MOS

MOS
公链技术白皮书

基于DAO2.0分布式自治社群架构的全新一代公链

用区块链技术实现金融普惠

目录

1. 摘要

自中本聪（Satoshi Nakamoto）于 2008 年 11 月发布《比特币：一种点对点的电子交易系统》(Bitcoin: A Peer to Peer Electronic Cash System)论文以来，以区块链技术为支撑，以比特币为代表的加密数字资产市场已经从无到有，发展成为了一个**总市值超越 2000 亿美元、日交易额高达近 800 亿美元**的产业。同时随着区块链技术的兴起，包括传统 IT 供应商、金融机构、公共部门在内的各种公司、组织，都在尝试寻求基于分布式账本技术（DLT）的解决方案，升级现有的产品或服务，特别是在供应链、信息管理系统、金融清算、结算和托管服务等应用领域。**区块链技术有可能彻底改变国内和国际商业环境中金融交易的构建和完成方式，是过去十年来全球金融领域出现的最大变革。**

简而言之，区块链就是一个不断增长的记录列表，使用加密技术进行链接和保护。区块链可以作为一个开放的分布式账本，以可验证的、永久的方式有效记录双方之间的交易。区块链通常由对等网络（P2P）管理，共同遵守验证新块的协议（即“共识协议”）。一旦被记录，任何给定区块中的数据都不能在没有对所有后续块进行更改的情况下进行追溯性更改，因而可以避免欺诈行为，降低信任成本，从而实现一系列潜在的应用。**区块链解决了传统金融中“大而不倒”、“中心化”的难题，为去中心化的、分布式的金融组织形式提供了基础。**

正如著名的康威定律（Convey's Law）所揭示的：**“一个系统的功能，最终受限于设计该系统的组织的构建形式。”**区块链技术的发展和应用，也要求其组织架构，从传统的、集中式的公司制形式，转向开放的、分布式的组织模式。这催生了 DAO（Decentralized Autonomous Organization）的诞生，即 “分布式自治组织”。2013 年秋季，Daniel Larimer （也就是 BitShares、EOS 两个项目的创始者）在《Overpaying for security》一文中，提出了类似 DAO 的概念。

构建比特币和以太坊的社群就是典型的 DAO，即通过一系列公开、公正的规则，可以在无人干预和管理的情况下，自主运行的组织形式。这些规则往往会以开源软件的形式出现，每个人都可以通过购买该组织的股份权益，或者提供服务的形式，成为该组织的参与者。

- **从计算机科学的角度来看，DAO 就像一个全自动的机器人，当它全部的程序设定完成后，它就会按照既定的规则开始运作。**值得一提的是，在运作的过程中，它还可以根据实际情况不断的自我维护和升级，通过不断的自我完善来适合它周围的环境。
- **从经济学的角度来说，DAO 是一种通过经济激励和自我执行准则，自行组织、协调的集体，围绕共同目标合作。**在网络效应的支持下，DAO 为开放的、共享资源的生产提供了收入模式和激励机制。随着更多开放资源的融入，DAO 将能无限地扩展其规模，同时保持敏捷性和一致性，避免了对“中心”的依赖，从而在多个维度超越现有的公司结构。

事实上，DAO 的形态非常广泛，它可能是某种数字货币，也可能是一个系统或者机构，甚至可能是无人驾驶汽车。它们为客户提供有价值的服务。这种服务可以是货币交易（如比特币）、应用开发平台（如以太坊），或者是任意一种商业模式。每个 DAO 都有自身的条款和条件。每个成员都将永远有权查看自己拥有的、可支配的、数字货币形式的 DAO 权益，并有可能从中获得相应的回报。目前，区块链技术因为在可追溯、不可篡改、去中心化等方面的优势，在数字化资产的管理、交易、流动性等金融领域，已经得到了世界各地金融机构的广泛应用，并因此催生了建立针

对金融领域的DAO的需求。但是， 在构建针对特定金融领域的DAO时，下列痛点开始浮出水面，急需采用创新的解决方案：

- DAO需要社群成员对于某个重要的决策达成一定的共识，即所谓的“**决策共识**”。譬如比特币社群关于“扩容”的讨论，或者以太坊社群在被攻击后关于分叉的争议，都可以为理解为决策共识的案例。**如何高效地、低成本地达成“决策共识”，减少组织内耗，这是目前DAO在金融领域实践中面临的核心组织问题。**在过去的公司制治理中，这种方式往往以从上而下的方式决定，但是在分布式的DAO中，需要建立一些即能统一实行，又能针对个体需求灵活定制的规则，而目前的DAO模式，这方面还有待加强和完善。这些规则的特点包括：
    - 满足不同利益群体的个性化需求
    - 制定一定的治理结构和议事规则
    - 调和折衷相互冲突的利益或意见
    - 对成员形成普遍约束的群体决策
- DAO的发展壮大，离不开社群成员的积极参与和贡献，而这源自于对于社群成员贡献的认可和奖励。在区块链过去的发展历史中，存在着基于特定计算机算法的PoW（工作量证明）、PoS（权益证明）和DPoS（权益授权证明）等多种机制，即所谓的 **“算法共识”** 。但是针对各个细分金融领域的独特需求，包括代币融资、点对点抵押借贷、稳定币、去中心化衍生品市场、大宗OTC协作等等，每种业务的参与者需求不同，对于激励机制的要求也各有差别。因此，如果在一个DAO体系中，只采用单一的算法共识，就往往无法凝聚起整个行业的参与度。事实上，很多金融领域的区块链项目都在这方面顾此失彼，无法顾及不同领域、不同专业社群成员的特定需求，从而限制了社群扩大的规模。
- DAO的核心理念是**“去中心化”**，即由社群成员的共识来推动项目、服务、系统等的发展、壮大。只有真正的“去中心化”，才能避免集中式管理所带来的弊病，包括信息沟通不畅、个别人以权谋私等等，这也是区块链技术、DAO与所有传统金融体系、制度的最大区别。但是在目前，绝大部分的DAO项目，包括以太坊在内，个别通过组织、资源、算力等形式拥有特定“话语权”的个人和机构，控制了整个项目的主导权，普通社群成员既无法平等地参与决策，也无法享受到项目发展所带来的正当利益。这样的去中心化，实际上是“伪去中心化”，背离了DAO的根本原则。

为了解决这些由来已久的痛点，MOS团队结合业界最顶尖的计算机算法人才、区块链技术精英、通证经济专家和软件研发力量，汇聚多年来在金融领域的深耕经验，提出了基于**DAO 2.0**的新一代金融公链：**MOS公链**。它具有以下特点：

- 针对DAO目前存在的不足，MOS公链提出了全新的**DAO 2.0**体系，包含从组织构建到投票机制的一整套程序化设定，着力于解决 “决策共识”难题。通过从分布式规则入手，革新现有的所有DAO模式，实现真正的节点网络化，从而为各种分布式金融交易的灵活、稳定运行，消除阻力，让每个社群成员都能够自主地、独立地使用各种金融应用。
- 针对普遍的“伪中心化”现象，MOS公链创新地将VRF（Verifiable Random Function，即可验证随机函数）运用到了社群管理和建设之中，通过用VRF来周期性地挑选社群领袖和委员会，将管理权、自主权完全交由社群控制，实现扁平式的、透明式的管理机制。
- 采用**PoFC**（Proof of Finance Contribution，金融贡献证明）作为算法共识机制。“金融贡献”包括金融交易资源（即“权益”）和社群贡献（即“工作量”）的结合，允许公链上的各种应用针对不同的需求，采用不同的权重分配这两种贡献在于总体共识机制中所占的比例，

将其落实到智能合约之中，实现基于代码的**双重激励系统**。另外，在社群中，在 PoFC 机制的指导下对技术开发人员的特殊激励，也符合内生经济增长模型的设计理念：技术进步是促进经济总体增长的重要维度之一。

- MOS 公链借鉴 2018 年经济学奖得主保罗·罗默所建立的“**内生经济增长模型**”，将对普通经济体系的 GDP 估算模型，移植到了 DAO 2.0 组织，从而建立起了针对分布式组织所产生价值的统一评价体系。内生经济增长模型将储蓄率、人口增长率和技术进步等重要参数作为内生变量来考虑，可以由模型的内部来决定经济的长期增长率。而且，MOS 公链将分布式组织的令牌数、节点数和技术投入，作为类似参数，通过一定的转化和分析，可以量化 DAO 的价值，并预测未来其长期增长率。
- 针对金融领域的融资、借贷、代理、衍生品等特殊需求，MOS 公链开发出了专门用于消除金融领域去中心化各种痛点的 DAF（Decentralized Autonomous Finance）协议组，并开发出了相应的 MOSDAO DAPP，这些协议包括：
    - 基于智能合约的代币发行和融资
    - 分布式的订单提交和撮合
    - 基于自动发现机制的借贷利率和抵押方式

因此，无论是社群成员、投资者还是在 MOS 公链上开发应用的区块链项目方，都可以借助它所提供的分布式规则、共识机制、基础设施、智能合约，实现下列目的：

- 基于社群自治的加密货币资产交易流通
- 发行新型代币
- 特定加密货币社群的建设、协作、管理、投票、决策
- 开发针对社群节点权益和工作量双重因素的智能合约系统
- 针对不同权益的节点自定义激励标准

本白皮书将深入介绍 MOS 公链所要解决的问题、采取的方案路径、总体架构设计、技术创新、团队构成、发展愿景和路线图。

MOS 公链所采用的平台代币名为 **MOS 代币**，关于 MOS 代币的运营、流转和销售规则，请参阅同步推出的《MOS 商业白皮书》。

2. MOS 公链项目理念

1.1 区块链技术发展现状：从 1.0 到 2.0

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网时代的全新应用模式。区块链技术被认为是继大型机、个人电脑、互联网之后，计算模式的颠覆式创新，正在全球范围引起一场新的技术革新和产业变革。联合国、国际货币基金组织，以及美国、欧盟、日本等诸多发达国家均对区块链的发展给予高度关注，积极探索推动区块链的应用。目前，区块链的应用已延伸到金融交易、物联网、智能制造、供应链管理、数字资产等多个领域。

区块链技术起源于化名为“中本聪”（Satoshi Nakamoto）的学者在 2008 年发表的奠基性论文《比特币：一种点对点电子现金系统》。狭义来讲，区块链是一种按照时间顺序，将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证其不可篡改和不可伪造的分布式账本。广义来讲，区块链技术是一种全新的分布式基础架构与计算范式 ，利用块链式数据结构来验证与存储数据，

利用分布式节点共识算法来生成和更新数据，利用密码学的方式保证数据传输和访问的安全，再利用由自动化脚本代码组成的智能合约来编程和操作数据。

目前，区块链技术被很多大型机构称为是彻底改变业务乃至机构运作方式的重大突破性技术。同时，就像云计算、大数据、物联网等新一代信息技术一样，区块链技术并不是单一的信息技术，而是依托于现有技术，加以独创性的组合及创新，从而实现以前未实现的功能。至今为止，区块链技术大致经历了 3 个发展阶段，如图 1 所示。

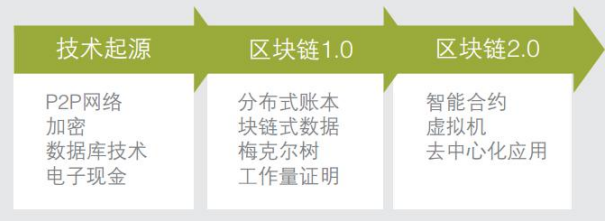


图 1 区块链的发展阶段

区块链 1.0 的核心基础包括：

- P2P 网络技术是区块链系统连接各对等节点的组网技术，学术界将其翻译为对等网络，在多数媒体上则被称为“点对点”或“端对端”网络，是建构在互联网上的一种连接网络。图 2 左侧所示为一种 P2P 网络模式，右侧为典型中心化网络模式。

