BOSCore 技术白皮书

2018年 9月

- 参考

背景

EOS的出现给区块链带来了新的想象力，主网启动短短几个月以来，版本经历了几十次升级，不仅稳定性得到了很大提高，并且新功能也逐步实现，各个节点团队也积极参与建设EOSIO生态。让人更加兴奋的是，EOS已经吸引了越来越多的开发团队，当前已经有数百个DApp在EOS主网上面运行，其交易量和流通市值远超以太坊，可发展的空间愈来愈广阔。

在EOS主网逐渐发展的过程中，我们发现了一些偏离期望的地方。作为最有竞争力的第三代公链，大家希望看到的是能够有更多、更丰富的应用能够在EOS上面运行，开发者会将EOS作为自己应用开发的首选平台，但是由于目前EOS的资源模型的限制，导致了很高的使用成本，包括为用户创建更多的账户，以及部署运营DApp需要的较高成本。针对白皮书中要实现的上百万TPS需要的关键技术IBC，一直没有进行推进，主网多次出现CPU计算资源不足的情况，更是加剧了对跨链通讯需求的迫切性。此外，由于EOSIO采用的Pipeline-DPOS共识机制，一个交易需要近三分钟才能保证不可更改，虽然相较比特币、以太坊是有很大的进步，但是这也给EOS的应用场景带来很大限制，快速支付只能聚焦于小额转账，大额转账必须要等待足够长的时间才能保证不可更改，这就限制了链上、链下用户支付体验。

除了上面提到的情况，还有很多其他改进想法一直在我们社区进行活跃的讨论，由此，我们觉得应该基于EOS进行更多的尝试，让更多的开发者或者团队来参与到EOSIO生态的建设中来，一起为区块链在不同行业不同场景中的落地做出一份努力。BOS作为一条完全由社区维护的EOS侧链，在继承其良好功能的基础上，会进行更多的尝试，并且会将经过验证的新特性、新功能反哺给EOSIO生态。

概述

BOS致力于为用户提供方便进入并易于使用的区块链服务，为DApp运营提供更友好的基础设施，为支持更丰富的应用场景努力，为DApp大繁荣进行积极尝试。除了技术改进以外，BOS也会进行其他方面的尝试。比如，为了提高用户投票参与度，可以通过预言机技术来针对符合明确规则的账户进行激励；BOS上面的BP的奖励会根据链上DApp的数量、TPS、市值、流通量等指标进行调整，鼓励每个BP为生态提供更多资源；一项社区公投达成的决议将会尽量被代码化，减少人为的因素在里面，流程上链，保持公正透明。

BOS链的代码完全由社区贡献并维护，每个生态参与者都可以提交代码或者建议，相关的流程会参考已有开源软件来进行，比如PEP(Python Enhancement Proposals)。

为鼓励DApp在BOS的发展，BOS基金会将会为其上的DApp提供Token置换的低成本的资源抵押服务，降低DApp前期的运营成本；此外还会定期对做出贡献的开发者提供BOS激励，以便建立起一个相互促进的社区发展趋势。

共识机制

EOSIO采用的是基于流水线的拜占庭容错机制 (Pipelined Byzantine Fault Tolerance)，对于一个Block需要经过Propose、Pre-Commit、Commit、Finalize [1] 几个步骤，最后不可更改的块范围由Last Irreversible Block (LIB) 标明；一笔交易基本上需要约3分钟 (理论最低为325个出块时间，即162.5秒) 才能进入LIB，虽然相比BTC、ETH等其他数字通证的交易可靠时间有很大提高，但是对于很多应用场景来说还是有很大限制。比如支付场景，由于不能立即确定该笔交易最后是否成功，需要等待一段的时间才可完成商品的交易，这就增加了很多限制。

