

AOS 白皮书



AOS 创始团队

AOS 白皮书 Version1.0

2018 年 5 月 21 日 本文档将根据项目进展持续更新

摘要

AOS (Application Operation System) 是一个以全球战略定位为出发点的开源社区项目，致力于打造安全、高效、易用的区块链公共操作平台。AOS 支持全局统一账户、智能合约，通过 Sharding 技术采用主链、应用链并行的分层的技术框架。在 AOS 中，特别强调对个人信息资产的保护，提供了个人完全控制的数据存取技术和基础设施，这是 AOS 公链平台的一个特色和亮点。开发者和社区是公链价值生态系统的基础，AOS 为开发者提供友好的 Dapp 创建模板和高度模块化的社区协同工具。AOS 以比特币为前瞻先驱，摆脱行业束缚，以其灵活特性与模块化的自由重组，应用于各细分领域。

目录

| | |
|---------------------|----|
| 摘要..... | 1 |
| 1、项目背景..... | 3 |
| 1.1 区块链创新价值..... | 3 |
| 1.2 面临的问题..... | 4 |
| 1.3AOS 团队共识..... | 6 |
| 2、AOS 的价值与愿景..... | 8 |
| 2.1 AOS 价值..... | 8 |
| 2.2 AOS 愿景..... | 8 |
| 3、AOS 技术架构..... | 9 |
| 3.1 主链与应用链..... | 9 |
| 3.2 大数据私有链..... | 10 |
| 3.3 应用协议栈..... | 12 |
| 3.4 模块化..... | 13 |
| 3.5 技术实现路径..... | 14 |
| 3.6 创新和核心技术..... | 16 |
| 3.7 整体技术方案..... | 16 |
| 4、AOS 生态及运行机制..... | 17 |
| 4.1 AOS 生态..... | 17 |
| 4.2 激励机制..... | 18 |
| 4.3 运行机制..... | 21 |
| 5、开发路线图..... | 21 |
| 6、Token 分配..... | 22 |
| 7、团队介绍..... | 23 |
| 8、风险说明..... | 23 |
| 8.1 免责声明..... | 23 |
| 8.2 竞争风险..... | 24 |
| 8.3 人才流失风险..... | 24 |
| 8.4 项目技术风险..... | 24 |
| 8.5 项目缺少关注度风险..... | 24 |
| 8.6 黑客攻击风险..... | 25 |
| 8.7 密钥丢失风险..... | 25 |
| 8.8 目前未可知的其他风险..... | 25 |

1、项目背景

1.1 区块链创新价值

2009 年中本聪正式发布比特币 (BitCoin), 开创了区块链价值互联网新纪元。在近 10 年的发展过程中, 区块链技术大致经历了三个阶段。第一个阶段 (约 2009-2015), 以比特币为代表, 区块链技术主要用于数字货币发行, 区块链技术实现不依赖于各国央行的数字货币发行。第二个阶段 (约 2015-2018), 以以太坊 (Ethereum) 为代表, 发展和完善了智能合约技术, 使得区块链技术突破了货币发行和价值转移应用, 图灵完备的智能合约技术, 理论上区块链可以实现世界上任何应用。第三个阶段, 从 2018 年开始, 致力于突破现有区块链存在的效率瓶颈问题, 与各领域实际应用相结合, 实现区块链真正落地。

区块链是分布式数据存储、点对点 (P2P) 网络、共识机制、加密算法等计算机技术的创新应用模式。去中心化、公开透明、不可篡改、可追溯等是区块链技术最主要特征。区块链的去中心化, 意味着区块链不受某个中心组织的垄断和控制, 每个参与者都是平等的, 能够自由进入和退出。区块链中包括源代码, 一切都是公开透明的, 所有的重大决策都是通过参与者共同协商与投票来解决。

我们认为, 区块链技术最大的创新和贡献, 是通过技术手段, 重构了一种新型的社会协作关系, 一种新型的经济体或经济组织。区块链通过真实可信、无法篡改、可追溯的行为 (数据) 记录, 提供了可信的信用基础。区块链中通过发行数字货币提供了统一的价值表示和计量单位。信用+激励+参与者, 就构成了一种独立的、自洽的、能够自我成长的经济系统, 或区块链社区。

区块链这种协作式社区与传统的公司制社会经济组织是完全不同, 主要体现在以下三个方面:

- 组织方式: 公司是分层和逐级授权的经济组织, 区块链社区是对等协商和投票决策的经济组织;
- 参与主体: 公司是以人为核心的经济组织, AI、IoT 技术发展和普及, 区块链中参与者不仅仅是人, 各种智能硬件将会成为参与的主体;
- 驱动方式: 公司以绩效和制度考核驱动, 区块链以智能合约驱动, 实现

自动化经济；

从以上比较我们看到，区块链不仅仅是一种技术创新，首先是对现有社区经济组织形式和结构的一种颠覆性创新，是代表了在 AI、IoT 等技术驱动下，社会未来发展的主要模式，这是区块链具有广阔前景和无限价值的基础。

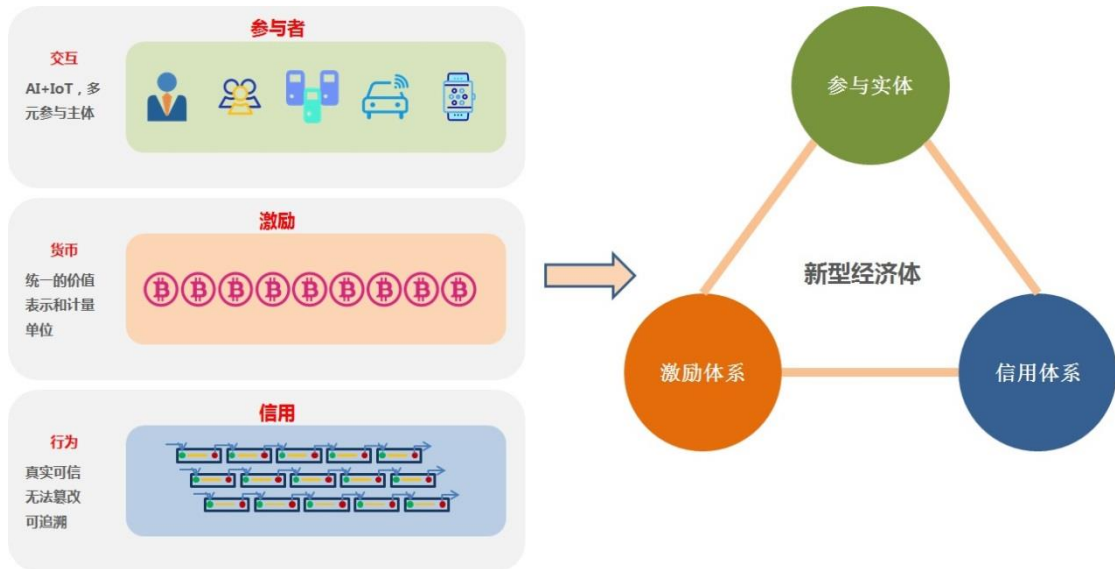


图 1 区块链重构社会经济组织

1.2 面临的问题

比特币通过区块链技术，不依赖于中心机制，基于工作量证明（POW: Proof of Work）的共识机制，解决了数字货币的“双花”问题，实现了去中心化的数字货币发行。比特币是在 2008 年由金融危机引发席卷全球的经济危机背景下而出现，在很大程度上，比特币是对中心垄断的金融体系和货币滥发的一种反对。因此，比特币中的区块链，其初衷是为了解决数字货币发行中的难题，效率并不是其关注的问题。但是，随着区块链技术的发展和应用的逐渐深入，区块链的性能问题已经成为制约区块链广泛应用的第一首要的瓶颈。

