安链云链网络白皮书

V1.0

2017.01

众安信息技术服务有限公司

1 摘要

区块链（Blockchain）[1-3]是一种分布式可共享的、通过共识机制可信的公开账本。纵观区块链发展的历程，区块链已经从最早的“为币而生”逐渐发展成为贯穿信用、银行、保险、安全等各行各业的“革命者”。

经过在区块链行业的深耕积累，我们清晰地看到，未来区块链的价值绝不仅限于数字货币。赋予区块链在商业中的价值，使其为传统的商业模式注入新鲜的活力，才是我们打造区块链产品的使命。

本文介绍了安链云网络，安链云网络是由链路由和安链以及其他区块链系统组成的区块链云网络。

链路由提供了区块链之间的联通与分发的功能。链路由制定了区块链之间的通信协议，使不同的区块链之间可以像网络中的各种设备一样相互通信。在链路由的网络中，一些区块链可以起到类似路由器的功能，根据通信协议将通信请求解析并转发，动态维护一个区块链系统的网络拓扑结构。

为支撑商用区块链系统对监管、隐私和复杂业务的支撑，我们设计了安链，一个满足以上要求的企业级区块链产品。本文将详细说明安链架构、技术特色与优势和应用案例。

2 前言

区块链的商业价值，已经通过比特币[4]，以太坊[5]等区块链项目得到了最好的印证。数字加密货币通过去中心化发行，不易篡改等特性为广大用户所接受。当前，很多数字加密货币区块链项目都形成了相对成熟稳定的生态。然而，由于区块链自身与外界封闭的特性，目前的这些区块链生态形成了一个个彼此隔绝的孤岛。除了，BTCRelay 等少数项目在链间的交互上做出了探索之外，最常见的还是独立于链外的数字货币交易所这样的机构，通过传统的运营模式将区块链当做金矿，把数字货币当做货物来交易。只能发挥出有限的价值。

纵观互联网的发展历程，以及其产生的巨大变革，我们无法否认通信所具有的巨大力量。其实，区块链的诞生本身就是带有着互联网的前瞻性的，在不依赖中心化服务的情况下，节点之间通过 P2P 通信，共识，备份数据，创立了彼此之间的信任。互联网发展至今，越来越深刻的体会到骨干网络负荷增加，攻击频发等弊病所带来的问题，并积极寻求解决方案。例如，IPFS[6]作为基于内容的分布式网络文件存储协议，就可以应对传统基于 IP 地址的网络协议所面临的的上述问题。

通过与互联网类比，我们不难发现，在当前阶段区块链的网络属性仅仅被发挥到类似局域网的程度，不同的链之间不仅无法联通，更无信任可言。此外，对一条区块链而言，我们也饱受其能力不足的困扰，全局共识机制在提供安全性的同时也大大限制了区块链系统的发展，我们无法通过增加节点的方式提高交易的处理能力。如果区块链想要拥抱更光明的未来，上述问题必须得到解决。

在商业应用场景下，企业级区块链产品无论从技术特点还是服务人群上都与以比特币，以太坊等为首的公有链有很大的区别。企业级区块链产品的首要要求是满足监管和隐私保护。此外，支持高吞吐量，支持数据分享，防止“拜占庭将军问题[1]”[7]也是提供高质量服务所必备的素质。

本文的结构安排如下，第三章介绍链路由的设计理念，包括设计灵感与愿景，第四章详细讲解链路由的架构，第五章讲解的跨链通信协议，第六章设计了解决复杂的商业需求的子链——安链，第七章对链路由及安链的商业应用进行展望。

---

[1] 拜占庭将军问题是指如何在一个不基于信任的分布式网络中就信息达成共识的问题。

拜占庭问题是一个协议问题，拜占庭帝国军队的将军们必须全体一致决定是否攻击某一支敌军。但这些将军在地理上是分隔开来的，并且在将军中存在叛徒。叛徒可以任意行动以达到以下目标：欺骗某些将军采取进攻行动，促成一个不是所有将军都同意的决定，或者使某些将军无法做出决定。如果叛徒达到了这些目的之一，则任何攻击行动的结果都注定是要失败的，只有完全达成一致的努力才能获得胜利。

拜占庭假设是对现实世界的模型化，由于硬件错误、网络拥塞或断开以及遭到恶意攻击，计算机和网络可能出现不可预料的行为，拜占庭容错协议必须处理这些失效。

3 设计理念

针对区块链发展所面临的种种问题，我们提出“链路由”的概念。这样做主要有两个目的，其一，增强区块链系统对交易的处理能力，实现区块链交易处理能力的水平扩展；其二，打通链与链之间的通信壁垒，实现链与链之间的互联，互通，互信。

3.1 设计灵感

链路由的概念是源于互联网中的路由结构。一个简单的路由网络是由路由器和终端设备组成的。其中，终端设备拥有唯一的 IP 地址，路由器维护的路由表反应的是其可以跳转到的地址，所有路由器的路由表组成了整个网络的拓扑结构。

在我们的设计中，形如比特币、以太坊、安链等区块链系统对应的是路由网络中的终端设备，我们称之为“子链”。子链可以收取发自链路由的消息，也可以向链路由发送消息，但是不能直接在彼此之间建立通信。

除子链外，我们设计了对应网络中路由器角色的“链路由”。一个链路由动态维护着注册在其上的所有子链的相关信息，用来联通链网络的诸多子链。子链必须通过跨链通信协议首先与链路由建立链接，才可以与其他子链进行通信。链路由可以与子链或者其他链路由进行通信。链路由之间通过彼此交换与其相连的子链的信息，来维护网络通信的顺畅。

