合约大陆：打造高性能应用项区块链框架

拟稿

ContractLand Foundation

合约大陆基金会

team@contractland.io

www.contractland.io

引言

现今的区块链技术已经慢慢在匿名支付，廉价汇款，无信任数字资产交易所和智能合约等应用场景上展露头脚。然而，各公链系统仍然受制于可扩展性和可延伸性等方面的问题，这些问题严重限制了各公链生态系统内去中心化应用的大规模落地。

在本文中，我们提出通过高性能特定应用链来解决区块链的可扩展性限制。为了有效解决以上问题，合约大陆将从共识层，链间通信层等其他逻辑层分别优化，从而搭建一个高效地平行可扩展架构。

1.介绍

比特币的问世使区块链技术渐渐走入人们的视野，这个革命性的技术使任何人都可以在开放的金融网络中，在无需信任第三方的前提下，自由地拥有和转移资产。以太坊和智能合约的诞生使区块链技术得到进一步推广。与此同时，智能合约的概念赋予了区块链技更大的责任和能力，它不仅改变了人类信任和交互的最基本形式，任何人都可以使用智能合约在区块链世界中通过运行开放代码来建立契约关系。然而尽管有区块链技术给我们很多美好的承诺和遐想，但是我们还没有看到现有区块链技术在现实生活中有任何的重要部署。我们认为限制其发展的主要原因可归结为以下三个：

- 可扩展性：区块链系统在数据处理，传输带宽和数据存储等环节消耗了巨大的资源。在网络传输高峰时，用户发起的交易往往没有办法得到及时的处理。

- 可分离性：单独一个区块链系统往往没有办法同时满足该生态系统内的多个应用的最佳配置需求，换而言之，公链系统不可能根据生态上的某个应用而改造整个生态。

- 可交互性：各个公链系统是相互独立的，公链内的数据也被局限于系统内部，最终也就导致了不同系统之间无法彼此通信。

截至目前，大多数真实的区块链项目的结算速率小于平均每秒 30 笔交易，而像比特币和以太坊等共识机制为工作证明共识机制（PoW）的公链系统的速率尤为低下。其主要问题来自于出块者选举过程，整个过程是随机执行且会导致系统长时间的冻结。比 PoW 共识机制效率更高的区块链系统，比如使用委托证明共识机制（DPoS）的 EOS [1]，又比如授权证明共识机制（PoA）上运行的以太坊[2]，这两种系统均可以在高性能消费级硬件上处理超过每秒超过 3,000 笔的交易。以上的效率优化是通过将区块链的出块者选举和交易序列化两个步骤剥离到两个独立的平面中分别实现。出块者是随时间推移而改变的，在每个时间窗口内，出块者的选举都是一个独立事件。

然而，上述系统仍不足以支持高迸发的交易量，一个基于 Web 的简单应用程序有可能会产生每秒数以万计的交易请求。由于公链系统内的所有应用程序共享整个网络的处理机能，单个应用程序的短暂火热可能会造成整个网络的不必要拥堵，从而影响网络内其他应用的用户体验。用单一区块链系统解决所有问题的概念是不切实际的。现代公链系统虽被誉为“世界计算机”，但其逻辑并不适合运行搭建多个大型应用程序。且我们不难得出一个结论，仅通过优化共识机制来改进区块链系统的性能是不够的，如何让区块链系统更好的服务于实际应用程序才是让区块链技术更好落地的关键。

因此我们认为，并行扩展是搭建一个可扩展地去中心化平台的合理探索方向。根据这个判断，合约大陆将应用程序层与共识层分离，再根据各个应用程序的不同属性需求定制特定区块链系统（或称应用链），与此同时实现链与链之间的通信交流。

2. 概要

合约大陆搭建一个能够支持高迸发交易的区块链框架。我们可以在这样的框架来上来部署一些针对不同应用的应用项区块链，以此替代在公链网络上搭建应用程序的解决方案。应用项区块链应该具有与公链系统相当的安全性和去中心化属性，同时由于网络的算力能够集中处理单个应用程序，而使数据传输速度和用户体验得到大幅提高。

2.1 系统概览

为了能够搭建一个可以支持海量交易的高性能公共账本，我们需要同时解决去中心化，可扩展性和可交互性三个问题。所以合约大陆决定从头改造整个网络架构，这其中涵盖了从底层的区块链层到跨链通信层，一直到特定应用程序的应用逻辑层。每一层设计都是模块化定制，且逻辑最简化。