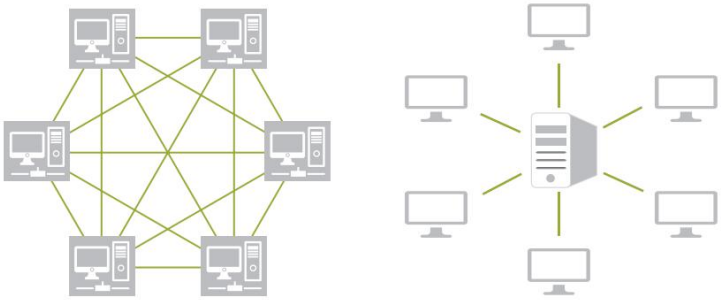


图 2 P2P 网络和中心化网络的对比

不同于中心化网络模式，P2P 网络中各节点的计算机地位平等，每个节点有相同的网络权力，不存在中心化的服务器。所有节点间通过特定的软件协议共享部分计算资源、软件或者信息内容。在比特币出现之前，P2P 网络计算技术已被广泛用于开发各种应用，如即时通讯软件、文件共享和下载软件、网络视频播放软件、计算资源共享软件等。

- 非对称加密算法是指使用公钥和私钥，对数据存储和传输进行加密和解密。公钥可公开发布，用于发送方加密要发送的信息，私钥用于接收方解密接收到的加密内容。公私钥对计算时间较长，主要用于加密较少的数据。常用的非对称加密算法有 RSA 和 ECC。非对称加密算法的过程如图 3 所示。区块链正是使用非对称加密的公私钥对来构建节点间信任的。

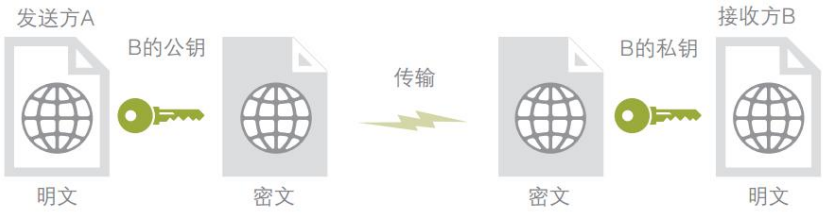


图3 非对称加密算法图示

- 以区块为单位的链状数据块结构： 区块链系统各节点通过一定的共识机制，选取具有打包交易权限的区块节点，该节点需要将新区块的前一个区块的哈希值、当前时间戳、一段时间内发生的有效交易及其梅克尔树根值等内容一起，打包成一个区块，再向全网广播。由于每一个区块都是与前续区块通过密码学证明的方式链接在一起的，当区块链达到一定的长度后，要修改某个历史区块中的交易内容，就必须将该区块之前的所有区块的交易记录及密码学证明进行重构，从而有效地实现了防篡改。
- 全网共享账本： 在典型的区块链网络中，每一个节点都能够存储全网发生的历史交易记录的完整、一致账本，即对个别节点的账本数据的篡改、攻击不会影响全网总账的安全性。此外，由于全网的节点是通过点对点的方式连接起来的，没有单一的中心化服务器，因此不存在单一的攻击入口。同时，全网共享账本这个特性也使得防止双重支付成为现实。

以上技术的组合，就是区块链 1.0 的典型实现，其完整的技术架构如图 3 所示。

图4 区块链1.0 的技术架构

2014 年前后，业界开始认识到区块链技术的重要价值，并将其用于数字货币以外的领域，如分布式身份认证、分布式域名系统和分布式应用（DAPP）等。用区块链技术架构从零开始构建 DAPP 非常困难，但不同的 DAPP 共享了很多相同的组件。区块链 2.0 试图创建可共用的技术平台，并向开发者提供 BaaS（Blockchain as a Service）服务，极大提高了交易速度，大大降低资源消耗，并支持 PoW、PoS 和 DPoS 等多种共识算法，使 DAPP 的开发变得更容易。区块链 2.0 的典型特征如下：

- 智能合约： 区块链系统中的应用，是已编码的、可自动运行的业务逻辑，通常有自己的代币和专用开发语言。
- DAPP： 包含用户界面的应用，包括但不限于各种加密货币，如以太坊钱包。
- 虚拟机： 用于执行智能合约编译后的代码。以太坊虚拟机是图灵完备的，可以完成自洽的逻辑计算。

区块链 2.0 的技术架构如下图所示：

图5 区块链 2.0 的技术架构

随着区块链技术和应用的不断深入，以智能合约、DAPP 为代表的区块链 2.0，将不仅仅只是支撑各种典型行业应用的架构体系。在组织、公司、社会等多种形态的运转背后，可能都能看到区块链的这种分布式协作模式的影子。可以说，区块链必将广泛而深刻地改变人们的生活方式。目前，区块链的应用已从单一的数字货币应用，例如比特币，延伸到经济社会的各个领域，其应用的场景如图 6 所示。

考虑到各个行业应用的可行性、成熟度和重要性，目前除金融服务行业的应用相对成熟外，其他行业的应用还处于探索起步阶段。本项目，就主要针对区块链技术在金融服务行业的应用。

图6 区块链的应用场景

1.2分布式自治组织（DAO）介绍

美国计算机科学家马尔文·康威于 1967 年提出了著名的康威定律（Convey's Law）：**“一个系统的功能，最终受限于设计该系统的组织的构建形式。”**也就是说，一个系统的设计，本质上反映了在开发该系统的生态体系中，各个成员之间的组织形式。系统各个节点之间的沟通、合作方式，也反映了各个成员之间的信息流动和合作方式。

在康威定律的基础上，人们得出了系统设计的下列原则：

- 人与人的沟通是非常复杂的，一个人的沟通精力是有限的，所以当问题太复杂需要很多人解决的时候，我们需要做拆分组织来达成对沟通效率的管理；

- 组织内人与人的沟通方式决定了他们参与的系统设计，管理者可以通过不同的拆分方式带来不同的团队间沟通方式，从而影响系统设计；
- 如果子系统是内聚的，和外部的沟通边界是明确的，能降低沟通成本，对应的设计也会更合理高效；
- 复杂的系统需要通过容错弹性的方式持续优化，不要指望一个大而全的设计或架构，好的架构和设计都是慢慢迭代出来的。

图 7 1967 年发表康威定律的论文

区块链技术的发展和应用，本质上就具备了分布式系统的特征，即所有节点分布在联网的计算机上，节点之间通过传递消息进行通信和动作协调的系统。这里的节点可以粗略地认为就是一个软件，或者某个软件的可独立运行的一部分。

这种分布式特征，按照康威定律，即要求其生态体系的组织架构，从传统的、集中式的公司制形式，转向开放的、分布式的组织模式。这就催生了 DAO（Decentralized Autonomous Organization）的诞生，即 “分布式自治组织”。

2013 年秋季，Daniel Larimer （也就是 BitShares、EOS 两个项目的创始者）在《Overpaying for security》一文中，首次提出了类似 DAO 的概念。起初，它的名称为 DAC，意即 "Decentralized Autonomous Corporation"。顾名思义，当时 Daniel 是将其认定为企业这种组织形态的，区别就是它是“去中心化 / 分布式的”。他指出，在 DAC 中，加密资产即股份，并且相关的规章是由源代码确定的。DAC 的目的在于通过为自由市场提供有价值的服务，来为股东赚得利润。

同年，Daniel 创立了 BitShares 来推行他的 DAC 概念，这也被认为是随后的 Steemit、EOS 两个项目的治理模式中，也有 DAC 概念的影子。2014 年，Daniel 进一步扩展了 DAC 的概念，并且明确它的四个核心特性：

- 必须有其可用于交易的股份（即 Token/Coins，通证/代币）；
- 其价值不得依赖于某一个体或公司；
- 组织必须透明，不得控制任何私钥；

- 不得依赖任何法律合约，如版权以及专利

同期，Vitalik Buterin 先后在自己的博客和 Bitcoin Magazine 杂志上阐述了其对 DAC 概念的认识，并经由 Daniel Suarez 的《Daemon》一书启发后，创造了区块链语境下的 DAO 这一语汇。

进一步，随着 Vitalik 在 2015 年之后，先后发布了以太坊与智能合约，DAO 的可编程性大大增加，其能承载的规则与价值也随之上升。而在经历了 2016 年 DAO 被盗事件后，DAO 类项目的安全性逐渐提升，受到黑客攻击的事件减少，区块链行业的注意力也愈发转移到了如何实现 DAO 的治理，以及如何为 DAO 赋予商业价值上来。

构建比特币和以太坊的社群就是典型的 DAO，即通过一系列公开、公正的规则，可以在无人干预和管理的情况下，自主运行的组织形式。这些规则往往会以开源软件的形式出现，每个人都可以通过购买该组织的股份权益，或者提供服务的形式，成为该组织的参与者。

对于这种新兴的组织形式，我们可以将其与传统组织形式进行对比：

- 传统组织遵循具有自上而下的治理结构，而 DAO 是各种利益相关者的自治式、分布式网络，任何成员都可以提交议案，发起改进建议。
- 传统组织是一个法人实体，而 DAO 没有中心化的法律实体。
- 传统组织向其员工提供人为执行的法律合约，而 DAO 使用智能合约作为运营规则。
- 传统组织的运转需要大量的维护和管理，而绝大多数 DAO 的规则和政策在运行伊始就已经设置完成，一旦规则建立，DAO 的运行便不再需要去管理，实现了高效率和自动化。
- 传统组织的利益分配机制、权益信息是集中管理和控制的，而在 DAO 之中，每个成员都将有权通过区块链，随时查看自己拥有的权益，从而大大提高了整个组织的透明度。

顾名思义，DAO 的核心特点是：

- **“自治”**

DAO 的基本特性是，DAO 是通过编程来执行具体的操作规则，这意味着当程序中指定的条件得到满足时，DAO 将会自动执行相应的操作。而在传统组织中，必须有人专门来解释和指导具体的规则。假设在现实生活中有个组织的成员希望通过专家委员会为各种项目分配资金。对于传统的组织，一旦专家委员会给出了意见，执行者必须通过许多步骤来才能释放资金。对于 DAO，只要委员会批准，资金就会立即转移。无论是内部利益相关人、银行都没办法阻止它。

为了使 DAO 的操作规则完全自动化和操作的安全有效执行，DAO 必须运行在公共的、不需许可的区块链上，比如以太坊。

这主要有两个原因:

1）传统的软件平台无法直接处理资金，它只能向负责转移资金的金融机构发送指令。DAO 通过使用公共区块链可以将加密货币或其他数字资产置于智能合约的直接唯一控制之下，DAO 能够将组织及其具体操作规则进行软件表达。

2）传统软件依赖第三方基础设施。如果软件平台运行在云服务平台上，那么在操作规则的具体表达上就很依赖于云服务器，云服务器很容易出现中断、错误或者外部因素导致软件无法正常运行。而公共的区块链从不会出现这些问题。

简而言之，DAO 之所以能够自治，是因为 DAO 是依照规则自我执行，没有人能阻止它，也没有人能从外部改变它。

- **“去中心化”**

去中心化可以从两个层面去理解，同时也能解释“去中心化”和“自治”相呼应的部分。

DAO 之所以是去中心化的，是因为它运行在去中心化的、无许可（Permissionless）的区块链之上。区块链专家 Yalda Mousavinia 将 DAO 定义为： “在数字规则管辖下运行的组织”。类似地，Tim Bansemer 指出：“DAO 实质是运行在无许可区块链（例如以太坊）之上的智能合约的组合。”

DAO 之所以是去中心化的，因为它不像传统公司一样围绕高管或股东按等级进行组织的。DAO 的权力行使是通过集体进行的，基于不隶属的合作机制，权力结构是 “分布式的” 。与传统的、呆板的等级结构相比，DAO 的新颖之处在于它能够协调的人非常多，而且可以分散在世界各地。这一特点使 DAO 在根本上有别于传统组织。

基本上所有的 DAO 项目都是围绕着以上两种观点而开展。Aragon 的定位主要落脚在第一层，强调“为自由而战” 。Tim Bessemer 的定义为 “合作的未来” ，完美地表达了第二层的含义。

如果考虑到 DAO 的本质特征是能够避免权力被第三方夺取，这两种观点其实是互补的。

- **“组织”**

第一个 DAO 项目是“The DAO”，创建于 2016 年，用于资助有助于以太坊发展的项目。使用 DAO 而不是基金会或风险资本的想法符合以太坊社群所珍视的分权精神。事实上 The DAO 是一个投资基金，它的决策是由投资者直接做出的，而不是委托给专门的经理。