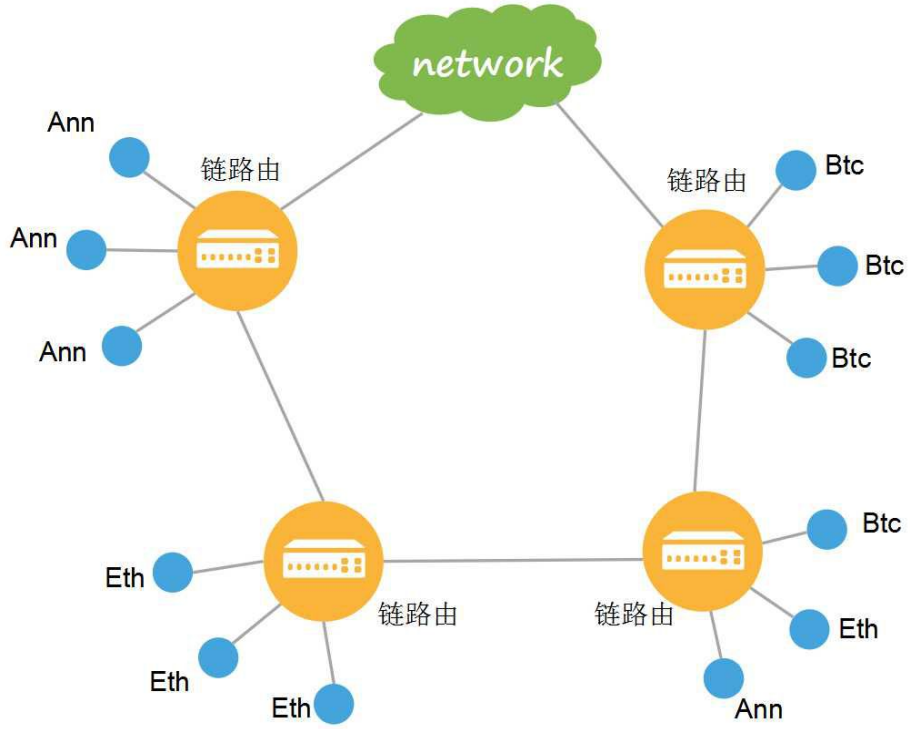
3.2 愿景

在这种结构下，我们可以根据不同业务逻辑和用户需求部署适合的区块链网络系统。

我们通过链路由实现了区块链的分片，提高区块链系统的交易处理能力。相较于一条单独的区块链系统，链路由系统可以通过连接多条子链的方式在交易处理能力上直线增长。交易的请求通过链路由的分配进入不同子链，可以有效规避针对一条子链的集中请求。此外，我们可以在链路由上部署同构子链的不同节点数的集群，对于同构链而言，多节点数量的集群会有相对较高的安全性，少节点集群的处理速度则更快。通过链路由实现区块链的分片，可以帮助链网络根据业务需求灵活部署，为用户提供更高质量的区块链服务。

当然，除了实现区块链分片之外，链路由的另一个重大意义在于打通各子链，在链与链间建立信任桥梁。连接在链路由上的各子链之间通过链路由得以彼此传递消息，协同工作，实现“1+1>2”的效果。我们也可以部署多个链路由系统，每一个链路由系统中都可以部署包括比特币，以太坊，安链在内的各种子链。因此每一个链路由都可以服务一个更完整的业务生态。同理，我们可以根据节点数量，地理位置，业务分类等不同需求，部署不同的链路由集群，根据路由规则，对应不同需求将请求分发到合适的集群之中处理。

链路由网络的最终形态，是通过链路由的无限扩展和彼此之间的相互连接，形成连接不同集群的复杂区块链星状网络。创造一个由区块链组成的，互联，互通，互信的网络世界。



4 链路由(Ann-Router)

在链路由网络中，一些子链，如比特币，以太坊等，是先于链路由存在的，而且在设计之初这些子链也不具有与其他链通信的功能。而链路由则要像路由器一样能够接纳一切子链，因此我们提出了一套链路由的设计方案以及跨链通信协议，符合这套协议的区块链系统可以轻松接入链路由。对于此前的区块链系统，在不改变其本身设计的基础上，需要额外设计一套适配系统来辅助其与链路由之间的通信。本节我们将对链路由进行详细介绍。

4.1 共识算法

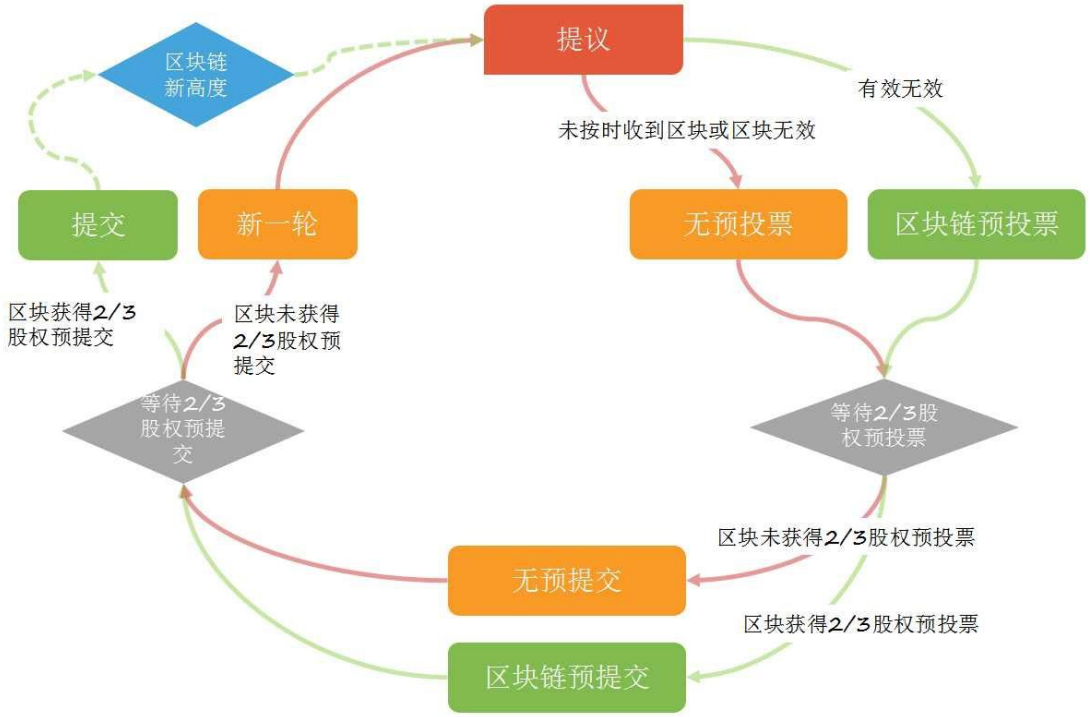
工作量证明算法（PoW）是被应用在比特币和以太坊上的一种拜占庭容错（BFT）共识算法。自比特币开始发行至今，工作量证明算法已经证明了其可靠性，但其中对资源的浪费也是有目共睹。权益证明算法（PoS）是一种为了解决工作量证明算法中对资源浪费问题的共识算法，通过投票人在投票权益池中的权益比重来代替矿工在挖矿时贡献的算力，配以相应的处罚机制，确保投票人的诚信。然而，算力和权益之间还是有很大区别的，最重要的一点区别就是在于算力是不能分散的，一个算力固定的矿工不可以同时在两条链上挖矿且保持总算力翻倍，但是拥有一定权益的投票人却可以对每一个可能的区块投票，只要任何一个区块成为了将来的胜出者就可以保证自己的权益不受损。但这样做是有很大的安全隐患的，因为这样大大降低了作恶者所需要的作恶成本。

Raft 作为一种常用的高效共识算法，其最大的弊病在于不能防止拜占庭节点，一个拥有强大网络配置的拜占庭领导者节点会给 Raft 算法的共识带来毁灭性打击。在拜占庭容错共识算法的发展历程中，一些结合 Raft 和 BFT 的算法被提出来。以安链所使用的 PBFT 为例，一部分可靠的节点被称为验证人，验证人具有成为领导者的机会，在每一轮区块链生成的过程中，都会有一个新的验证人会默认成为该轮的领导者，领导者负责打包新的区块，并将一个自己认为合理的区块广播给所有验证人。经过两轮超过 2/3 的全部验证人的投票确认，新的区块才会被共识。这种共识方式大大提升了出块速度，而且只要保证小于 1/3 的验证人不是拜占庭节点，区块就可以被持续生产。