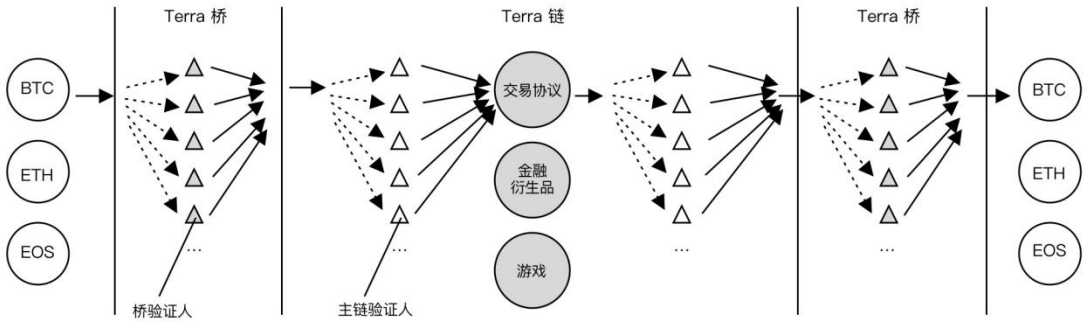

图 1:特定应用链架构概览

2.1.1 链层

与现有的公共区块链不同的是，合约大陆在设计区块链层时就把支持高迸发交易作为首要目标。它不会继承其他区块链的全部功能，并把之前在区块链层实现的应用逻辑嫁接到应用程序层实现。与 EOS 或以太坊或其他开放式公链相比，合约大陆在初始设置时，会严格控制区块链上逻辑执行的权力，同时也会限制智能合约的数量，确保网络网络算力可以最大限度服务于某个应用程序。这是一种有意识的设计策略，旨在减少不同应用程序在同一个公共区块链系统中稀释交易吞吐量，从而避免网络拥堵等问题。鉴于每个层在设计上是模块化的，不同的应用程序逻辑可以分别部署在不同的应用链上，且链链在之间可自由相互通信，最终从而实现平行扩展。

2.1.2 跨链桥层

跨链桥为各应用链提供了在多链生态系统中必备的跨链通信能力。它也是整个框架的一个关键组成部分，因为它不仅允许各个应用链可以相互通信，还使它们能够与其他公链网络进行通信。就像区块链层架构类似，跨链桥也有独立的共识机制和激励机制，在确保安全性和去中心化属性的同时服务跨链交易。

2.1.3 应用层

如上文提到的，应用程序层的主要包括为特定应用服务的程序逻辑，可以通过任何 EVM 兼容的语言（如 Solidity [3]）进行编写。由于整个系统的模块化，应用程序的逻辑不再局限于某个特定的行业，通过改编该模块逻辑，即可应用于诸如交易所，支付，金融和游戏等其他应用场景。

3．系统参与者

合约大陆系统的运转和维护主要依靠三个基本角色：主链验证人，桥验证人和委托人。

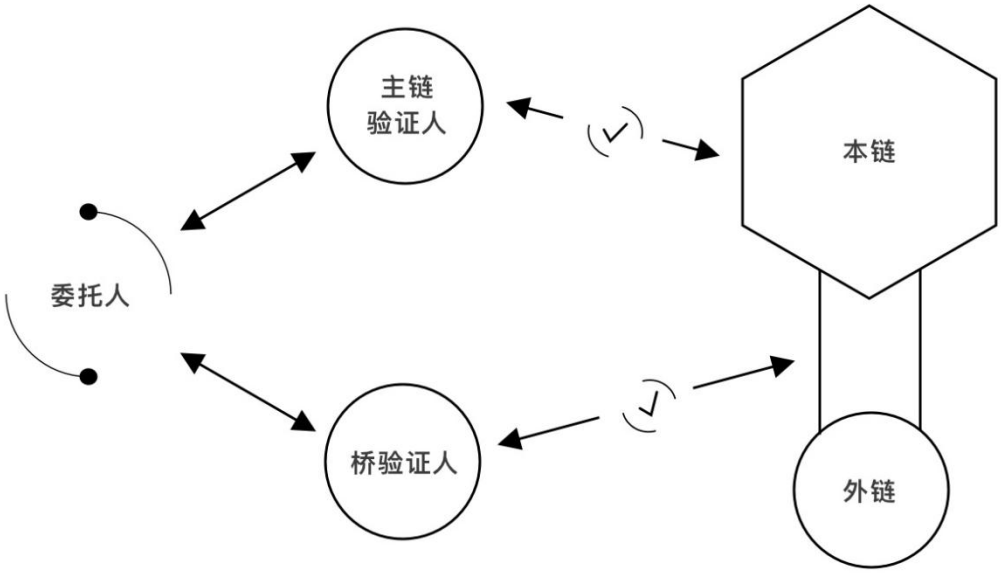

图 2:应用链内的各角色间关系

3.1 主链验证人

主链验证人是整个系统的中最重要的角色，他们的主要职责是确认主链上新区块的生成。主链验证人的基本资格取决于是否在智能合约内存入足够的数字货币债券，同时我们允许系统内的其它通证持有人将通证存入某个或某几个验证人智能合约内，委托验证人代理行使权力，因此验证人的抵押通证不一定全部归验证人所有。