例如，比特币平均交易处理能力是 6.7 TPS，以太坊也只有 15 TPS，这种效率远远不能满足现实需求。为了解决区块链的效率瓶颈，人们提出了各种各样的解决方案。

1. **闪电网络**：闪电网络的主要思路是将大量交易放到比特币区块链之外进行。核心的概念主要有两个：RSMC（Recoverable Sequence Maturity Contract）和 HTLC（Hashed Timelock Contract）。前者解决了链下交易的确认问题，后者解决

了支付通道的问题。闪电网络通过 2 层网络的结构，试图通过整体分解为局域的方式，提高整体的处理效率。以太坊也提出了类似的项目：雷电网络。

2. 分片技术：分片（Sharding）就是每一笔交易不必发动全网节点来处理，根据交易的类型和重要程度，只让网络中的一部分节点处理就好了，从而提高全网的交易处理效率。

3. DAG 技术：DAG（Directed Acyclic Graph），是放弃了区块链数据的块状结构，不必等待块生成的时间，通过交易之间的偏序关系，可以做到交易的及时确认。

4. 改进共识机制：POW 共识机制是一种全网共识机制，Internet 网络是一个不一致的环境，当节点非常多的时候，共识过程必然成为一个瓶颈，同时 POW 共识机制因为大量的电力消耗而广受诟病。因此，很多项目通过权益证明 POS 或授权权益证明 DPOS 等方式实现共识，减少计算复杂度或减少节点，以提高出块效率和整体网络性能。

以上列出了提高区块链处理效率的技术，除此之外，很多项目还通过数据块的扩容或缩短块生成时间等技术方式来提高区块链的处理效率。每一种方案都有其利弊，闪电网络，是根据交易类型的轻重进行分类，建立交易通道，减少主链的压力，从而提高 TPS 效率；分片技术，是对记账节点进行划分，与应用的实际规模相匹配，减少了主链的快速膨胀，有利于横向扩展；DAG 技术，没有了出块的等待时间，在 IoT 相结合的区块链应用领域，局部性很重要，也具有其特有的优势；而从效率的角度来看，以 DPOS 方式解决区块链性能瓶颈的项目，具有很强的说服力，通过采用超级节点大幅度提高区块链的处理效率，比如 EOS。

区块链，尤其是公链，作为一种社会应用的基础操作平台或者操作系统，目前的区块链项目的完备性和基础性还不够，只能支持某特定领域的应用，这是区块链项目第二个需要改进的问题。主要体现在以下几个方面：

1. 大数据支持不足：区块链是一种分布式数据存储，具有固定大小的容量和固定数据格式，显然与大数据处理需求相冲突。大数据是当前信息社会的最基础特征，区块链与大数据相融合，是区块链发展的必然；

2. 个体化支持不足：区块链最主要的功能是处理交易数据，区块链以数字资产交易和管理为核心，抽象了通用的用户模型，对于用户个体化支持还很不够。

3. **模块化不足：**虽然区块链（公链）都采用了开源的策略，但是因为区块链模块化不足和开发文档缺乏，基于区块链的开发和应用还是具有一定的门槛，限制了区块链生态的快速成长。

4. **智能硬件的支持：**智能硬件是越来越重要的区块链参与者，对智能硬件普遍支持不足；

总之，区块链作为一种创新型、颠覆性未来社会经济运行模式的基础设施，还处在其非常的早期阶段，还处在不断的发展完善中，还有很多的问题需要解决。

1.3AOS 团队共识

除了以太坊、EOS 等区块链明星项目，国内外还有其他大量的区块链项目正在开发或者已经运行，我们为什么还要做 AOS 区块链项目？

对于 AOS 项目，团队目前在区块链的技术发展及价值共识，我们认为有必要告知每一位读者。

1. 区块链技术还处在非常的早期

到目前为止，区块链技术还处在非常早期阶段，与区块链创新性、颠覆性社会经济运行模式相比，区块链技术还远远没有达到要求。区块链技术还处在早期不断的探索和积累阶段。

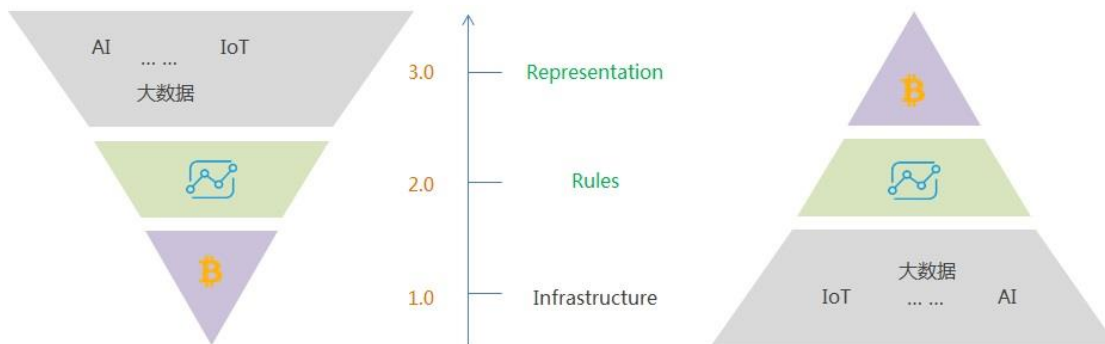


图 2 区块链发展与运行

如图 1 所示，区块链技术发展起于数字货币独立发行和价值传输（BTC），在数字货币之上，通过智能合约实现价值转移规则（ETH），然后是 dApp 完成应用落地。目前所谓的 dApp 应用落地，相当于工业时代的手工作坊，与人工智能、IoT、大数据技术现状和基础还远远没有实现对接和适配。只有与人工智能、IoT、大数据等相适配，构成完整的区块链应用协议栈，才能够做到真正的实际应用落

地。因此，虽然目前已经有很多的区块链项目，但基本都还处在起步和探索阶段，还有非常大的发展空间，这是 AOS 项目的技术共识。

2. 区块链价值网络与互联网信息网络的的模式不同

互联网注重可复制性，通过快速复制，能够进行很快的垄断。因此，在互联网领域，我们将只有头部能够生存。而我们认为区块链的不同恰恰在于，价值不能复制。从比特币到目前为止，区块链所有的努力的核心在于保证价值的唯一性和不可复制性。区块链是通过“参与者”的贡献性行为，创造出具有锚定、唯一的价值，这个价值以 Token 的形式存在于区块链网络上，既不能凭空产生，也不能凭空消失。因此，在区块链网络中，规模不是问题，只要创造一个有“参与者”有兴趣参与的区块链社区，价值就能够完成自我激励、自我生长。这是 AOS 对于区块链的价值共识，愿意通过 AOS 项目的开发和建设，提供一个区块链应用的基础平台，创造一个真正的区块链价值生态。

