众链之母

（MOAC）

技术白皮书

June 2017

[目标]

MOAC 项目旨在提供一种可扩展且有弹性的区块链，通过分层化的结构来支持数字资产交易，数据访问，和流程控制。 它创建了一个框架以允许用户用高效的方式执行智能合约。 它还提供了开发的体系结构，采用底层基础设施来快速简便地产生子区块链。 它是一个区块链平台，可以为子区块链的架设提供必要的部件，同时为新想法的测试，私有链的部署，复杂任务的处理和智能合约的应用提供解决方案。

[当前的问题]

自从 2008 年中本聪的比特币项目引入了区块链技术以来，这项技术的发展非常迅猛。在过去近十年的时间里，开发者们以极大的热情来探索区块链技术这个新领域，试图拓展区块链的应用，提高区块链的效率和促进区块链的商业化。

区块链系统中的原生数字货币在区块链推广中起到了至关重要的作用，比如比特币系统的比特币，以太坊系统的以太币等。这些原生数字货币不仅推动了更多的参与者来进入区块链生态系统，也为当前存在的支付系统提供了更有效的方案。

当然，目前区块链技术还处于发展的早期阶段，现有区块链系统都有以下一个或多个问题。

1. 难以尝试新的想法

   新的想法意味着要建立一个新的区块链系统。 这意味着有大量的额外开销和精力要用来设置服务器，培训开发团队，建立社区，吸引新用户等。

2. 难以升级

   一旦区块链被部署和进入生产模式，很难在功能上进行添加/修改/删除。 区块链修改的结果就是会造成区块链系统的软分叉或者硬分叉。 而每个分叉都需要大量的精力来处理，也必须承受由此带来的经济后果。

3. 区块链系统之间不相容

   不同的区块链有不同的模式，如共识协议，货币特征和适用要求。 模式的差异阻止了多个链之间的互连或互换。

4. 分裂的用户群

   对于每个区块链，用户群是不同的。 一个区块链系统的矿机和验证节点仅能用于该区块链。 没有两个区块链可以共享它们。

5. 性能瓶颈

区块链作为分布式系统，与传统中心化的系统相比在吞吐量，响应时间等性能上还是有较大差距。而在维持分布式拜占庭容错性的前提下，提高性能是非常困难的。

还有一点，当大多数原生数字货币的价值迅速增长的时候，基于它们开发的各种应用的手续费也相应增长，网络延迟时间也在增长。

[解决方案]

过去几年来，包括工作量证明（POW），权益证明（POS）和授权权益证明（DPOS），拜占庭容错性（BFT），以及由这些方法结合的多种共识方案已被尝试和应用。 但是，没有一个协议可以解决所有的问题。 通常，POW 可以部署在大型网络中，并且可以很好地扩展。 它是验证最为广泛的共识协议。 但是它受到像大量电力消耗，低吞吐量，高延迟和高参与障碍这样的问题的困扰。 POS 和 DPOS 虽然没有大量的电力消耗，并且执行速度更快。 但是，这类协议实施比较复杂，通常以较小的网络规模部署，并且未得到大规模的全面测试。 通常 BFT 系列的使用要在小得多的系统上，并且可以在吞吐量和延迟方面表现更好，所以大都是用于私有链或企业内部应用。

为了能够在大型网络中部署分布式系统，吸引更多的参与者，同时保持高吞吐量和低延迟时间，MOAC 提出了用分层的共识堆栈技术来解决问题的方案。 它是区块链的区块链。 MOAC 本身将部署在具有大量验证节点的公共网络中。 它提供以下内容：

1. 分层配置结构
2. 交易，智能合约和数据访问支持
3. 数据存储，流程控制和处理单元，形成一个分布式的冯•诺依曼（Von Neumann）架构。
4. 验证节点可以配置为多个重叠的子区块链服务。
5. 可插拔验证方案，支持注入式的用户协议，可以使用现有验证节点来轻松部署新的子区块链。

1. 鼓励具有较小处理能力的用户参与验证过程。
2. 使用分流方案来提高系统性能。

[共识协议]