验证人要维护区块链网络的正常运行，必须在一个稳定且高带宽的网络环境下运行主链客户端。验证人的具体任务包括：维护过程包括数据接收，交易验证和发布候选块。除此之外，验证人还负责批准新的跨链桥集成。合约大陆核心开发团队虽然负责与其它公链的跨链协议的评估与开发，但是最终新桥是否能加入生态系统而是由主链验证人投票表决决定。

在一个健康积极的生态系统中，验证人的行为准则必须要遵守系统内的共识准则，未履行其共识义务的验证人也应当受到惩罚。验证人的一般违规行为将导致他们失去部分担保债券。而恶意违规行为，例如双重签名或密谋制造无效区块，给系统带来严重损失的，将会导致整个抵押债券的损失。不管是对于一般违规还是恶意违规，被没收的抵押债券大部分将作为奖励奖与举报人，和其它诚实的验证人，剩余的部分将会在智能合约内烧掉。

在某种意义上，验证人类似于当前 PoW 共识下的区块链系统内的矿工。

3.2 桥验证人

桥验证人与主链验证人扮演着类似的角色，而维护的对象由主链变成了桥。每个链上的跨链桥拥有独立的共识机制和安全机制，这个独立生态系统的维护者就是桥验证人。与主链验证人类似，每个桥验证人必须运行一个桥客户端，并负责相对应的节点作为两个不同区块链间的信息中继，跨链传导消息。未能履行职责的桥验证人员将同样受到没收抵押债卷的处罚。

3.3 委托人

委托人是通证持有人，也是主链验证人或桥验证人履行职责的担保方。他们在系统所内发挥的作用是将个人的数字资产提供给所信任的验证人做信用背书，作为他们所承担的资本风险的补偿，委托人可分享验证人收取交易费用的收益，而委托人收益的多少则与委托人出资成正比。

4. System Design 系统设计

整个区块链系统可以大致分为四个部分：链操作系统，共识机制，跨链交易协议和应用程序协议。

4.1 链的运转原理

应用项区块链系统结构是与以太坊系统有很多相似点。一方面因为它们的系统都是基于状态的，且状态可以通过映射地址找到账户信息。另一方面两种系统通过记录账户余额（以防止重置）和交易计数器来记录账本。两个系统最大的不同之处在于应用链的交易不能在已部署的智能合约中发生。为了使应用链的逻辑最简化，所以不会保留除服务应用程序逻辑之外的其他功能，它不支持公共部署智能合约。

应用链的虚拟机将基于 EVM，在保持其图灵完整性的前提下，通过一些修改使逻辑最简化且足以支持应用层逻辑。在应用链内可能会有许多内置合同（类似于以太坊地址 1-4 的 n 合同），合同内会注明平台规则和参与者职责，其中包括共识合同，验证人合同和许可合同等。

可供公众使用的功能将消耗固定数量的平台计价通证（Gas），在所有情况下都将收取固定费用。虽然从理性角度考虑，应用中的通证消耗应该取决于功能的不同收取不同 Gas，但在这里为了避免区块链层和应用层之间的逻辑耦合，所以将应用层中交易 Gas 设计为恒定值。

4.2 共识机制

合约大陆是通过现代异步拜占庭容错（BFT）算法而产生的一系列的区块的底层共识。该算法是受到 Parity Aura 的启发，Parity 的权威证明共识（PoA）的具体实现 [4]。 PoA 是一种新的 BFT 系列算法，可在一组可靠的验证人中实现容错。对于联盟链而言，这样的共识机制是足够满足各方面的需求，但应用链与联盟链不同，我们希望在一个完全开放和公开的环境下，无需任何信任的中介机构或组织维护整个生态系统。因此，我们需要一个选拔验证人的机制，并用合理的奖励激励他们诚实履行验证人职责。根据以上提到的要求，合约大陆将涉及一套基于 PoS 的验证人选择标准。