DAO 的概念是 Dan Larimer（EOS 创始人）在 2013 年提出的，他创造了术语 “DAC” ——去中心化自治公司。Dan Larimer 把比特币比作一个公司，它的股东是比特币持有者，雇员是矿工。同年，Vitalik Buterin 提出一个问题：一家公司在没有经理人的情况下如何运作？从而概括了 DAO 这一理念。商业自动化通常被大众认为是用机器人或电脑取代低技能人员，让更多合格的员工来管理的过程。然而，Vitalik 提出了相反的建议，即用一种软件技术取代管理，这种软件技术能够招募人员并支付薪水，来驱动执行有助于公司使命的任务。“DAO”清楚地指明了比“组织”的典型定义更广泛的东西“一个把人们聚集在一起，朝着一个共同目标工作的社会群体。”因此，Vitalik 将 DAO 定义为“一个独立存在，依附于网络的实体，但也严重依赖于雇佣个人来执行 DAO 本身无法完成的某些任务”。

综上所述，DAO 在共识机制和分布式网络的共同作用下，成为一种介于产业和企业之间的组织形式。一方面，它以分布式网络实现了资本的高效率分配，解决了信息的不对称问题。另一方面，通过共识机制建立起超越简单熟人关系的信用体系，从而能够形成以共享经济（或者叫分享经济）的新经济模式，从而打破了新古典经济中关于企业和市场关系的一系列限制，创造了新的组织结构。

1.3分布式自治组织公链的发展方向

自 2016 年以太坊的 The DAO 被攻击以来，DAO 逐渐远离了人们的视线。然而 DAO 的发展和试验却从未停止。到了 2019 年，随着相关技术、理论的进一步完善，DAO 的发展又开始重新崛起。例如：

1、Aragon、DAOstack 和 Colony 已经支持在主网创建 DAO 合约。

2、KyberDAO （Kyber Network）、PolkaDAO （Polkadot）和 dxDAO （Gnosis）等项目已经在尝试使用 DAO 进行协议治理。

3、Kleros、Aragon Court 等 DAO 项目可以提供去中心化的仲裁服务。在现实世界中，美国佛蒙特州、马耳他和英国已经为 DAO 创建司法管辖颁发了相应的牌照。

4、总部位于英国的 Nexus Mutual 是第一家由 DAO 驱动的去中心化互助保险公司，他们发行由智能合约支持的保单，项目旨在承保传统保险公司通常承保的其他类型风险。

5、在法国，La Suite du Monde 计划使用 DAO 管理其资金和项目计划。与其他项目很不一样的是，该项目的建立是在当前工业文明崩溃的前提下，向“公社”提供土地，财政和法律支持。这些“公社”是地方性的、具有自我恢复能力的、独立的、自我组织的合作社。

总而言之，从布拉格到库拉索、从雅典到纽约，新的 DAO 项目随处可见。这些项目都极具发现和实验精神，更加去中心化，为了创建更公平的系统。这些项目的目标和运作方式又是非常多样化的，这也侧面说明了 DAO 未来应用的广泛性。

DAO 与传统组织的最大区别，在于它对于基于智能合约的自动化规则的支持。目前，最常见的智能合约是各种加密货币合约，即开发者可以很容易地透过部署一个智能合约，来提供、发行运行于以太坊或者其他公链上的新型加密代币。如果这份智能合约兼容 ERC20 标准，开发者不需要重新开发从挖矿到交易的整个代币生态系，新型加密代币就可以直接使用支持以太坊的电子钱包来收送，大大降低了建立新加密代币的门槛。

智能合约也可以用来运作各种公开公正的自动服务机构。透过分散在全球各节点上运作的智能合约，所有运作与决策都是公开透明的，降低了交易的不确定性。

DAO 在智能合约的支持方面，目前出现了一些重要的新趋势：

- 多协议兼容，即不止支持 ERC20，还拓展到其他协议；
- 结合 VRF 等随机机制，实现真正分布式运行，避免了过去的“伪中心化”、“伪智能化”；
- 降低交易成本，提高交易速度（TPS）。

另外，目前基于 DAO 的公链，对于跨链技术也有了强大的支持。所谓跨链，指的是不同公链之间的交互、通信与支持。目前主流的跨链技术包括：

- 公证人机制（Notary schemes）
- 侧链/中继（Sidechains/relays）
- 哈希锁定（Hash-locking）
- 分布式私钥控制（Decentralized private key control）

公证人机制是最简单、最常用的一种跨链技术。侧链和中继有很多相似的地方，只有一些微妙的地方稍有不同。哈希锁定很像闪电网络，且是相对来说更具有技术含量的一种方式，经过了数学的形式化证明，是经过论证的原子级交换模型。分布式私钥控制则是通过由多个公链共同保管私钥，加强单个公链上资产的安全性。

早期跨链技术包括以瑞波和 BTC Relay 为代表，它们更多关注的是资产转移；现有跨链技术 Polkadot 和 Cosmos 为代表更多关注的是跨链基础设施；新出现的一些新型跨链技术则实现了多币种智能合约，在其上可以产生丰富的跨链金融应用。

从有项目最早开始提出来用 DAO 作为开发去中心化的基础设施这个构想，到现在已经将近三年的时间，一些主要的基础设施都已经陆续建立起来了。这不仅体现在与 DAO 有关的项目的数量上，还有整个 DAO 生态的不断拓展上。DAO 从中心化的赏金平台，开始逐渐过渡到分布式存储、交互界面和更广泛的去中心化金融服务平台，不仅在智能合约的安全性上得到了大幅提升 ，且发展重点也从单一的引导去中心化基础设施的建设，转移到管理和运用已有的系统、协议和平台。

综上所述，DAO 公链可以根据逻辑、事实，做出对整个社会有利的即时和透明的决策。它们允许专家成员为社群做出决策，对于金融服务行业甚至更广泛的服务行业来说，都可以起到非常重要的作用。

1.4去中心自组织系统与加密货币金融行业的结合

目前，区块链技术因为在可追溯、不可篡改、去中心化等方面的优势，在数字化资产的管理、交易、流动性等金融领域，得到了世界各地金融机构的广泛应用，并因此催生了建立针对金融领域的 DAO 的需求，并衍生出了 DeFi（Decentralized Finance）的概念，即去中心化金融，它主要指去中心化的金融衍生品和相关服务，背后是分布式账本和区块链技术。

从稳定币、去中心化代币兑换平台到信用借贷，目前 DeFi 项目已有数千个，整个生态系统正在蓬勃发展。其中，最具有代表性的 DeFi 项目莫过于 Bancor 和 MakerDAO 的 DAI，前者是对于交易所的变革，后者则是对于传统央行和稳定币的变革。

Bancor 协议通过多种智能合约将传统的人人交易转变为人机交易，项目方可以通过 BNT 作为保证金之一发行代币，代币市场价格和供需关系直接相关。然而，就现阶段的加密货币市场而言，Bancor 的弊端已经在机制相似的 DAPP 游戏 FOMO3D 和 P3D 兴衰过程中暴露无遗。

同时，根据 Delphi Digital 提供的数据，MakerDAO 作为基于以太坊的借贷抵押平台，“目前占有去中心化金融项目中锁定代币总价值的 90%”，常被喻为“去中心化央行”。其他稳定币，如 Tether（USDT）等，只是通过中心化机构发行可赎回标的资产的 IOU 实现，不属于 DeFi 范畴。而 MakerDAO 的用户可以通过抵押 ETH，获取和美元 1:1 锚定的稳定币 DAI，这一过程由用户通过 Maker 的核心智能合约 CDP 自主完成，而 MakerDAO 团队也直接表示： “DeFi 的核心与优势在于，用户无需批准即可参与。”

不论是 DAI 还是 Bancor 的变革，其实现的核心方式就是采用复杂的智能合约，辅以相当的治理能力和社群共识去解决智能合约之外的问题。这些 DeFi 项目的火热，或许意味着区块链金融已经从游戏中的实验逐步走向实战。

综上所述，区块链技术因为在可追溯、不可篡改、去中心化等方面的优势，在数字化资产的管理、交易、流动性等金融领域，已经得到了世界各地金融机构的广泛应用，并因此催生了建立针对金

融领域的 DAO 的需求。但是， 在构建针对特定金融领域的 DAO 时，所有的项目方和投资者、社群成员都面临着下列挑战：

- 如何高效、方便、快速地达成“决策共识”，避免意见分歧、难以达成一致所造成的损失；
- 如何公平地、灵活地奖励社群成员（包括矿工等节点）对于整个社群的贡献，形成可以积极扩大社群规模的“正反馈”；
- 如何真正地实现“去中心化”，防止社群、平台被部分精英人物或者掌握重要资源的节点所掌控，导致普通成员无法公正地享受到社群增长所带来的利益。

1.5MOS 公链设计理念

MOS 项目团队在金融领域扎根多年，积累了丰富的金融应用经验，并拥有专业的区块链技术开发团队，通过将技术和金融的无缝结合，提出了可以完美解决上述当前难点、面向金融行业的新一代公链平台：**MOS 公链**。该平台主要具有下列创新：

- MOS 公链设计了包含社群成员、评审团、社群领袖、开发团队等角色在内的新型组织架构，这些角色之间通过分布式的规则互相关联、彼此激励，避免了传统 DAO 架构中缺乏自动执行机制、缺乏有效激励、由部分人员主导社群等弊病，为各种分布式金融应用的运行奠定了坚实的基础，从而形成了全新的 DAO 2.0。
- MOS 公链的 DAO 2.0 架构中，为评审团的筛选流程，采用了基于 VRF（Verifiable Random Function，即可验证随机函数）的随机机制，即在每次决定议题、项目，提交投票的过程中，加入一定的随机因素，避免了过于依赖特定成员，以及利益相关方对已知成员行贿的可能性，真正地实现了“去中心化”。
- 一个去中心化组织的发展，离不开矿工和节点的支持，这需要对它们的贡献给予相应的奖励。在过去的 DAO 1.0 项目中，都只依赖于工作量（PoW）、权益（PoS）等等单一机制，从而限制了组织中衍生出各种应用的灵活性。因此在 MOS 公链中，创新地采用了名为 PoFC（Proof of Finance Contribution，金融贡献证明）的共识机制，它首次将两种不同类型的激励方式，以权重的形式组合到了一起：一种是鼓励成员拥有更多的金融交易资源，一种是对其社群贡献提供回报。每个项目、社群，都可以针对其所有实施的金融应用，采取不同的组合策略，这大大提高了 MOS 公链平台上所衍生应用的灵活性。
- 成员和投资者，在评估每个项目的发展前景时，过去往往依赖于各自的经验，导致了很多的不确定性和风险。为此，MOS 公链采用了 2018 年诺贝尔经济学奖得主保罗·罗默所建立的“内生经济增长模型”（Endogenous growth theory，简称 EGT）来分析每个项目未来的发展趋势和增长率，其中用到的参数包括项目的代币数量、矿工个数、节点个数和开发投入等等，经过基于 EGT 的经验公式转化，得到每个项目的量化增长曲线，从而大大降低了成员、投资者在选择项目时的盲目性。

MOS 公链作为一个平台，主要面向各种金融应用，包括但不仅限于融资、销售、代理、委托、信贷等等。为此，MOS 公链平台为各种应用项目提供了一整套“DAF”(Decentralized Autonomous Finance，即去中心化自治金融) 协议组，并开发出了相应的 MOSDAO DAPP。这样，项目方可以方便地利用这些协议和基础设施，开发自己和成员需要的应用场景和服务。

1.6MOS 生态设计愿景

正如本白皮书开宗明义所揭示的：“社群由你我自治，金融因共识赋能”。

DAO 是区块链技术最令人期待的应用之一。毕竟，这是历史上第一次我们有能力以一种无信仰和匿名的方式协调，集体为某一件事做出决定。这种去中心化的社群治理模式对促进行业发展、加强企业治理，乃至疏通全人类的沟通协调，都有极其深远的影响。在金融领域，以 DeFi 为代表，DAO 正在得到越来越广泛的关注和应用。

MOS 公链项目的愿景，正是让每个社群成员，都能够平等地获得金融服务的自治权，共同建设、打造最符合社群成员需求的，通过合理激励机制鼓励贡献的，不依赖于单个“中心”的新一代分布式自治组织。