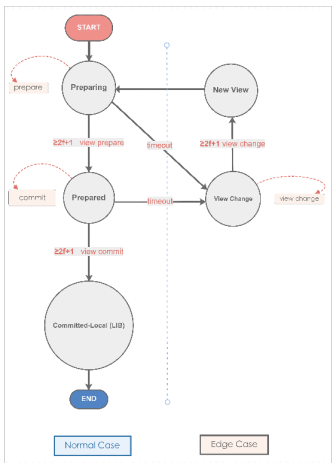
造成交易需要较长确认时间的原因是在DPOS BFT共识算法中，所有块同步后的确认信息都只有轮到该节点出块的时候才会被广播出去。举个例子来说，在BP1出块(所出块为BLKn)，BP1 ~ BP21轮流出块的情况下，BP2 ~ BP21会陆续收到并验证BLKn，但所有BP只能等到自己出块的时候才能发出对BLKn的确认信息。

在分析过EOSIO共识算法的问题以后，为了缩短一笔交易变成不可更改状态的时间，BOS将采用PBFT (Practical Byzantine Fault Tolerance[2]) 来替代Pipelined BFT，让BP之间实时地对当前正在生产的区块进行确认，能够使整个系统最终达到接近实时的共识速度。

BOS的共识算法是在 PBFT 理论基础上，结合EOSIO代码进行的改进，在保证实现拜占庭容错的前提下，会进行以下部分的改动：
1. 保留Pipelined BFT的BP 轮流出块的机制，并且和EOS一样对同步时钟和出块顺序进行强约束
2. 移除Pipelined BFT共识部分的逻辑，即去掉原本出块时的implicit confirm 和 (explict) confirm 部分，避免在极端情况下与PBFT的共识结果产生冲突
3. 共识的通讯机制使用现有p2p网络进行，将会使用PBFT机制广播prepare和commit信息，并保证通信成本在可接受范围内。

4. 采用批量共识替换PBFT中对每个块进行共识的要求，通过一次广播多个块的相关信息，以此来逼近实时BFT的理想状态并减轻网络负载。

BOS PBFT中状态描述如下：
pre-prepare，*指出块节点出块以后，广播给网络里的所有其他中继节点。可以类比为EOSIO中BP出块并广播至全网。*
prepare，指中继节点收到请求后向全网广播将要对此请求进行执行。可类比为EOSIO中所有节点收到块并验证成功后广播已收到的信息。
commit，*指中继节点收到足够多的对同一请求的prepare消息，向全网广播执行此请求。可以类比为EOSIO中节点收到足够多对同一个块的prepare消息，提出proposed lib消息*
committed-local，指中继节点收到足够多对同一请求的commit消息，完成了验证工作。 可以类比为EOSIO中的LIB提升。
view change，*指出块节点因为各种原因失去其他节点的信任，整个系统更改出块节点的过程。由于EOSIO采用了Pipelined BFT的算法，所有BP是通过投票的方式提前确定的，在一轮出块中整个系统的出块顺序是完全不变的。当网络情况良好并且出块节点没有发生改变的时候可以认为不存在view change状态。当引入PBFT后，为了避免分叉导致共识不前进的情况，加入view change机制，抛弃所有未达成共识的块进行replay，不断重试直到继续共识。*
checkpoint，指在某一个块高度记录共识证据，以此来提供安全性证明。当足够多的中继节点的checkpoint相同时，这个checkpoint被认为是stable的。checkpoint的生成包括两大类：一类是固定k个块生成，另一类是特殊的需要提供安全性证明的点，例如出块BP排名发生变更的块。



通过对现有EOS主网进行的观察来看，全球节点之间的网络延迟大部分都在1s以内，按照BOS PBFT的共识机制在绝大多数场景下可以做到3s (pre-

prepare, prepare, commit) 不可更改。将一笔交易的可信时间从分钟级缩短成秒级将会让很多应用场景可以在BOS链上面进行实现。

链间通讯

EOSIO技术白皮书中把链间通讯作为实现高并发的解决方案，以链间通讯技术构建多条链间的流转通道，通过水平拓展的方式来增加EOSIO整个生态的承载能力。跨链通讯的本质问题是解决对各个链之间交易可信度的证明。异构的区块链系统（例如EOS、ETH）因为区块生成速度、内部数据结构、共识机制等都有很大差异，因此异构去中心化跨链的实现难度相对较高，相比而言而对于以EOSIO为基础的不同链之间的交易验证更具有实际意义。