不可否认的是，PBFT 中所使用的拜占庭节点容错算法能够保证 1/3 以下拜占庭节点的网络的安全。但是，在实际应用中，尤其是当与经济利益相关时，即使验证人是经过挑选的可靠节点，我们也不能单纯的依赖没有处罚机制的 1/3 的安全，保证安全必须要做到赏务速而后有劝，罚务速而后有惩。而其中的赏与罚必须是与经济利益直接关联的。因此，我们对原有的共识机制进行了修改，使验证人投票的权重与其所抵押的链上代币权益相对应。

这样一来，原本需要超过 2/3 投票人才能确认生成区块的机制被修改成超过 2/3 的总权益。此外，在 PBFT 共识算法中，普通节点仅同步来自领导节点发来的新区块，并不参与共识，而觉得其共识算法的安全性仅依赖于验证节点的数量，因此普通节点的数量增加并不能提升拜占庭容错的安全性。新的共识机制中增加了非验证节点的参与性。一个验证节点对应一个验证人账号，非验证人可以通过将权益委托给验证人，从而授权该验证人代理投票的方式赚取属于自己的利益。因为利益的关系，非验人会慎重选择代理验证人，从而做到了所有人都参与到共识中，而又没有所有节点参与共识而带来的效率降低的缺陷。

这样的共识算法我们称之为代理权益拜占庭容错算法（Delegated Stake-PBFT），简称 DS-PBFT。



4.1.1 轻客户端

普通的区块链客户端需要同步该区块链中的所有区块才可以验证交易，这样的客户端虽然功能强大，但是由于需要存储的数据太多导致其本身过重，在实际应用中往往有着诸多不便。链路由使用了通过验证人投票实现的 DS-PBFT 共识算法，这为我们打造轻量级的客户端奠定了基础。

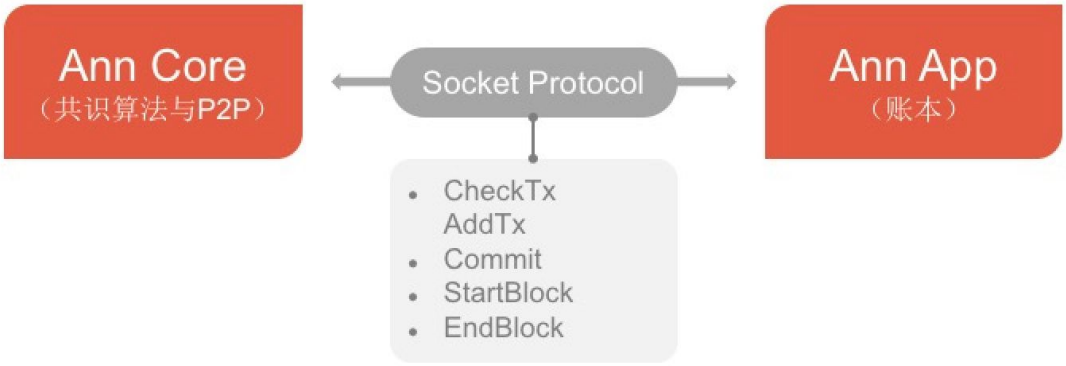
轻客户端中只需要实时同步某条区块链上的最新验证人组，就可以对该区块链上的一些信息进行验证。如，轻客户端只需要连续同步某区块链区块头并更新验证人信息，就可以实时跟进并验证该区块链上的最新的区块高度，世界状态等信息。当然，相较于全节点客户端，轻客户端能实现的功能是有限的，但是这样的客户端更适合被使用在硬盘空间不够大的移动端或物联网设备上，帮助其获取重要的状态。

4.2 结构解析

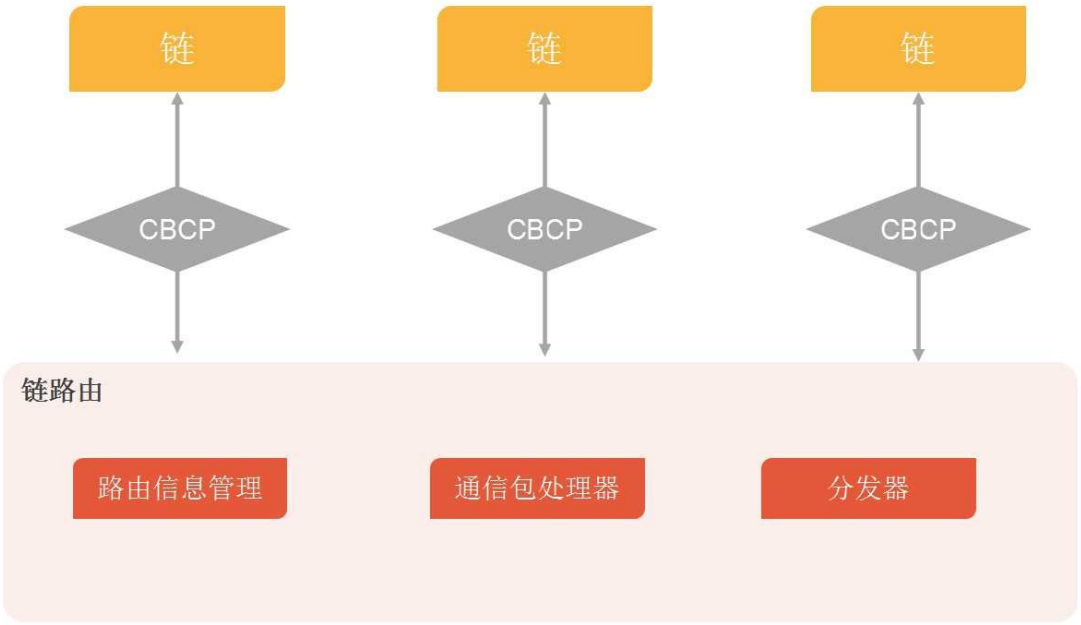
4.2.1 链路由结构

不同于传统区块链系统的机构，链路由中的共识算法和 P2P 网络是与账本逻辑分离开的，将链路由分割为两个部分。其中共识算法与 P2P 网络的部分被称为 AnnCore，AnnCore 负责交易的广播，共识等。账本部分被称为 AnnApp，AnnApp 负责验证，查询等逻辑。二者之间通过套接字协议被结合在一起。因此，AnnCore 可以替代诸多区块链系统中的共识及 P2P 网络

部分。



当链路由作为链网络的路由器时，能够使用通讯包处理器解析通信包，然后根据其动态维护的路由表，通过跨链通信协议(Cross Blockchain Communication Protocol)将消息转发给子链。