MOS 公链项目将依托于精心的架构设计、先进的技术手段、缜密的逻辑设定、强大的智能合约支持和独特的跨链、侧链技术，满足各种金融行业应用和衍生付的需要，成为金融服务行业的首选公链。

图8 MOS 公链项目标志

3. MOS 公链项目实施架构

3.1. 分布式自治社群架构设计 DAO 2.0

迄今为止，已经出现了包括比特币、DashDAO、The DAO 等数十个不同类型的 DAO 组织形式和公链。按照区块链专家 Vu Gaba Vineb 的观点，所有的 DAO 都可以从三个维度加以衡量：

- 决策方式
- 参与激励
- 去中心化程度

现有项目在这三个维度上都各有千秋，没有能够在三方面都保持比较均衡的状态，可以统一归为 **DAO 1.0**。针对目前 DAO 体系的各种痛点，MOS 创新地提出了 **DAO 2.0** 的自治社群架构设计方案，从上述三个角度，进行了全面的改进和提升。

在过去的 DAO 1.0 中，社群的决策基本上可以分为以下几步：

- 通过空投、众筹、私募、公募等方式，发放 DAO 的权益和管理代币，只有持有这些代币的用户，才算是社群成员。
- 针对一个特定的议题，由一部分社群代表进行讨论，提交给开发团队，这些议题包括但不仅限于：
    - 某个项目是否适合在社群中发行代币
    - 某种新的投资机制是否得到认可
    - 某个关键算法是否需要调整，例如挖矿、激励等
- 开发团队设置投票接口（网页或者 DAPP），供所有社群用户在一定期限内完成投票。
- 根据最终投标结果，做出决策。

这里面存在多个潜在的问题：

- 把所有的提案都提交投票显然是不可行的，但是选择哪些议题提交投票呢？目前，提案权大多控制在部分社群代表手中。这主要体现为 DAO 的发起者、主要权益持有者（即拥有多数代币的机构或者用户）和部分 KOL（社群领袖）手中，这不仅削弱了 DAO 的“去中心化”特性，而且也给这些“话语权”拥有者提供了操纵社群主要走向的机会。更重要的是，他们可能会排斥对其利益有影响的议题，而只提交对自己有益的议题。
- 社群成员的投票动机得不到激励。目前普遍存在的情况是，大部分 DAO 在就某个议题进行投票时，投票率非常低，从而进一步导致了中性化的加剧，无法体现普通社群成员、投资者自主治理、协作的诉求。这个原因有很多，一方面是投票方式的不便，但是更重要的，是缺乏有效的投票激励机制。社群成员不能通过投票直接获益，自然降低了对于投票的兴趣。
- 整个投票过程存在人为步骤，缺乏自动执行机制，开发团队的参与过程中，可能会引入人为因素的影响，譬如团队在投票页面、选项的设计上，偏向于某个议案等，这些都会影响整个 DAO 的去中心化水平。

因此，MOS 公链在决策方式上，设计出了全新的模式 DAO 2.0，可以完美地解决上述问题，其结构、流程如下图所示：

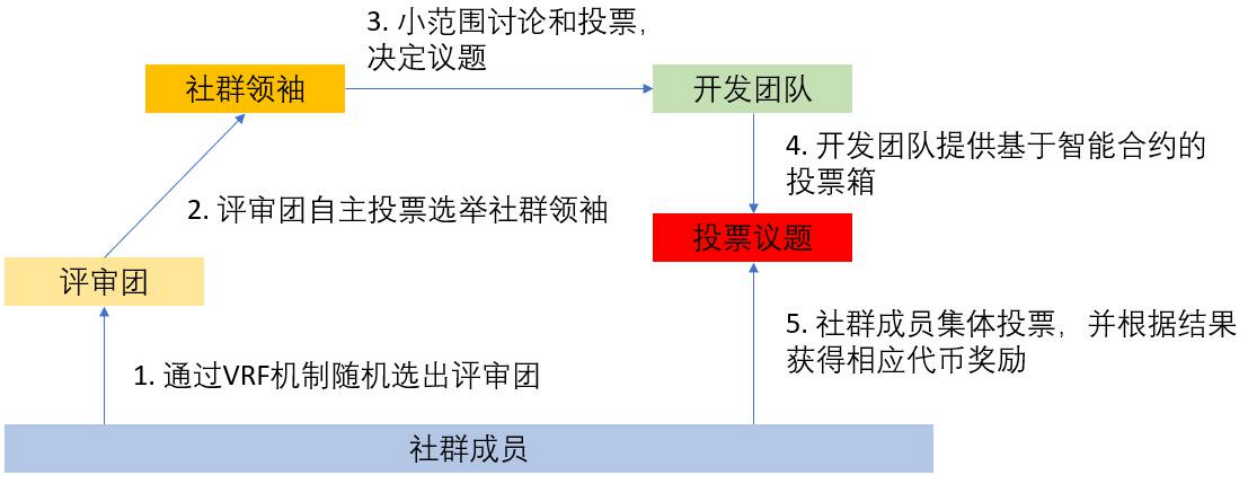


图 9 DAO 2.0 的决策流程

可以看到，其中分为下列角色：

- 社群成员（Community Member）：即拥有 MOS 公链平台代币 MOS 的用户，即称为社群成员。社群成员需要锁定一定数量的 MOS 代币，才会进入随机选择评审团的候选池。
- 评审团（Committee）：社群成员通过 VRF 算法，自动选出部分成员成为评审团成员。针对每个议题，都会重新进行计算。评审团的成员会持续更新。
- 社群领袖（Leader）：随机生成的评审团，会以投票形式，选出一些具有影响力、判断力、执行力的社群领袖，由他们代表所有成员提出需要投票的议案。
- 开发团队（Developer）：开发团队负责公链的建设、开发和维护，以及投票等 DAPP 的设计与制作。

下面是对整个决策流程的逐步分解：

1）社群成员通过 VRF 机制随机选出评审团

针对若干个需要讨论的议题，首先开发团队将设定一个投票期（T）。在这个期间，第一步是，从所有选择抵押 MOS 的社群成员中，随机筛选出评审团。

针对普遍的“伪中心化”现象，MOS 公链创新地将 VRF（Verifiable Random Function，即可验证随机函数）运用到了评审团的选举之中，通过用 VRF 来周期性地挑选评审团成员，将管理权、自主权完全交由社群控制，实现扁平式的、透明式的管理机制。这里面涉及到 VRF 和随机数生成的原理。

依靠随机数来分配社会资源 ，已经应用到日常生活的方方面面。从经济角度上来讲，随机数广泛应用于密码学、数值计算模拟、统计研究、乐透博彩、游戏抽奖等场合，具有极高的商业价值。

人们为产生随机数，也发明了掷骰子，转转盘，抛硬币等统计方法，通过计算机生成伪随机数，利用量子力学原理获取随机数等。这些方法虽然很好的解决了随机数的随机性、不可控制性、不可预测性等方面的问题，但是却缺乏去中心性与可证公平性。自然地，人们希望找到一种更公平的随机数生成和发布机制。而区块链作为一个去中心化 的平台，为可证公平的随机数生成提供了天然的基础。

但是在公有区块链上设计一个可用的随机数发生器难度更大。除了基本的随机数统计学要求外，公有链上一个可用的随机数发生器至少要满足无法预测、不可操控、难以串谋、可证公平、可审计这几个特点。

伪随机数一般由确定的算法生成的，其分布函数与相关性均能通过统计测试。但与真随机数相比，它们由算法生成，而不是一个真实的随机过程。伪随机数也只是尽可能地接近其应具有的随机性，但是因为有“种子值”，所以伪随机数在一定程度上是可控可预测的。伪随机数可使用取中法、同余法、移位法、梅森旋转算法等方式产生。

真随机数的产生不可预计，也不可能重复产生两个相同的真随机数序列。真随机数一般使用物理现象产生，比如掷钱币、掷骰子、晃动鼠标、转转轮、使用电子元件的噪音、使用大气噪声、核裂变等。真随机数发生器的技术要求一般比较高，生产效率一般比伪随机数低。另外， 如果信息熵的信息量很有限，不一定能产生真随机数。真随机可以进一步区分为统计意义上的随机以及量子效应上的随机。一般认为，由于量子力学内在的随机性，其产生的随机数比传统物理学通过统计产生的随机数更“真”。

Linux 内核提供了统计方式的真随机数生成器。它利用机器的噪音生成随机数，噪音源包括各种硬件运行时速，用户和计算机交互时速，比如击键的间隔时间、鼠标移动速度、特定中断的时间间隔和块 IO 请求的响应时间等。另外，通过监听真空内亚原子粒子量子涨落产生的噪音，澳大利亚国立大学的科学家们建造了随机数发生器并提供给互联网用户。

量子现象利用了在原子尺度下粒子的行为具有随机性，而且其本质还未被人类发现，因此可以将其看作一个具有良好不确定性的熵源；混沌现象是指在混沌系统中， 初始量的微小差异会导致未来的发展截然不同，因此除非获得初始时刻的全部准确信息，则无法预测未来的发展趋势。

因此，如何在区块链上设计并实现可证公平的随机数发生器成为近年来一个重要的研究问 题。自从 Randao 团队在 2015 年提出使用 Commit Reveal 方案后，又分别有 Vitalik Buterin 提出的 Randao++ 方案、部分 DAPP 使用 预言机（Oracle），从链下服务获取随机数的方案，来实现区块链随机数生成。

关于随机数生成方案衡量标准，主要需要考虑以下指标：

- 不可预测：不可预测是针对所有参与者的，不管是生产者和消费者，都无法根据历史数据预测下一个随机数的可能值，即便是稍稍提高一点点预测的成功率都做不到，即具有马尔可夫性质。在公共随机数的方案中，还要求任何人根据任何公开信息也都不能提高预测概率，例如 Bitcoin Beacon 的方案中，即便知道区块的历史数据，矿池的公钥，待打包的交易列表等，也无法获得预测上的优势。
- 不可串谋：在随机数的生成过程中，部分参与方联合起来，互相交换各自的私有信息，并不能影响随机数的生成过程或改变随机数的结果，或具有其他比较优势，比如相比其他人提前获得即将生成的随机数的结果。
- 不可提前获知：随机数的参与方同时知晓该随机数，任何一方不能提前知道结果。
- 不可篡改：即随机数的生产者不能伪造一个随机数出来，而当一个随机数生成好后，该随机数无法被任何人修改。
- 不可选择：随机数的生产过程可能同时有很多个随机数生成，生产者无法只选择其中的某一个提供出去，或用其中一个替代另外一个。

- 不可隐瞒：生产者在随机数生成完成后，不能拒绝公开该随机数。即生产好的随机数一定会被公开，无法被隐藏或者撤回。
- 可参与：随机数的生成过程中，随机数的相关方可以容易的参与进来，随机数生成方案应该为一般人的广泛参与提供便利，降低或消除参与门槛，参与的权力不应该被剥夺。
- 可审计：在随机数生成过程结束后，其整体过程是可以被审核、检查的。
- 成本：随机数的生产成本应该尽可能低。
- 响应速度：随机数的生成过程应该足够快。

综合考虑这些因素，MOS 公链平台选择了 VRF 作为随机选择的依据。VRF（Verifiable Random Function）算法于 1999 年由莫卡利教授提出，由于其较好的安全性与效率，被越来越多区块链项目拿来优化共识过程，让共识的随机数部分占用计算资源变少，让资源更多地被交易的确认与合约的运行所占用。

要理解 VRF 的原理，先解释一下这里说的“随机”是什么意思：一个理想的哈希函数，其值域应该是离散的、均匀分布的，给定不同的输入值，其输出值应该没有规律，随机的洒落、分布在值域区间内。

再看一个简单的哈希函数变种，即结合了密钥的哈希函数，比如：

result = SHA256（secret，info）

那么要得到结果 result，仅仅拥有 info 是不够的，必须要知道 secret 才能计算出来，即密钥。或者说已经拥有了结果 result 和 info，但是必须知道 secret 才能验证 info 和 result 是否是对应匹配。

这就是带密钥的哈希函数。然而这里引申出了一个问题：有没有可能在不出示密钥的情况下，验证 result 和 info 是对应匹配的？于是就有了可验证随机函数 Verifiable Random Function（VRF）。