AOS 创始团队基于以上对区块链技术和价值的共识，在研发 AOS 区块链时，综合考虑当前区块链存在的问题，在以下两个方面进行了较大的改进，同时也成为 AOS 的亮点：

1. 区块链的可扩展性

AOS 作为一个区块链应用开发平台或者基础设施，其目标是在 AOS 之上开发丰富的 dApp，从而形成一个丰富的价值生态。因此，可扩展性是 AOS 必须首先要考虑的问题。AOS 采用分片的技术保证其可扩展性，AOS 分片技术的独特性在于，主链与应用链通过区块头相互关联，既保证了应用链的独立性，又保证了应用链可以共享全网的安全性。

2. 区块链可应用性

作为一个支持各领域应用落地的公共区块链基础开发平台，就不能只是提供简单的支持代币发行、转账、智能合约等简单的金融性功能，尤其是在当前 IoT、人工智能、大数据等已经成为社会经济和社会生活的技术基础，如何在区块链上提供与之相适配的基础通过功能支持，是面向应用开发的公共区块链项目成功的关键。AOS 另一个鲜明的特征，是充分考虑到 IoT、人工智能、大数据等应用技术基础，在 AOS 中采用了开放的应用协议栈架构，并采用完全模块化实现机制，为 AOS 之上开发丰富的 dApp 打下了坚实的基础。

2、AOS 的价值与愿景

2.1 AOS 价值

AOS (Application Operation System)，聚焦区块链新型经济体的创新价值，以区块链实际应用落地为目标，实现区块链应用的快速构建，提供一个安全、高效、易用的区块链公共操作平台。

AOS 价值体现在：

- **高 TPS 支持：**通过主链与应用链的架构，根据应用交易类型的灵活共识机制定制化配置等技术创新，AOS 目标达到全网百万级 TPS 处理能力；
- **个性化支持：**平台提供个人数字资产之外的基础支持，如个人大数据的支持，在平台上以私有链的形式，为个人提供区块链级别的个人数据资产保护和服务；
- **完整的应用协议栈：**通过对大数据、智能硬件的抽象与定义，实现与区块链的无缝对接，实现完整的区块链应用协议栈；
- **高度模块化：**P2P 网络、共识机制、账户和钱包等区块链核心功能采用独立的模块化，并且构建模块库，能够进行灵活的选择和配置。除此之外，AOS 引入了开放算法库 (Open Algorithm Library) 和开放协议栈 (Open Protocol Stack)，按照标准，不同的组织和个人，都可以提交相应的开发产品，以方便不同应用和数据等处理选择；
- **积木式应用搭建：**通过模块化，平台提供不同的应用模板，用户可以通过模板选择和参数设置，实现积木式应用搭建，大大加快了应用生态的建设；
- **活跃的开发社区：**平台在算法级别提供基础支持和标准，促进各类应用技术人员参与和交易，建设活跃的开发社区和开发者生态；

2.2 AOS 愿景

AOS 秉承区块链公开、公信、公正的核心精神，通过不断的技术迭代和社区建设，打造一条安全、高效、易用的区块链应用操作平台，以 AOS 平台为基础，

吸引各领域应用 Dapp 的入住，让 AOS 成长为一个丰富的价值生态平台，促进社会的进步和发展。

3、AOS 技术架构

3.1 主链与应用链

AOS 致力于区块链应用基础平台的建设，在 AOS 之上，将有各种各样丰富的应用，不同的应用具有不同的交易类型和需求级别，如果按照统一的区块链全网处理，既造成区块链的快速膨胀，又使得区块链的效率低下。

AOS 区块链采用主链、应用链的双层结构，通过对统一的矿池分片 (Sharding) 技术，不同的应用按照需要进行灵活的节点配置，构造应用区块链网络。主链提供统一账户、资产发行、应用管理、SPV 确认、跨链操作等功能，应用链实现具体的应用功能。采用主链、应用链的双层区块链架构，达到功能的合理治理，避免了主链的快速膨胀，提高了区块链整体处理效率，满足了实际应用需求。

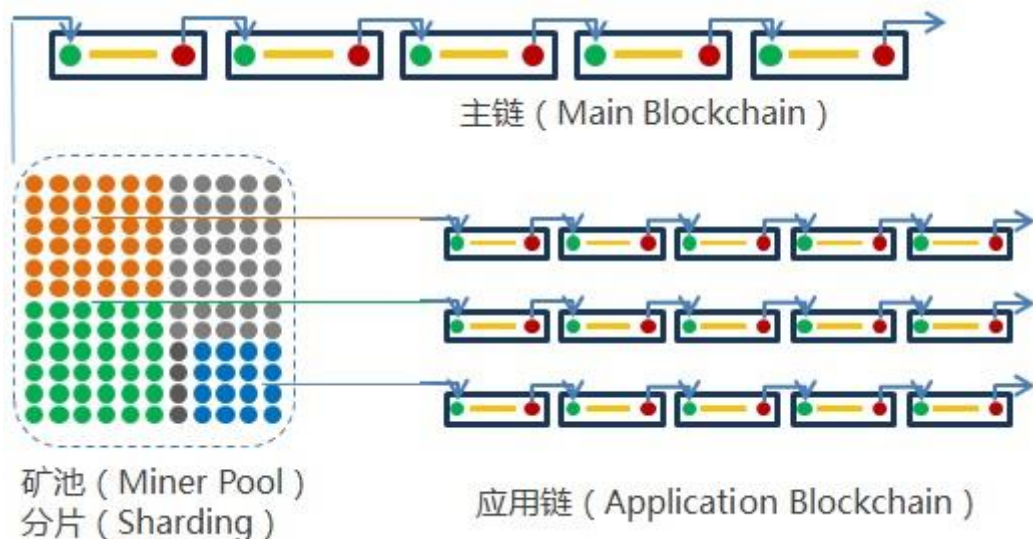


图 3 AOS 区块链两层架构

应用链与主链的关系是既独立又联系，共享区块链基础的矿池和协议栈，又做到合理的功能自治，构建和谐、平衡、共享的价值生态。

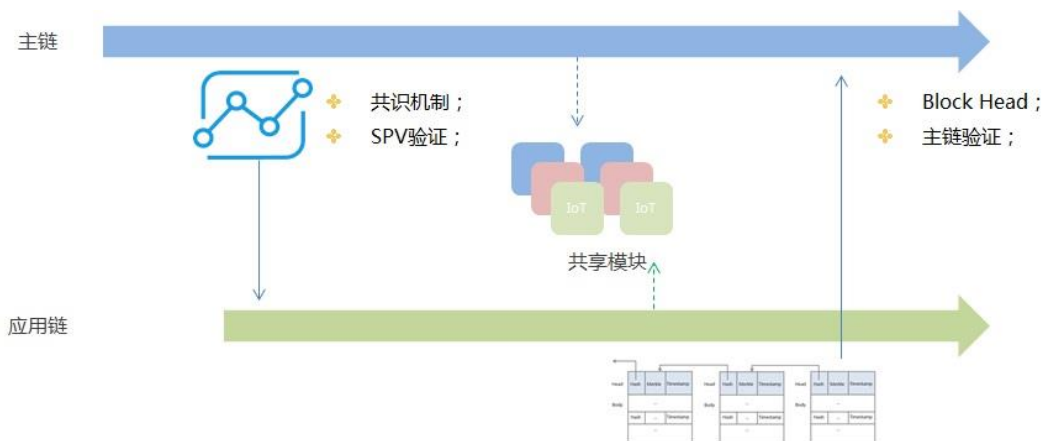


图 4 应用链与主链关系

AOS 应用链：

1) 创建应用链智能合约：在 AOS 主链上创建一个应用链智能合约，根据应用链的实际应用场景和目标，选择应用链使用的共识机制，AOS 会提供 POW、POS、DPOS、PBFT 等多种共识机制供应用链选择；选择应用链是否需要主链验证，可以通过选择主链验证，增加应用链的安全性和用户体验；

