白皮书

2019年4月

通过分层分片的群链架构
提升智能合约的执行性能

MOAC基金会
新加坡
www.moacfoundation.org

MOAC 平台:

通过分层分片的群链架构提升智能合约的执行性能

MOAC 基金会

2019 年 4 月 1 日

第三版

摘要

MOAC 基金会（下简称 MOAC 或墨客）发布了新一代区块链平台。凭借开创性的群链分层技术架构，MOAC 不仅致力于解决现有区块链系统（包括比特币和以太坊）在性能和成本方面的问题，还通过引入新功能，最大限度地降低了开发人员、用户、企业以及整个区块链生态系统的进入门槛和使用成本。MOAC 平台使用分层的群链架构，运用分片、跨链以及通过子链方式执行智能合约等技术来实现这一目标。

MOAC 平台的基础架构是由一条称为“母链”的主链和众多子链组成的群链组合。使用分片技术，每条子链在母链平台上以子区块链的模式运行，负责智能合约管理。每条子链还可以使用不同的共识算法实现大规模交易。（共识算法是一种提供区块链上去中心化交易认定和验证的系统算法）。

MOAC先进的分层分片的群链技术将区块链平台的交易处理速度在现有基础上提高了100倍。同时，子链可将通证（token）并发量提高10,000倍，从而使其成为真正具有可扩展性的商业解决方案。

子链能显著降低智能合约的操作成本，支持开发人员快速测试不同的应用程序和服务创意。MOAC 的子链能够使用跨链技术与所有其他非 MOAC 的区块链底层技术实现互连。用户及其去中心化应用程序（DApp）能轻松迁移到 MOAC 平台，而无需掌握更多的区块链技术细节。子链还提供了一种去中心化的文件存储解决方案，这在目前主流区块链中尚属首例。

MOAC 鼓励挖矿并对整个生态系统进行奖励。其母链采用成熟的工作量证明 Proof-of-Work（PoW）共识机制，与以太坊类似，矿工和矿池有机会参与母链的挖矿。同时，MOAC 平台提供额外的子链挖矿和验证功能，并提供用智能手机等移动设备进行子链挖矿的机制。

通过降低移动用户和服务器领域的进入门槛，MOAC 平台为开发人员及其智能合约提供了真正可扩展的生态系统。对于开发人员而言，在 MOAC 平台创建的 DApp，在安全性有保障的前提下运营成本更低，平台功能更多并且性能更强。

目录

简介

区块链技术、加密货币和智能合约都有改变开发人员构建去中心化应用程序（DApp）方式的巨大潜力，并且已经在改变全球商业运作模式。

自 2008 年比特币问世以来，以加密货币身份亮相的区块链技术，已奠定其通过分布式账本技术提供数字化金融交易的身份，并且成为了一种非常有效的价值储存手段。不需要依靠中心化货币当局，比特币使用单一的去中心化共识模型就能验证交易并保障安全性。详情参阅 https://bitcoin.org/bitcoin.pdf 以阅读更多内容。

2015 年，以太坊等平台提出并且实现了在区块链平台上的智能合约，并进一步开创了 Decentralized Application（DApp）的概念。智能合约是一种计算机程序，在特定方或开发者定义的程序条件下，直接控制各方之间进行数字货币或有价资产的转移。详情可参阅 https://github.com/ethereum/wiki/wiki/White-Paper。

第二代区块链技术的“DApp”是一种去中心化的应用，不依赖中心服务器运行，但依赖类似 BitTorrent，Napster 和 Kazaa 的点对点（P2P）网络进行互连。P2P 网络要维持来自多个数据源的最佳数据传输。智能合约和 DApp 都使用区块链处理和存储数据，并提供额外的计算功能，与比特币这样的纯粹提供交易功能的第一代区块链技术已大为不同。

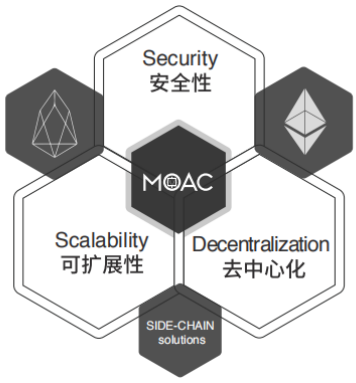
自比特币创建以来，区块链技术（即分布式平台和通证）已经得到长足发展，但在功能、性能、安全性和可扩展性方面尚需进一步加强才能真正获得用户接纳，从而最终使得区块链技术可以在广阔的商用领域满足真实商业需求。

本白皮书将描述一种开创性解决方案，将现有区块链最佳实践与新型可扩展群链技术相结合，从而显著推进智能合约性能。本白皮书所阐述的技术已不是停留在纸面上的纯理论探讨，而是已经在开发、测试并即将投入生产的真实落地技术。

问题说明

现有技术和区块链平台对于用户来说学习曲线非常陡峭，技术复杂的同时使用费用也很高昂——所有这些都会影响区块链技术的市场接受度以及可扩展性。现有平台交易处理速度很低，共识模型固定，并且无法快速适应开发人员不断增长的需求。迄今，区块链社区的挖矿高度集中，并且由于复杂性和硬件成本的问题，未能有效激励更多的新用户和感兴趣的消费者进入区块链领域。

这些区块链平台也彼此隔离，每个区块链平台上的通证和智能合约与其他区块链底层难以进行有效沟通。于是现有区块链市场根据不同的平台技术形成了各自封闭的圈子，其平台、技术、用户基础和行业也是彼此隔离的。