整个过程如下图所示：

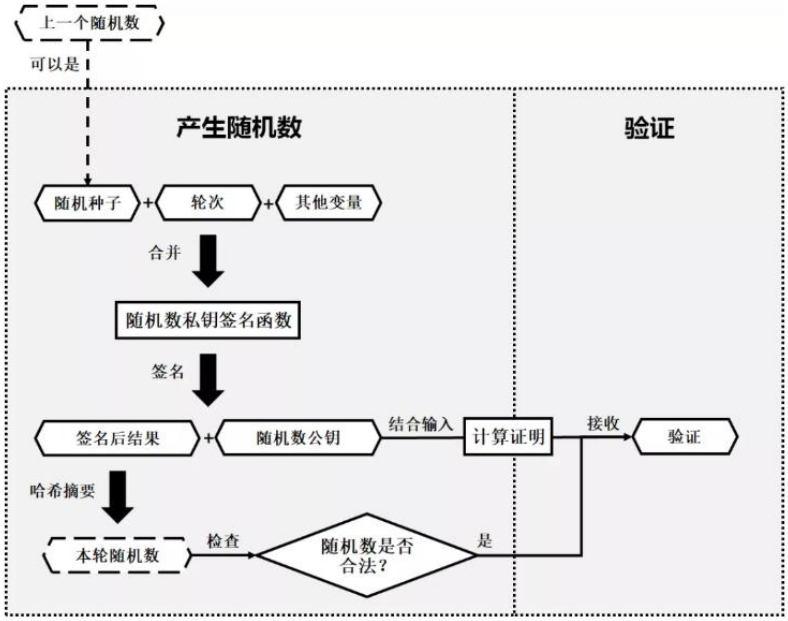


图10 VRF 的流程示意图

简单来说，也就是结合了非对称密钥技术的哈希函数，比如 result = VRF_Hash（SK，info），SK 是私钥，不公开，秘密保存，和 SK 配对的 PK 是公钥，需公开给验证者。具体的操作流程如下：
1）证明者生成一对密钥，PK、SK；

2）证明者计算：result = VRF_Hash（SK，info）；

3）证明者计算 proof = VRF_Proof（SK，info）；

4）证明者把 result 和 proof 递交给验证者；

5） 验证者计算 result = VRF_P2H（proof）是否成立，若成立，继续下面的步骤，否则中止；

6） 证明者把 PK，info 递交给验证者；

7） 验证者计算 True/False = VRF_Verify（PK，info，proof），True 表示验证通过，False 表示验证未通过。所谓的验证通过，就是指 proof 是否是通过 info 生成的，通过 proof 是否可以计算出 result，从而推导出 info 和 result 是否对应匹配、证明者给出的材料是否有问题。

在整个操作流程中，证明者始终没有出示自己的私钥 SK，验证者却可以推导出 info 和 result 是否对应匹配，这就是 VRF 的功用。这样，在通过私钥生成了 result 之后，这个 value 实际上可以看作是大的正整数，假设是 256 位的，那么它的取值范围应该处于 0 到 2 的 256 次方之间。

将其与 2 的 256 次方相除，可以得到一个 0 到 1 之间的值。将这个值放到二项分布的累积分布中进行比对，可以得到相应的值。如果这个值大于零，就相当于抽到了可以进行下一步的签。将这个值和之前 VRF 生成的放在一起，广播给其他用户，其他任何收到的用户结合广播者的公钥以及全网都知道的值，则可以验证以下两个条件是否成立：

1、利用验证是否正确

2、利用通过二项分布函数得到 j'是否与 j 相等，如下图所示：

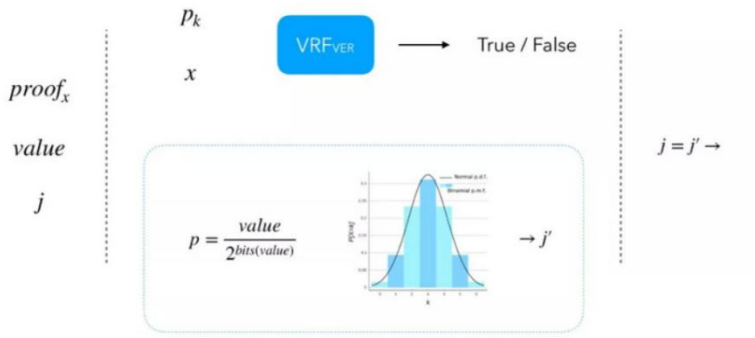


图 11 VRF 的验证机制

假设两个条件均成立，那么就证明这个抽签结果是正确的，是可信的。到此为止，从抽签生成到验证的过程就完成了。

可以看到，VRF 的优点在于：

1）首先它的抽签过程不需要与其他通信，直接在本机就能够的到这个抽签结果，而且这个 x 输入是大家公认的，针对同一个 x 的输出值是固定的，因此无法通过多次尝试来改变抽签结果。

2）某个节点收到其他节点的抽签信息之后，可以用附带的证明，来证明这个随机数的正确性，保证它的确是由私钥的拥有者计算出来的。因此这个抽签结果是无法被伪造的。

3）VRF 主要用来的得出一个伪随机数，抽签的部分主要是由一个二项分布函数负责，而通过构建二项分布的参数，我们可以很方便的控制需要被得出的中签权益的个数，适配不同的需要抽签的场景。

因此，通过这样真正随机的方法，可以实现评审团的公平、公正选拔，避免任何的人为因素干扰，选出一定数量的评审团成员。

2）评审团自主选择社群领袖

接下来，随机产生的评审团，将会有机会选择社群领袖。这里面面临的关键在于，怎么样激励评审团选出真正优秀的、合格的社群领袖，为此，我们设计了如下的激励机制：

首先，每个评审团成员抵押一定数量的 MOS 代币，作为奖池。在这个奖池的基础上，每个评审团获得的激励分为三个部分：

- 如果评审团成员投票选择的领袖，通过了评审团的投票成为社群领袖，成员可以从奖池中获得若干枚 MOS 代币作为奖励。
- 来自于社群领袖的成绩激励：如果投票选出社群领袖提出的提案获得了所有社群成员的最终投票通过，即得到了大部分用户的许可，那么评审团成员也将再得到若干枚 MOS 代币的激励。

具体而言，规则如下：

1） 每个评审团成员先抵押一定数量的 MOS 代币，作为奖池。

2） 每个评审团成员，最多可以提名限定数量的社群领袖，并说明理由。
3） 所有评审团成员针对全部提名出来的社群领袖进行在线投票。
4） 每个评审团成员最多可以投票选择限定数量的领袖（即如果只能选择三个领袖，意味着每人只有三票）。
5） 跟踪总票数进行评估，如果评审团成员投票选择的领袖，通过了评审团的投票成为社群领袖，成员可以获得若干枚 MOS 代币作为奖励。
6） 之后，如果投票选出社群领袖提出的提案获得了所有社群成员的最终投票通过，即得到了大部分用户的许可，那么选择该领袖的评审团成员也将得到若干枚 MOS 代币的激励。

整个过程都由开发团队所编写的智能合约自动控制，不涉及任何人为干预，避免了个别评审团成员和社群领袖操纵整个选择的可能性。

请注意，具体的奖励 MOS 枚数、评审团成员个数和社群领袖个数，会在主网上线后的新版白皮书中说明。

3）社群领袖小范围讨论和投票，选出议题

在这一步中，由评审团选出的若干个社群领袖，将对在投票期 T 中，需要讨论的议题进行讨论，决定是否提交给开发团队。

社群领袖作为筛选优质资产及进行社群代币发行的重要节点，出于自己长久获利的利益，会持续筛选好的项目并做好风险控制，以保证普通社群投资者参与公募时可以获益。

在一个投票期内，往往有多个议题和项目需要筛选，那么社群领袖就需要对这些议题和项目进行打分和评级。MOS 公链制定了一套针对金融行业项目的评级框架，提炼出了五个方面 109 项评估指标，如下表所示：

评估大类	权重	评估小类	权重	评估指标个数
项目概况	16%	项目基本情况	22.5%	8
		团队基本情况	20%	6
		资本市场认可度	12.5%	3
		项目推广力度	22.5%	2
		项目热度	22.5%	3
项目团队	26%	创始人背景	49%	10
		核心管理团队	25%	5
		核心开发团队	26%	5
项目方案	20%	项目市场分析	28%	4
		项目方案分析	34%	4
		项目治理架构	18%	3
		项目信息披露和风险管理	20%	4
项目技术	20%	区块链技术	40%	10
		应用创新性	6%	1
		技术适用性	6%	1
		技术成熟度	16%	2
		技术健康度	32%	7
经济机制	18%	代币基本情况	20%	8
		代币分配方案	24.5%	8
		代币释放模式	20%	5
		代币流动性	11%	5
		经济模型设计	24.5%	5
合计	100%			109

表1 MOS 公链项目评级体系

并在此基础上给出风险等级，如下表所示：

风险等级	描述
低风险	优质项目，在市场上有很强的竞争优势，管理规范，信息披露真实、及时，开发实力和运营实力雄厚，发展前景良好，有极强的抵御和承受重大的内外部不利因素的能力，
中风险	项目在市场上具有一定的竞争优势，管理比较规范，信息披露真实、较及时，具有一定的开发实力和运营实力，具有一定的抵御和承受内外部不利因素的能力，但是潜在的内外部不利因素会在某种程度上影响项目的发展。
高风险	项目表现尚可或不佳，管理水平一般，信息披露真实但不及时，开发和运营面临一定压力，项目发展具有较高的不确定性，一旦出现内外部不利因素，随时可导致项目迅速恶化。
不推荐	项目管理水平很差，开发停滞，几乎无法持续运营，或项目失败，或信息披露失真，存在欺诈可能。

表 2 风险等级划分

最终的项目评级如下表所示：

评级符号	风险等级	评分区间
AAA	低风险（极低）	[90，100]
AA	低风险（较低）	[80，90]
A	中风险（较低）	[70，80]
BBB	中风险（较高）	[60，70]
BB	高风险（较低）	[50，60]
B	高风险（极高）	[40，50]
CCC	不推荐	[30，40]
CC	不推荐	[20，30]
C	不推荐	[10，20]
D	不推荐	[0，10]

表 3 项目评级指引

如果社群领袖推荐的议题、项目表现不佳，在下轮评审团投票时就会面临被淘汰的风险。因此，他们会积极考察、审核和评估需要提交给投票的议题和项目。另外，MOS 公链还为他们设立了相应的奖惩机制：

- 在提交议题之前，社群领袖需要抵押一定的 MOS 代币，作为奖池。
- 如果提交的议题在成员具体投票中获得通过，社群领袖将会从奖池中获得 MOS 代币奖励。
- 每个社群领袖对于每个项目的评级，都会被记录到其个人记录之中。
- 但是，如果提交的议题在成员具体投票中没有获得通过，即没有得到大部分成员的认可，那么社群领袖的品牌分数依然会大大折扣
- 评审团在投票选举社群领袖时，可以看到每个领袖的能力，显然越高的越有可能继续当选，而越低的就有可能被淘汰。

4）开发团队提供基于智能合约的投票箱

MOS 开发团队，将会根据社群领袖所推荐的议题，提供一个供所有社群成员投票的“投票箱”。同样，整个投票程序将会以智能合约形式呈现，用户只需要在 MOSDAO 程序中，查看投票议题的相关信息，以及提出该议案的所有社群领袖的信息（包括“信用勋章”个数），选择支持或者反对（YES 或者 NO），就可以完成投票。

通过智能合约投票的关键，是如何将权限分配给正确的投票人，阻止非法的投票人，并且允许用户之间代理投票，同时自动计算票数且整个投票过程完全透明。下面是 MOS 开发团队所开发的、基于 Solidity 的投票箱智能合约代码实例。