4.3 签封机理

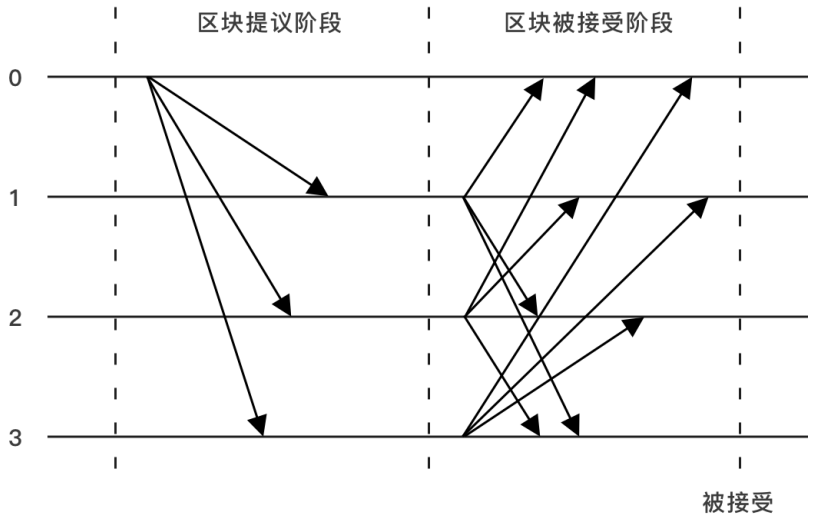

图 3:信息在验证人间传播并达到共识。

（在这个图示中，0到 3 分别代表个验证人 0，1，2 和 3，且该步骤的出块人是验证人 0）

首先，我们假设网络是同步的，并且所有验证人的节点可以在同一 UNIX 时间 t 内同步。每个步骤的索引 s 是由每个验证人计算出的 s（s = t /每步时间）决定，其中每步时间是一个固定的常数时间。步骤 s 的出块者的选举代码为 l（ l= s mod Ns 除以 N 的余数）标识的验证人。

验证人在本地的主要职责是维护两个队列，一个是交易列 Qtxn，另一个是待处理区块列 Qb。每个已发布的交易都由验证人收集入交易列 Qtxn。对于每个步骤，出块者 l 将所有交易列 Qxn 中的所有交易放入区块 b 中，并将其广播给其他验证人（区块提议的过程请参考图一）。然后每个验证人将自己接收到的区块发送给其他验证人（Round Block Acceptance）。如果最后所有验证人都接收到相同的区块 b，则验证人将把区块 b 排入区块列 Qb 中。在区块 b 传播的任何一个阶段，若有任何一个验证人收到的区块不是由当前出块者发出，该区块应被拒绝接收。出块者不管在什么时候都应该发送一个区块，如果网络内无交易递交，出块者必须发送一个空区块。如果验证人在区块广播期间对被广播区块

有所异议，可触发投票环节以确定当前的出块者是否有作恶，决定是否将出块者的角色剥夺。验证人可以对当前出块者的以下三种恶意行为进行投票：（i）它没有发出任何区块，（ii）它提出了比预期更多的区块，或者（iii）它已经向不同的验证人发出了不同的区块。投票环节是通过智能合约实现的，当票数过半时领导者 l 将从合格验证人的名单中被剔除。当发生这种情况时，区块列 Qb 中由出块者 l 通过的所有区块将从序列中被删除。请注意，出块者行为不当可能是由系统故障（例如，网络异步，软件崩溃）或拜占庭式故障引起的（例如，出块者已经被之前的恶意行为所影响）。

4.4 最终性

假设网络是同步的，且消息传播的时间长为 t，让 SIG_SET（B）等于区块集 B 内所有区块中验证人的签名集：

$$SIG\_SET(B)=\{a|\ \exists b \in B:AUTHOR(b)=a\}$$

如果存在以一条以 C [K ..]结尾的有效链 C，其中 SIG_SET（C [K ..]）的绝对值大于 n / 2，则 C [K]及其所有之前的区块将被最终确认。

最终区块的确认原则是最公平公正的多数投票原则。在此设置中，2f +1≤n，因此故障节点无法自行生成一个区块。

4.5 验证人的选举

候选验证人通过将通证存入智能合约作为抵押来参加验证人的选举。 每一个候选验证人必须存入至少为 S 价值的通证。存入抵押合约超过 S 的用户都可以成为绑定验证人。鉴于总供应量为 T 个通证，理论上最在任意给定时间最多有 N 验证人，即 N <= T / S. 而实际情况中，我们预计至少有总量 T 的 20％通证将在流动性市场中自由运转，这就意味着最多只有 80％的 T 将被存入合约作为验证人的抵押。

抵押合同管理验证人名单。它都包括：

- 当前验证人账户
- 最近绑定的候选验证人账户，且将会在下个区块成为验证人

- 已将抵押通证存入委托给验证人账户
- 每个验证人的抵押通证数量
- 一般和作恶行为证明和惩罚逻辑

这个合约还可以处理以下情况：它允许用户递交成为绑定验证人的申请（合同内会表明要求），并将权力委托给另一个指定代理人；对于已经成为绑定代理人的用户，它同样可以接受已绑定用户的退出申请；合约还可验证验证人的不当行为证明并执行相应的惩罚。