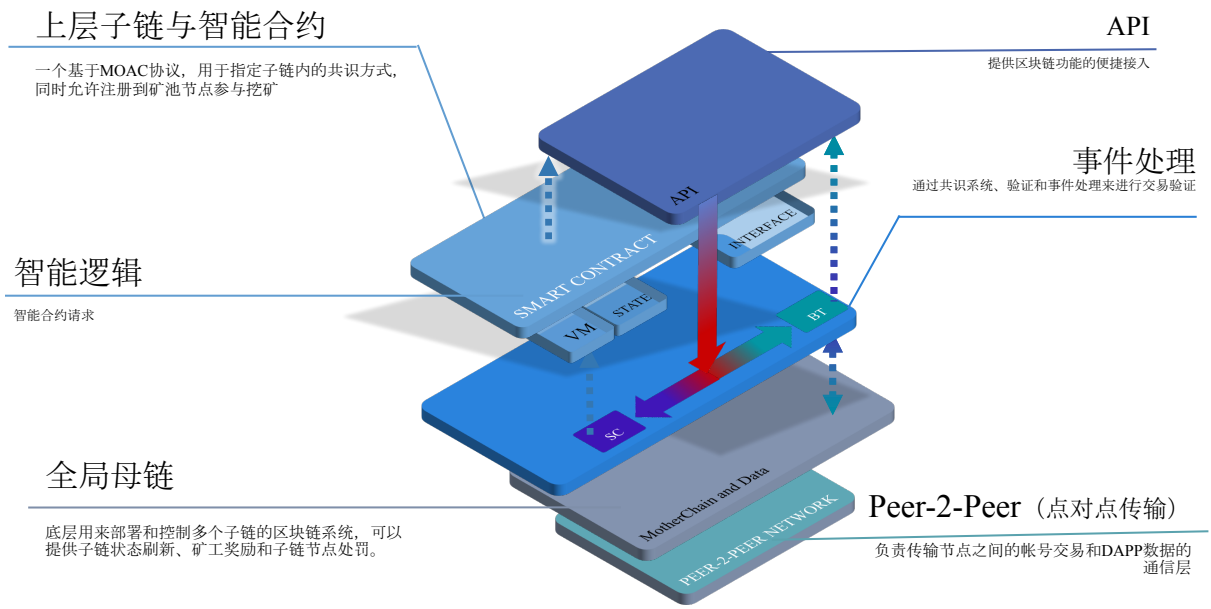
即使对于有经验的技术开发人员来说，构建新的区块链目前也极具挑战性。导致局面更加复杂的是大多数区块链底层技术很难升级；同时，不同底层技术使得整个区块链的用户被低效的分离到不同的区块链底层平台上。

群链技术解决方案:MOAC 平台

MOAC 基金会（MOAC）通过开发分层分片的群链技术解决了现有区块链平台的低效问题。MOAC 平台采用先进的分层架构，可降低 DApp 开发人员的成本，提供可扩展性并降低开发复杂度，同时使用分片技术提高交易速度和交易量。MOAC 在其平台内利用群链技术，包括母链（基于工作量证明的底层区块链）和子链（使用多种共识机制的上层区块链），来支持多种共识机制的智能合约。MOAC 平台还具有跨链功能， 不但支持 MOAC 平台上不同子链间的互联，也支持与其他区块链底层及其上的加密货币的互联互通。

MOAC 平台

通过将交易和智能合约分开，MOAC 先进的分层群链体系在整体交易处理速度上比以太坊提高了 100 倍。以下是 MOAC 体系架构概况，具体包括母链、事件处理系统、通过子链实现智能合约执行的技术、分片技术、跨链技术、安全性能和 API 等部分。



母链:采用工作量证明 PoW 的区块链

母链 - 不要与 MOAC 混淆 – 是一个跨系统的使用工作量证明为共识算法的区块链，可为智能合约和 DApp 解决数据存储和计算处理工作。

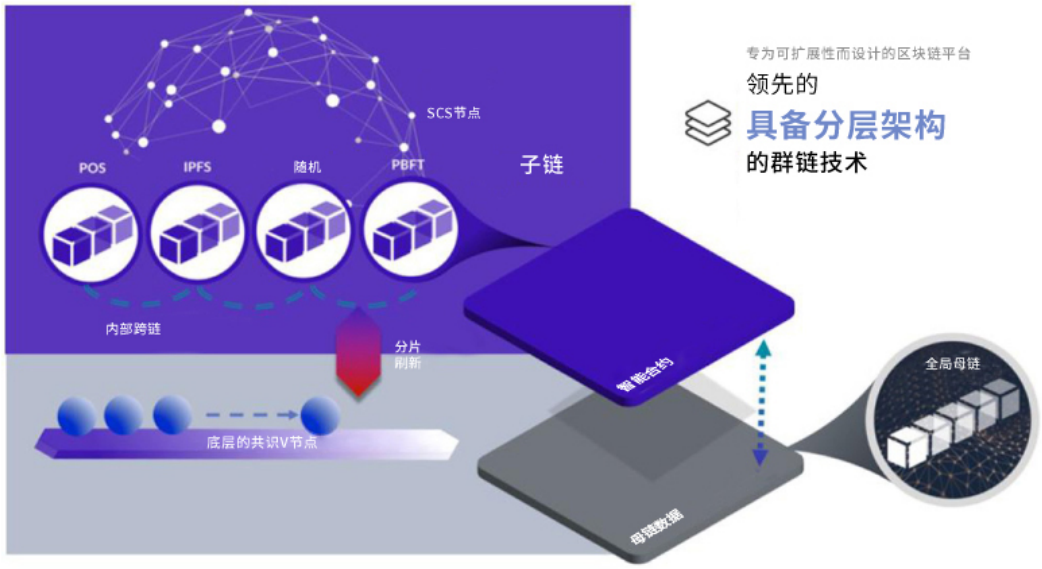
工作量证明 Proof-of-Work（PoW）算法是一种行之有效的措施，可以阻止并最终禁止第三方干扰，包括拒绝服务攻击，其他服务以及网络滥用（如垃圾邮件）。 PoW 要求服务请求者提供一些工作量证明，通常是在规定的处理时间内由计算机完成特定处理任务，从而消除错误的系统威胁。