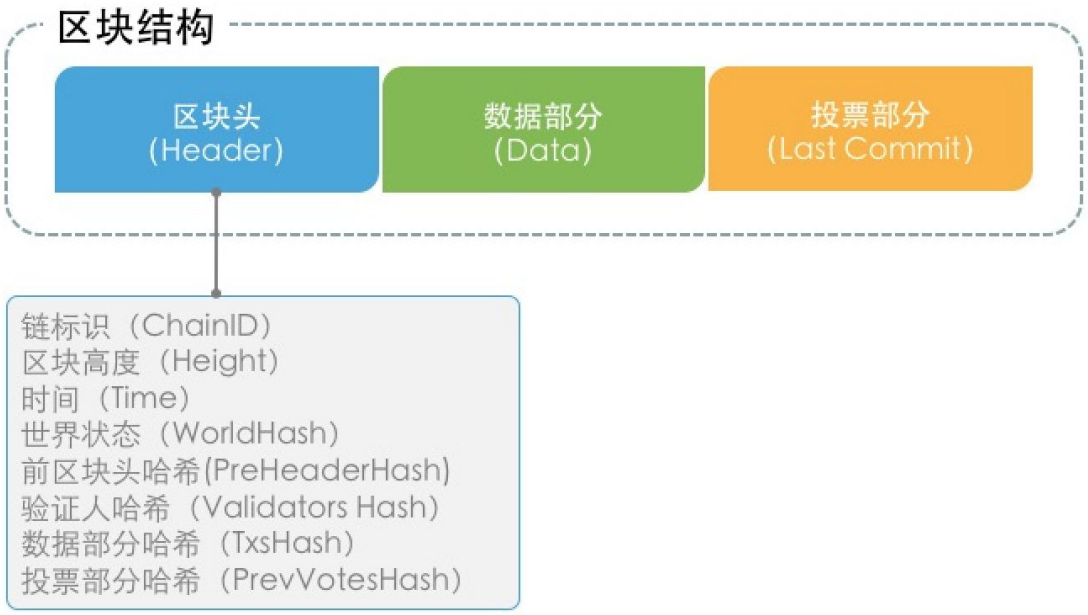
4.2.2 区块结构

由于链路由采用了 DS-PBFT 共识算法，其区块的结构与比特币、以太坊等区块链系统的区块的组成有很大不同。从结构上来看，一个链路由的区块主要包含三个部分，区块头部分，数据部分，以及认证上一个区块的投票部分。

区块头部分包含链标识，区块高度，时间，世界状态的哈希值，前区块头的哈希值，前区块分块，验证人哈希值， 数据部分的哈希值， 投票部分的哈希值等等。其中，后两部分是对本区块整体性的检查。数据部分包括了本区块中的所有交易。比较不同的是投票部分，这个部分的目的是建立新的区块与上一个区块之间的链接。

之前我们提到过，区块的共识需要两轮超过 2/3 验证节点权益的投票。其中第二轮的全部

2/3 验证节点的投票（Commit）会被暂时保存起来，等到下一个区块被提议时，再被放在该区块的投票的部分（LastCommit）。所以一个区块的投票部分包括了上一轮投票中超过 2/3 验证人的投票。



4.2.3 分层结构

在理想状况下，链路由本身是一条链，所有子链通过这一条链进行通信，这样的好处是通信速度快。但是随着新子链的不断增加，通信量也会增加，链路由节点的存储和计算负担将以平方级增加，因此链路由需要采用分级结构。

这里将问题简化，假设链路由只有两层：底层链负责连通上层链，负责维护上层链之间的通信。即，如果目标链在同一个上层链中，那么就直接通过上层链通信。如果目标链不在同一个上层链中，则需要通过底层链通信。在实际应用中，链路由将不止两层，最底层构成路由主干，并形成网状结构。

链路由分层带来的问题是通信时延和存储冗余。如果通信平均需要通过多层路由转发，那么会导致网络时延，并加重链路由整体的存储负载，因此需要优化路由算法。链路由算法需要能够快速收敛选择最佳路径，并可以快速、准确地适应各种不可预料的网络环境。链路由算法使用多种度量来选择路由，通过一定的加权运算，将它们合并为单个的复合度量，再填入路由表中，作为寻径的标准。这些度量包括时延、负载、通信成本等。

4.3 状态维护

作为不同子链之间沟通的桥梁，链路由要负责维护关于子链的一些状态。

首先，子链若希望与链路由进行通信，则必须在链路由上进行注册。包括子链的身份标识（ChainID），子链上验证节点的信息，子链上资产的种类等。以此来帮助链路由能够在接收到通信请求时解析出对应的子链，完成转发操作。

其次，链路由需要实时接收子链的最新区块信息和对最新区块的投票（Commit），以此来维护子链的基本状态，帮助轻客户端的用户实时查询子链高度、状态，验证从子链发来的交易等等。

此外，因为验证节点的身份是实时变更的，链路由还需要维护所有子链上的动态验证节点信息，以此来验证一笔来自子链的交易是否为合法。

同理，子链上也需要维护关于链路由上的相应信息，以此来确定一笔交易确实是由链路由发来的。包括链路由的身份标识，链路由上的验证节点信息，链路由上的最新区块及投票等。

4.4 动态扩容

前文提到，链路由机制的一个重大意义在于实现区块链系统的水平扩展。因此，我们可以在现有链路由系统交易处理能力接近饱和之前在链路由上加入新的子链，降低每条链上所承载的交易数量。为了让新加入链路由的子链可以迅速分摊压力，我们制定了能够实时反应的动态路由规则。

首先，链路由会维护一个关于注册在其上的子链列表，在子链加入到链路由之前，子链列表会先行更新。轻客户端会效仿分布式配置管理机制，不定时向母链读取当前的最新子链数量。轻客户端每次会在 0.5 至 1 秒之间随机选取一个时间，倒计时触发向链路由查询子链数量，并存储在本地文件中。若查询结果与本地存储数字不同，则向其他轻客户端广播最新子链数量及时间戳。收到消息的其他轻客户端对比本地文件，数量若一致，则重置倒计时；若数量不一致且时间戳晚于本地数值写入时间，则向链路由发起关于子链数量的查询，写入新数据之后，重启倒计时；若数量不一致但时间戳早于本地写入时间，则忽略消息。此外，我们还可以设定一个屏蔽机制，若一个轻客户端收到来自另一个轻客户端的广播，然后触发了向母链的查询，但是发现数量与本地储存的子链数量一致。这时可能是因为两次查询中，母链上的子链增减数量相同，广播者没有撒谎；或者广播者撒谎。但是这个轻客户端可以主动选择屏蔽接受来自对方的消息，每次的屏蔽时间随受欺骗次数增加。