我们意识到仅仅在任何目前的共识协议基础上拓展将无法满足所有的要求。已有的解决方案是通常是采取多个链或侧链的方式来结合两种不同共识协议的。这是我们想避免的方法，因为这种方式会引入更多问题。我们解决共识困境的是建立一个分层的共识堆栈，并保持一切都在同一个区块链上同步。

我们利用 POW 作为底层的主要共识协议，因为 POW 是一个经过广泛测试，并具有抗攻击性和拓展性的解决方案。目前 MOAC 使用类似于以太坊的 POW 协议。

MOAC 在设计了顶层补偿了 POW 的缺点。只有关键的交易和控制流程交易在 POW 层中处理。顶层采用 POS 协议和分片技术提供更快更高的吞吐量解决方案。

每个 POW 节点都有一个智能合约服务器（Smart Contract Server - SCS）节点。SCS 身份是由相应的 POW 节点完全验证。每个 SCS 节点将能够处理顶层的用户请求。

SCS 处理智能合约的调用。顶层的所有交易都是以智能合约调用的形式进行。并非所有 SCS 都将同时处理单个事务。相反，部分选定的 SCS 将处理特定的事务。

SCS 的选择是通过初始化智能合约调用或刷新调用（init / flush）。init / flush 调用实际上是传递交易给 POW 节点，并在底层达成共识。 init / flush 调用将会设定如何选择合约的 SCS，以及处理节点的百分比。然后每个 SCS 的相应 POW 节点都会使用 EHDRand 算法在其 SCS 上调用该调用。 SCS 可以决定是否选择处理这个智能合约。注意这是一个确定性的过程，SCS 的参与可以被任何人验证。

一旦选定了智能合约的 SCS 组合，它们将相互通信并形成一个小的共识组。该组将处理智能合约的所有调用过程。此外，他们如何达成共识的行为可以由 init / flush 指定。这些 SCS 节点会形成一个子区块链并执行基于预定协议或用户自定义协议的共识。请注意共识协议与实际的智能合约代码不同。

智能合约的状态保存在每个 SCS 中。但是，这并不是保存在完整的区块链系统中。而为了达成完整的共识，合约状态需要定时或按要求写入底层的 POW 节点。

在共识模式下，当刷新（flush）时， SCS 节点将接受来自底层 POW 节点的数据存储请求。当前状态将被写入区块链系统并生成相应的 HASH。注意所有 POW 节点将执行相同的操作。对于那些不参与此次刷新的智能合约的 SCS，它们不会做任何事情。参加智能合约的 SCS 将获得的提交状态并用自己的状态进行验证。如果可以证明之前提交的状态是不正确的，它将会发起更新一个具有正确状态的数据存储请求并引用不正确状态的 HASH。如果之前提交的状态没有争议的数据存储请求，SCS 节点将最后刷新具有正确状态 HASH 的智能合约。同时每个 POW 节点也会处理与合约状态相关的交易。发出不正确状态的 SCS 节点将会被取消权益。

在 MOAC 中，大多数交易将在顶层处理，而只有一小部分流程控制在 POW 层中处理。这是可行的，因为顶层提供快速，灵活和低成本的服务，而 POW 层提供缓慢，但可靠和完整的服务。

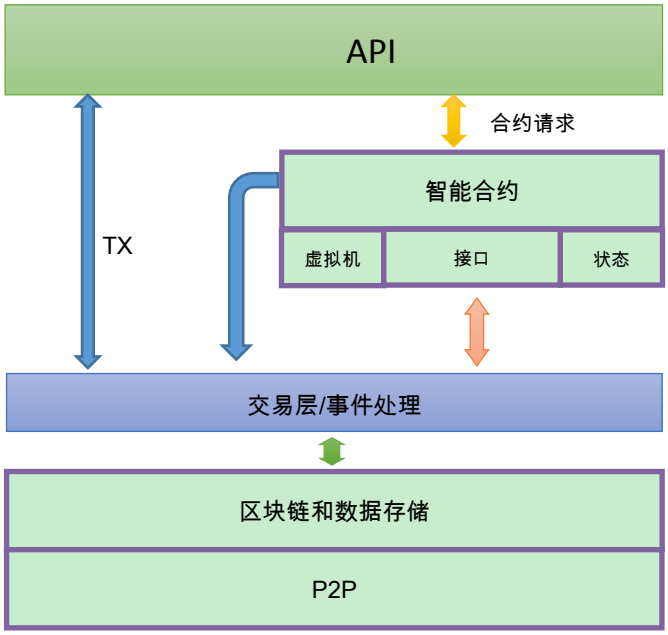
[分层结构]