去中心化跨链通信的基础是轻客户端（Light Weight Client）和交易验证技术（SPV/Simple Payment Verification）。轻客户端是由区块头构成的一条链，不包括区块体，所以轻客户端只占用很小的空间；SPV技术使用merkle路径来证明一个交易是否存在于某个区块中[3]。

BOSCore采用的跨链方案优势有以下几点：
1. 完全去中心。轻客户端在智能合约中实现，当初始化了正确的起始区块信息，合约就可以完全自主验证后续所有区块的有效性，无需依赖对中继或合约外部信息的信任。
2. 轻量。轻客户端无需连续同步原链所有区块头，只根据需要同步区块链的一部分片段即可获得可信区块用于验证交易。
3. 快速的跨链交易。一个跨链交易从产生到在目标链上产生对应交易只需要不到3分钟时间。
4. 跨链交易并行。不同的跨链交易之间互不影响，可以并行执行，因此支持很大的并发量。
5. 安全。由于采用了生产者签名效验和严格的逻辑检查，可以保证轻客户端自身的正确性，无法被恶意攻击，因此可以安全的验证交易的真实性。

BOS基于该IBC方案提供与EOS主链的兑换通道，EOS可以十分方便的在BOS侧链和EOS主链之间流通，包括EOS上面的其他优质数字通证；与此类似，BOS将会推进与其他基于EOSIO技术的侧链建立流通通道，让整个

EOSIO生态开始迈进生态网络的建设，BOS将会作为一个核心流通纽带，加速整个EOSIO生态的发展与进化。

锚定币

为了丰富整条链的经济生态，BOS除了使用IBC机制实现与EOSIO主网建立流通渠道以外，还将采用“公证人机制”，联合世界顶级交易所将BTC、ETH映射到BOS链上。通过该可信通道，BTC、ETH都可以在BOS上面轻松进行跨链流通。这意味着对于BOS上面运行的DApp来说，在支持EOSIO生态数字资产的同时，可以将更多其他共识机制的数字资产方便的进行支持。此外，该方案也可以作为提高其他低TPS数字通证流动性的方案。

BOS将会提供一种机制，可以针对不同的数字通证发行 1 : 1 的锚定币，并且通过BP多签的方式来针对可信中间人的身份进行认证。每个可信中间人都需要抵押一定的BOS作为保证金。具有实力和公信力的组织或公司可以发起“公证人”身份的申请，在通过前30名BP中有25名BP通过以后就可以进行锚定币的发行。

账户

低保

从EOS主网上线以来，对于普通持币人往往都会遇到由于抵押资源不够导致转账失败的情况，这种情况下用户也无法自救，就只能求救于他人，导致了很差的用户体验，提高了使用门槛。

对于一条链来说，活跃用户量的增长在促进链发展的同时，更会促进链上DApp的发展，对整个生态都至关重要。为了解决这个问题，BOS链进行了改进，可以通过链的参数来调整分配给每个用户免费的资源额度，相当于BOS链上的“低保”机制。这样大部分用户日常的转账等基本需求都能被满足，无需再为较少的初始资源抵押担心无法使用链上功能。对于更多使用需求的用户，超出低保额度的资源使用仍然需要进行抵押。

红包创建账户

对于EOSIO主网来说，创建账户成本是一个不可忽视的问题。BOS的定位是为丰富链上DApp为目标，所以也提供了解决用户创建账户成本的方案。参考

生活场景中发红包的例子，BOS会将社区开发的“红包DApp”进行内置，并且会由BOS基金会持续提供一定量的免费创建账户数量。其他DApp项目方或者组织都可以方便的通过红包的形式给用户免费创建账户。红包DApp相关的功能可以通过官网访问，也可以通过每个BP提供的接入点进行访问。