通过以上方法，我们保证了轻客户端中存储的子链数量与母链中所存的保持实时一致。每当一笔请求从轻客户端发起时，轻客户端需要指定交易的触发链，轻客户端计算应用标识的哈希值，并对本地储存的子链数量取模，所得值即为该请求的目标链的编号。

4.5 链路由管理

从管理的角度来说，子链链路由相互独立，子链不会影响链路由，反之链路由也不会影响子链。这里主要讨论链路由的管理规则。

4.5.1 验证节点管理

验证节点与链路由的正常运转直接相关，因此在链路由初始化时会指定一批节点成为首批验证节点。此后，随着总节点数的增加，验证节点会同比增加，直至验证节点总数达到上限。到达上限后，验证节点总数将不再增加。但为了确保流动性和安全性，我们引入了验证节点的剔除机制，针对腐败验证节点，可以通过全体验证节点投票的方式将其剔除网络。

验证节点具体分配机制如下：链路由起始第一年验证节点上限为 200 个，之后每年呈线性增长，增长率为 10%，上限取整也就是说第二年验证节点上限为 220，第三年验证节点上限为 242，第四年验证节点上限 267 等，如果发现验证节点上限不满足当前网络需求，可通过管理端发起提案投票，调整其上限值。

4.5.2 代币发行

链路由会通过权益证明的方式发行代币 ZAC。针对起始 ZAC，在链路由初始化前会发起众筹，众筹占 55%，众安科技占 10%，上海区块链产业联盟占 35%。起始 ZAC 会在 1 年内平均按天返回给参与者，即每个参与者每天会收到所占起始 ZAC 份额的 1/365。ZAC 是通胀发行，每年的通胀率为 10%，每两周会产生新的 ZAC，做为验证节点维护网络结构奖励发放给验证节点，奖励按照验证节点投入 ZAC 参与记账权益的比例分配。ZAC 也做为链路由交易流通中的交易手续费，来防止对链路由产生的 DDoS 恶意攻击，这些手续费同样作为奖励分发给验证节点。

4.5.3 权益管理

每个持有 ZAC 的参与者，都有机会成为验证节点，成为验证节点必需抵押持有 ZAC 到共享资金池，验证节点投票权重根据其抵押 ZAC 占有资金池比例来计算。当验证节点总数未达到上限时，每个 ZAC 持有者都可以申请成为验证节点，而当验证节点数已达到上限时，非验证节点想成为验证节点，其抵押的 ZAC 数必需大于当前验证节点权重最小者抵押的 ZAC 量。持有 ZAC 量少的非验证节点也可以把 ZAC 委派给一个代表，而代表可以把其获得的奖励按比例分发给这些委托者。这样持有 ZAC 少的参与者也可以通过找代理的方式参与共识，并来减少 ZAC 每年通胀量给自己带来的损失。

4.5.4 奖惩机制

验证节点可以发起提议，提议拥有2/3同意投票就可以通过。投票的种类可分为同意、强烈同意、反对、强烈反对和弃权。如果出现1/3的强烈反对票，则提议不通过，并对投赞成及投强烈反对票的节点进行惩罚，双方抵押在资金池里的ZAC都会相应的减少。并将减少的ZAC放入奖励池中。投票通过的提案会在两周后强制执行。

奖励池的设计是一种鼓励机制，网络漏洞发现者及黑客，可通过 ReportBugTx 提交漏洞说明以及其奖励地址，经过验证节点投票，2/3 通过后，可从奖励池中获取所要求奖励。

ZAC 作为数字货币，与比特币，以太币一样，可以在交易所中被交易。因此，用户持有 ZAC 的目的可能是为了投机。当市场上 ZAC 的价格突然增高，验证节点通过投票生成区块获得的利益会小于直接交易 ZAC 的获利。因此，验证节点会倾向于解绑其 ZAC，退出验证节点集

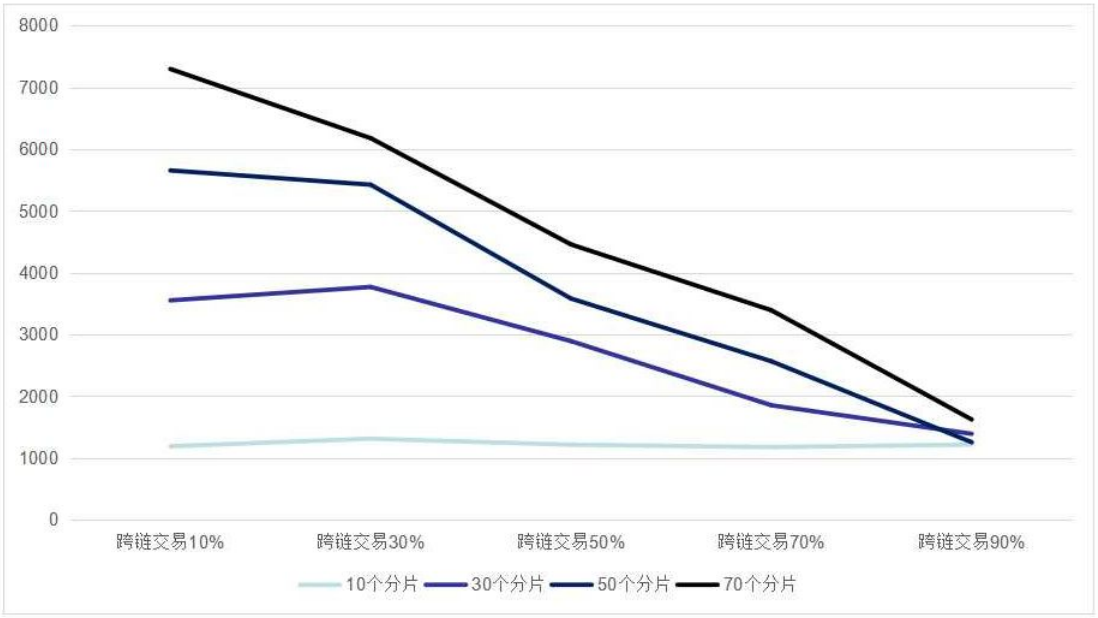
合。为了保证链路由的安全性，当验证节点数在最大上限的 30%-50%时，新区块生成的奖励额度调整为之前 1.5 倍，当处于最大上限的 30%以下时，奖励上升到之前 2 倍。极端情况下，全体验证节点可以通过提案投票的方式来调整奖励。

验证节点在有意或无意的情况下会做出影响链路由的行为，因此在DS-PBFT共识算法中必须存在针对验证节点的惩罚机制。下面以双签和不履行投票义务为例，解释相应的惩罚机制。双签是指验证节点在同一高度同一轮，对两个不同区块进行双重签名，这种行为会影响DS-PBFT共识。针对这种行为，验证节点的名声及绑定的ZAC都要有所损失。当验证节点的名声积累为负，就要强行被移出验证节点集。验证节点可能由于网络或者机器原因导致长时间离线，没有履行其投票义务次数过多，超过其ValidatorMaxTimeout次数过多，其权益也要受到相应惩罚。