在 MOAC 平台上，母链是处理交易和其他区块链操作、共识和数据访问的公共区块链层。MOAC 还支持使用子链来实现其他共识算法 。

通过子链形式实现的智能合约

MOAC 首先提出并实现了为每个智能合约提供定制子链的区块链解决方案，比现有智能合约执行的解决方案效率更高，且扩展性更强。

MOAC 平台使用子链来实现智能合约的业务逻辑，从而避免了在同一条链上同时处理常规的区块链任务（如交易的共识和记录）和与业务紧密相关的逻辑（通过智能合约方式实现）。通过为每个智能合约提供为其定制的子链，开发人员可以自由选择最适合其使用场景的共识算法，并确定分配给智能合约的节点数量，从而可以支持更多的使用场景。智能合约的所有状态都保存在本地子链中，且可根据需要将数据写入母链。



可定制共识算法的子链

子链架构于母链上层，每个子链都可以拥有自己独特的共识系统和算法。

例如，想要获得快速高并发的交易效果，您可以创建一个使用权益证明 Proof-of-Stake（PoS）共识模式的子链。PoS 是区块链网络旨在实现分布式共识的一种算法。

采取权益证明共识的区块链，依赖网络中的验证节点来检验交易，而不像严格的工作量证明(PoW)那样需要处理大量数据。在权益证明共识中，下一个区块的创建者是根据诸如持币量或币龄等因素（即股份）的随机算法来选择的。

权益证明系统的优点在于它可以完全扩展到企业量级的交易、能效高并支持多种交易。随着网络中的节点数量增加，其验证能力也会同步提升，在无需不断地访问母链的情况下，允许 DApp 子链开展小额交易。

除了权益证明和工作量证明外，MOAC 平台还可以支持额外的即插即用共识系统，例如活动证明（Prove of Activity）、销毁证明(Proof of Burn)、耗时证明（Proof of Elapsed Time），存储证明（Proof of Capacity）等。

目前 MOAC 平台已经实现两种子链节点：ProcWind 和 FileStorm。

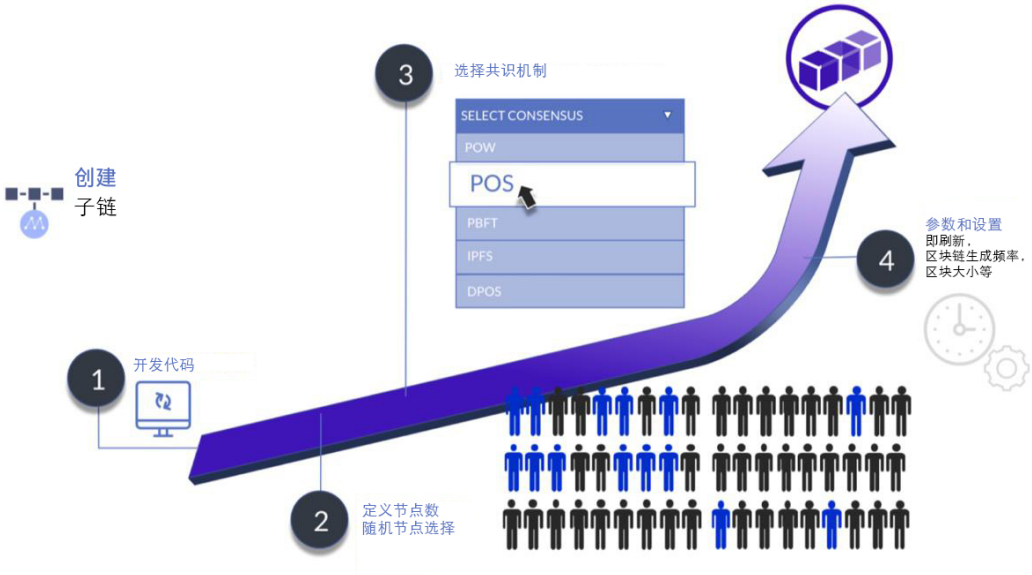
1. ProcWind 是采用 PoS 共识，支持多合约部署的子链节点。目前 ProcWind 也支持两种原子跨链交换，可以完成母链原生通证或者 ERC20 通证和子链原生通证之间的互换；
2. FileStorm 是可以使用星际存储系统（IPFS）的子链节点。在 FileStorm 节点组成的子链上，用户可以通过调用智能合约把文件写入和读出 IPFS 系统。FileStorm 子链定期对文件验证并对存储节点支付收益；

此外，MOAC 平台有两种新的子链类型正在开发中：RandDrop 和 IoTMist。

1. RandDrop 采用 BLS 签名，从共识层支持多个节点的签名片段进行合并得到阈值签名，以此为基础产生随机数。随机数可以在 RandDrop 的智能合约里面直接调用。RandDrop 随机数的优点是可以杜绝单个节点对最终签名的可操作性，更加安全可靠。同时，RandDrop 的信息量是 O(n)，比其他类似的随机数区块链具有较大的优势。RandDrop 已于 4/15/2019 完成初期开发，很快可供测试使用；
2. IoTMist 子链采用横向与纵向扩展相结合的方式，在共识层和 p2p 层更新了对海量节点的支持。采用 IoTMist 的子链，可以有效支持大规模的物联网的应用，在不妨碍单个子链的 TPS 的情况下，通过多个水平子链和垂直子链的组合，实现对物联网应用的支撑。

子链即服务

由于子链间是隔离的，因此它们可以在一个实例中为智能合约运行不同的虚拟机。这使子链能够启动各种业务逻辑并为 DApp 提供公共服务，包括部署类似 IPFS 的文件系统、构建用于数据存储的传感器网络，甚至还可以通过子链实现人工智能服务。



由于 DApp 部署在开发人员选择的虚拟机中，因此不需要额外编程。MOAC 可以通过更低的费用运行现有的以太坊智能合约，开发人员可以利用平台的 API 扩展现有的智能合约功能，而无需学习如何编程区块链。

通过使用自己独特的虚拟机和子链隔离每个智能合约，MOAC 平台可提高智能合约执行效率，并使低成本的处理费用成为可能。这显著降低了开发人员的部署成本，并使他们能够构建基于高交易量的 DApp。

异步智能合约

在使用群链架构的基础上，该平台利用异步智能合约与子链加速 DApp 的开发和部署。这种先进的架构设计还扩展了 Solidity（以太坊编程语言）和以太坊智能合约的功能。

