委托签名是密码学中的一种特殊签名算法，它能够使一个个体，即委托者或原始签名者（Original Signer），将自己对消息签名的权利委托给另外一个个体，即被委托者（Proxy Signer）。被委托者能够计算出一个委托签名，任何拥有原始签名者公钥的个体均可以验证签名的合法性（见图 8）。严格来说，委托签名算法为多个算法的集合，其中一个是标准数字签名算法（比如 ECDSA），一个是委托和接受委托的算法，一个是委托签名生成算法，一个是委托签名验证算法。

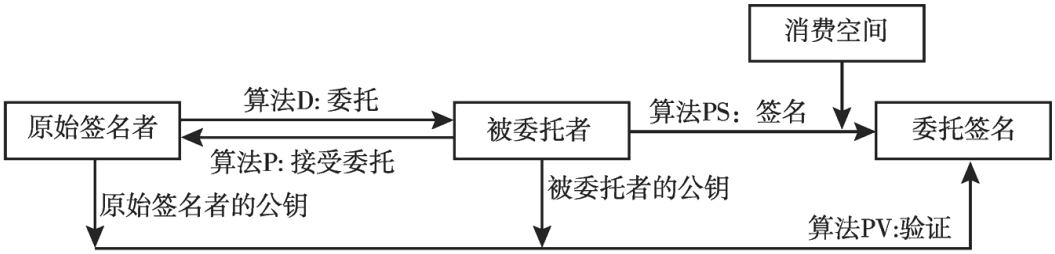

图 8 委托签名流程

（四）星系共识委托机制的流程

星系共识的委托机制基于 T-ECDSA 委托签名算法（Triple ECDSA Proxy Signature）实现，这一算法由 Wanchain 理论团队设计提出，兼具通用性、安全性和高效性。同时结合智能合约，星系共识实现了完整的委托机制，使任何 WAN 的持有者均可以加入星系共识中，维护网络安全，并获取共识收益。假设 Alice 为一名普通的 WAN 持有者，公私钥对为 pki/ski；Bob 为一名星系共识的受托验证节点，公私钥对为 pkj/skj；Proxy_SC 为一个特殊智能合约，用于验证并存储委托过程中的相关数据。现在 Alice 要委托 Bob 去代替自己参与星系共识，具体流程如下（见图 9）。