4.6 常见攻击

在这一部分，我们将介绍 PoS 共识下的区块链系统面临的一些常见攻击及其解决方法。

4.6.1 无利害关系

无利害关系是形容验证人通过投票给多个存在逻辑矛盾的区块以有效地打破安全防护，且攻击成本较低。

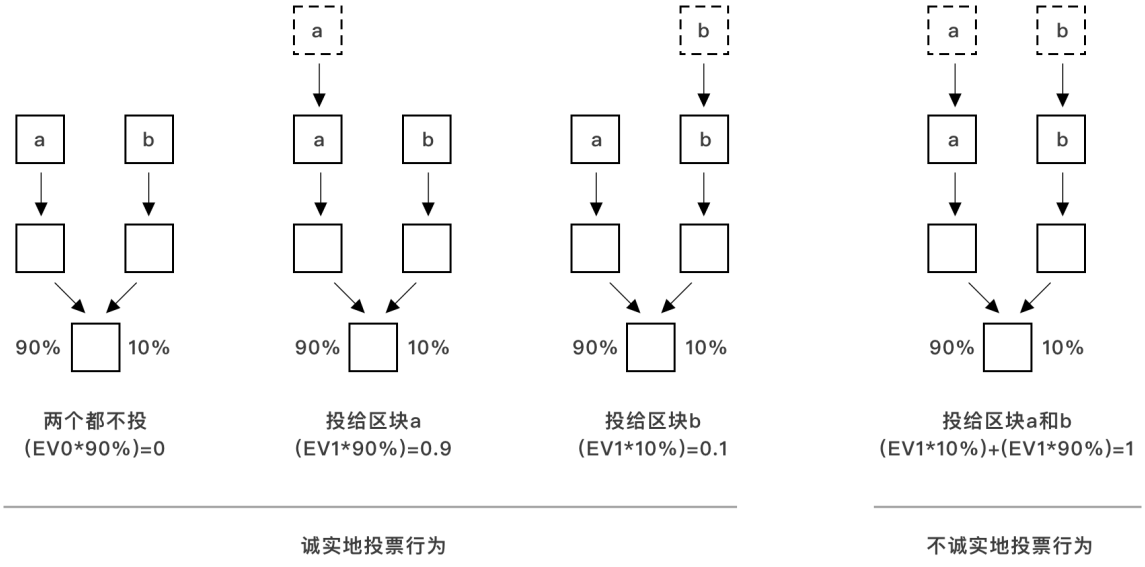

图 4:投票给不同区块的预计收入

（图中可以看出，在 PoS 系统中，同时投票给两个相互矛盾的链可获得最大的利益）

“单纯“的 PoS 共识很容易受到这些攻击。对于验证人来说一直保持（投票）区块链系统单一性缺乏经济鼓励，收入上远不如给几跟链相互冲突的区块链系统投票回报高，当一条链分叉之后，矿工可以获得更多的新区块奖励。在 PoW 共识下，上面提到的多链挖矿的“惩罚”是矿工必须在物理上将不同链的哈希功率分开，这使得多链挖矿的成本更高，受益反而降低。

最原始的 Aura 版本已经包含了对验证人的拜占庭行为进行投票的机制，其中也包含了关于验证人投票给不同的区块。而在应用链的共识机制中增加了一项额外的经济惩罚，以进一步抑制这种行为，拜占庭验证人的抵押通证会通过燃烧的形式被没收。这个概念在海外程序员社区里被广泛地称为“slasher”，翻译成中文可理解为“斩断机制”，是由以太坊创始人之一 Vitalik Buterin [5]最早推广开来的想法。

4.6.2 远距离攻击

在 PoW 共识下的区块链系统中，最长的链也是全网拥有最大哈西功率的一条链。要想从过去的一个区块上创造一个分叉链需要消耗的大量计算功率和资源，而使分叉链在短时间内生成足够多的有效区块赶超主链更是难上加难。