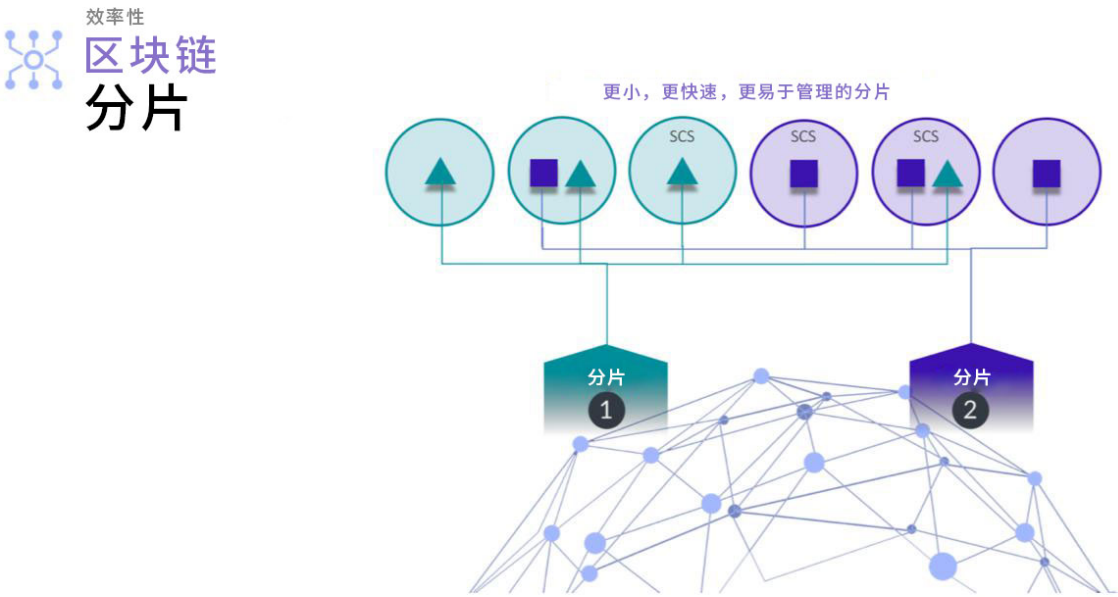
MOAC 平台支持两种类型的智能合约：

1. 子链智能合约是基于协议的合约，用于定义子链中的共识系统，还使节点能够注册使用矿池。

2. 母链全局智能合约，定义了多个子链控制流程的行为，包括刷新、奖励矿工以及如何惩罚不良行为者。它提供了一个灵活的环境，使 DApp 能够使用不同类型的虚拟机，包括 Ethereum，Java（JVM）和其他开发人员选择的虚拟机。

区块链分片

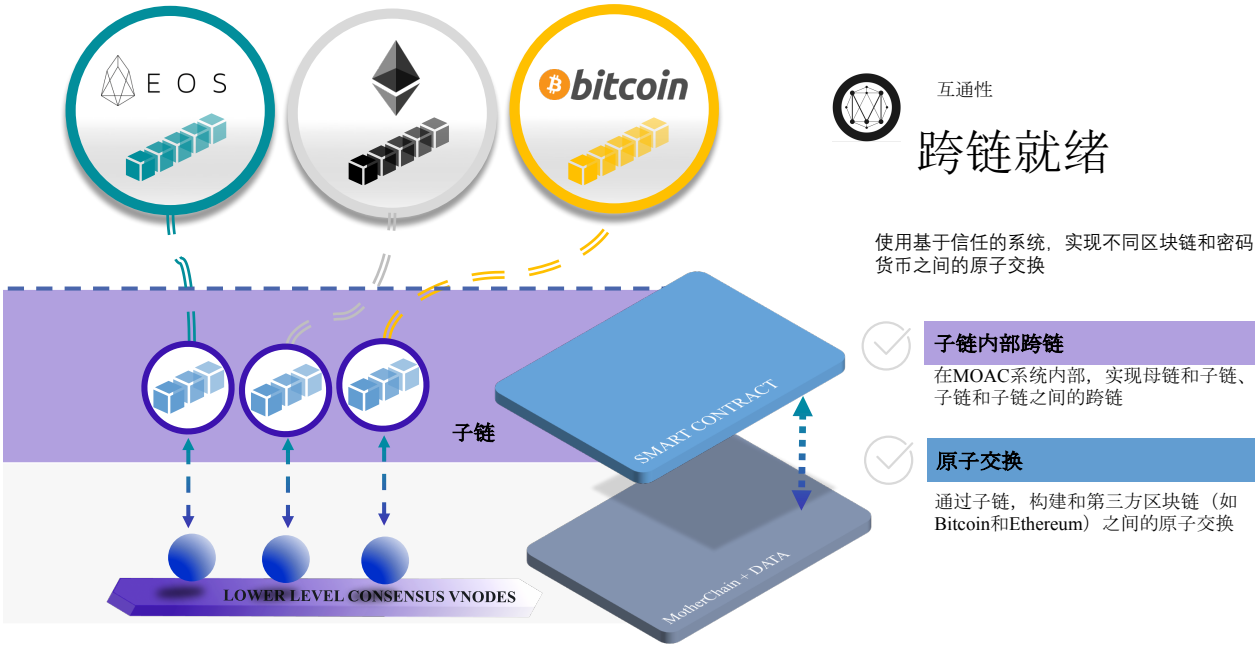
MOAC 平台还提供区块链分片功能，可以跨多个区块链和节点对数据进行横向划分。现有的区块链解决方案效率低下的原因之一是所有节点都需要多次处理相同的任务。分片技术通过将节点分片，提供与网络中节点数量成正比的更强大的处理能力。