ThunderNode

通过改进共识机制，BOS链上的一笔交易的可靠时间可以缩短到3s以内，这个时间相比中心化的系统还是有些差距。所以为了满足这种接近中心化系统的需求，BOS上面会提供一种可以达到毫秒级确认的节点，称之为ThunderNode。

类似于闪电网络，ThunderNode 的交易大部分都是在一个局部网络完成，ThunderNode 会保证交易在BOS链上可见并不可更改。使用者一旦决定使用某一ThunderNode就需要锁定部分余额，这部分余额只可以在该ThunderNode进行使用，在决定不使用时可以将剩余BOS解锁，恢复正常使用，用户选择使用那个ThunderNode以及锁定对余额都需要在BOS链上发送注册并等待生效以后才能开始使用。

ThunderNode的运营者是完全开放竞争的，没有硬性的限制条件，使用者也是可以根据自己的需要来选择，ThunderNode的提供者可以通过收取一定手续费用的方式来获取奖励。

更可用

更安全随机数方案

目前EOSIO上面已知的随机数方案基本上都是结合可预知的多个字段，比如blockid、timestamp等作为随机种子的一部分，然后再结合用户端、DApp项目方或者直接由DApp方线下生成。该类方案存在一定的安全风险，无法降低对DApp项目方可信度的依赖，以及无法避免一些重放攻击(比如INLINE_ACTION形式)。针对以上问题，BOS启用了block_extension特性，提供了 bpsig_action_time_seed 方案，bpsig_action_time_seed 不仅可以防止重放攻击，而且还需要BP节点的签名私钥进行签名，并把生成的seed存入block_extension，便于其他节点进行验证。

结合 bpsig_action_time_seed 就可以构造出用户、节点、DApp项目方三方参与的更安全的随机数方案。bpsig_action_time_seed 的生成方式如下：

```
bpsig_action_time_seed = sign(BP_Sign_Key, F(block_timestamp, 0.
```

注：
* BP_Sign_Key : 使用BP私钥签名的目的就是避免他人进行投机计算
* F：将block_timestamp按照0.5向下取整的函数，降低BP调整时间戳来进行投机概率
* global_action_sequence: 全局action自增标识，可以用于防止 INLINE_ACTION 攻击

预言机

预言机是图灵机模型引入的概念，由于停机问题以及数学不完备性的原因，引入该概念后会得到一些标准图灵机所不能得到结果。在图灵机里它是确定性的，但在区块链中引入的预言机却很难得到理论上定义的特点，究其原因是因为区块链本身就是建立在容错逻辑之上，其本身并不要求输入的确定性，甚至允许存在欺骗行为，这也是区块链建立拜占庭容错结构之上的原因。因此在区块链的预言机与传统意义上的预言机有着本质的区别。

面对非可信预言者问题，简单的确定性计算模型显然已经无能为力，为此我们尝试着引入博弈的系统模型来解决这些问题。概括的讲，不单纯的将预言机看作是系统的信息提供点，而是将其看作博弈的参与方与信息使用者共同构建博弈模型。并通过引入惩罚机制以及多回合博弈机制来建立可信承诺，通过多信息提供点的信息选取机制达到谢林点，从而提高信息的可信性；此外通过引入检验员并加入连带奖惩机制，构建对信息提供角色的囚徒困境，进一步保证可信性。

基于上面的分析，BOS会实现一套基于博弈系统模型的预言机机制，拓宽DApp可以涉及的应用场景，让区块链技术可以和生活中的多种场景进行结合。

节点配置上链

EOSIO中一些细节做的不够到位，其中黑白名单的配置就是很好的例子，由于黑白名单配置问题就导致至少两次冻结账户失效。BOS会将黑白名单等此类公共配置信息上链，由BP多签生效，避免由于其他原因导致配置在某些点上失效，进而导致损失。BOS不仅仅会关注重要特性的开发，而且在基础细节上面也会做的更到位。