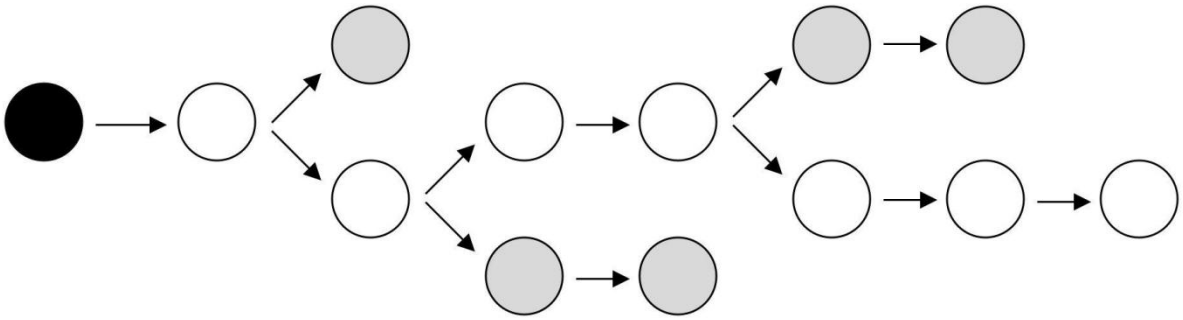

图 5:PoW 共识下的主链应该是有最多区块的一条链

（在这个图示中，主链是由透明区块构成的链）

在 PoS 共识机制的协议中，最长的链则不一定可以被判定为主链，因为 PoS 系统中的验证人能够在短时间内快速制造出超过主链长度的一条链而不会花费太多成本。与 NAS 问题不同，燃烧抵押品的惩罚措施并不能防御验证人制造这种远距离的攻击，因为验证人可以放弃验证人身份并撤回其抵押款。一旦恶意验证人退出，它就可以建立一个分叉，再也不用担心被“斩断”。

应用链的区块最终性和密封机制天然的帮助我们抵御这种远程攻击。区块最终性的规则指的是，任意一个应用链 C 得倒超过 N / 2 个验证人验证过之后就被确定为主链，且决策不

可更改。因为由作恶领导者提出且不符合共识的区块已经被其它验证人拒绝，从链 C 上被剔除。而攻击者将也被剥夺验证人资格并被没收押金。

4.6.3 DDoS

分布式拒绝服务攻击（DDoS）在云计算领域是常见的攻击形式[6]。对于区块链网络来说，DDoS 攻击可以影响节点的正常运行，扩大系统攻击面。例如，一次执行良好的 DDoS 攻击可能会使很大一部分验证人节点掉线，在此期间，攻击者可以趁机获得足够大部分的验证功率来接管网络。在我们的设计架构中的验证人存在绑定关系，很可能称为 DDoS 攻击的目标。

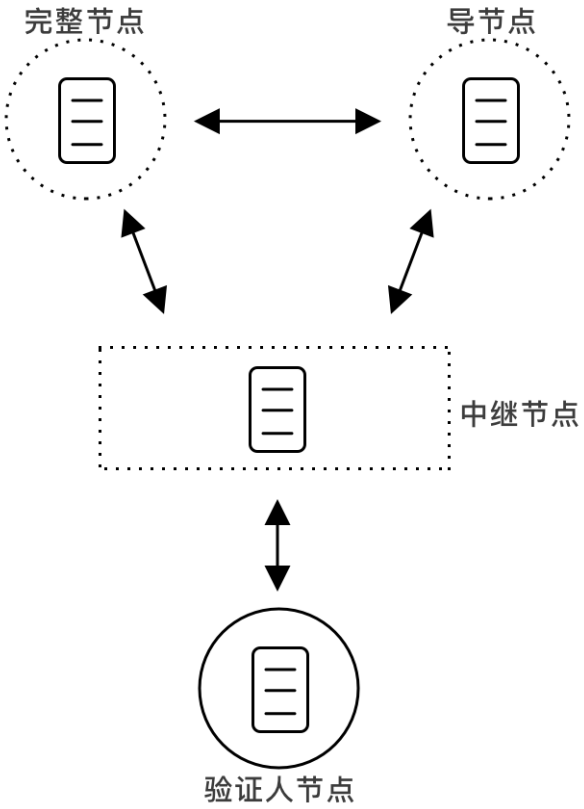

图 6:中继节点负责连接验证人节点和公共网络

对于 DDoS 攻击，除了一些验证人常用的预防措施之外，合约大陆所设计的框架还提供了一个额外的保护层，其中包含名为 Sentry Nodes 的专用类型节点。 Sentry Nodes 是借鉴了哨兵建筑模式的概念。他们充当验证人节点的守护人，并为验证提供对网络其余部分的访问权限。守护人应该保持与网络上的其他完整节点连接，而验证人节点在公共网络内保