上述违规行为比较容易被检测到，对于那些不易发现的违规行为，我们设定已绑定的 ZAC 解绑需要两周时间，延长发现违规的时间。

5 链路由性能指标

在实验室环境中，测试表明，链路由的总体交易性能随着子链数量的增长而线性增长。一条安链的性能根据交易复杂程度，性能在 20-180tps 之间。我们通过安链对链路由的动态扩容进行了测试，得到了输入不同的分片数量、跨链交易比例时，链路由系统的交易处理性能变化图。



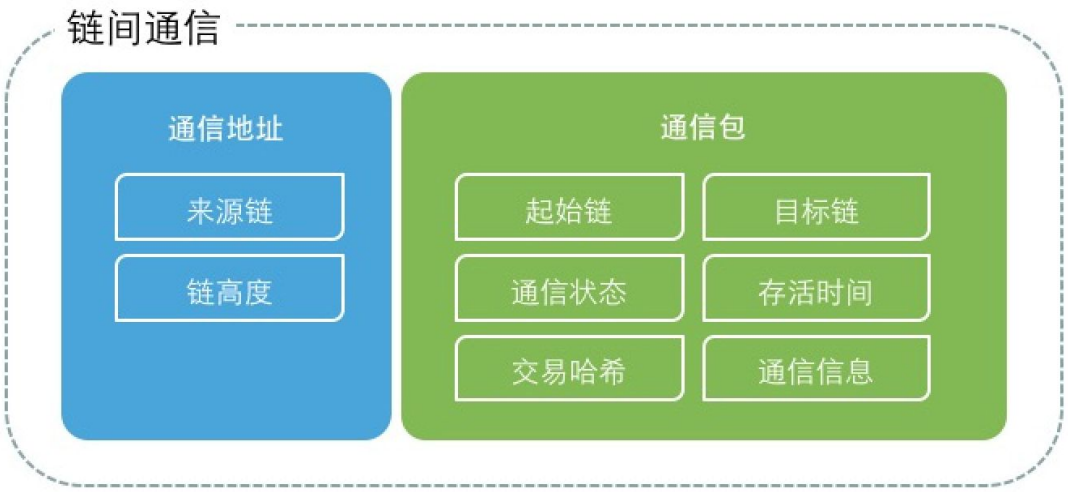
6 跨链通信协议(CBCP)

区块链之间的通信协议与传统网络中的 TCP/IP 等通信协议类似，通过建立可靠的连接传递消息。消息分为消息头（Header），和通信信息（Data）两部分。其中消息头会记录消息的源头，目的地，长度，类别等。在传递过程中，消息头会被逐层剥离，修改，信息则会被传到消息的目的地。此外，消息的传递具有状态性，发送方可以根据接收方的反馈了解当前通信所处的状态，做出正确的反应。

6.1 协议结构

一个完整的跨链通信协议（Cross Blockchain Communication Protocol）主要包括两个部分，通信地址，通信包。

通信地址包括消息来源链的链标识（fromChainID）和当前链高度（Height）。通信包则由部分，通信包头（Header）和通信信息（Data）组成。其中，通信包头包括了，起始链标识（srcChainID），目标链标识（dstChainID），通信状态（Status），通信存活时间（TTL），触发通信交易等。通信信息在传递过程中则不会被打开。



通信状态对应的是网络通信协议中的通信状态机制。当一个通信包被发送的时候，通信状态是“接收待定”。当接收方收到消息，会返回给发送方一个通信包，其中通信状态为“发送成功”，若发送方收到了含有“发送成功”标识的通信包，发送方会再回复给对方一个含有“接收成功”标识的通信包。以上便是一次成功通信的。如果过程中，有通信包接收失败，如，接收方一直不回复“发送成功”，则发送方会在一定时间后重发交易，试图再次建立通信。

除上述状态外，我们还规定了“连接超时”状态。当一笔交易从子链 1 发往子链 2 时，会标明其指定的以链路由区块高度为准的通信存活时间。在到达通信存活时间之前，链路由会将通信结果的状态返回给子链，若超过通信存活时间，则链路由直接返回给发送方“连接超时”

状态。发送方子链将该次通信记录为通信失败。

6.2 通信验证

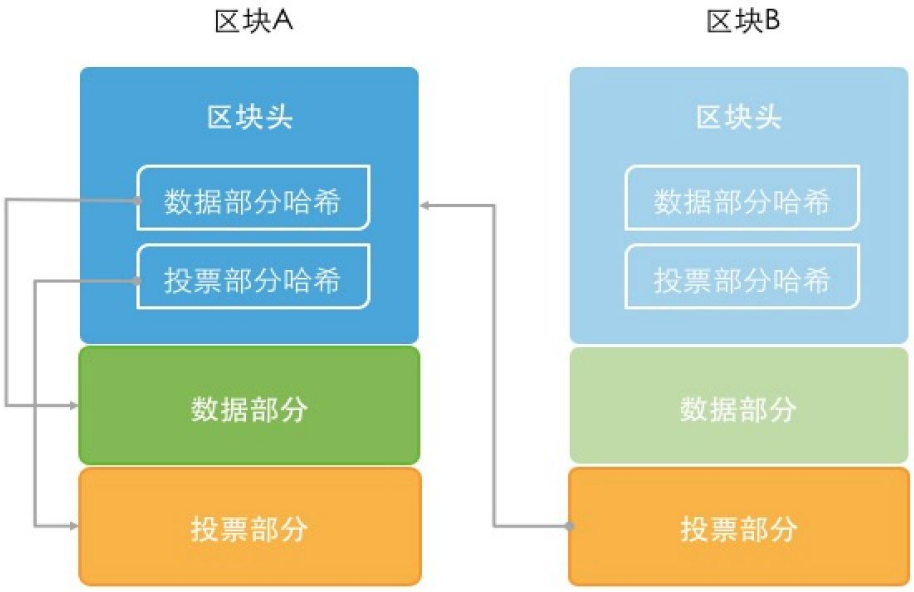
与网络通信类似，区块跨链通信也可能遭到攻击，尤其是 DDoS 攻击。因此，我们需要一套验证容易，伪造困难的通信验证机制，来防止链路由因遭到攻击而瘫痪。

第四章提到的链路由的结构是我们认为子链应该符合的一种标准结构。在标准结构的框架下，链路由将更容易验证子链发来的通信请求。前面提到，子链随时向链路由传送最新的区块以及最新区块的投票（Commit），当一笔交易从子链向链路由发来的时候，会在通信地址中体现出该交易所在区块的高度。我们只需要查找在该高度的区块中是否存有这笔交易即可。因为通过提交最新的区块及其投票（Commit）便足以证明一个区块的真实性。具体证明如下：

首先，单靠一个区块本身是不能孤证其合法性的。因为针对一个已有的区块，我们完全可以仿造一个不合法但是符合区块结构的假区块。例如，修改区块数据部分的交易，并修改位于区块头中的交易哈希值。