第 1 步：Alice 在本地将自己的私钥、Bob 的公钥输入 T-ECDSA 算法中，生成委托证书。

第 2 步：Alice 构造一笔交易，将委托证书发送到 Proxy_SC，同时委托资金锁定在 Proxy_SC 中。

第 3 步：Proxy_SC 验证 Alice 所发委托证书的合法性，并生成代理公钥和委托证书一同存储在合约中。

第 4 步：Bob 对 Proxy_SC 中存储的证书进行解析，利用自己的私钥计算得到代理私钥。

第 5 步：代理私钥作为独立身份参与星系共识，Bob 通过代理私钥完成共识过程，获取共识收益。

第 6 步：共识收益按照委托约定，在 Alice 和 Bob 之间进行分配。

第 7 步：委托期结束后，Proxy_SC 将委托资金返还到 Alice 账户中。

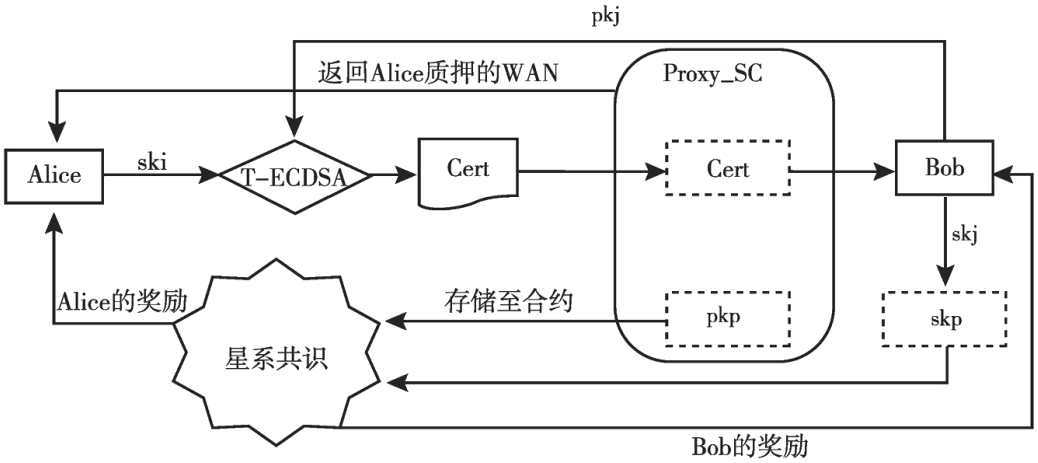

图 9 Alice 委托 Bob 代为参与星系共识

（五）星系共识委托机制的优势

1.通用性

星系共识的委托方案在标准签名、权利委托和委托签名中均使用 ECDSA 签名算法，这一算法也在区块链领域广泛使用。它与已有的区块链技术架构完全兼容。无论是直接注册加入共识机制中，还是通过委托机制加入，对参与者出块的验证逻辑完全一致。

2.非交互

委托的过程是非交互的，因此委托者和代理节点之间不必建立安全的通信信道，完全通过链上交易完成委托，在共识过程中更加高效。

3.高安全性

已有的一些委托机制，往往需要委托者将资金转入代理节点账户，由代理节点直接参与共识，并完成收益分配。这种方式是中心化的，对代理节点诚信度要求较高，容易发生“携款跑路”的现象，对委托者资金安全产生巨大影响。星系共识的委托机制基于密码学算法实现，委托者的本金被锁定在智能合约内，代理节点只获得委托者的参与共识的权利，并不对用户资金具有任何控制权，因此能够充分保障用户的资金安全。

4.公开透明

星系共识委托机制中，委托的过程以及代理节点参与共识的数据都在链上进行存证，所有数据公开透明。一方面，保证代理节点能够公平分配共识收益，无法作恶；另一方面，也方便委托者能够对代理节点的活性进行甄别，从而选择合适的代理节点。

六 维持共识正常运转的原动力——经济激励

（一）经济激励机制的重要意义

经济激励机制是共识协议设计的核心部分之一，一个合理的经济激励机制之于共识协议就如同共识协议对整个区块链生态系统一样，有着极其重要的意义，它是激励共识节点诚实运转、抑制恶意行为的经济运行体系，是建立在技术基础之上的经济驱动力。

狭义上看，经济激励机制是维持节点运行、保证链安全和链活性的基本保障。

对于区块链系统来讲，共识节点负责打包交易、生成区块，承担着链发展延续的重任，是保证链安全的关键，也是维护链活性的主体，所以在共识协议的设计过程中，大量的技术手段被反复研究和实践，核心目的就是要建立一个健康高效的共识运行体系。但在这样的协议设计下，节点为何要参与其中，是什么驱使节点维护区块链系统呢？这就是共识设计中经济激励机制需要发挥的作用，它为共识节点注入了利益驱动力，让节点在运行共识协议的过程中获得经济奖励，这部分奖励需要覆盖节点维护运行的成本，同时需要把额外部分作为节点的收益，这样节点才可能在参与共识中有利可图，才会有意愿去维护系统的发展运行。一个好的经济激励机制设计，是鼓励共识节点诚实运行的正能量，它会将诚实节点的利益最大化，只有忠于协议的行为才会让节点收益最高，同时令恶意行为成为损害节点利益的原罪，如此从经济环境上营造协议健康运行的良好氛围，让共识节点积极主动地承担起保证链安全和链活性的职责，保障了整个系统的健康发展。

广义上看，经济激励机制是区块链生态运转、承载价值流通的基础支撑。

经济基础决定上层建筑，在整个共识协议的体系之中，经济激励机制起到了支撑性作用。当前，区块链技术正在推动信息互联网向价值互联网转变，第一个分布式网络的出现建立了一个去中心化的价值体系，将价值的定义摆脱中心化的控制，转换成共识意义下的价值存在。我们知道，价值重在流通，只有可以自由流通的价值才有其自身存在的意义，中本聪设计的经济激励机制是产出价值的源泉，节点通过记账工作获得价值，同时又在记账工作中完成了价值的传递和流通，这就让整个价值体系形成了完整的闭环，拥有了迭代延续的活力。由此可见，经济激励机制是推动区块链生态系统的动力之源，它激励着共识的运转，共识承载着价值的流通，而流通赋予了价值意义，有意义的价值再反补经济激励机制的运行，在这个完整的闭合流程中，经济激励机制既是起点又是中继，是整个价值体系的点火器和助燃剂，起到基础支撑性的作用。