2) 主链验证：应用链将数据块 Head 提交到主链，主链进行全网验证和存储，应用链能够实现在主网 SPV 验证。AOS 实现区块链的双层架构和双层验证，保持了应用链的灵活、效率，继承了主链的安全。

AOS 通过区块链双层架构，实现区块链的横向扩展，通过双层的数据验证，保证了区块链去中心化的安全性。这种合理的架构设计和服务治理，是 AOS 实现高 TPS 的基础，AOS 最终的目标是实现 100 万+全网 TPS 的处理能力，真正达到区块链价值生态的技术基础设施目标。

3.2 大数据私有链

区块链是互联网技术的升级，随着区块链逐渐向社会的基础设施演变，区块链已经远远超出了价值表示和价值传输的金融领域，向更广泛的应用领域发展。数据真实可信、不可篡改、可追溯是区块链的基本特性，大数据是现在应用的最重要特征，而目前的区块链公链，都还没有很好的将二者相结合。

针对这一区块链需求，AOS 为用户提供私有链支持。当用户有大数据存储的需求时，用户创建一个智能合约，选择定制的配置参数，就可以定制一条属于自己的私有链。用户通过密钥，完全控制数据的访问权限，使得用户拥有数据的完

全产权。

AOS 的私有链主要是针对用户的大数据应用场景和对用户数据资产提供保护。AOS 秉承比特币的精神，不重复发明轮子，通过技术场景和架构创新为用户提供最实用的区块链基础设施。AOS 的私链主要满足于大数据的应用需求和应用场景，因此，AOS 对 IPFS 进行了 fork，重新封装了接口，实现与 AOS 对接。在 fork 的 IPFS 中不再实用 Filecoin 作为价值表示和激励，而是统一实用 AOS 作为存储节点的激励。

在 AOS 中存在两类矿工，一类是进行记账的矿工，一类是完成数据存储的矿工，按照数据存储量进行激励。想通过数据存储挖矿的矿工，需要在 AOS 上注册账号，启动数据存储节点后，并绑定账号。

AOS 的参与者，不只是独立的个人，会有企业和组织，对于比较大的企业的企业用户，可能会有非常巨大的数据存储和后续的数据分析处理需求。在这种场景下，数据通过分布式的区块链存储是不合适的。或者，用户要求数据必须存储在自己的云平台上，还要能够共享区块链所保证的数据价值。随着区块链的发展，针对 AOS 将要面临的这些需求，AOS 对大数据操作进行了抽象和定义，封装了大数据操作通用接口和功能，为用户的大数据需求提供了灵活的选择。

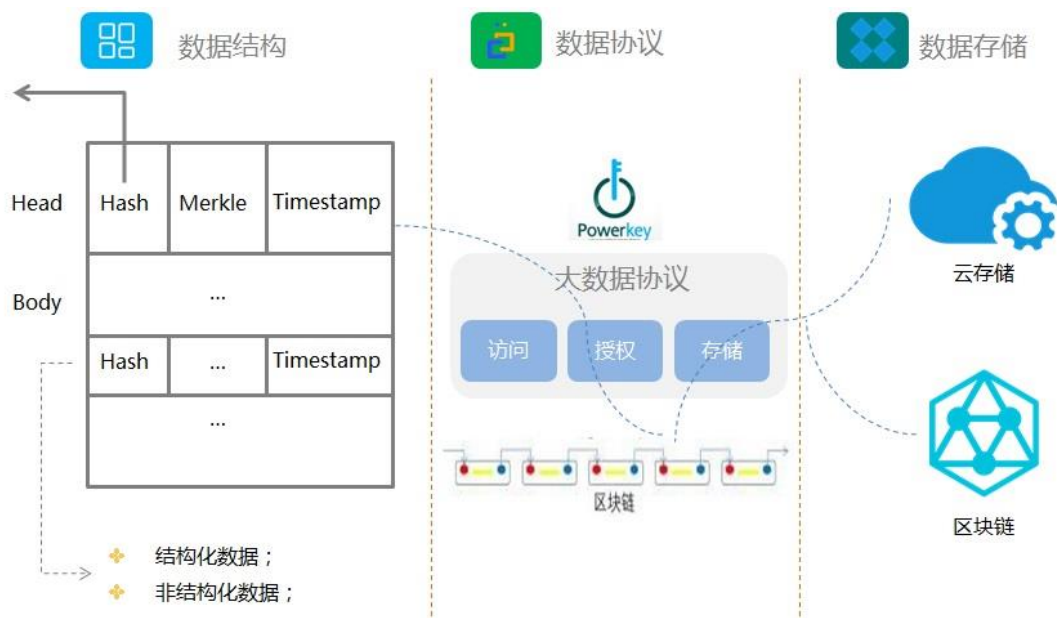


图 5 AOS 大数据协议栈

在 AOS 中，大数据处理设计为三个阶段：

1) 数据结构：采用二级数据存储结构，大数据的数据类型和数据大小差别

- 很大，包括结构化数据，又包括图像、视频等非结构化数据。首先采用区块链数据块的结构，对所有的数据进行抽象，对数据进行统一的定义，任何数据定义为一个资源引用条目，打包成数据块，并做 Hash。具体的原始数据通过引用来检索，原始数据可以根据需要进行加密或者不加密；
- 2) 数据协议：AOS 定义数据的访问控制、授权、存储等标准操作和接口，构成大数据操作协议栈，实现区块链对大数据的标准操作；
 - 3) 数据存储：根据场景的实际需要，数据存储云平台或者区块链上，存储在 AOS 区块链上的数据，需要支付存储矿工的费用；

3.3 应用协议栈

区块链是构建在互联网信息网络之上的价值网络，随着人工智能、IoT 技术的发展，则产生价值或创造价值的将不仅仅是人或者以人为主的企业等组织，也就是说，未来将会有越来越多的代替人的智能硬件参与到区块链这个价值网络中来。还有人工智能（AI），上节提到的大数据等也越来越成为社会价值创造和价值网络中必须的基础功能。这些基础功能与区块链相融合，才能够真正的为社会提供一个“信任的机器”，实现区块链金融领域之外的落地。

AOS 的一个突出特征提供了一个完整的区块链应用协议定义和实现规范，从而为区块链的应用落地和价值生态生成打下了坚实的基础。



图 6 应用协议栈

AOS 中，应用协议栈与普通软件架构中功能模块不同之处在于，每一个应用协议都由定义、实现、接口三个部分组成，构成一个实体，由一个智能合约来表示。AOS 中应用协议栈采用开放的策略，充分发挥社区开发者的力量，以创造繁荣的 AOS 应用协议簇，发开着还可以通过开发特定的应用协议，供其他用户使用，并且可以获得一定的收益。