前面提到，一个区块被提议之后会经过两轮投票来共识，其中第二轮共识的投票会被暂时存起来，并当作下一轮所生成的区块中连接上一个区块的部分。基于此，如果子链一次性提交某个区块及其投票，我们便可以在一轮区块生成时间内证明这个区块的可信性。而不用花费两个区块的生成时间，等待到下一个区块生成，通过其中的对上一个区块的认证部分来验证前一个区块的可靠性。

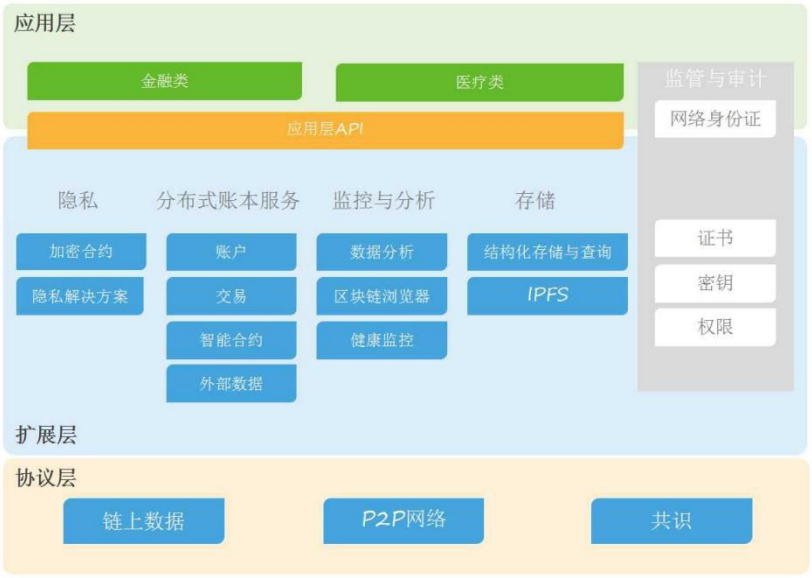
通过共识来验证一个独立区块的合法性的流程为，先通过区块头中本区块数据以及投票部分的哈希值来验证除区块头以外，本区块是没有被篡改过的。又因为投票（Commit）是该链超过 2/3 验证节点对本区块区块头的签名，除非消息的发送方可以同时掌控超过 2/3 的该链上的验证人的私钥，否则没有人可以伪造区块。



7 安链(Ann-Chain)

在设计安链之初，我们就严格将其定位为企业级区块链产品。安链的设计目标是满足商业应用的各类要求，具体包括：建立切实可行的监管审计机制；交易隐私的保护；稳定高效可靠；为数据分享搭建平台。

下图展示了安链所参考的架构，这些是逻辑结构，而不是对具体步骤、地址空间或机器组件的物理描述。为了解决区块链技术在应用落地过程中可能面临的各种阻碍，安链采用三层架构：（1）协议层：提供区块链底层原始数据不可篡改的存储，同步等基础服务（2）扩展层：实现安链的各种功能，包括监管、隐私、智能合约[8]、监控分析与结构化数据存储与查询等功能。（3）应用层：运行于安链上的各种应用，例如银行，医疗等等。



安链的功能主要在扩展层实现，包含的模块主要有：

- **监管与审计模块：**负责链上交易的授权与监管，提供证书发放，权限管理。
- **隐私模块：**提供加密合约交易，并提供不同场景的隐私解决方案，如多方计算[9]、PGP通信以及环签名。
- **分布式账本服务：**提供交易与智能合约的解释与执行，交易管理，并提供外部数据服务。
- **监控与分析：**支持系统和硬件环境的监控，并提供多种可视化管理工具，满足管理和维护需求。
- **存储：**提供文件存储和结构化数据存储与查询。

区块链协议层存储区块链上原始数据，并在节点间同步全局状态。协议层由三个部分组成：链上数据、P2P 网络、共识管理器组成。

- **链上数据：**安链的数据都以交易表示，每笔交易包含一个签名。交易打包在区块中，相邻区块采用哈希链连接。安链采用状态模型，每一笔交易都改变区块链上的状态。交易引起的状态变化的解释由上层账本服务提供。
- **P2P 网络：**区块链网络是一个多中心节点的网络，节点之间的消息传递和发送采用了 P2P 模式。在 P2P 网络中，每个节点既可以从其他节点得到服务，也可以向其他节点提供消

息服务。安链的 P2P 协议采用了授权加密的安全通信机制。

- **共识：**安链的共识算法是一种基于 PBFT 的共识算法。算法生成的区块是经过投票的过程产生的，生成区块的时间是平稳的，而基于工作量证明的共识算法中区块的生成时间是基于概率的。平稳的区块生成时间保证了交易延时的稳定。算法中交易所在区块在区块链上确认后即为终态，区块链不会分叉，也没有叔伯区块，从而可以提升吞吐量。算法可以抵御节点的错误消息，以及节点互相勾结（最多 1/3 拜占庭节点）。共识算法的节点带有一个信用评分，在参与投票时会依据判断正确与否增减。信用评分用于调整节点选为领导节点的权重，新投票节点加入退出的投票等等。

7.1 监管模块

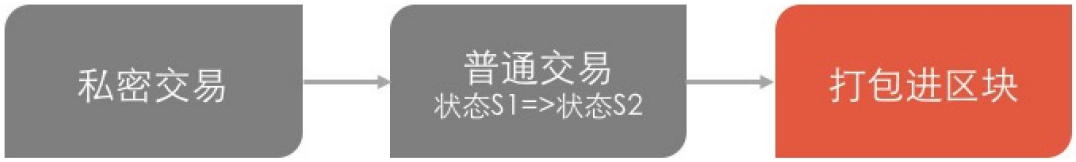
监管模块负责链上交易的授权与监管。监管模块由网络身份证和授权管理服务组成。

- **网络身份证：**网络身份证是一套对用户的实名身份信息进行认证，并在联盟方中共享信息的系统。网络身份证采集的信息包括基本信息、财务信息以及行为信息。网络身份证是对账户持有人的强审查，能够在保护客户隐私的情况下满足监管需求。
- **授权管理：**授权管理为节点与交易提供授权并审计。权限管理：提供完整的权限管理机制。权限管理根据归属公司和职级为用户授权，为节点发放证书或者授予密钥。证书管理：为节点加入区块链网络，获得交易身份以及参与交易提供授权。证书管理服务相应的发放三种证书，包括通信证书、身份证书和交易证书。节点加入区块链网络需要获取通信证书得到授权。节点在区块链网络中获取身份证书以获得身份授权。节点每发送一笔交易必须拥有交易证书才能执行。密钥管理：密钥管理的框架与权限管理结构相对应，不同级别的权限对应不同级别的密钥，当用户获取相应的证书后，可以在密钥管理模块申请密钥。