（二）经济激励机制需要考虑的几个基本问题

说明经济激励机制的重要意义，我们需要知道一个好的经济激励机制是鼓励诚实行为、抑制恶意行为，那么在设计中需要考虑哪些基本问题呢？

1.哪些主体需要被奖励

显然，我们设计共识协议中的经济激励机制，自然是要奖励共识节点，然而在不同的协议设计下，共识节点的范围和外延也并不相同。

在采用 PoW 共识协议的主流公链系统里，“挖矿”或者“矿工”是一个耳熟能详的概念，而这些节点之所以被称为“矿工”，是因为其提供了算力进行哈希运算，在这样的共识中，只有这部分节点为共识做出了贡献，所以其可以在每个自己提出的区块中给自己发放一定量的奖励，当然后续在共识的开发中为了奖励那些虽然提出了合法区块，但最终没被选中的区块提出者设定了“叔块”的概念，并给予少量的奖励，以表示对其工作的认可，这里不进行详细解释，感兴趣的读者可以参考以太坊网络创始人 V 神的文章（参见 https：//blog.ethereum.org/2014/07/11/toward-a-12-second-block-time/）。

在 Ouroboros 和 Dfinity 等采用 PoS 共识协议的系统里，参与共识的不仅提出区块的这些节点，在上面解读文章中都有反复强调，而且为了在共识协议中引入熵，必须有一个可信的随机源，而采用某些历史数据的组合运算得到的只能是伪随机源，所以这里就需要有一组节点专门来产生随机数，这些节点的工作也是共识中必不可少的一部分，其当然也就是需要被奖励的共识主体之一，也就是说，在这种类型的协议中，被奖励的主体有区块提出者和随机数生成者两类节点。

在 EOS 和 Cosmos 等采用拜占庭容错（BFT）共识协议的系统里，参与共识的节点需要为候选区块进行投票，只有获得一定比例投票的区块才会被确认合法，其中候选区块的提出也由这些共识节点轮流负责或概率性选择进行，所以相对简单地，在这类共识协议中，需要被奖励的主体就是这些负责投票的节点。

2.奖励来源，如何保证奖励的持续性

对于奖励的来源，一般分为两种。一种是在系统运行初始时就设定好了奖励的总额，然后按照分阶段等比例递减的方式释放，在每个区块中自然添加固定数额的奖励，这也是“挖矿”说法的来源；而另一种往往在 PoS 的共识协议中出现，常常是由基金会拿出一定量的初始资金用于奖励共识，这部分资金的释放也采取分阶段等比例递减的方式进行。

显然，我们上面讨论的都是无增发状态下的奖励来源，我们不对增发奖励的情况进行讨论，因为没有依据的增发只会稀释奖励的价值，对整个生态系统的价值体系造成伤害。而上面的两种方式很显然是无增发的，这种情况下，在生态系统建立健全的过程中，价值是在无形之中被提高的，也就维护了价值体系的稳定。然而，我们可以看到，这种奖励是随着时间自然减少的，会不会出现运行时间越久，共识节点积极性越差的情况呢，这就涉及如何保证奖励的持续性。这个问题在设计中必然是要考虑的，除了调整奖励变动比例和变化周期等参数的方法之外，最重要的是，奖励除了上述固定来源之外，还有每个区块中的交易费，这些交易费是由交易发起方为共识节点记账工作提供的报酬，随着生态系统的