持隐身状态。 Sentry 节点可以是动态平衡的，该节点不仅会保持与彼此的某些随机子集持久连接，同时还应该接受从验证人节点及其备份直接传入的连接。

4.7 链间通信

该框架的一个重要组成部分就是链与链间的通信。而跨链的通信正是通过跨链桥的概念实现的。概念本身的逻辑很简单：在被连接的链中执行的交易（根据该链的逻辑）能够实现将交易转移到应用链中。为了使逻辑最简化，风险最小化和前期结构最优化，这些跨链交易际上与标准的外部签名交易是不加以区分的。

4.7.1 桥的运作原理

该桥是一种双向挂钩机制，通过两个桥契约（ “契约” 在这里指的是其链中的可执行逻辑）。桥契约被设置在本链（Home Chain）和外链（Foreign Chain）上。 “Home” 和 “Foreign” 的概念是相对的，具体取决于相对参照物而言。从应用链的角度来看，Home 代表该应用链本身，而 Foreign 的概念是指的是通过跨链桥连接的任何其他应用链或公链系统。

桥契约必须能够支持接受和锁定资金，且可以验证传入契约的跨链交易上的加密签名，并在交易成功后将通证释放到用户的钱包地址。与主链验证形式相同，桥验证人以拜占庭容错的方式在不同链上的两个跨链桥之间的传输消息。

图 7:Terra 链和链接链之间的信息交流

以下是桥和桥验证人之间执行传输的简略流程介绍：

1. 用户 U 将一些数量为 T 的通证 Cf 存入外桥合约地址 Bf。该交易包含验证人中继传输的元数据：

- 通证在外链的地址
- 交易的通证数量
- 接受人地址

2. 验证人发起询问并接收到一个在外链地址 Bf 上查找到的新交易。
3. 验证人（1..N）向本桥合约地址 Bh 的发送消息，以使用以下参数中继传输：

- 通证在外链的地址
- 接受人地址
- 交易的通证数量
- 把交易存入合约地址 Bf 的哈西值
- 消息上的验证人签名

4. 本桥接收到传入消息，他将验证消息上的签名并将验证人收集的签名入档。当本桥收集到包含 TX 交易的超过 N / 2 个验证人签名时，合约内生成 T 个 Ch 通证，对应外桥上 T 个 Cf 通证，并将在通证从合约 Bh 转移到接受人地址 R.

4.7.2 连接 EVM 链的跨链桥

由于合约大陆的应用链与其它基于 EVM 的链相似，我们希望这条应用链可以与任何基于 EVM 的链自由交互。外桥的功能可以使用 Solidity 语言编写智能合约实现。通过使用 EVENT，桥验证人可以有效地收到来自桥两侧的传入传输请求。由验证人中继到桥接合同中的消息可以使用椭圆曲线数字签名（ECDSA）进行签名，并通过 ecrecover [7]在链上进行验证。

通过选择 BFT 共识机制，验证人由于通证抵押而成为社区的利益共同体。通过对合理的控制验证人数量，并严格按照公式协议定期调整验证人名单确保我们有一个安全且稳定的共识机制。当 N / 2 + 1 验证人确认并验证交易时，跨链交易的最终性会被触发（Finality）。

在此模型中，桥接验证人节点除了负责监听事件之外，签署消息和发送交易到桥接智能合约也是桥验证人的主要职责所在。从接收交易请求，到实际传输至外链或本链，这条传输通路主要依靠两种方式，一个是假设验证人本身也将驻留在相应的链上（即运行对应链自的完整节点），而另一种是利用专业的公共节点服务（例如 Infura [8]为以太坊网络提供节点服务）。后者虽然是一种更简洁的解决方法，但公共节点提供者的信用也变成一个需要考虑的安全因素。

4.7.3 类比特币链的跨链桥

跨链比特币面临的所挑战是如何在轮转验证人的同时保证储蓄的安全。与能够依靠签名组合做出任意决定的以太坊不同，比特币本质上更受限制，大多数客户只接受最多 3 方的多重签名交易。根据当前的协议，将其扩展到十个、百个、甚至是几千个签名，几乎是不可能实现的。摆在我们面前有几种选择，一种是通过改变当前比特币协议来实现这样的功能，提到修改比特币协议就不得不说区块链世界所谓的“硬分叉”，但是通过最近几次分叉尝试，大家可以看出想组织这样的一次“硬分叉”是非常困难的。另一种替代方案是使用阈值签名，加密设计是通过拆解单个可识别的公钥成多个秘密“零件”，所以想要创建一个有效签名，验证人必须需要收集一部分或所有“零件”才能完成。不幸的是，与比特币的 ECDSA 兼容的阈值签名在创建较为复杂的和多项式计算成本过高。诸如 Schnorr 签名之类的其他解决方案虽然成本低廉，但是它们被引入比特币协议的可能性和时间点都很难被确定。