当部署智能合约时，开发人员将定义服务节点的数量、共识协议、区块大小、区块生成时间和刷新频率。这将形成分片并为该智能合约提供拜占庭容错方案，然后形成子链。

更多信息参见：https://en.wikipedia.org/wiki/Byzantine_fault_tolerance 了解更多信息。

这与数据库分片非常相似，但区块链分片是一种区块链分区，可将非常大的区块链节点分成更小、更快、更容易管理的分区。使用这种方法，MOAC 可以更有效地扩展，利用更多的节点来扩展网络，显著提高了每秒交易数（TPS）。分片技术将整个网络细分为多个分片，只要每个分片中有足够的节点，系统仍然具有高度的安全性。分片技术还允许对并行交易进行安全处理，从而进一步增加每秒交易处理数量（TPS），远超现有区块链解决方案。



跨链技术就绪

跨链技术使母链与各种子链可以进行交互，也可以与第三方区块链及其上发行的加密货币进行外部交互。

MOAC 平台能够在多个区块链之间交换区块和数据，并使用基于原子交换的跨链。跨链是一种基于信任的系统，用于在单个交易中进行各种区块链和加密货币之间的原子交换。

MOAC 平台提供三种类型的跨链：

1. MOAC 平台内母链和子链之间的原子交换跨链：目前已经实现，可以完成母链原生通证或者 ERC20 通证和子链原生通证之间的互换；
2. MOAC 平台内子链之间的原子交换跨链；
3. 与其他非 MOAC 区块链系统（如比特币和以太坊）进行原子交换跨链交易；

事件处理

在母链这一分布式网络层之上是用于网络事件请求和回复的事件处理系统。 它还处理控制流请求并可调用智能合约相关操作。事件处理系统以多向的方式在平台内的多层之间中继转发交易请求，主要用于交易、全局智能合约控制、状态刷新以及其他与共识相关的消息。

挖矿

挖矿是验证交易的过程。通过这种方式，新的通证被发布并奖励给提供验证计算处理能力和存储的矿工。

MOAC 平台有两种类型的挖矿：

1. 子链挖矿

子链位于 MOAC 平台的上层，由节点验证智能合约和其他共识系统的交易。每个处理智能合约和验证交易的节点将会获得奖励。针对子链的挖矿将获得该特定子链的通证奖励或者 MOAC 通证奖励。

2. 母链挖矿

平台下层是工作量证明母链，它是数据处理和存储的基础层。母链的挖矿功能类似于以太坊，现有的 ETH 矿工可以轻松切换到 MOAC。母链挖矿可以获得 MOAC 通证。

钱包和支付系统

MOAC 平台具有功能齐全的钱包协议。因此 MOAC 能够与各种第三方钱包解决方案一起工作。 任何与 MOAC 协议兼容的钱包都可以在平台上顺利运行。

MOAC 平台目前已经上线了一个基于开源软件的 web 版钱包（https://www.moacwalletonline.com）， 并且和第三方合作提供了移动端 Android 和 IOS 钱包，以及可在 Windows、Mac 上使用的桌面钱包。

API

平台的 API 为 DApp 提供容易使用的访问点，给 DApp 开发人员提供了一个快速入门途径，以便他们使用区块链特定功能，而无需知道区块链实施的具体细节。开发者只需从 MOAC 平台调用这些功能，即可构建复杂的应用程序。

安全

MOAC 将安全放在第一位。在开发平台时，MOAC 团队审查了所有主要区块链系统的安全设置和措施，以便采纳可用的最佳方案。在对现有区块链平台进行安全审计期间，MOAC 团队发现了几处漏洞，这些发现的漏洞都在 MOAC 平台中得到了修补。

当智能合约代码提交给平台时，需要通过非常全面的安全审查流程，以避免合约中的安全漏洞。MOAC 团队与其他知名安全机构合作，制定了应对未来常见攻击的对策和解决方案。MOAC 定期使用合约黑帽和白帽安全公司来分析平台的漏洞。

MOAC 还将发布一个发现漏洞的奖励计划，使黑客更愿意向平台通告安全问题，而不是试图勒索用户。同时，该平台的智能设计架构隔离了不同的子链，从而限制了对每个智能合约的潜在攻击能力。

生态系统

社区

MOAC 平台的核心正是支持它的用户，包括创建 DApp 的开发人员，使用这些 DApp 的终端用户以及保持网络正常运行的矿工和节点操作员。

MOAC 将提供广泛的维基、教程、词汇表、白皮书、知识库、服务台和其他用户资源，包括在电报、脸书、推特和其它社交媒体平台上积极与用户群体互动。

MOAC 平台可以部署到所有主流操作系统中，如 Windows、Mac OS 和 Linux / UNIX 等。MOAC 客户端程序目前是用 Golang 语言编写的。当然，通过提供的 MOAC 协议，开发人员可以使用其他编程语言编写智能合约。

社区也包括 DApp 实验室，鼓励开发人员进行测试和实验，使开发人员能够在将 DApp 发布到公共网络之前对其进行隔离测试。测试网的状态可以在 http://testnet.moac.io 上查看，并且可以在 https://faucet.moacchina.com/上获取测试网的原生币用于开发。

除了支持与其他区块链和加密货币互连的跨链功能外，MOAC 平台还运行在基础 P2P 分布式网络上。通过使用 P2P 网络，该平台能够为 DApp 提供分布式网络以进行交互。

P2P 网络是运行相同协议的任何单个或分组节点之间的底层通信。本案例中的一个节点是指在网络上共享区块和交易的客户端。节点通过使用 RLPx 发送消息进行通信，这是一种加密和认证的传输协议。

DAPP 开发者的红利

- 服务质量

与其他平台相比，DApp 可在 MOAC 平台上更高效地运行。以太坊受其可扩展性和每秒交易处理量的限制，本身无法处理大型交易和高并发量。这就是为什么像 CryptoKitties 如此简单的游戏会造成整个以太坊网络的拥堵。 在以太坊上同时运行 10 个或 100 个应用程序导致的类似堵塞可能会更具有灾难性。