完善、交易的增多、价值的增长，这部分报酬将逐步成为奖励的主体，成为支持共识运行的持续动力。

3.如何保证奖励的公平性

谈到奖励的公平性，这是一个很宽泛的概念。我们在星系共识的黄皮书中提到经济激励机制的基本原则，第一条就是贡献越多，奖励越多，这是一个自然合理的要求。举例来说，如果节点参与共识，然而报名之后却什么工作都不做，既不在自己该提出区块时去打包交易构造区块，又不在自己该参与随机数生成的时候去完成信息提交，那么这种懒惰的节点显然就不应该被奖励，否则就是对其他完成工作的共识节点的不公平，所以在进行奖励的时候就要有一个评判的标准。而在星系共识中提出了活性系数的概念，依据活性系数，为积极完成好工作的节点提供应得的奖励，而消极怠工的节点将被扣除部分甚至全部奖励，以营造公平合理的良性竞争环境，确保共识协议的健康运行。

4.如何在经济激励中权衡委托机制

先从委托机制的意义入手来思考这个问题，首先它是为了降低共识参与门槛，也就是给少量权益持有者一个参与共识的机会，相当于给自身的权益寻找代理，自己并不运行节点，那么其就应该给被委托人提供代理的手续费用，所以我们设置了委托费率，这些委托人需要从获得的奖励中拿出一部分给被委托人，作为代理的报酬。同时，必须思考另一个问题，当被委托人接受了大量权益委托时，虽然其自身持有的权益并不多，但其在共识中的话语权很大，那么这个被委托人可能愿意冒着自身少量权益受损的代价去做出恶意行为以企图获得更高的收益，这显然是我们不愿意看到的，所以在委托机制的激励中设置了“天花板”的概念，直观来讲就是为可接受委托额设置了上限，我们并不直接制止超过上限的委托行为，但是我们从经济激励中添加了控制的元素，我们希望通过正常的市场行为来调节委托机制的运转，既体现了委托的意义，又控制好安全的风险，在经济激励机制设计中做好对委托机制的权衡。

（三）常见的经济激励方式

说明经济激励机制的重要意义和需要考虑的几个基本问题后，我们来讲讲经济激励有哪些常见的方式。一般来讲，经济激励有两种方式，即正向鼓励和反向抑制。

正向鼓励，鼓励的是忠于协议的诚实行为。简单来说就是，对于那些按照协议要求严格完成自身工作的行为，通过发放奖励的方式进行支持，例如，在星系共识中，对参与并完成每轮随机数生成的 RNP 节点，给予相应的奖励；对参与并完成秘密信息序列（SMA）共享的 EL 节点，给予相应的奖励；对在自身负责的 slot 中打包交易提出合法区块的 EL 节点，给予相应的奖励，这就是正向鼓励，是刺激协议良性运行的推动力。

反向抑制，抑制的是不良企图的恶意行为。这种方式出于保证安全性的考虑，希望能够从利益驱动角度消除作恶的动机。抑制的方式往往也有两种，一种是常见的 slash，也就是惩罚，这种方式往往需要有一个监督的体系配合，需要有恶意行为的证据提交，再基于这些证据对节点恶意行为进行制裁，一般是通过扣除节点质押金实现，而怎样鉴定一个恶

意行为是这里的难点，目前已经实现的有双签、长程攻击等。另一种是降低出现恶意行为节点的收益，也就是我们在先前提到的只有忠于协议的诚实行为才能利益最大化，举例来说，在星系共识中，如果参与随机数生成的节点试图扰乱这一过程，在不同阶段提交不相协调的信息，那么这些信息将被排查出问题而无法上链，在奖励分发的时候，这些节点将得不到奖励，这样就抑制了这种恶意行为的出现，这种抑制方式的设计难点在于如何在奖励清算中涵盖对恶意行为的考虑并有所体现，这将是一个需要持续深入研究的问题。

（四）Galaxy 经济激励机制模型原理

围绕经济激励机制介绍了这么多，最后回到我们的主题——Wanchain 星系共识的经济激励机制，经过诸多考虑和研究，最终星系共识的经济激励机制实现了一个完整的闭环，营造出一个良好的共识运行环境。

星系共识的奖励来源于一部分的万维链基金会通证发行总量，此后等比例逐年递减，在同一阶段内按 epoch 均分，当然每个 epoch 内所有交易费用也将计入奖励之中，这里并不按区块分发，而是每个 epoch 进行一次结算，交易费用计入奖励总额在 RNP 和 EL 节点间分配，这是基于交易费将逐步成为奖励主体而进行的考虑，以保证所有参与共识节点的利益。我们认为，在共识运行中，RNP 和 EL 节点的作用与贡献是同等重要的，所以在每个 epoch 结算中，奖励将在 RNP 和 EL 节点间平均分配，即如果每个节点都诚实运行，完成自身工作，那么获得的收益是相同的。下面我们分 RNP 和 EL 节点两个主体进行具体介绍，并将委托机制作为单独一部分说明。