以一个人工智能的算法模块实现为例说明：

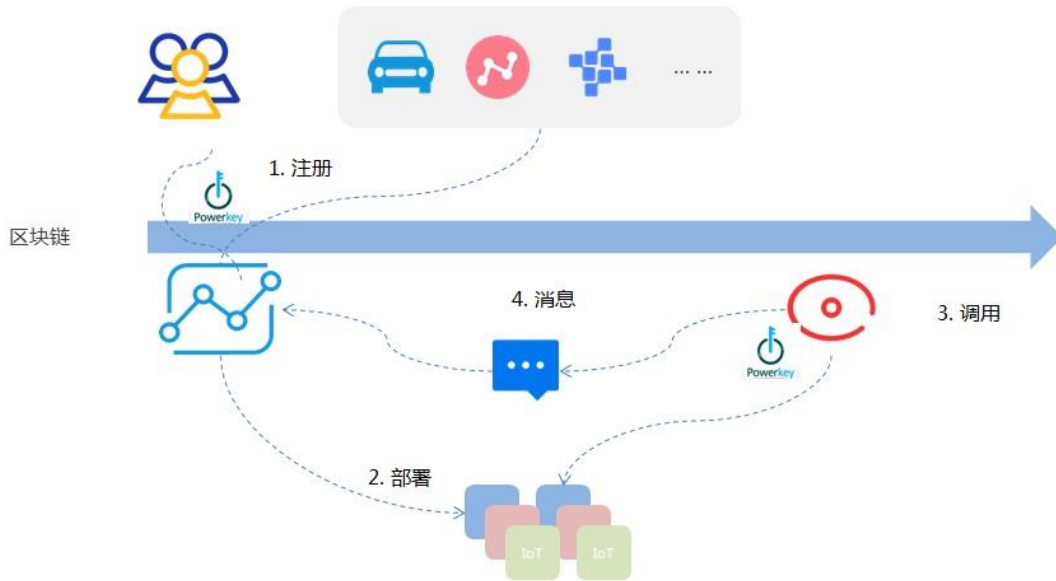


图 7 应用协议实现

通过在 AOS 上创建一个智能合约，注册一个人工智能的算法模块，并定义使用规则。将模块在 AOS 中进行部署，其他用户通过智能合约来调用，结果通过消息触发模块隶属的智能合约，如费用支付等。

3.4 模块化

在 AOS 中，模块化有两种特别的意思。一个是技术实现上的功能独立，可根据实际场景需要的配置化装配的软件组件包，主要应用在区块链核心协议层；一个是上节说明的区块链开发和使用策略，主要应用在教育层。

1) 区块链核心协议栈，区块链的 P2P 网络、共识机制、加密算法等核心协议栈，在 AOS 中采用统一标准接口，多模块实现的策略，用户可以根据不同的实际场景来灵活配置。这一策略在 AOS 中是贯穿始终的，这与 AOS 的两层区块链架构及便于横向扩展的目标是一致的。

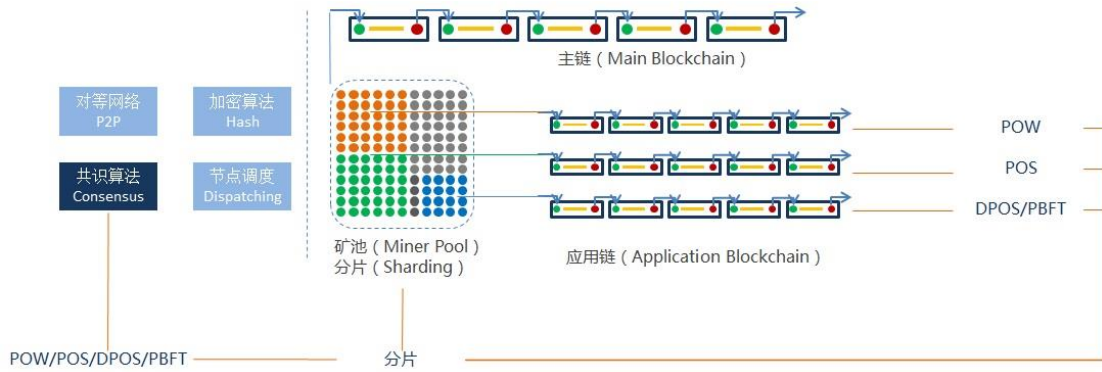


图 8 AOS 的模块化

在图 8 中，以 AOS 共识算法为例来做一个说明。AOS 采用了统一的矿池，分片的技术的技术，这与一主链、多应用链的结构相一致。AOS 是一个面向公众的公共平台，在 AOS 上的不同应用链具有非常大的差异，其在规模、价值、使用频度、应用领域等等很多方面都存在巨大的不同。因此，不同的应用链采用不同的共识算法具有不同的性价比，这就需要为不同的应用链、不同的场景能够提供不同的共识算法模块支持。AOS 的区块链建构设计和应用目标决定了 AOS 必须采用一个更加模块化并且是同一协议、多种模块实现的平台策略。

2) 应用层协议栈，AOS 未来所需支持区块链应用的丰富性，决定其必须具有良好的可扩展性，在这一点上，仅靠创始团队远远不能够完成这个任务，则必然需要更多的开发者加入到 AOS 生态系统的开发中来。因此，AOS 在应用协议层采用了上节描述的架构和策略。

AOS 从架构到实现，都采用了高度模块化的策略，并与区块链的激励机制相结合，使得 AOS 区块链价值生态的建设更加容易，这是 AOS 最大的一个特点和亮点。

3.5 技术实现路径

AOS 认同区块链协作式、创新型经济运行模式理念，以构建区块链价值生态为最终目标，遵循不重复发明轮子的开发策略，为公众以最快速度提供一个高效、安全、易用的区块链应用开发平台。

因此，AOS 的区块链核心协议栈功能的具体实现遵循以下路径，在相应的项目中，这些技术都有相应的详细描述，在此不再展开阐述，只做一个简略的说明。

- 1) 具体实现语言:Go 以良好的并发性能和网络支持被很多项目所采用, AOS 区块链核心协议部分, 以 Go 语言为主;
- 2) 区块链区块: 支持比特币 UTXO 和账户余额两种区块链数据结构;
- 3) 虚拟机: AOS 虚拟机 (AVM: AOS Virtual Machine) 采用与以太坊 (Ethereum) 兼容的虚拟机技术, 以太坊虚拟机是现在最常用的执行引擎, 这将能够使得目前大量的构建在以太坊 EVM 上的 Dapp 直接转移部署在 AOS 上, 便于 AOS 生态快速发展;
- 4) 智能合约: AOS 采用以太坊智能合约技术, 基于智能合约, 在 AOS 上开发各种分布式应用;
- 5) 开放应用协议: 应用层协议进行开发策略, 吸引更多的开发者加入 AOS 价值生态建设;