更多Plugin

对于想要实现监听一个账户具体交易情况，对于现在的EOSIO来说方案比较复杂，往往通过kafka的插件来实现。这个又是对DApp、钱包或者交易所来说很需要的一个功能。对于普遍需求的功能点，BOS就会进行支持。BOS内置 Notify Plugin，提供与History Plugin类似的使用方式，可以低成本、快速的获得账户监听功能。

除此之外，BOS还会将社区里面优秀的插件进行集成，降低编译成本，方便开发者使用。

按时区出块

EOSIO当前使用的是按照BP账户名称的字典序进行出块，从实际运行效果来看往往会导致多次的小分叉：最后2-4块不能及时广播到下一个出块BP。为了降低前后BP之间的网络延迟，BOS将会采用按照时区顺序进行出块，尽量降低物理距离以及网络抖动导致小分叉情况的出现。

BOS有计划在正常的连接网络之外，再搭建一条使用专线互联各个节点的网络，保证块数据更高质量、低延迟的传输。

BOS Toolkit

BOS所追求的其中一点就是尽量降低用户的使用门槛，并通过易用、易懂的方式来展现给用户使用，所以BOS官网会提供一个功能集合页面，该页面主要是将BOS相关特性转变成用户可用的接口，比如红包、账户管理器等工具。BOS Toolkit的定位不是钱包应用，只是提高链上功能的易用性，让好的设计发挥作用。

账户管理器

EOSIO引入了灵活的账户体系，可以针对不同权限等级、不同的动作进行相对复杂的操作。虽然该机制可以实现操作系统级的账户方案，但是对于用户来说还是过于技术和复杂。所以BOS在这方面多做了一步，让用户可以方便的使用起来。

通过账户管理器不仅可以设置账户active key的每笔、每天转账限额，对于更高级的owner权限，用户不仅要输入正确的密码，还要回答正确的问题才可

以进行使用或者导出，这样做的目的是帮助用户去理解账户权限的设计规则，提高用户的安全意识。

P2P自发现

在EOSIO的实现中，与那些节点建立连接依赖于配置文件的静态配置，从整体上面来看当一个新的节点加入时，只能通过从其他地方获取到公布的信息，但是这个公布的信息很难保证是全面且是最新的，这就会导致一些节点连接通道是片面的，进而会降低整个网络的联通质量。

BOS在这点上进行了增强，可以通过配置项决定是否将一个节点设置为可自发现，并且同样受最大连接数的整体限制，这样只要在每个团队节点中有至少1台开启了自发现，都将会帮助BOS链上的节点之间建立起一个更高互通质量的网络。

为了降低安全风险，一个节点只会向配置文件中的已有节点获取可连接的节点信息，不是无限制的自动创建连接。

生态模型

发行方式

BOS初始发行量为10亿，分配方式如下：

- 1亿进行生态空投
- 5千万直接空投EOS主网账户
- 5千万根据DApp和节点的实际情况情况进行空投
- 1亿战略伙伴基金，用于BOS链上项目投资及BOS运营
- 4亿进行生态激励，向在BOS链上产生的支付及BOS交易业务进行补贴
- 2亿进行创始团队激励，分4年解锁
- 2亿进行私募，分四期进行募集每期5千万

每年增发量 2%，分配方式如下：
- 节点奖励为 1%
- 开发者奖励 0.8%
- 治理激励 0.2%

开发者激励

增发0.8% 面向BOS生态贡献代码的开发者，由社区提出50名奖励名单，由前50名BP投票选出40名的获奖者获取对应奖励：
- 前10名获取40%
- 11到20名获取30%
- 最后20名均分30%