1. P2P 网络层： 这个层定义了基础的 p2p 协议。
2. 区块链层：该层处理与区块链操作相关的所有操作，如共识，数据访问等。

3. 交易（TX）层： 该层处理 TX 请求和回复。 它还处理控制类 TX 请求，并在必要时调用与智能合同相关的操作。

4. 智能合同层： 该层执行虚拟机内的智能合同执行，并保持临时合同状态。

5. API 层：API 用于处理终端用户输入并获取下层的输出及返回。

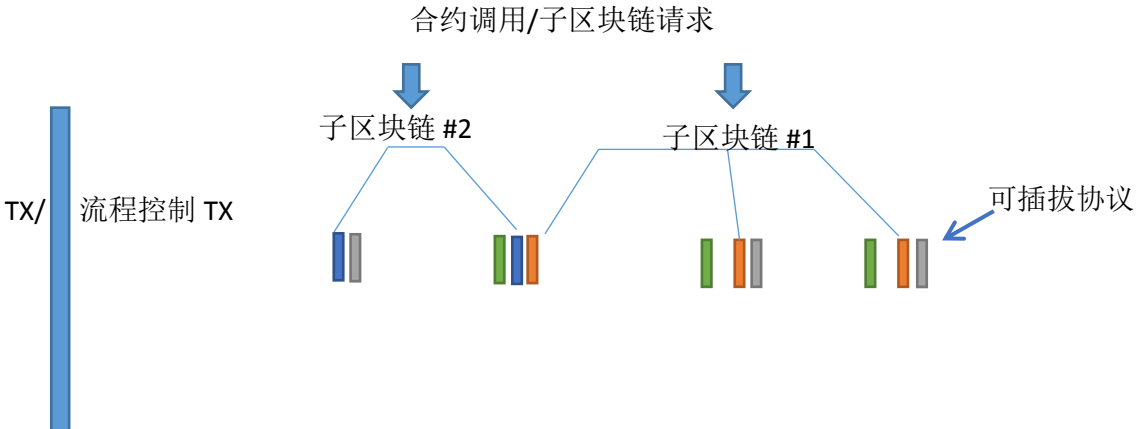


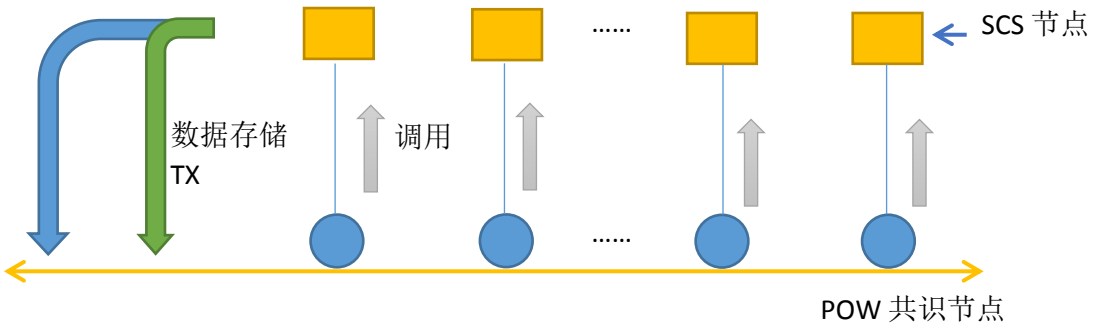
MOAC 拓扑结构

POW 共识节点采取志愿参与的方式。 每个节点贡献其计算能力来解决计算密集型问题，并验证约定交易集中交易的有效性。

除了 POW 对交易和数据存储集的共识之外，每个 POW 节点都会与一个智能合约服务器（Smart Contract Server - SCS）相关联。 SCS 节点可以是 POW 节点的本地节点，也可以是一个远程节点。 SCS 的身份可以由相应的 POW 节点来完全验证。