开发团队会为每一个议案创建一个合同，并提供一个简称。合同的创建者也就是开发团队，会根据 MOS 代币抵押情况，将投票权分配到每个合格成员的地址。被分配了投票权的地址可以选择自己投票，也可以将投票权代理给自己信任的人。

```
pragma solidity ^0.4.4;
// 授权投票


contract Ballot{
   //授权投票结构体
   struct Voter{
        uint weight;//累积的权重
        bool voted;//如果为真，则表示该投票人已经投票
        address delegate;//委托的投票代表
        uint vote;//投票选择的提案索引号
   }

  //这是一个独立提案的类型
  struct Proposal{
        bytes32 name; //短名称（32 字节）
        uint voteCount;//累积获得的票数
  }

  //状态变量以及其他参数声明
  address public chairperson;
  //这里声明一个状态变量，保存每个独立地址的 Voter 的结构
  mapping (address => Voter) public voters;
  //一个储存 Proposal 结构的动态数组
  Proposal[] public  proposals;


  // 创建一个新的投票用于选出一个提案名称 proposalsNames
  function Ballot(bytes32[] proposalNames) {
        chairperson = msg.sender;
        voters[chairperson].weight = 1;
  //对提供的每一个提案名称，创建一个新的提案
  //对象添加到数据末尾
  for (uint i= 0;i<proposalNames.length;i++){
  //创建一个临时的提案对象
  //添加到一个提案数组 proposals 末尾
  proposals.push(Proposal({
            name:proposalNames[i],
            voteCount:0
    }));
    }
  }
```

```
  //给投票人 voter 参加投票的投票权
  //只能由投票主持人 chairperson 调用
  function giveRightToVote(address voter) public{
    if(msg.sender !=chairperson || voters[voter].voted)
    throw;
    voters[voter].weight = 1;
  }



  //委托你的投票权到一个投票代表 to
  function delegate(address to){
    // 指定引用
    Voter  storage sender = voters[msg.sender];
    if (sender.voted)
    throw;
    //当投票代表 to 也委托给别人时候，虚招到最终的投票代表
    while (voters[to].delegate !=address(0)&& voters[to].delegate !=msg.sender)
    to = voters[to].delegate;
    //当最终投票代表等于调用者，这是不予许的
    if (to ==msg.sender)
     throw;
    //因为 sender 是一个引用
    //这里实际修改了 voters[msg.sender].voted
         sender.voted = true;
         sender.delegate = to;
         Voter delegate =voters[to];
     if(delegate.voted){
    //如果委托的投票代表已经投票，直接修改票数
        proposals[delegate.vote].voteCount +=sender.weight;
    }else{
    //如果投票代表还没有投票，则修改其投票的权重
        delegate.weight += sender.weight;
     }
  }

 //投出选票（包括委托给该用户的选票）
 //给 proposals[proposal].proposalNames
function vote(uint proposal){
    Voter  storage sender = voters[msg.sender];
    if (sender.voted)throw;
    sender.voted = true;
    sender.vote = proposal;
 //如果 proposal 索引超出了给定的提案数据范围
 // 将会自动抛出异常，并撤销所有改变
    proposals[proposal].voteCount +=sender.weight;
 }


 //根据当前的所有投票计算出当前的胜出提案
 function winningProposal() constant returns (uint winningProposal){
    uint winningVoteCount = 0;
    for(uint p =0; p<proposals.length;p++){
        if(proposals[p].voteCount >winningVoteCount){
            winningVoteCount = proposals[p].voteCount;
            winningProposal = p;
    }
  }
```

```
  }
}
```

5）社群成员集体投票，根据结果获得相应代币奖励

最后，所有抵押了一定数量 MOS 代币的社群成员，将参与投票。为了提高成员的投票率，鼓励成员为了积极谋求自身的利益，MOS 公链设计了下列激励机制：

- 一旦自己所投票的议题选项得到大部分成员的认可，即获得了通过，就可以从奖池中获得一定数量的代币奖励。
- 如果自己所投票的选项没有通过，成员所抵押的代币将被用于奖励其他获得通过的成员。

这样不仅将鼓励成员参与投票，也会鼓励他们仔细分析每个议题、每个选项的实际价值，做出做适合社群的选择。激励机制与其自身利益达成“互动”，实现正反馈。

综上所述，这就是 MOS 公链所提出的 DAO 2.0“决策共识”流程。可以看到，整个流程完全基于智能合约自动运行，而且通过 VRF 随机筛选、激励机制等，有效地减少了中心化的可能性，提高了社群成员参与决策的积极性和效率。

3.2. MOS 公链的算法共识机制

一个公链的发展壮大，离不开矿工、节点的积极参与和贡献，而这源自于对于这些成员贡献的认可和奖励。在区块链过去的发展历史中，存在着基于特定计算机算法的 PoW（工作量证明）、PoS（权益证明）和 DPoS（代表式权益证明）等多种机制，即所谓的 **“算法共识”** 。

区块链是一个公共账本、公开的数据库，同时也是一个点对点的协作网络。协作方（节点）共同维护数据，每个节点都有一份完整的数据备份，所有节点的数据内容必须完全一致，每个节点都可以在本地查找交易记录，每个节点也可以在本地添加交易。没有一个中心来指挥、协调，要完成这个协作，区块链就必须有一个共识机制，这个机制必须解决两个基本问题：

- 谁有权写入数据——一次只有一个人可以记账；
- 其他人如何同步数据——因为要保持账本的一致性。

数据写入（区块添加）的过程是这样的：有权打包交易的节点，将打包的交易（区块）放在既有的数据库（区块链）上，并向全网广播，其他节点收到信息，验证区块无误，就会同步这个新打包的交易。每个打包的交易叫做一个区块，区块不断叠加，延长区块链。同步数据有一个问题，就是如何对在一定时间段内发生的交易的先后顺序达成一致。由于各个节点都在自发地记账或者同步，在点对点相互通信下的情况下存在较高的网络延迟，因此各个节点收到数据的先后顺序是不一致的，那么保证每个节点副本数据的一致性就变成了非常重要的问题。

区块链的共识是：以最长链作为主链，即每个节点总是选择并尝试延长主链，也就是各节点都以区块最多的那条链作为自己添加、更新区块的选择，这样多节点就能同步一个权威的公共账本了。那么，区块链共识机制重点要解决第一个问题：**谁有权写入数据**。随着区块链的发展，已经有多种方法解决这个问题。下面介绍一下三个主要的：PoW、PoS 和 DPoS。

1） PoW（Proof of Work，即工作量证明）

这里的工作量，指的是计算机计算 Nonce（随机数)的过程。每个节点都去计算一个随机数，一定时间段内，找到随机数的难度是一定的，这就意味着，得到这个随机数必然要经过一定的工作量。最先得到这个随机数的节点，将打包的交易区块添加到既有的区块链上，并向全网广播，其他节点验证、同步。

优点：

- 安全，由于矿工们都是花钱购置矿机参与挖矿，矿机的花费是实打实的沉没成本，所以集中作恶（比如集体记假账欺骗全网等）的可能性较低，比特币经历近 10 年时间从未出现任何错漏或是被攻击，已经足以证明 PoW 算法最为优越的安全性，其他诸如 PoS、DPoS 等机制都是近几年才兴起的新共识机制，并未经过时间检验，即便短期内并未出现大的问题或是漏洞，仍无法断言在以后一定不会出现重大安全问题。
- 优质项目易吸引早期矿工，由于早期参与者更容易获取较大奖励，且不需要专门的矿机，矿工们往往更倾向于参与这种早期的优质 PoW 项目，如果项目发展良好，能够获得较高额的收益。这一优点是仅针对今天而言的，因为比特币 PoW 的成功，显卡矿工们四处寻找优质项目挖矿，无形中为早期项目贡献了一份力量，但比特币问世时，上述两个优点其实都不存在，因此这一共识机制其实是个经历的时间越久越安全，也越有魅力的机制。

缺点：

- 资源浪费，由于计算能力的竞争导致参与者们不断升级硬件（显卡）以获得更大的计算能力，甚至生产专门用来计算 SHA-256 或是其他数学难题的机器（矿机），这些机器的生产和运行造成巨大的人力、电力资源浪费，只为了计算一道毫无意义的加密数学题，这也是比特币最为人所诟病的一点。
- 升级困难，由于整个计算和竞争的过程全部写在各式各样的矿机当中，任何针对原有共识机制的升级都很难在短时间内通知并实现所有参与人的变更，且由于参与者个人意愿的不同，很难实现整个机制和系统的平滑升级，造成分叉和安全性下降几乎很难避免的。

2）PoS（Proof of Stake，权益证明）

PoS 是系统根据节点持有的 Token（代币）的数量及时间的乘积（币*天数）分配相应的记账权，拥有的代币越多，获得记账权的概率越大。Token 就相当于区块链系统的权益（Stake），因此被称为基于权益的证明。

优点：

- 无资源浪费，没有矿机，获得大收益的方式是成为更大的利益相关者。
- 升级相对容易，都通过电脑在软件和线上进行，不涉及硬件的运算重写。

缺点：

- 安全性无法完全确定，部分持币人可能是使用其他数字货币与 POS 币种交换而来，不存在实质上的沉没成本，作恶成本相对较低，且机制未经时间检验，无法短期内确定安全性。
- 通货膨胀和财富集中现象更为明显，由于有增发机制，在货币全部发行完毕之前每年均存在通货膨胀的情况，财富也会趋于集中化。

3）DPoS（Delegated Proof of Stake，即权益授权证明）

PoS 是拥有 Token 就拥有获得记账的权利，而 DPoS 是指拥有 Token 的人投票给固定的节点，这些节点作为权益人的代理去行使记账的权利。这些获得投票认可的代表根据一定的算法依次获得记账权。不同于 PoW 和 PoS 理论上全网都可以的参与记账竞争，DPoS 的记账节点在一定时间段内是确定的。权益授权证明能够让每个节点首先通过权益，选举出 n 个记账节点，类似于公司中的董事会制度，后续提案由这些被选中的节点轮流处理。权益授权证明理论上不要求选出的代表个体本身是权益所有人，看起来更民主、更开放。如果选出的代表不作为（轮到自己记账时不记账），或者作恶，可以把他们筛除，如有必要则进行惩罚（选民们也有可能被惩罚）。股份授权证明机制大大提高了效率，但是减少了记账节点的规模，属于弱中心化。

优点：

- 易用性最优，特殊节点数量不多，验证效率高，使用人体验好。
- 特殊节点往往是持币量巨大的利益强相关团体或个人，具备更高的社会影响力，随着币价的上涨，记账奖励将为特殊节点带来巨大的收益，因此特殊节点的宣传意愿较上述机制最为强烈。

缺点：

- 安全性较弱，验证节点过少，通过牺牲安全性交换更良好的易用性，本质上已经不能算是去中心化的记账方式了，特殊节点的实质可能只是分布在世界各地的寥寥几台服务器而已，安全隐患较大。
- 特殊节点权利过大，也很难做到完全匿名，集体作恶或者集体受胁迫作恶的可能性无法排除。
- 个人投票意愿弱，且由于特殊节点本身也是持币量巨大的权益人，通过票选的方式想变更节点必然是利益集团的博弈，社区分裂的可能性较高。

4）PBFT（Practical Byzantine Fault Tolerance，实用拜占庭共识算法）

实用拜占庭容错算法是一种基于消息传递的一致性算法。它与之前三种都不相同，PBFT 以计算为基础，也没有代币奖励。由链上所有人参与投票，少于（N-1）/3 个节点反对时，就获得公示信息的权利。该算法经过预准备（Pre-prepare）、准备（Prepare）和确认（Commit）三个阶段达成一致性。这些阶段可能因为失败而重复进行。实用拜占庭容错算法信息在节点之间互相交换后，各节点列出所有得到的信息最后以大多数的结果作为解决方法。

拜占庭将军问题是由 Leslie Lamport 在 1982 年提出的，具体描述如下：拜占庭帝国派出了 m 支军队去围攻一个敌人。由于拜占庭的军队在不同的地点，所以必须在分开的包围状态下同时攻击。他们任一支军队单独进攻都毫无胜算，除非有多于 n 支军队同时袭击才能攻下敌国，而军队之间只能依靠通信兵相互通信来协商进攻意向及进攻时间。但是在拜占庭将军之间可能存在叛徒，这些叛徒的目的是通过故意传出虚假消息或者不传出任何消息等行为，来阻挠其他忠诚的将军达成一致的作战计划。

拜占庭将军问题是现实的分布式系统的模型化，其中的军队对应于分布式网络中的节点，是否能达成行动协议并消灭敌人对应于分布式网络中是否能达成一致性，而将军中的叛徒行为则对应于当计算机出现故障节点表现出前后不一致的情况，如信道不稳定、导致节点发送给其他节点的消息发生了错误，或者消息损坏等，上述分布式系统故障也被称为拜占庭错误。当分布式系统中仅出现消息丢失或者重复，但是不会出现内容损坏的情况则被称为非拜占庭错误。容错性指的处理