1.RNP 节点的经济激励

前面我们反复强调共识协议中随机数的重要作用，也说明 RNP 节点必然是需要奖励的主体之一。对于 RNP 节点来说，工作逻辑相对清晰，如何鉴定其工作诚实完成也相对容易，首先我们来看 RNP 节点参与随机数生成需要完成的工作：①在 DKG1 阶段提交承诺；②在 DKG2 阶段提交加密数据和 proof；③在 SIGN 阶段提交签名碎片。而这三者是一个完整的过程，只有全部正确参与才算完成了随机数生成的工作，所以对于 RNP 节点来说，必须正确完成上面三项工作才能得到奖励，缺少或错过任何一项都拿不到任何奖励（见图 10）。

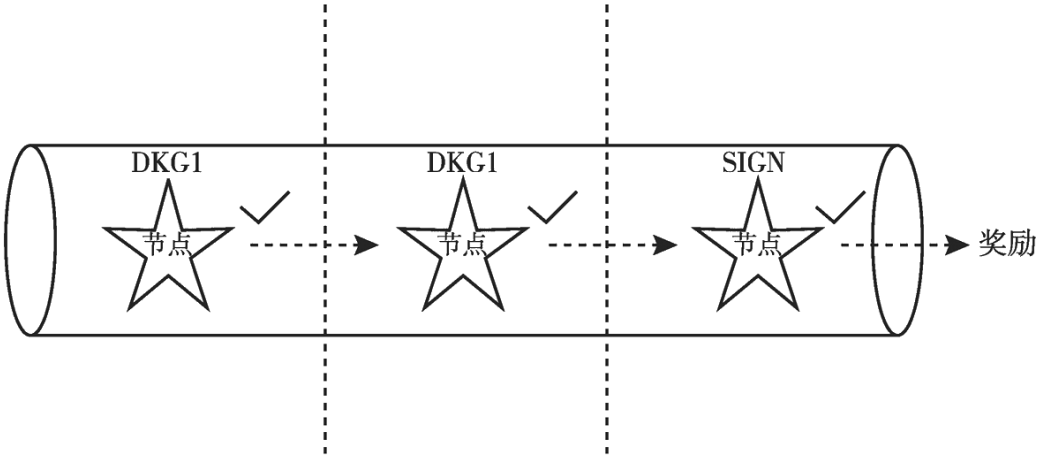

图 10 RNP 节点的经济激励示意

2.EL 节点的经济激励

类比于 RNP 节点，我们先梳理 EL 节点需要完成的工作：①在 SMA1 阶段提交承诺；②在 SMA2 阶段提交加密数据和 proof，完成秘密信息序列共享；③完成自身负责的 slot 打包交易，提出区块。显然可以按照工作内容切分为两部分，前两项为秘密信息序列共享，后一项是生成区块，所以 EL 节点的总体奖励将拆分为两部分，一部分用于奖励秘密信息序列生成，另一部分用于奖励区块生成。与随机数生成类似，秘密信息序列生成的两个阶段是一个完整的过程，只有全部正确参与才算完成，所以 EL 节点只有正确完成这两阶段工作才能得到这部分奖励，缺少或错过任何一项都拿不到这部分奖励。而对于生成区块的奖励，我们加入了活性系数进行调节，将所有 EL 节点作为一个整体，依据 epoch 内最终区块数和 slot 数的比例均分这一部分奖励，群体活性越高，完成工作越好，得到的奖励越多，从而促进链的高质量生长（见图 11）。