智能合约服务器（SCS）身份可由相应的 POW 节点完全验证。 智能合同请求（创建/调用/刷新）包含在流程控制 TXc 中，并首先在底层中处理。 然后每个 POW 节点通过异步调用向其 SCS 发送合约请求。合约请求在 SCS 中处理。如果需要，SCS 将向底层发送附加的控制流 TXc 和数据存储 TXs。





执行智能合约的方式是通过高效的分片技术实现。所有 SCS 都可以在运行时进行配置，以处理不同部分的智能合同。 整个系统吞吐量可以比传统方式快 10 倍 - 100 倍。 分片的执行组通过控制流 TXc 和数据存储 TXs 将分片状态记录到底层块链中。

[钱包/地址]

钱包和地址两个名称在本文档中是可互换的。 每个钱包/地址是由一个私钥生成的，并保存有数字货币的余额，可以接收和发送交易。 钱包/地址对于区块链的用户是可见的。私钥则是用于签署起源于这个地址的交易，仅对拥有者可见。

[智能合约]

每个智能合约与普通钱包相同，都有一个独特的公共地址。 区别在于智能合约的私钥在合约创建完成时就会被丢弃，所以除了共识机制外，没有人可以在智能合约创建后发送里面的数字货币。

智能合约有四个基本要素：{代码，状态，[调用]，余额}。 代码由用户生成。状态持有合约当前的内部信息。 余额是合同中的数字货币。 它也是存储该合同的调用历史。

[交易]

交易是 MOAC 系统内的基本操作。每个地址可以与其他地址之间交换数字货币。还有基于智能合同的流程控制交易（TXc）。这些 TXc 用于控制智能合约的工作流程。

MOAC 系统中的三种存在基本交易类型：支付交易 TXp，数据存储 TXs，流程控制 TXc。它们都是在底层的 POW 共识节点中被处理。所有节点共识并保持同样的系统状态。

a）支付交易（TXp）：{sender-> receiver：数字货币金额}

将数字货币从一个地址转移到另一个地址的基本交易。发送地址将需要使用私钥签署交易，而签名的真实性可由任何人核实。

b）数据存储（TXs）： {sender-> contract_address：要存储的数据}

在 POW 节点处理的此交易类型不会验证任何与余额相关的操作。

c）流程控制（TXc）：

1）Contract init TX {code， sender， init_amount， execution type， sharding config}

用户发送 init TX 启动新的智能合约。在智能合约中，用户需要指定合约代码，初始资金，执行类型：快速或正常，分片配置。

2）Contract Flush TX {contract_address，flush_target_state，flush_steps}

Flush TX 是允许 POW 节点同意已经执行的批量事务，并将它们写入区块链。

3）Contract Payment TX {sender-> contract_address：

类似支付交易。不过 POW 验证节点会通知相应的 SCS 相应帐号的余额更新。

[子区块链]

MOAC 系统可以执行普通支付交易，数据存储交易和智能合约（流程控制）交易。此外，在此架构上部署子区块链是非常方便的。

用户可以使用智能合约来定义子区块链的属性（系统参与验证节点的百分比，共识协议，安全策略，状态存储等）。子区块链的创建通过控制流程 TXc 完成。一旦建立子区块链，每个参与者 SCS 将在其执行中采用可插入的协议。对子区块链上的随后请求将由选定的 SCS 来验证。

子区块链的区块生成可以配置为按需生成或按照设定的周期生成。按需功能是首选项，因为它只在需要时生成区块，从而节省宝贵的资源。

子区块链的部署可以像发送智能合约请求一样简单。但是，它继承了安全和强大的底层区块链属性。并且，它可以重用已有的大量的验证节点池，并从分布式的设置中受益。

子区块链可以通过刷新操作来随机更换参与的 SCS 节点，达到更高的分布式和安全性能。

升级子区块链也很容易，只需重新部署到具有更新的区块链属性的新集合 SCS 上。

[节点的经济效益]