了解更多信息，请访问 http://www.bbc.com/news/technology-42237162

	特点	ETH 07.2015	ETH 2.0 2019秋	MOAC 2019秋	EOS 06.2018	ADA 09.2017	NEO 07.2016	ICX/ICON 02.2018
	去中心化	✓	✓	✓	✗	✓	✗	NA
	跨链互用性	✗	✗	✓	✗	✗	仅在白皮书中	仅在白皮书中
	IPFS 功能	✗	✗	✓	✗	✗	✗	✗
共识算法	主链	POW	POW+POS	POW	DPOS	POS	DBFT/DPOS	LFT
	子链	NA	POS	DPOS,POW, 其它	NA	NA	NA	NA
	成本问题						成本极高	

	性能	ETH 07.2015	ETH 2.0 2019秋	MOAC 2019秋	EOS 06.2018	ADA 09.2017	NEO 07.2016	ICX/ICON 02.2018
每秒交易	TPS(主要节点)	15	15	1,000+	100	NA	1,000	9,000
	TPS(分片/ 子链)	NA	NA	100000+ 及扩展性	NA	NA	NA	NA
分片	可扩展分片	✗	✓	✓	✗	分层	✗	✗
	灵活分片	NA	✗	✓	NA	✗	NA	NA

智能合约	ETH 07.2015	ETH 2.0 2019秋	MOAC 2019秋	EOS 06.2018	ADA 09.2017	NEO 07.2016	ICX/ICON 02.2018
灵活的系统合约	✗	✓	✓	✗	✗	✗	✗
智能合约	✓	✓	✓	✓	✓	✓	✓
异步智能合约	✗	✗	✓	✗	✗	✗	✗
EVM兼容性	✓	✓	✓	✗	✗	✗	✗
智能合约语言	以太坊编程语言	以太坊编程语言	以太坊编程语言及其它	WEBASSEMBLY	以太坊编程语言及其它	C#,JAVA, PYTHON AND ETC.	NA

➢ 费用

在以太坊上运行智能合约或 DApp 的成本非常高。智能合约启动或触发的每笔交易都需要一定量的 gas。每次交易的平均 gas 非常高，这意味着每笔交易的成本非常高。如果某些智能合约触发了许多交易行为，这意味着智能合约的开发者或用户必须支付大量货币，加密货币或其他代价来维护 DApp。

MOAC 平台的底层交易 GAS 成本是以太坊成本的十分之一，而上层子链合约的交互是免费的。

智能合约		MOAC
区块GAS上限	8,000,000	9,000,000
交易手续费	21,000	1,000
全局合约调用	100,000-200,000	100,000-200,000
子链合约调用	N/A	免费

智能合约		MOAC
部署	支付费用	向母链支付费用
维护	免费	子链需要向子链节点提供费用
用户调用	支付费用	免费
共识方式	POW	母链为POW，子链可配置

➢ 灵活性和简洁性

大多数 DApp 只在以太坊中拥有自己的交易逻辑，而其余的逻辑和组件则是“链外”解决方案，依靠传统的服务器和数据库，使其成为中心化系统。相比之下，在 MOAC 平台上部署的 DApp 仍然保持真正的去中心化。MOAC 还提供用于 CPU 计算、GPU 计算、文件存储、数据库和许多其他服务的上层子链，同时保持去中心化结构。

➢ 跨链

MOAC 平台目前已经实现具有跨链功能的区块链平台。

现在开发人员可以在特定的 DApp 之间切换加密货币，并且不限于任何特定的平台或技术。如比特币，以太坊或其他加密货币都可以与 MOAC DApp 进行交互，而无需在交易所之间来回切换。如果没有 MOAC，用户无法轻松处理比特币和以太坊之间的交易。

不幸的是，每个现有的区块链系统就像一个岛屿，它们之间没有任何桥梁。想象一个世界、每个网站和移动应用程序都无法通过我们今天所知的互联网和物联网互相沟通。MOAC 跨链技术使不同区块链系统之间互通成为可能，其潜力尚未完全展现，更大的应用场景还有待开发。

➢ 一键发链

目前 MOAC 已经将部署子链的过程简化成为一键发链的脚本，便于用户使用。只有用户选择目前 MOAC 平台提供的子链模板，设定子链参数，就可以使用脚本完成部署子链的工作。通过这种方式，项目方不需要浪费精力来开发和维护自己的区块链。也不需要部署自己的节点服务器，只需付出一定的 moac 来维持子链运营。通过这种方式，MOAC 希望帮助项目方集中实现应用的逻辑方面，不需要花额外的精力去开发区块链。

交易所

该交易所是一个去中心化交易所（DEX），用于交换各种加密货币，无需中心化的服务器或第三方权限管理。它由一个去中心化的系统来管理。

在 MOAC 平台上，可以部署子链以提供 DEX 的基础。此外，基于子链的 DEX 可被开发来收集交易信息，匹配买卖双方，并为用户提供去中心化的原子交换。子链可实现跨链协商一致协议，并为矿工提供对两者的访问权限。

跨链一致性协议利用平台的独特功能来创建哈希和时间锁定交易。子链将提供 MOAC 平台与外部区块链之间兑换的原子交换功能。可以部署类似的子链以实现 MOAC 代币、BTC、ETH 或 LTC 之间的兑换。

用户通过 DEX 将所有代币保存在他的钱包中，直到交换成功。与中心化交易所不同，用户可以降低代币被盗的风险。所有的 DEX 交易信息都是公开的，并可供所有人使用，从而减少伪造订单的现象，提供更健康的市场环境。

通证

MOAC 的智能合约系统完全兼容以太坊的 EVM 系统，支持 ERC20 和 ERC721 通证标准。

MOAC 的通证市值

MOAC 通证的起始供应总量为 1.5 亿枚。目前由 MOAC 基金会本身持有 5300 万，其余部分都在流通中。MOAC 通证的价值可以在 CoinMarketcap.com 上查询。MOAC 区块链每年将通过挖矿产生 600 万个通证，进一步增加流通中的供应量。4 年后，产量减半至 300 万，接下来的 4 年再减半。到 2058 年，总供应量将达到 2.1 亿枚。