这些异常或故障的协议。能够处理拜占庭错误的算法称为拜占庭容错，而能够处理非拜占庭错误的则被称为非拜占庭容错。

优点：

- 无需算题挖矿，节约能源。
- 确定信息正确性的速度非常快。

缺点：

- 在节点增加时，需要进行大量的信息交互，整个系统的负担大大加重，因而扩展性较差。
- 安全性差（容错率仅为 1/3）。

综上所述，区块链解决了在不可信信道上传输可信信息、价值转移的问题，而共识机制解决了区块链如何分布式场景下达成一致性的问题。针对各个细分金融领域的独特需求，包括代币融资、点对点抵押借贷、稳定币、去中心化衍生品市场、大宗 OTC 协作等等，每种业务的参与者需求不同，对于激励机制的要求也各有差别。因此，如果在一个公链体系中，只采用单一的算法共识，就很容易无法凝聚起整个行业的参与度。事实上，很多金融领域的区块链项目都在这方面顾此失彼，无法顾及不同领域、不同专业社群成员的特定需求，从而限制了社群扩大的规模。

为此，MOS 公链首次提出了采用 **PoFC**（Proof of Finance Contribution，金融贡献证明）作为算法共识机制。**“金融贡献”**包括金融交易资源（即“权益”）和社群贡献（即“工作量”）的结合，允许公链上的各种应用针对不同的需求，采用不同的权重分配这两种贡献在于总体共识机制中所占的比例，将其落实到智能合约之中，实现基于代码的**双重激励系统**。注意，这里的**“金融交易资源”**并不仅限于拥有的代币数，还包括：

- 交易量；交易越频繁，贡献越大。
- 委托销售和委托代购的金额
- 邀约的挖矿节点个数
- 代币发行数量

记录这些资源的目的，是鼓励矿工、节点积极参与社群的金融活动、交易，从而提高社群的活跃度和融资效率。**社群贡献**（即“工作量”）部分，则需要按照已有的挖矿算法计算，根据每个矿工、节点的算力，提供相应的挖矿机会和代币奖励。

MOS 公链综合考虑这两方面因素，并且允许每个项目、社群，根据自己的需要，针对金融应用的实际需求定制相应的共识机制，即分配这两种因素的权重，做到一项目一共识，其相关流程如下图所示：

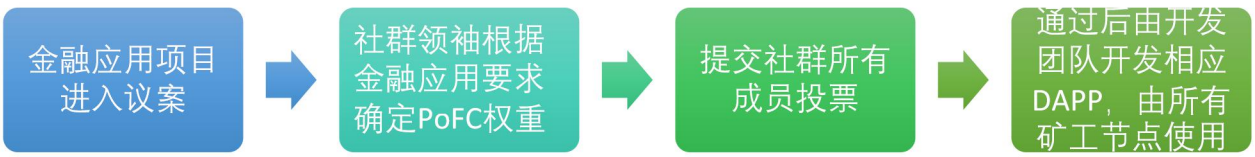


图 12 MOS 公链共识机制形成流程

3.3. 基于内生经济增长模型的 DAO 2.0 发展模式

MOS 公链借鉴 2018 年诺贝尔经济学奖得主保罗·罗默所建立的**“内生经济增长模型”**（Endogenous growth theory，简称 EGT），将对普通经济体系的 GDP 估算模型，移植到了 DAO 2.0 组织，从而建立起了针对分布式组织所产生价值的统一评价体系。

自亚当·斯密以来，整个经济学界围绕着驱动经济增长的因素争论了长达 200 多年，最终形成的比较一致的观点是：一个相当长的时期里，一国的经济增长主要取决于下列三个要素：（1）随着时间的推移，生产性资源的积累；（2）在一国的技术知识既定的情况下，现在资源存量的使用效率；（3）技术进步。但是，60 年代以来最流行的新古典经济增长理论，依据以劳动投入量和物质资本投入量为自变量的柯布-道格拉斯生产函数建立的增长模型，把技术进步等作为外生因素来解释经济增长，因此就得到了当要素收益出现递减时长期经济增长停止的结论。

可是，90 年代初期形成的“新经济学”即内生增长理论则认为，长期增长率是由内生因素解释的，也就是说，在劳动投入过程中包含着因正规教育、培训、在职学习等等而形成的人力资本，在物质资本积累过程中包含着因研究与开发、发明、创新等活动而形成的技术进步，从而把技术进步等要素内生化，得到因技术进步的存在要素收益会递增而长期增长率是正的结论。当然，许多经济学家早已看到了人力资本和技术进步对经济增长的作用，但是，他们都是把它们看作是外生因素。

这样，这两种理论的政策含义出现了分歧：尽管财政经济学家一直认为财政政策能够影响经济增长（因为财政政策与经济增长间的内在联系表现在许多方面，诸如扭曲性税收的负效应、累进税对储蓄倾向的不利影响以及增加税收动用额外资源以提高公共投资水平等等），但是新古典增长论却认为，长期经济增长完全是由理论本身的外生因素决定的，因此无论采取什么政策，长期增长都不变，或者说，财政政策对经济增长充其量只有短期效应，而不能影响长期增长；而内生增长论则认为，一国的长期增长是由一系列内生变量决定的，这些内生变量对政策（特别是财政政策）是敏感的，并受政策的影响。如果增长率是由内生因素决定的，那么，问题就是经济行为主体特别是政府如何能够影响增长率的大小，因而财政政策对经济增长的影响再次成为关注的焦点。

罗默模型、卢卡斯模型和格鲁斯曼一赫普曼模型只是最著名的内生增长模型，还有很多其他模型侧重不同的增长方面，诸如金和罗伯森的知识传播内生增长模型、阿格赫恩和豪威特的模仿与创造性消化内生增长模型以及杨氏国际贸易内生增长模型。所有这些模型表达出来的一个重要思想是：**企业是经济增长的最终推动力，特别是这些模型试图说明企业如何积累知识，这种知识广义地包括人力资本和技术变化**。这种知识积累表示为增加人力资本、生产新产品和提高产品质量。这些模型表明，知识和积累过程会出现外部性或知识外溢效应，需要政府政策的干预：各种政策旨在扶持研究与开发、革新、人力资本形成甚至关键性产业部门。

综上所述，可以对内生增长理论所表达的经济增长的原因做出如下简单的非技术性陈述：

1） 技术创新是经济增长的源泉
2） 劳动分工程度和专业化人力资本的积累水平是决定技术创新水平高低的最主要因素
3） 政府实施的某些经济政策对一国的经济增长具有重要的影响。

类似的，MOS 公链将每个金融应用、项目的代币数量、矿工数、节点数和技术投入（MOS 基金会开发团队用于各个项目的开发投入），作为类似参数，通过一定的转化和分析，可以量化各个金融项目的价值，并预测未来其长期增长率。

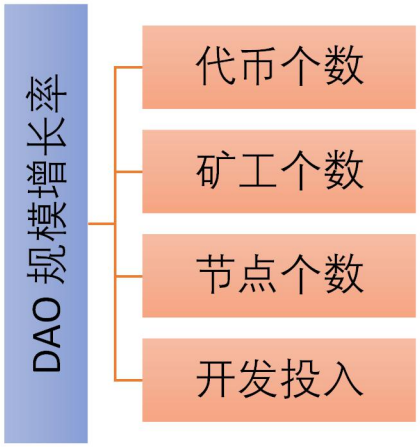


图 13 基于内生经济增长模型的 DAO 增长率预测

3.4. DAF (Decentralized Autonomous Finance) 协议组

MOS 公链作为一个平台，通过对 DAO 2.0 的创新设计，得以形成社群共识，从而在这基础上逐步衍生出多种金融应用。

首先，针对金融领域的融资、借贷、代理、衍生品等特殊需求，MOS 开发出了专门用于消除金融领域去中心化各种痛点的“DAF”(Decentralized Autonomous Finance，去中心化自治金融) 协议组。

最后，MOS 公链还将继续加强各方面的特性，包括跨链、侧链等支持，完善公链生态，逐步成为金融行业首选的第一公链。

3.4.1 基于智能合约的去中心化自治社区发行

DAF 协议组的首要应用，是实现真正基于智能合约的、去中心化的自治社区代币发行。这种发行机制的核心理念是，只要若干个节点达成共识，就可以通过设定节点权利、决策共识规则（譬如投票制、随机制等等），就可以发布基于智能合约的代币。对此代币感兴趣的社群成员，就可以直接向这些节点购买代币，或者通过其他代理委托购买。代币销售所产生的收入，按照节点之间达成的共识，在所有节点、成员之间分配。

与传统的区块链融资方式相比，这种模式具有下列优势：

- MOS 生态坚信，由更多的社群领袖、优质节点带领下的社群共识，能够真正地辨别出项目的优劣，而不需要中心化的机构进行项目的信任背书。凡是中心化的机构，必定会以自己的利益为主，无法为普通投资者负责。
- 对于投资者来说，因为这个过程完全基于智能合约，透明、可追溯，避免了项目方营私舞弊，大大降低了投资风险。

- 对于发行方而言，整个过程不需要依赖于任何第三方或者交易所等，避免了中间架构赚取高额不透明差价等问题。
- 发行方、项目方可以把精力集中于项目的价值拓展和社区的建设上，而把代币发行的具体事项交由社群自治。
- 确保代币的二级市场价值源于社群共识的力量。真正通过社群共识进行代币发行，会激发市场价格的自我调节能力，从而让公开二级市场交易的价格趋于稳定。

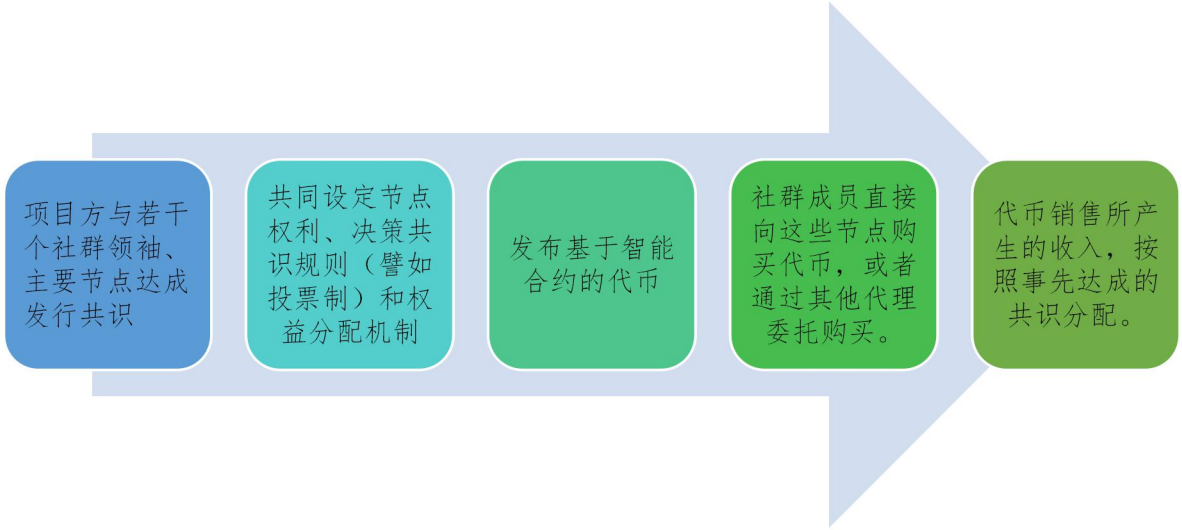


图 14 通过 DAO 2.0 发行代币的流程

3.5. 生态系统

综上所述，在整个 MOS 公链构建了一个分布式的、面向金融行业的全新生态系统。该系统主要包含了下列要素：

- 基金会：MOS 基金会作为整个公链的组织者、运营者，承担着构建基础设施、组织开发团队、更新智能合约、提供核心服务等功能，为所有公链用户、社群成员提供全方位的支持。基金会将通过 MOS 代币得到前期投入资金，用于各个系统、产品和合约的开发和维护。
- MOSDAO：MOSDAO 程序运行在每个成员的客户端之中，是链接所有成员的核心手段。MOSDAO 具有下列特色：
  - 基于云服务，多点备份，高度安全、可靠
  - 支持 HD 钱包功能
  - 支持多重签名，在启用时成员可以选择由几个其他成员协同情况下可以解锁，从而避免单个成员因为密钥丢失而失去账户所有权
  - 社群共识功能，包括委托、投票、抵押、奖惩等等多种机制，都会通过 DAPP 所支持的智能合约完成，实现基于社群自治的金融交易。
- MOS 代币：详见第四章。