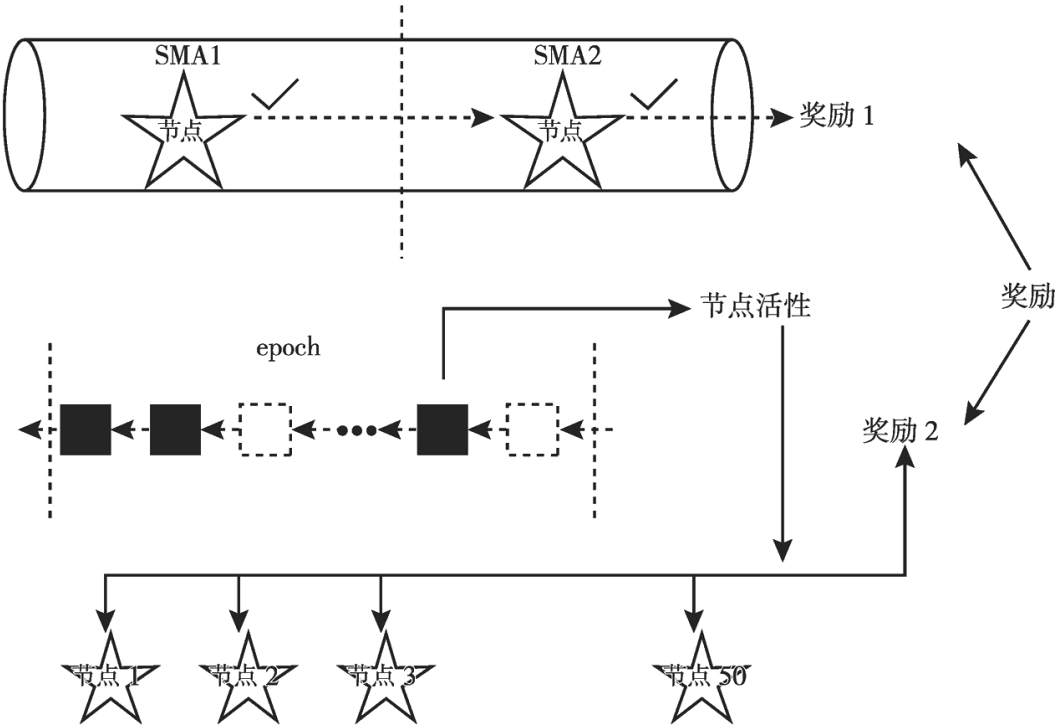

图 11 EL 节点的经济激励示意

3.委托机制

前面已经提到，在委托机制中，委托人需要从奖励中依照委托费率的比例拿出一部分交给被委托人作为报酬，剩余部分作为委托人参与共识的收益，而两者的奖励都受到被委托人当前接受委托值和可接受委托上限的影响，当接受委托值超过上限，两者的奖励都将减少，直至最终归零（见图 12、图 13）。