AOS 最终将实现一个高度模块化, 应用开发者通过选择配置, 可“一键”创建自己区块链分布式应用 (dApp) 的公共开发平台。

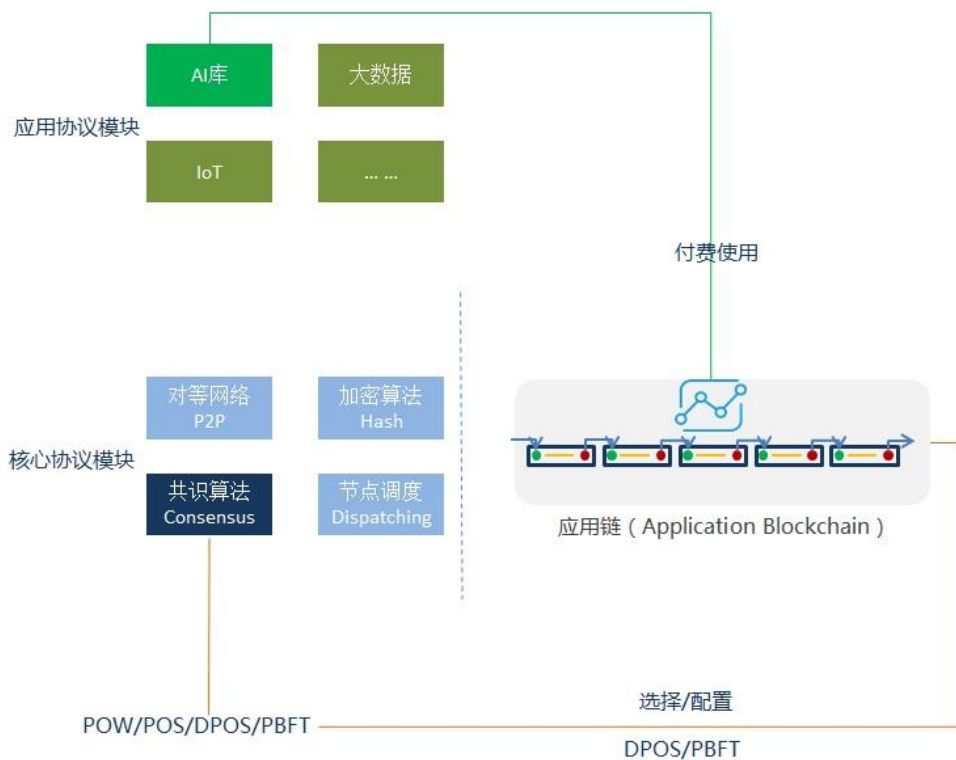


图 9 AOS 模块使用

在 AOS 中, 核心协议模块通过选择、配置, 构建用户基础区块链, 应用协议层模块通过付费使用, 构建繁荣、活跃的开发社区。

3.6 创新和核心技术

AOS 项目立足于区块链应用场景实际落地场景需求，与目前其他区块链项目相比较，在以下三个方面具有创新，构成项目的核心技术。

1. 大数据处理

在目前所有的区块链项目中，对于大数据的处理，采用了分离的方式，比如采用 IPFS 实现大数据的处理。AOS 采用了一体化处理方式，对于领域应用开发具有巨大的优势，便于区块链生态建设。

2. 应用协议栈

在前面章节已经做了阐述，区块链的本质和价值在于构建协作、自治、自动的生态系统，而目前的区块链系统，缺乏在 IoT、AI 等 IT 基础领域方面的支持，每个基于区块链的应用开发，都需要从底层做起，门槛极高，极大阻碍了区块链应用开发。AOS 在 IoT、AI 等基础应用以协议栈的方式进行了标准化和规范化，实现区块链和互联网的真正互相赋能和融合。

3. 分片技术

很多区块链都采用了分片的技术，以提高区块链 TPS 处理能力。AOS 采用了具有自己项目特色的动态分片技术，在 AOS 中对所有的节点建立了动态的性能评价体系，和独特的动态分配和调度算法，既实现了高 TPS 和节点算力复用，又能够提升节点矿工的挖矿奖励。

3.7 整体技术方案

通过对 AOS 技术特点和技术实现的描述，AOS 采用的是一个分层、高度模块化的区块链公链基础平台项目。

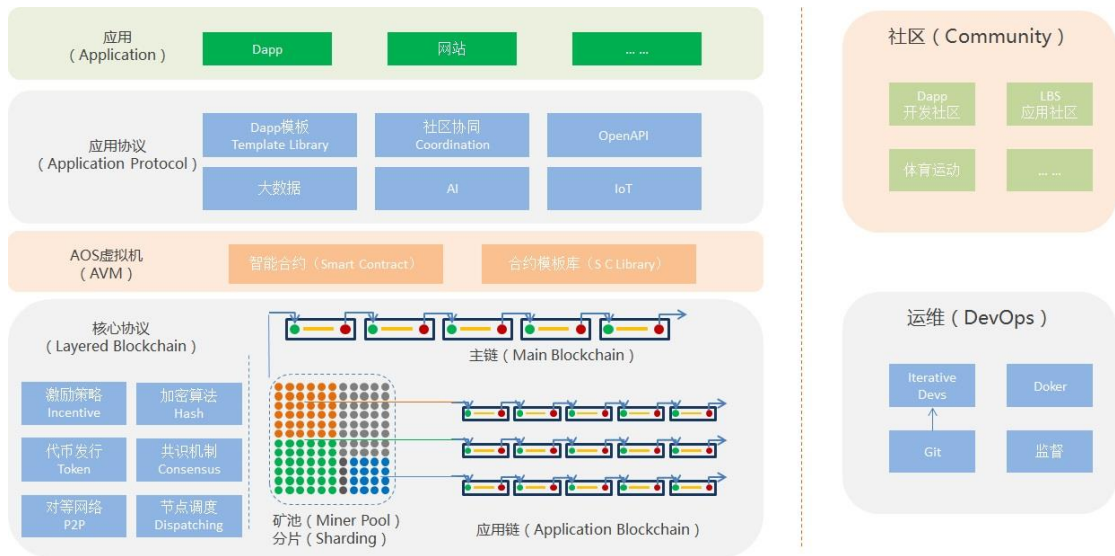


图 10 AOS 总体技术架构

AOS 项目将采用开源策略，所有的源代码和开发文档将在适当的时候，逐渐在 Github 上公布，以供区块链开发者使用。建立开发者社区，开发者可以参与平台的开发和应用的开发，并在 AOS 价值生态建设中获得收益。