7.2 隐私模块

隐私模块提供加密合约相关服务以及各类隐私解决方案。

- **加密合约：**对有隐私需求的智能合约，提供了加密合约解决方案。在加密合约中，智能合约中的信息是经过加密的，调用合约的交易也是加密的。私密交易采用局部共识的方法，一笔私密交易的执行分为两步：第一步是预处理，将隐私交易转成一笔普通交易[S1=>S2]（S1 和 S2 分别为交易执行前后智能合约的密文状态）；第二步是将[S1=>S2]做为一笔普通交易打包进区块。



- **隐私解决方案：**安链针对不同场景提供了不同的隐私解决方案，如多方计算和 PGP 通信。通过安全多方计算，安链可以实现隐私的原始数据的完全隔离访问。PGP 安全通信解决方案为安链带来了快速安全的数据分享服务。

7.3 分布式账本

分布式账本模块提供账户服务，交易服务，智能合约服务以及外部数据服务。

- **账户服务：**账户服务提供账户通用服务，包括地址生成以及编码，密钥对生成和管理，签名服务等。
- **交易：**安链支持三种交易：部署代码交易、代码调用交易和代码升级交易。部署代码是将智能合约部署至区块链，而代码调用则是执行链上代码。值得一提的是，安链引入代码升级交易的概念，即可以升级已部署的代码，在这个过程中，验证节点必须保证其执行环境的真实性与完整性。
- **智能合约服务：**智能合约服务提供智能合约的执行。提供执行的虚拟环境，和标准化的合约解释逻辑，保证同样的交易有相同的执行结果。
- **外部数据服务：**传统的区块链就像是一个与世隔绝的花园，区块链里的智能合约没法主动拿到外部数据。为解决这个问题，安链中引入了外部数据服务。外部数据服务在安链中承担着可信数据源的角色。当智能合约有外部数据需求时，只需要在外部数据服务中登记。外部数据服务会根据要求获取外部数据，供智能合约调用。

7.4 监控与分析

监控与分析模块由区块链浏览器，健康监控及数据分析模块组成。

- **区块链浏览器：**实时显示最新区块、交易、合约和账户信息，提供搜索功能，可根据交易、地址、区块信息查询相关信息，并提供智能合约说明。
- **数据分析：**提供了各种标准化的数据查询接口以及批量导出的定制化服务，以满足各种数据需求，如审计、监管等。
- **监控模块：**实现了对底层区块链健康状态的实时监控，包括物理状态（CPU 温度、内存、磁盘）、网络状态（时延、断线）及应用状态（区块生成、交易验证）。

7.5 存储

安链含有两方面的链外存储模块。IPFS 用来在链外存储大型文件，而结构化存储用来保存结构化记录，并且支持结构化查询语言。

- **IPFS 模块：**安链为支持大文件存储，引入了 IPFS 技术。文件通过 hash 存储，具有防篡改、永不丢失、防泄漏和访问安全等特性，避免意外事故对数据安全的冲击，确保用户信息、电子保单、客户信息、电子合约、资产证明、理赔凭证等信息的永久保存，保证数据安全和用户隐私的不可泄露和丢失。
- **结构化存储模块：**结构化存储用来保存结构化记录，并且同区块链上的记录保持同步。

8 商业展望

区块链是随着比特币的诞生而诞生的，这说明，其固有属性就是适合商业应用的。当前，区块链系统大致可以被分为两类，一类是以比特币等为首的数字货币区块链系统，另一类就是以以太坊等为首的智能合约数字货币区块链系统。智能合约利用了区块链的不可篡改性，加上其本身图灵完备的特征，可以在被触发时执行事先规定好的合约内容，而且不同的人执行同一个智能合约会得到相同的结果，从而杜绝分歧，创造商业上的互信。目前，单凭一个个独立的区块链系统，就已经让世界感受到了区块链的强大力量，我们相信，作为打通跨链通信的链路由系统，将会为区块链系统的商业价值带来质的提升。

分布式交易所

分布式交易所是基于链路由的一个很重要的应用。相比之下，中心化交易所往往更为我们所熟知，这类交易所配有成熟的撮合系统和处理高频交易的能力。通过中心化交易所交易数字货币看似顺理成章，但实际上，中心化交易所的理念是对区块链属性的误读。正如前面所提到的，区块链的诞生对于现有网络结构而言是具有前瞻性的。将去中心化网络中产生的价值以中心化的形式交易，这本身就是违背区块链精神的。

当然，受限于诸多问题，分布式交易所暂时还很难成为现实，但是链路由至少解决了此前阻碍分布式交易所成为现实的两个核心的问题，即交易速度与跨链通信。首先，链路由解决了此前链间无法通信的问题，链间的通信为链间智能合约协作架起了桥梁，链间通信协议结合智能合约为跨链交易的原子性提供了保证，稳定的通信是一切跨链商务开展的基石。其次，集成了 DS-PBFT 共识算法的 AnnCore 通过投票的方式决定区块的生成，每轮的时间在 2 至 5 秒之间，拥有极快的出块速度，再加上，链路由和子链均具有水平扩展性，因此链网络完全有能力处理跨链交易。

我们相信，链路由技术一定可以推动分布式交易所的实现，为数字货币交易带来新的活力。

9 总结

在经过详细的市场调查和应用案例研究后，我们相信区块链将会成为众多行业的核心技术，改变这些行业的基础设施，推动革新。当前市场上并没有一套能够同时满足高流量、监管、隐私及可扩展性的完整的区块链架构。很多不同的应用场景，对区块链架构也会有不同的要求。

区块链路由网络是通过类比互联网路由的模式，将信息传递里理念放到区块链上的应用。链路由网络可以打通当前各区块链之间相互孤立的格局，最大限度的提升区块链的潜力，实现区块链之间的互联，互通，互信。

参考文献

[1] Economist Staff. "Blockchains: The great chain of being sure about things". The Economist, 18 June 2016.
[2] Morris, David Z. "Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting". Fortune (magazine), 2016-05-23.
[3] Popper, Nathan (2016-05-21). "A Venture Fund With Plenty of Virtual Capital, but No Capitalist". New York Times, 2016-05-23.
[4] Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". https://bitcoin.org/bitcoin.pdf, 2008.
[5] Buterin et al. "A Next-Generation Smart Contract and Decentralized Application Platform". https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper, 2014.
[6] Juan Benet. "IPFS - Content Addressed, Versioned, P2P File System". https://arxiv.org/abs/1407.3561, 2014.
[7] Lamport, Leslie et al. "The Byzantine generals problem". ACM Transactions on Programming Languages and Systems (TOPLAS) 4.3 (1982): 382-401.
[8] Szabo, Nick. "Formalizing and Securing Relationships on Public Networks". First Monday, 6 March 2014.
[9] Goldreich, Oded. "Secure multi-party computation". Manuscript. Preliminary version (1998): 86-97.