- 社群自治管理系统：每个社群的社群领袖，都可以自定义社群的自治管理系统，这包括了基于 DAF 的一系列智能合约，譬如：
    - 可以把社群销售额的部分作为社群成员的激励
    - 可以让每个成员缴纳会费，所有会费作为奖池进行社群成员贡献的激励。具体的网络设定及节点激励的比例，则全部由社群组织者通过合约进行自定义，再由所有成员集体投票决定（通过“决策共识”机制）。
- 社群：社群是 MOS 生态系统中至关重要的组成部分，其中包括社群成员、社群领袖、委托代理商等角色。
- 开发团队：开发团队由基金会管理，负责为所有社群提供技术支持，包括智能合约开发和维护，公链基础设施管理等。
- DAPP：针对各种不同类型的金融应用，包括抵押、借贷、委托等，每个项目方可以在 MOS 公链基础上开发 DAPP。MOS 基金会为此提供了强大的 SDK（软件开发工具包）和 API 接口，方便项目方开发创新的金融应用。
- 跨链支持：MOS 公链不仅支持自己生态系统中的金融应用，也会通过跨链支持，对主流加密货币公链（包括比特币公链、以太坊等）给于全面支持，从而大大增加了金融衍生品的支持种类，让项目方和社群成员可以搭建结合 MOS 代币和主流币种的交易对、衍生抵押/借贷服务。

4. MOS 代币介绍

4.1. 属性说明

MOS 代币是 MOS 公链的平台币，类似于币安币（BNB）和火币代币（HT）等平台币，属于权益型代币，可以进行社群投票、质押、购买权益等各种金融场景下与用户权益相关的应用。在前期，MOS 代币将只在部分 MOS 公链系列交易所中流通使用，但是会逐渐上架主流交易所。相比常规加密货币，拥有更多的属性和权利。

与其他平台币相比，MOS 代币具有以下特征：

- 持有者可以用于 MOS 公链内部的各种权益，包括投票、VRF 筛选、抵押、委托等。
- 持有者可以获得 MOS 生态社群治理权。
- MOS 公链会经常开展回购 MOS 代币活动，销毁回购的 MOS，保障 MOS 价值的稳定提升。

4.2. 发行方式

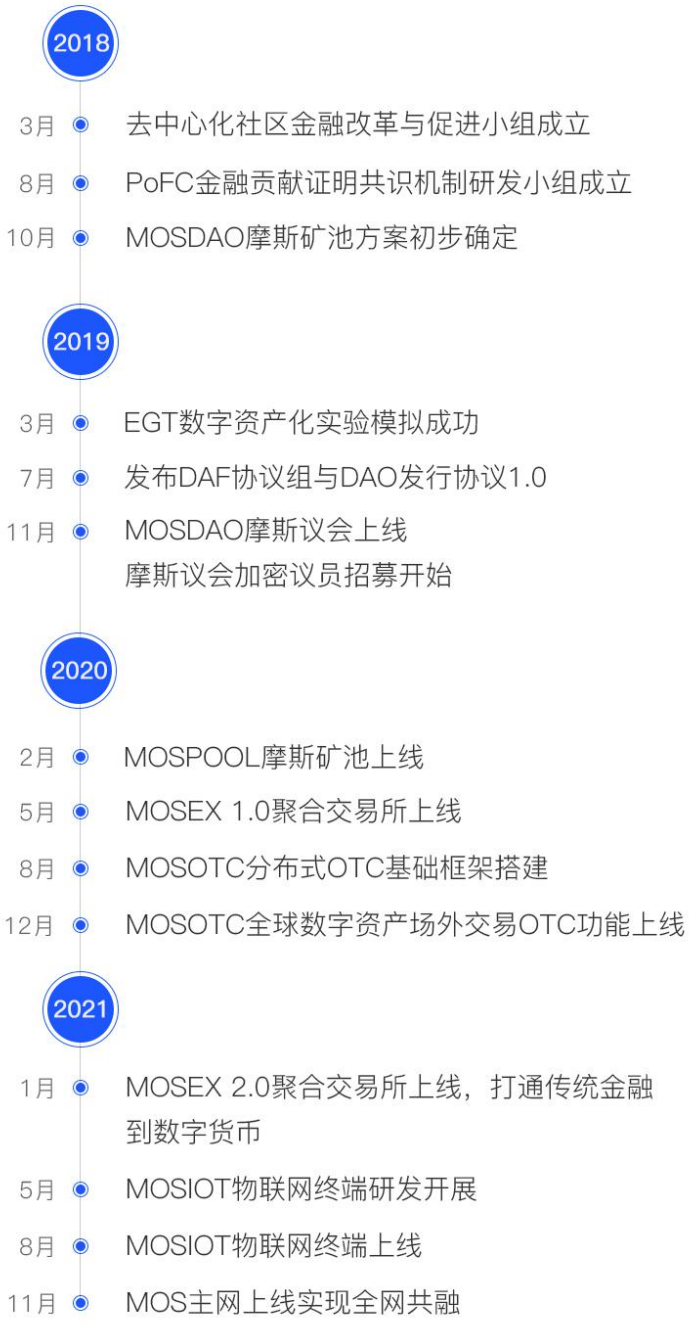
MOS 的总量 5 亿，永不增发。主网上线之前，MOS 基于 ERC20 发行。主网上线后，这让它成为 DAO2.0 技术和商业理念下的新型 Token。

<table>
<tr><th>总发行量</th><th colspan="2">发行规划</th></tr>
<tr><td rowspan="3">5 亿 MOS</td><td rowspan="2">2500 万 MOS 作为基础建设基金</td><td>2000 万代币作为 MOS 全球团队的代币激励，分五年解锁，每年解锁 500 万。第一年解锁 500 万，半年解锁完毕。</td></tr>
<tr><td>500 万代币作为 MOS 星光计划，帮助 MOS 在前期建立去中心化自治营销网络的奖励用途，详见 MOS 星光计划。</td></tr>
<tr><td colspan="2">4.75 亿 MOS 通过 DAO 发行池进行发行</td></tr>
</table>

关于这些代币的具体分配、空投和流通方式，请参阅《MOS 商业白皮书》。

5. 项目路线图

*具体时间可能会有变化，请关注 MOS 公链项目方的官方公告



6. 风险提示

本白皮书内的任何内容均不构成法律，财务，业务或税务建议，在参与本白皮书中任何活动之前，请咨询相关的法律、财务、税务或其他专业顾问。鉴于本项目商业模式的属性和项目处于早期发展阶段，本白皮书中的 MOS 代币应当被视为是高风险项目。购币者应当已经了解本项目的潜在风险，本项目仅适合能够承受本项目风险的购币者。此外，购币者在购买 MOS 代币前应考虑其他的风险，并建议在购买之前就所得税、法律及其他相关事宜咨询相关的专业人士。

司法监管相关的风险

区块链技术已经成为世界上各个主要国家的监管主要对象，任何国家之中现有的对于 MOS 代币或本次公开售卖的监管许可或容忍可能只是暂时的。项目方可能会不时收到来自于一个或多个主管机关的询问、通知、警告、命令或裁定，甚至可能被勒令暂停或终止任何关于本次公开售卖、MOS 代币开发的行动。MOS 代币的开发、营销、宣传或其他方面以及本次公开售卖均因此可能受到严重影响、阻碍或被终结。同时，MOS 代币可能随时被定义为虚拟商品、数字资产或甚至是证券或货币，因此在某些国家之中按当地监管要求，MOS 代币可能被禁止交易或持有。此外，在特定司法管辖区域被禁止或限制的程序，如涉及赌博、投注、彩票、乐透、色情等等的程序，可能利用 MOS 区块链的无准入要求来开发、促进、营销或运营。特定司法管辖区域的监管当局可能对特定程序甚至其开发者或用户采取相应行政或司法措施。任何政府当局的处罚、惩罚、制裁、镇压或其他监管措施，或多或少会惊吓或威慑到既有或潜在 MOS 代币用户使用 MOS 公链平台并持有 MOS 代币，从而对 MOS 公链的前景造成重大不利影响。

黑客或盗窃的风险

黑客或其它组织或国家均有以任何方法试图打断 MOS 公链功能的可能性，包括服务攻击、Sybil 攻击、游袭、恶意软件攻击或一致性攻击等。

漏洞风险或密码学科突飞猛进发展的风险

密码学的飞速发展或者科技的发展诸如量子计算机的发展，或将破解的风险带给加密货币和 MOS 公链平台，这可能导致 MOS 公链的用户遭受损失。

应用存在的故障风险

MOS 公链平台可能因各方面的原因故障，无法正常提供服务，严重时可能导致用户遭受损失。开源软件中被忽视的致命缺陷或全球网络基础设施大规模故障造成的风险。虽然其中部 分风险将随着时间的推移大幅度减轻，比如修复漏洞和突破计算瓶颈，但其他部分风险 依然不可预测，比如可能导致部分或全球互联网中断的政治因素或自然灾害。

代币销售市场风险

由于代币销售市场环境与整个数字货币市场形势密不可分，如市场行情整体低迷，或存在其他不可控因素的影响，则可能造成数字货币本身即使具备良好的前景，但价格依然长期处于被低估的状态。此外，代币在公开市场上交易，通常价格波动剧烈。这种波动可能由于市场力量（包括投机买卖）、监管政策变化、技术革新、交易所的可获得性以及其他客观因素造成，这种波动也反映了供需平衡的变化。无论是否存在 MOS 代币交易的二级市场，项目方对任何二级市场的 MOS 代币交易不承担责任。因此，MOS 代币交易价格所涉风险需由 MOS 代币交易者自行承担。

信息披露不完备风险

MOS 公链项目仍在开发阶段，其哲学理念、共识机制、算法、代码和其他技术细节和参数可能经常且不断地更新和变化。尽管 MOS 公链项目的白皮书包含了 MOS 公链项目最新的关键信息，其并不绝对完整，且仍会被项目方为了特定目的而不时进行调整和更新。项目方无能力且无义务随时告知参与者 MOS 公链项目开发中的每个细节(包括其进度和预期里程碑，无论是否推迟)，因此并

不必然会让参与者及时且充分地获悉 MOS 公链项目开发中不时产生的信息。信息披露的不充分是不可避免且合乎情理的。

私钥丢失的风险

购买者的数字货币 MOS 代币，在提取到自己的数字钱包地址后，操作地址内所包含内容的唯一方式就是购买者相关密钥(即私钥或是钱包密码)。用户个人负责保护相关密钥，用于签署证明资产所有权的交易。用户理解并接受，若丢失或损毁了存取 MOS 代币 所必需的私钥，这可能将是不可逆转的。只有通过本地或在线钱包来占有相关的独一无二公钥和私钥，才可以操作 MOS 代币。每一购买者应当妥善保管其钱包的私钥。若 MOS 代币购买者的该等私钥丢失、遗失、泄露、毁损或被危及到，项目方或任何其他人士均无法帮助购买者存取或取回相关 MOS 代币 。此外，保管好钱包的安全（尤其是其中的私钥），才能享受到购买 MOS 代币所附带的奖励、赠送等福利。MOS 代币均应当提取至由用户绝对控制的钱包内。一旦 MOS 代币因任何原因而被转让或转移走，MOS 代币所附带的未兑现奖励和赠送将无法获得。最好的安全储存登录凭证的方式是购买者将密钥分开到一个或数个地方安全储存，且最好不要储存在公用电脑。任何通过解密或破解 MOS 代币购买者的密码而获得购买者注册邮箱或注册账号访问权限的人士，将能够恶意认领所窃取的 MOS 代币 。

无法预料的其它风险

除了本白皮书内提及的风险外，此外还可能存在着一些 MOS 公链团队尚未提及或尚未预料到的风险。

关于本文版权

THANKS!