由于储蓄的最终安全取决于一些绑定验证人，还有另外一个选择就是将多重签名密钥持有人减少到几个少数验证人，从而使阈值签名的方案变得可行，这几个验证人会比其它验证人存入更多的押金。（或者，最坏的情况下，使用成本较高的比特币原生多重签名）我们可以根据 BIP-13 [9]使用 M-of-N P2SH 多重签名地址来实现这一点。通过参考比特币协议，P2SH 兑换脚本为最多 520 字节的。兑换脚本的格式为：

[M pubkey1 pubkey2 ... N OP_CHECKMULTISIG]

因此，所有公钥的长度加上公钥的数量不得超过 517 字节。对于压缩公钥，这意味着 N 最大时 N = 15。

如果验证人存在作恶行为，这当然会导致验证人抵押债券的总额减少，以赔偿造成的损失，但这对系统来说是一个无伤大雅的存在，只需要设置一个转账资金的上限就可以确保资金能在两个网络之间安全转账（或者实际上，如果验证者的攻击成功，则按百分比从验证人抵押金中扣除）。

4.8 应用层

应用程序层包含区块链的应用程序域的逻辑，其表现形式为智能合约。从链操作系统的角度来看，高级合同代码被编译为 EVM 字节代码，并存储在链上。应用程序链上的每个完整节点都应该以链状态数据的形式存有应用程序逻辑的副本。因此，任何一方都无法修改应用程序逻辑。设计框架不对应用程序逻辑施加任何限制或规则。设计决策和实施细节（例如可升级性和治理方案）也是开放式的，由应用链的开发人员来决定。

4.8.1 应用场景实例

在这里，我们列举一些可以从应用项区块链框架构建中受益的应用场景。

下一代去中心化交易所。大家最容易想到的一个应用场景应该就是去中心化交易所（DEX）。目前存在的大多数 DEX 都是半中心化的，通常会采用链下的订单薄与撮合引擎来帮助区块链系统卸载负荷。由于公链系统的性能限制，最终用户体验通常很笨拙。使用应用项区块链框架构建的 DEX 可以使整个交易系统搭建在链上，并使终端用户的用户体验趋近于中心化交易所。通过利用跨链桥，DEX 可以对有所有有交易需求的区块链系统及链上的数字资产开放交易功能，而不仅限于 DEX 上部署的链上资产。以这种方式构建的更加纯粹的去中心化交易所，可以不紧为用户提供更安全的保障，还能最大限度地降低中心化操作风险。

P2P 博彩游戏：任何一个 P2P 类的博彩类协议（诸如扑克和麻将等其具有相对较高的性能要求高级游戏），都可以在应用项区块链中实现。且在跨链桥的帮助下，可以将各种数字资产用作游戏的一部分。

游戏：基于区块链的游戏加密猫（CryptoKitties）的火爆中正是借助了区块链的不可变性（Immutability）特质。然而，由于目前主要参与游戏的玩家并不注重游戏本身的娱乐体验，更多是出于收集或获取通证的目的。但是随着区块链系统性能和资产可隔离性限制的提升，相信未来可以创建更复杂更多样的游戏，并且为去中心化游戏领域开辟更多可能性。

5.总结

以上内容概述了应用项区块链和跨链通讯桥两种技术，并且介绍了如何使用两种技术去制造有扩展性的去中心化应用。为了使系统能够健康自主地运转，我们设计了维护和运营需要所的不同角色，并通过合理的奖罚机制，间接规定了各个角色的行为准则。此外，我们还详细讨论了区块链层的共识机制的改进方法，跨链桥协议设计和不同区块链系统协议的局限性，并总结了应用链的几个应用场景。

6．参照

[1] DPoS: Delegated Proof-of-Stake consensus.
https://bitshares.org/technology/delegated-proof-of-stake-consensus.
[2] Go Ethereum (Geth). https://github.com/ethereum/go-ethereum.
[3] Solidity. https://solidity.readthedocs.io/en/v0.4.24.
[4] PoA: Proof-of-Authority consensus in Ethereum. https://wiki.parity.io/Proof-of-Authority-Chains.
[5] Slasher: A Punitive Proof-of-Stake Algorithm.
https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm.
[6] DoS and DDoS Evolution. http://users.atw.hu/denialofservice/ch03lev1sec3.html.
[7] Solidity, Mathematical and Cryptographic Functions.
https://solidity.readthedocs.io/en/latest/units-and-global-variables.html#mathematical-and-cryptographic-functions.
[8] Infura, public Ethereum infrastructure provider. https://infura.io.
[9] BIP13, Address Format for pay-to-script-hash.
https://github.com/bitcoin/bips/blob/master/bip-0013.mediawiki.