MOAC – 众链之母

June 2017

[目标]

该项目旨在提供一种可扩展且有弹性的区块链，支持基于分层结构的状态交易，数据访问，和控制流程。 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，为想法测试，私链部署，复杂任务处理和智能合同应用等提供解决方案。

[当前的问题]

目前已经有很多部署的区块链，但它们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。 需要设置服务器，开发团队，建立社区，吸引新用户等，需要大量开销来实施新的区块链想法。

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。 这样的修改要么是软分叉或者硬分叉。 处理分叉需要巨大的努力和承受由此带来的经济后果。

3. 区块链之间不相容

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. 分裂的参与者

对于每个区块链，用户群是不同的。 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。

[解决方案]

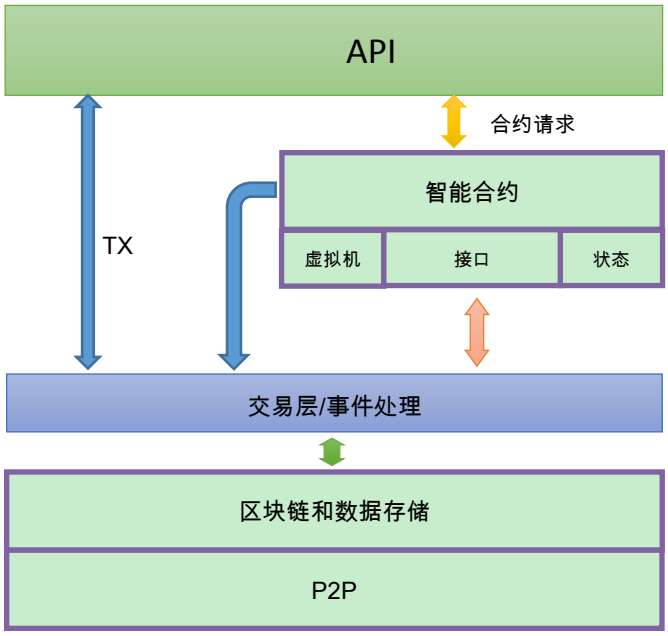
MOAC 是解决上述所有问题的解决方案。 它是区块链的区块链。 MOAC 本身将部署在具有大量验证节点的公共网络中。 它提供以下内容：

1. 分层配置结构
2. 交易，智能合约和数据访问支持
3. 数据流，控制流程和处理单元，形成一个分布式的 Von Newman 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。
6. 鼓励具有较小处理能力的用户参与验证过程。

[体系结构]

分层结构



1. P2P 网络层。 这个层定义了 p2p 协议，我们将采用 GOSSIP。
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. 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 处理最终用户输入并获取下层的输出及返回。

MOAC 拓扑结构

目前，MOAC 采用类似于 Ethereum 的 POW，加上创新的分片技术，实现底层的共识支持，另外在此基础上加上更多的创新：

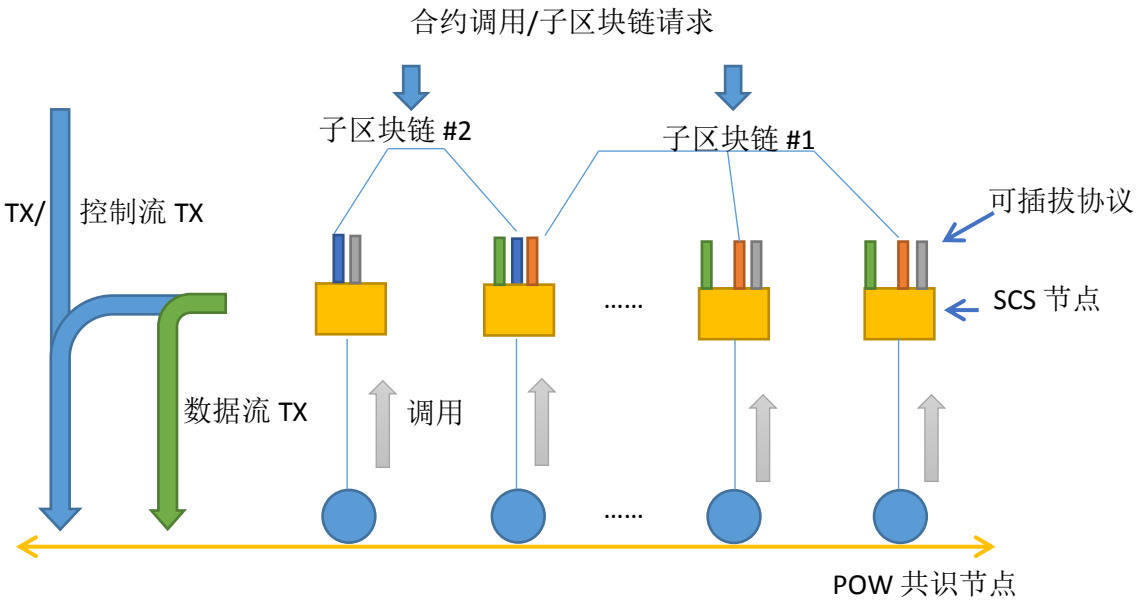
1. 数据存储与交易分离。

2. 共识在交易集和数据存储集上达成一致。
3. 智能合同由交易集调用，但智能合约状态不直接链接到交易。
4. 智能合同以异步方式进行调用。

系统中的三种基本交易类型：支付交易 TXp，数据存储 TXs，控制流 TXc。 它们在底层 POW 共识节点中处理。 所有节点都收敛于一个全局一致的状态。

除了 POW 对交易和数据存储集的共识外，每个 POW 节点都与一个智能合约服务器相关联.

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）包含在控制流 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。

[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同交易。此外，在此架构上产生部署子区块链是非常方便的。

用户可以使用智能合约配置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 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。

[经济效益分析]

验证节点可以从两方面通过其贡献的计算能力来获益。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 只能花费非常有限的资源进行验证。

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 设置中，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。 1Sand = 1000 Xiao。

Block#	Reward (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支付。 一个是通过交易。 另一个是智能合同或子区块链。

Transaction Type	Fee	Pay to
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

智能合约请求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。

[ICO 计划]

预发行货币总额 250 百万。 分配如下：

至多 50% 用于 ICO ， 价格 BTC:MOAC = 1:10,000 , 前三批分别享有折扣：

1-500 BTC: 比例为 1:13,000

501-1000 BTC: 比例为 1:12,000

1001-1500 BTC: 比例为 1: 11,000

1501 BTC - : 比例为 1:10,000

30% 用于开发团队

10% 用于运营

余额为保留基金

这个 ICO 的目标是至少有 500 个 BTC。 如果我们没有达到最低目标（500 BTC），所有捐款将被退还。

所有 BTC 将分配给创始团队和支持团队。 ICO 的目的是支持 MOAC 的开源项目开发，营销和广告，交易所，运营，或任何我们认为可能增加 MOAC 价值或 MOAC 使用的任何内容。 一旦钱包/软件在 2017 年 12 月 1 日之前发布，所有 MOAC 货币都可以发放到投资者。

[附录]

MOAC 货币每年的总量:

ICO	250,000,000
1st 年	256,000,000 (约)
2nd 年	259,000,000 (约)
3rd 年	260,500,000 (约)
4th 年	261,250,000 (约)
5th 年	261,625,000 (约)
6th 年+	261,625,000 + 300,000 * n