MOAC 通证最初在 2017 年 7 月以 ERC20 形式在以太坊平台发行。MOAC 主网在 2018 年 4 月上线以后，已经将以太坊上的 ERC20 合约关闭，按地址将 ERC20 通证全部 1：1 转换成为 MOAC 主网的原生通证。目前以太坊平台上没有 MOAC 通证。

治理

MOAC 区块链公链项目（MOAC）将由 MOAC 基金会管理，该基金会是一家在新加坡成立的合作性非营利组织。MOAC 基金会是负责有效使用由 MOAC 储备通证销售产生的资金的实体，并且承担 MOAC 平台开发（包括应用程序和相关服务的开发），维护和支持多方应用的责任（包括社区公共教育内容）。

MOAC 基金会的希望通过多方协作、公开透明、和简单易用的方式来支持和发展区块链市场。

MOAC 区块链科技公司（MOAC Blockchain Tech，Inc.）是一家在美国注册的营利性实体，受 MOAC 基金会委托作为技术开发方，在加州帕洛阿尔托设有执行办事处，并在中国上海设有拓展开发团队。

MOAC 基金会同时与多家技术研发机构合作来推广和丰富 MOAC 公链的生态，如中国的墨一客公司、墨客井链数字科技公司、井畅数字技术公司、烨链科技公司等。更多信息可以访问 MOAC 基金会网站（www.moacfoundation.org）。

子链项目

目前 MOAC 公链上已经有多个项目和应用实现。其中基于子链的典型应用有：

➢ 链问（Moodada）

链问是一个基于 MOAC 子链实现的完全去中心化的应用。用户即可以通过提问获得信息，也可以通过回答问题得到奖励。链问将处理提问和回答以及利益分配，这些逻辑都通过智能合约记录在一个 MOAC 子链上面。对于这样的应用来讲，不需要任何的后台数据库，也不需要开发区块链，只要通过平台的通证就可以完成整个商业逻辑。

➢ 星际风暴（FileStorm）

星际风暴是一个通过 MOAC 子链将星际文件系统（IPFS）和区块链结合而产生的分布式存储平台。星际风暴构建在 MOAC 子链之上，使得有存储需求的用户可以消耗通证来得到存储空间，而提供存储空间的节点提供者通过竞争来获得通证。这种激励方式可以鼓励大家把闲置的硬盘空间来共享，从而搭建一个可商用的全球化存储空间。更多信息可以访问项目网站（https://www.filestorm.net）。

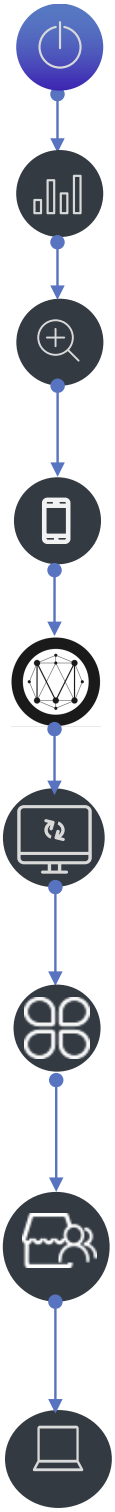
➢ 高精度信任链网（PAS）

高精度信任链网（Planet Accuracy Simpler - PAS）是一个通过 MOAC 子链和 GNSS 硬件终端，为用户提供厘米级高精度定位服务的系统。PAS 的目标是通过区块链的激励方式，将高精度的定位服务用去中心化的方式，快速、高效和廉价组成全球高精度地理网络，从而使得这些服务可以迅速普及到大众生活中。在这个项目服务模型的设计上，通过区块链的机制，使得使用者和建设者的经济效益形成正向反馈，利于将网络迅速覆盖到地球的每一个角落。同时使用者越多，网络的精度、可靠性和可用性越高 。更多信息可以访问项目网站（https://www.pasnet.io）。

➢ 大数据交易平台（BDE）

大数据交易平台（Big Data Exchange - BDE）是一个通过 MOAC 子链，对大数据产品进行确权和交易的平台。传统的数据交易需要将卖方的数据存储在数据交易所中，有数据安全和版权复制的隐患。同时在数据买方和卖方之间如何确认正确的交易记录也是一个容易引起纠纷的问题。大数据交易平台通过使用 MOAC 子链上的智能合约，匹配数据买卖双方的需求，及时追踪交易的行为，并将交易结果记录在可以公开查询的区块链上。通过这一平台，可以有效地保障数据交易中的数据安全和交易记录，解决当前数据交易中的问题，促进数据交易的健康发展。