参加验证的节点通过其贡献的计算能力，可以从两方面来获益。首先，POW 节点将获得挖到的每个区块的奖励。这与现在的 BITCOIN 相似。其次，SCS 服务器可以通过对子区块链的支持和智能合约的处理工作的交易费得到回报。请注意，这种服务可能并不是运算量密集型的。例如，如果子区块链基于 POS，则 SCS 只需花费非常有限的资源进行验证即可收取费用。

这对于普通 PC 用户甚至移动用户来说是一个很大的动力。对于纯粹的 POW 网络，普通用户几乎没有机会从采矿中获益。然而，在 MOAC 系统的设计中，用户可以设置一个轻型的 POW 节点，当然几乎没有机会在采矿竞争中获胜，但是他可以设置与该 POW 节点相关联的另外一个 SCS，通过 SCS 提供的服务获得奖励。这种模式将鼓励更多的用户加入共识系统并提供更多的 SCS 处理能力。另一方面，智能合约所有者或子区块链创建者将需要支付

所有 SCS 工作的费用，但考虑到获得的性能和低成本的启动，还是非常划算。这个过程将促进形成一个更为分布式的生态系统，并使各方受益。

[收益规划]

区块每 10 秒生成一次，每个块的奖励为 2 个 MOAC 币。 奖励计划每三百万块减半，相当于约 每 1 年减半。 在 18,000,000 区块之后，也就是 6 年后，每个区块的奖励将保持在 0.04 MOAC。 见下文。 我们定义 1 个 MOAC = 1,000,000 Sand。 1 Sand = 1000 Xiao。

区块数目	挖矿奖励(1 MOAC = 1,000,000 Sand)
1-3,000,000	2 MOAC
3,000,001-6,000,000	1 MOAC
6,000,001-12,000,000	0.5 MOAC
12,000,001-15,000,000	0.25 MOAC
15,000,001-18,000,000	0.125 MOAC
18,000,001-	0.1 MOAC

交易费用有两种方式收取， 一个是通过交易。 另一个是通过智能合同调用或子区块链的使用。

交易类别	费用	收取对象
Payment TX_p	20 Sand	POW miner
Data Store TX_s	20 Sand	POW miner
Control flow TX_c	50 Sand	POW miner
Smart Contract Call	1 Xiao	To each SCS

智能合约调用的交易费特意设置成低于底层的 POW 交易费，从而鼓励用户更多的使用 SCS。 这可以减轻下层的压力，也有利于 SCS 服务提供者。

[总结]

总而言之，MOAC 使用分层架构来把 POW 的难于攻击和易于扩展的特性，与 POS 的快速共识和短时间响应的特性结合在一起，避免了两者的缺点。智能合约层可以用于构成复杂任务和搭建各种子区块链的平台。而 POW 节点与 SCS 节点一起构建可以灵活和可扩展的框架，便于许多应用程序的使用。 MOAC 区块链对于轻量化参与者和计算密集型参与者都是有价值的。

[附录]

MOAC 货币总量是每年增加的:

阶段	发行量（个）	总量（个）
ICO	250,000,000	250,000,000
1st 年	6,000,000	256,000,000 (大致数量)

2nd 年	3,000,000	259,000,000 (大致数量)
3rd 年	1500,000	260,500,000 (大致数量)
4th 年	750,000	261,250,000 (大致数量)
5th 年	375,000	261,625,000 (大致数量)
5 年之后	300,000	261,625,000 + 300,000 * n （n=1,2,3……）

[免责声明]

本白皮书草案仅供参考。 Moac.io 不保证本文得出的结论的准确性，白皮书不提供任何声明和保证，明示或默示，包括但不限于：（i）适销性，适用于特定目的，所有权或非侵权的保证;（ii）本白皮书的内容不存在任何错误或适用的内容目的;（iii）此类内容不会侵犯第三方权利。所有保证是明确 Moac.io 及其附属公司明确表示不承担任何因使用，参考或依赖本文白皮书中包含的任何信息而引起的责任和损害，即使被告知这种损害的可能性。在任何情况下，Moac.io 或它的附属公司对任何个人或实体使用，参考或依赖本白皮书而导致的任何直接，间接，特殊或后果的任何内容的损害都不负赔偿责任。