奖励周期3个月一次，每次奖励名额都会进行为期一周的公示，如果有合理异议，将会重新评审，每次奖励名单都会上链记录。

随着BOS的不断发展，开发者奖励会适当调整，让社区为BOS的进化提供更多动力。

治理模型

在链上生态不断蓬勃发展的过程中，未来每一条链可以理解为一个“国家”。每条链都将会拥有自己的独一无二治理模型，不同的治理模型将会使得大家走向不同方向，并在链间产生竞争，并通过自由市场模型使得开发者和用户选择最优的模型进行发展。BOS的治理模型崇尚 “Code is the law”。保障DApp的平稳发展将会是BOS的最高准则。
BOS每年增发0.2%用于向帮助BOS持有人发起仲裁的治理组织或志愿者，在BOS中任何人都可以发出仲裁，一个提案获取越多治理组织附议，其可靠性就越高。如果仲裁生效，治理组织或者志愿者可以获得2000 BOS的治理奖励。
BOS的决策或者仲裁达成方式有两种：1. 不少于15个BP同意，2. 社区公投。BOS治理中不会存在唯一的ECAF机构，但是会存在多个中立的治理组织或志愿者，对提出有效方案或者改进建议的组织或都志愿者可以获得社区激励。

注：生效标准（例如不少于N个BP同意该仲裁生效）可能会随着BOS链的生态发展而变化，且任何变化也必须遵循当前治理规则投票。

经济模型

BOS是一个对区块链世界的自由市场经济十分有意义的尝试。由于中央银行的过度干预市场以及无法保持独立性所带来的问题，以比特币为代表的数字代币以完全自由市场的理念，试图通过理性人假设（hypothesis of rational

man）来解决现实经济中无法解决的问题。但当我们回顾现代经济学的历史时，治理和自由，公平与效率始终是处于互相博弈和再平衡的过程。从奉行自由市场的古典学派，到强调政府干预的凯恩斯学派、再到强调回归市场奥地利学派，任何一个方向都不会是一概而论的，一成不变，放之四海而皆准的。

BOS希望通过以商业发展为导向，通过调和BTC自由市场以及EOS目前过度治理的情况，平衡二者之间的优缺点，同时发挥效率和去中心化的优势将区块链真正实现商业落地。

BOS支持的链间通讯功能将会影响整个区块链行业的运行方式，各类数字资产均可通过链间通讯将传统孤岛化的数字资产链接成为一个网络。包括BTC、ETH、EOS或者其他通证资产均可以在BOS链上进行交易和划转，进而可以将BOS理解为一个数字货币的自由港，而BOS所带来快速交易系统将会使得BOS 具有十分可观的吞吐量。此外，低廉的账户创建成本将会吸引来自全世界的各类商家和应用入驻，进而繁荣整个BOS生态，进而反哺EOSIO生态。
当一个用户同时持有ETH、BTC、EOS，用户可以将以上代币通过跨链通道导入BOS链，在链上创建BOS-ETH、BOS-BTC、BOS-EOS，我们将此类资产称之为BOS资产。即用户将资产带入BOS自由港，用户可以在BOS这个自由港进行消费、投资、娱乐等活动，DApp的开发商可以为用户提供各类服务，在服务的过程中，BOS资产可以在不同的BOS账户内在进行交易和转让。BOS资产的持有人可以从链上随时通过跨链通信将资产从BOS链上流通回原有的BTC、ETH、EOS链。

BOS作为一种资源将会成为整个自由港的计价单位和基础设施平台，当多种资产在BOS链上产生交互的时候BOS将会向英镑和美元一样起到价值媒介的作用。

历史上英格兰银行第一次将足额黄金与英镑进行等额的双向兑换，结合以罗马法为基础的法律进而形成良好商业氛围吸引了当时全世界最优秀的资源，并最终确立了伦敦国际金融中心的地位，BOS也将通过完善的基础设施、良好的商业氛围来打造区块链的商业中心。

总结

BOS的目标是建立起一条支持更多DApp，能把更多现实需求和区块链结合起来的EOSIO生态链。从区块链的进化角度来看，BOS除了作为DApp的首

选基础链以外，还可以作为一个各种异构链通证的流通链，做区块链世界的自由港。BOS来源于社区，也会在社区的维护下更好的发展。

参考

[1] DPOS BFT— Pipelined Byzantine Fault Tolerance
[2] Practical Byzantine Fault Tolerance
[3] Chain Interoperability