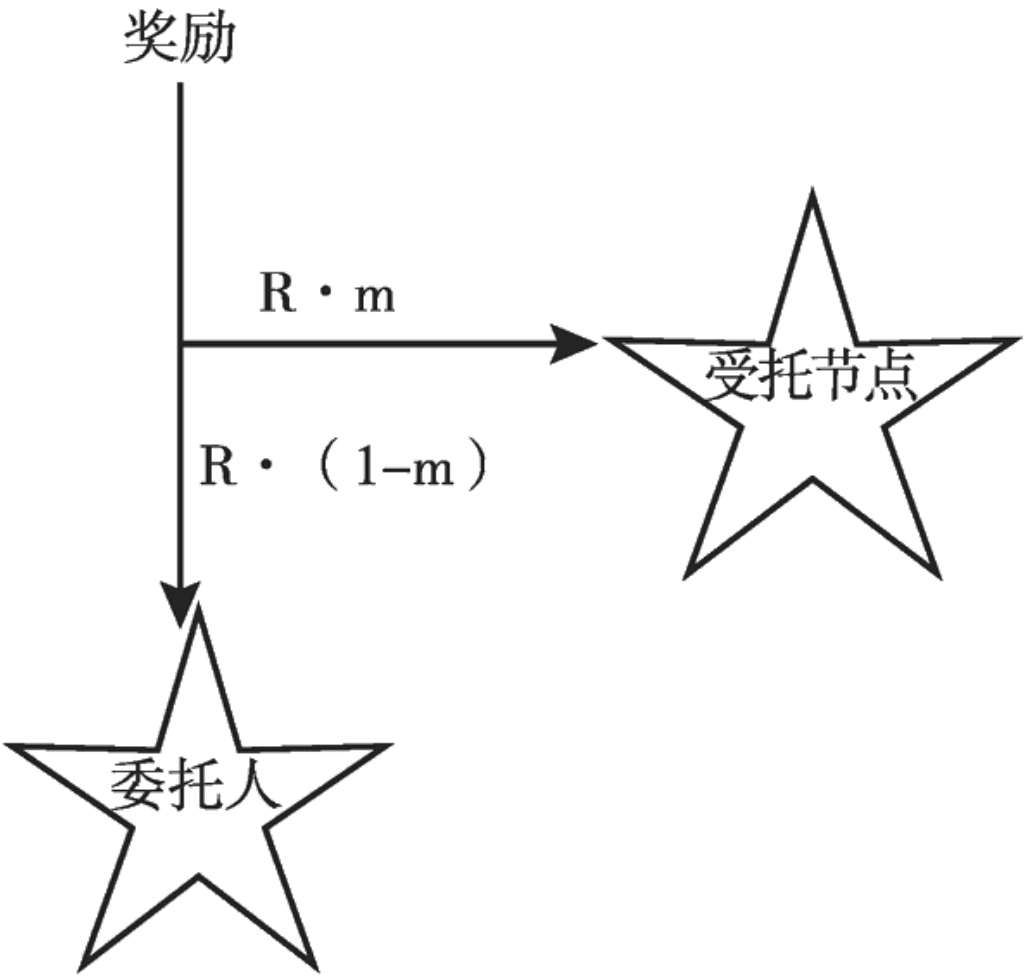

图 12 委托机制之受托节点和委托人的奖励分配关系

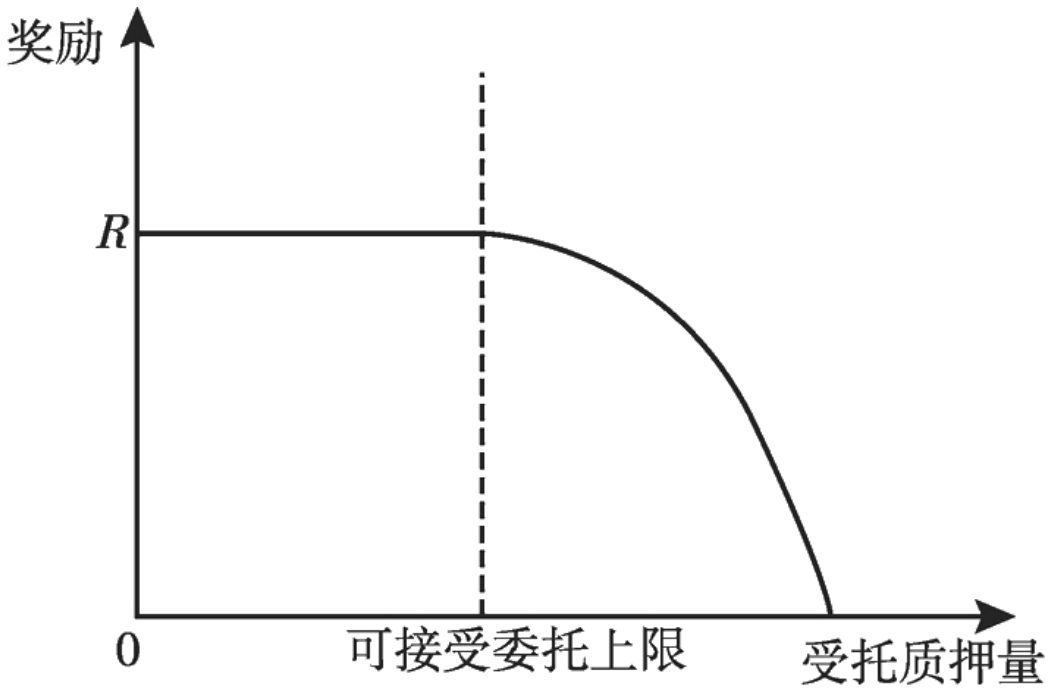

图 13 委托机制之奖励和可接受委托上限的关系