4、AOS 生态及运行机制

4.1 AOS 生态

AOS 是一个区块链应用基础开发平台，开发者、投资人、应用用户等参与者，通过 AOS 区块链信用体系和激励机制，将构建一个能够自我生产和自我发展的丰富价值生态。

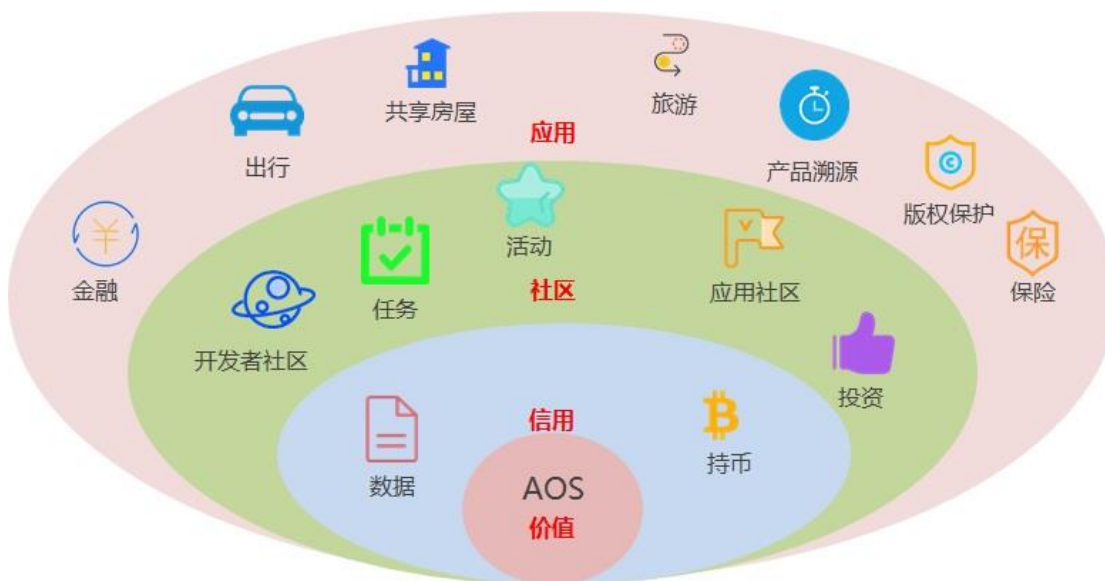


图 11 AOS 生态系统

1) 分层的生态系统

AOS 是一个分层的生态系统，AOS 通过发行 Token 实现了价值表示和价值传输和转移，用户的数据（行为），持币（价值认同）两个维度可以建立起用户信用体系，以价值和信用构成了 AOS 生态的核心层。开发者、投资人等构成了 AOS 社区，社区通过各种活动和任务为 AOS 提供了发展动力。最后是 AOS 的应用层，AOS 区块链应用于金融、保险、出行、共享房租、旅游、产品溯源、版权保护等等各种实际的应用，为用户提供区块链的技术解决方案和支持，应用的繁荣是 AOS 的终极目标，同时反过来也是 AOS 价值成长的基础。

2) 自我生长的生态系统

AOS 的分层生态系统，各层之间不是孤立、单向的关系，而是一个互相依赖、互相促进的双向流动、动态生长的系统。数据是信用的基础，而数据产生于社区活动和实际应用，因此应用越丰富，数据越丰富，信用体系越可靠；反过来亦然，可靠的信用和 Token 价值增长，促进开发者等社区的活跃，则会开发越来越多的应用。AOS 终极目标不是在于 Token 的价格升降，而是应用的实际落地。因此，AOS 的“价值 \leftrightarrow 信用 \leftrightarrow 社区 \leftrightarrow 应用”双向对流的区块链生态系统是一个自生长、自发展的生态系统。

4.2 激励机制

激励机制是区块链项目能够快速发展的核心，AOS 作为一个公链项目，用户

为保证项目安全、正常运行、数据存储等行为统称为“挖矿”，用户会因为参与“挖矿”而获得 Token 的奖励。

- **算力：**AOS 采用了混合的共识机制，用户可以通过贡献算力参与到 AOS 项目中，用户提供的算力保证了 AOS 的安全性和区块链的正常运行，会按照相应的算力得到 Token 奖励；
- **存储：**AOS 扩展了大数据应用，用户可以通过贡献数据存储空间参与到 AOS 项目中，按照用户共享的数据存储量的大小获得 Token 奖励；
- **智力：**AOS 是一个开放的体系，用户可以通过参与项目发布的开发任务，或者按照应用协议规范，开发和发布特定应用领域（比如人工智能、大数据、IoT 等）模块，获得用户使用支付的费用；
- **应用：**用户可以参与到某个具体应用项目中，按照具体应用项目制定的激励策略获得相应奖励；
- **投资：**随着 AOS 生态系统的不断发展，AOS Token 的需求必然增加，在发行量固定的情况下，Token 的价值和价格都会自然增长，用户可以在先期投资 AOS Token 参与到项目中，并将获得项目成长的回报；

以上是用户在 AOS 中能够得到奖励的主要方式，AOS 鼓励用户积极参与到 AOS 社区和价值生态的建设中，用户的贡献会给予相应的奖励。AOS 具体的设计了以下独特的任务激励和信用激励双重的用户激励模型：



图 12 AOS 激励模型

1. **任务激励：**用户通过贡献节点算力、存储等资源参与挖矿的奖励，或者参与社区开发、完成一个特定任务等得到的回报。任务激励是按照任务的类别和性质，比如按照每个区块、数据存储量等，给予用户固定的 Token 奖励。需要注意的是，在 AOS 中，对于任务型激励，比如区块打包这样的矿工节点，会针

对节点性能和完成任务的结果（漏块等）设计奖惩策略，对于不满足系统要求的矿工节点，会给予一定时间停止竞争任务的惩罚。

2. 信用激励：信用奖励是 AOS 所特有的设计，是为了提升用户的活跃度和粘性，为了用户能够真正的分享 AOS 长期成长价值所涉及的经济激励模型。在 AOS 中，用户所有的行为通过一个三元组来定义， $\langle \text{Behavior}, \text{Time}, \text{Value} \rangle$ ，Behavior 代表用户行为类型，Time 是时间戳，Value 代表以 Token 表示的行为价值。则用户所有的行为，会构造成一个行为矩阵：

$$\begin{bmatrix} B_{11} & B_{12} & B_{13} & B_{14} & B_{1\dots} \\ B_{21} & B_{22} & B_{23} & B_{24} & B_{2\dots} \\ B_{31} & B_{32} & B_{33} & B_{34} & B_{3\dots} \\ B_{\dots} & \dots & \dots & \dots & B_{\dots} \end{bmatrix}$$

图 13 用户行为矩阵

在 AOS 中，用户完成任务、社区活动、在线时长、持有 Token 数量及时间（币天）等行为对 AOS 的社区和生态建设都具有一定的贡献，AOS 不是直接对每个行为进行直接奖励，而是采用将用户行为折算为挖矿的“算力”（MF: Mining Force），按照用户算力大小，每天给予一定的奖励。

$$MF = \sum F(\lambda_i x_j) \quad (1)$$

$$F(x; \lambda) = \begin{cases} 1 - e^{-\lambda x} & x \geq 0, \\ 0 & x < 0 \end{cases} \quad (2)$$

图 14 挖矿算力计算公式

从公式（1）可以看出，用户的算力是可以累积的，用户算力具有累积效应，这种历史积累效应同时也构成用户在平台或社区中的信用，信用越高回报越多。公式（2）每项贡献算力计算的约束公式，即每项贡献算力有一个上限值，以促进用户行为的丰富性和避免用户“刷单”。

AOS 按照奖励策略，每天会拿出固定数量（C）的 Token 给予用户奖励，用户通过算力竞争，来参与奖励的分配。这种信用挖矿奖励（MR: Mining Reward）

按如下公式计算：

$$MR_i = C \frac{\sum F_i}{\sum \sum F} \quad (3)$$

图 15 用户信用挖矿奖励计算公式

AOS 这种独特的双重的激励模型设计，既保证了节点矿工、数据存储等固定收益，又能够覆盖更丰富的用户贡献行为，大大促进了社区繁荣和价值生态的建设。

4.3 运行机制

AOS 是一个面向公众的公链平台，一切采用公开、透明的策略，一切以社区共识为核心，以激励策略为基础，以 Token 的价值手段，实现 AOS 的自我发展和稳定运行。