产品演变与进程图



2017

MOAC

JANUARY 2017

成功募集到$6,998,723 USD

JULY 2017

测试网发布

NOVEMBER 2017 **已实现**

- MOAC测试网发布
- 异步合约调用上线

2018

FEBRUARY 2018 **已实现**

- MOAC钱包测试版发布
- 智能合约测试

主网盘古版本上线

APRIL 2018 **已实现**

- MOAC主网上线
- 主网DAPP
- 母链节点挖矿开始
- 网络浏览器上线

女娲版本上线

AUGUST 2018 **已实现**

- 实现两种SCS服务: ProcWind（POS）和 FileStorm（IPFS）
- 认证系统上线
- 无币子链解决方案
- ATO模式

子链版本更新

DECEMBER 2018 **已实现**

- 子链分片系统发布
- 一键发链工具发布
- 完全去中心化的DAPP应用链问（MooDaDa）上线

2019

JUNE 2019

- 星际风暴（FileStorm）
- 高精度信任链网（PAS）
- 大数据交易平台（BDE）

伏羲版本发布

DECEMBER 2019

- 功能强化和监测模块
- 随机数子链（RandDrop）
- 物联网子链（IOTMist）

团队

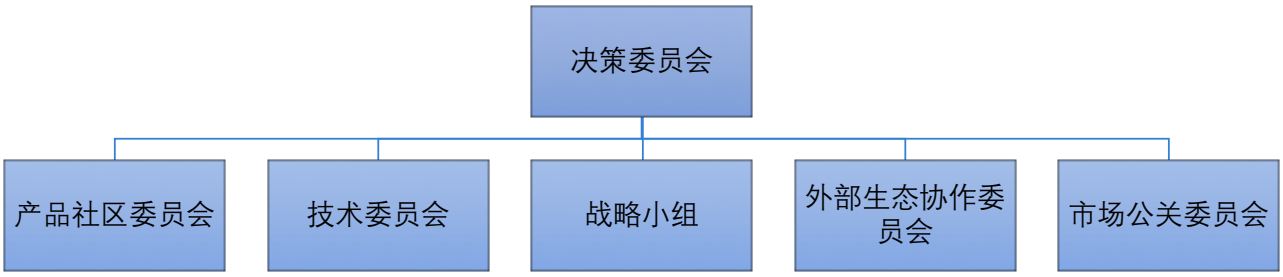
周沙

周沙是一位作家、极客、风险投资家，以及外交事务洞察者。他在北京奥运会、台湾贸易、人民币全球化和中国 1000 亿美元的一带一路项目中向中国中央政府提出建议。 周沙撰写了关于区块链和大数据的书籍（《大国游戏》、《区块链世界》和《区块链与大数据》），并受到中国科技精英的高度认可。他是企业井通科技有限公司创始人，MOAC 公链创始人，也是硅谷风投基金 Outpost Capitals 创始合伙人，早在 1996 年投身硅谷高科技行业，长期在硅谷从事高科技公司研发、管理和投资工作。

陈小虎

陈小虎是一位拥有丰富经验的区块链理论家和跨领域软件工程师。陈小虎对新兴技术拥有浓厚的激情，几十年来，他在硅谷一直是执行技术专家。此外，他是领先的区块链平台和实物资产通证化解决方案提供商---井通的首席技术官和创始人之一。

MOAC 基金会的组织结构图



附件 A：免责声明

本文中的所有技术目前都处于研发和测试阶段，并且会受到未来变化，改进和创新的影响。 尽管 MOAC 基金会很重视安全性，但平台可能仍然存在漏洞，这也是漏洞奖励计划的原因。

无法保证在平台上创建和处理加密货币的过程中，不会被干扰或没有错误，并且可能存在软件包含缺陷、弱点、漏洞、病毒或错误等固有风险。此外，所有加密货币都存在与获取、存储、转让和使用通证或代币相关的风险，并且 MOAC 平台也面临相同的风险。

有关使用 MOAC 平台相关风险的更多信息，请阅读我们网站上的服务条款。

附件 B：术语清单

比特币

Bitcoin，比特币是一个基于分布式账本的加密货币，它使用工作量证明共识系统，要求矿工处理新币的创建。

区块链

Blockchain，为去中心化账本系统和加密货币提供支持的一种底层分布式数据库技术。

共识系统

Consensus，用于达成一般性协议的系统、协议或算法。在本文中，指的是基于区块链的加密货币同意交易或智能合约的验证。

跨链

Cross-Chain，使用原子交换将数据从一个区块链移动到另一个区块链的能力。

加密货币

Crypto-currency，基于区块链技术支持的分布式账本的数字货币。

去中心化

Decentralization，一个不依赖中央权威批准交易的系统。

去中心化应用程序(DApp)

Decentralized Application，一个应用程序，其后端代码运行在具有多个节点或主机的去中心化的点对点网络上，而传统的云端 app 运行于一个中心化的服务器中。

分布式计算或网络

Distributed computing/network，一种软件系统的组件在多台计算机之间共享以提高效率和性能的模型。

以太坊

Ethereum，以太坊是智能合约的分布式计算平台，目前采用工作量证明(PoW)，要求矿工处理数据。以太坊计划未来将共识算法调整为权益证明（PoS）

子链

MicroChain or Subchain，MOAC 平台的上层交易处理区块链，由多个子链节点 SCS 组成，通过母链节点 VNODE 接入母链。一条子链进行操作。

子链客户端 SCS

Smart Contract Server(SCS)，构建 MOAC 子链的客户端软件，用于子链挖矿，子链账本同步以及子链业务逻辑执行的节点，也称为子链矿工。

MOAC

MOAC 基金会的简称。

母链

MotherChain，MOAC 平台中的底层数据处理和存储区块链层。

母链客户端（VNODE）

Verification node (VNODE or V-node)，构建 MOAC 母链节点的客户端软件，用于母链挖矿，账本同步，处理交易和合约调用，以及子链数据传输的节点。

MOAC 平台

MOAC chain， MOAC blockchain or MOAC platform，由 MOAC 基金会（MOAC）创建的公链系统。它利用群链架构作为其基础技术来实现高性能智能合约执行，大大提高了区块链平台每秒交易处理量（TPS），维护了平台的安全性，并提供了平台的可扩展性。

群链技术

Multi-blockchain，MOAC 平台中使用母链作为其底层主区块链和上层分片子链的架构。

节点

node，网络中的重新分配点，通常用于连接各点和（或）验证交易。

点对点网络（P2P）

Peer-to-Peer network，一种网络通讯方式，其中每台计算机都可以作为其他计算机的服务器，并允许共享访问文件、数据处理和存储，而无需中心化服务器。

权益证明（PoS）

Proof-of-Stake，一类算法，加密货币区块链网络用其实现分布式共识。区块的创建者是通过持币数量或持币时间等各种组合来选择的。

工作量证明（PoW）

Proof-of-Work，一种协议或算法，作为一种经济措施，通过要求服务请求者进行计算工作（通常由计算机处理时间来衡量）来拒绝服务攻击和其他服务滥用（如垃圾邮件）。

分片

Sharding，跨多个区块链和节点进行水平划分数据和事件的功能。

智能合约

Smart Contract，旨在数字化促进、验证或执行谈判或履行合约的计算机协议。智能合约允许透明地执行可信交易，无需第三方。

通过子链形式实现的智能合约通过子链形式实现的智能合约是一个拥有自己独特区块链或“子链”的智能合约，可与其他智能合约和整体系统之间实现隔离，并促进整体系统的智能合约执行性能。


MOAC
www.moacfoundation.org