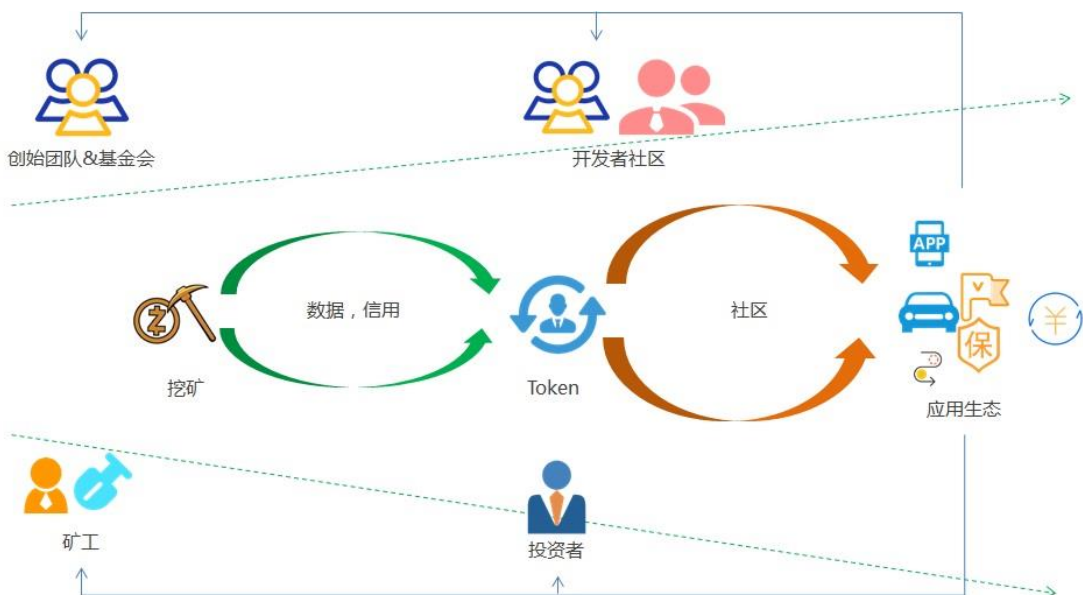


图 16 AOS 运行机制

5、开发路线图

2018 年

2018 年 1 月 AOS 项目正式启动

| | |
|------------|--------------------------------------|
| 2018 年 6 月 | AOS 0.1 测试版上线 |
| 2018 年 Q3 | AOS 0.1 正式版上线 |
| 2018 年 Q4 | AOS 0.2 完善智能钱包，部分程序开源 一个应用区块链项目上线 |

2019 年

| | |
|-----------|------------------------------------|
| 2019 年 Q1 | AOS 0.3 虚拟机技术迭代 |
| 2019 年 Q2 | AOS 0.4 智能合约迭代 2 个应用区块链项目上线 |
| 2019 年 Q3 | AOS 0.5 应用层协议开发 |
| 2019 年 Q4 | 马拉松编程大赛 建设开发者社区 5 个应用区块链项目上线 |

2020 年

| | |
|-----------|---|
| 2020 年 Q1 | AOS 1.0 AOS 虚拟机、智能合约迭代 应用协议栈迭代 10 个应用区块链项目上线 |
| 2020 年 Q2 | 两周年大型社区活动，AOS 开发者、创业大赛 |
| 2020 年 Q3 | 20 个应用区块链项目上线 |
| 2020 年 Q4 | AOS 2.0 |

6、Token 分配

6.1 代币发行量

AOS 代币发行总量：1 亿个，代币名称：AOS

6.2 代币分配计划



图 17 代币分配计划

7、团队介绍

- 叶帆，创始人

资深 IT 从业者，2009 年介入区块链，行业先驱者，拥有 BAT 背景及相关渠道，拥有 10 年以上互联网技术研发和运营推广实战经验。

- 李铭，CEO，合伙人

区块链爱好者，资深 IT 从业者，10 年网络营销推广和网站运营经验，多次创业经验。

- 史银龙，CTO，合伙人

人工智能方向博士，20 年技术研发经历，中科院、BAT 工作经历和多次创业经历，2011 年开始区块链相关技术研究，笃定“IoT+区块链+AI”必然是未来协作、自治、自动的社会经济发展和运行模式。

8、风险说明

8.1 免责声明

本文档仅作为信息传达和情况说明之用，文档内容仅作参考不构成在 AOS 及相关公司中出售股票或证券的任何买卖建议、教唆或邀约。本文档不组成也不理解为提供任何买卖行为，也不是任何形式上的合约或者承诺。

鉴于不可预知的情况，本白皮书列出的目标可能发生变化。文档的部分内容可能随着项目的进展在新版白皮书中进行相应调整，团队将通过在网站上发布公告或新版白皮书等方式，将更新内容公布于众。

AOS 明确表示不承担参与者造成的直接或间接的损失包括：

- 1、 依赖本文档的内容；
- 2、 本文信息错误，疏忽或者不准确信息；
- 3、 由本文导致的任何行为。

团队将努力实现文档中所提及的目标，但基于不可抗力的存在，团队不能完全做出完成承诺。AOS 发行的 Token 是在 AOS 平台发生效能的工具，并不是一种投资品。AOS 并不授予任何个人参与、控制、或任何关于 AOS 的决策的权力。

8.2 竞争风险

当前区块链项目众多，竞争十分激烈，存在较强的市场竞争和项目运营压力。AOS 项目是否能在众多的区块链项目中受到广泛的认可，既与团队能力、愿景规划等方面挂钩，也受到市场竞争的影响，其间存在恶性竞争的可能。

8.3 人才流失风险

AOS 汇聚了一支活力与实力兼备的人才队伍，吸引到了区块链领域的资深从业者，具有丰富经验的技术开发人员等。在今后的发展中，不排除有核心人员离开、团队内部发生冲突而导致 AOS 整体受到负面影响的可能性。

8.4 项目技术风险

密码学的加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 AOS 项目，这可能导致 AOS Token 丢失。项目更新过程中，可能会出现漏洞，漏洞发现后会及时修复，但不能保证不造成任何影响。

8.5 项目缺少关注度风险

AOS 项目存在没有被大量个人或组织使用的可能性，这意味着公众没有足够

的兴趣去开发和发展这些相关分布式应用，这样一种缺少兴趣的现象可能对 AOS 造成负面影响。

8.6 黑客攻击风险

AOS 有受到黑客或其他组织供攻击风险，包括但不限于 DDOS 攻击、女巫攻击、恶意软件攻击或一致性攻击等。

8.7 密钥丢失风险

AOS 是基于区块链技术，完全匿名的应用，用户丢失密钥后，将会永远失去平台上的虚拟资产的所有权。这种情况下，平台和其他任何个人和组织将不会不会为你的损失担保。

8.8 目前未可知的其他风险

除了本白皮书内提及的风险外，此外还存在着一些创始团队尚未提及或尚未预料到的风险。此外，其他风险也有可能突然出现，或者以多种已经提及的风险的组合的方式出现。请参与者在做出参与决策之前，充分了解团队背景，知晓项目整体框架与思路，理性参与。