# “以链治链”架构下的监管链共识算法

## 现有区块链共识算法存在的问题

在公链中，因不存在准入机制，所以采用计算密集的PoW算法，共识操作会消耗大量计算资源；同时，为了保证共识协议的安全性，区块的共识速率被人为地限制，导致网络吞吐量较差；目前区块链系统中算力多集中在少数的矿池，使得51%攻击变为会切实发生的威胁，影响区块链系统的安全性。

在联盟链/私链这类存在准入机制的区块链中，共识协议普遍采用Crash Fault Tolerance方案，这在提高性能的同时牺牲掉了安全性，同时还存在着过强的安全假设，即要求加入节点是完全可信的，没有考虑到节点作恶的情况。

在“以链治链”架构下，如何调和监管需求与共识算法效率、安全性之间的矛盾，是本任务要解决的关键问题。

## “以链治链”架构下监管链共识算法详细技术方案

### 监管链区块设计

本方案扩展了区块链基本块结构，提出了监管区块结构的设计。设计思路如图2-1所示，本研究扩展了区块的事务消息内容，包括基本的操作信息Base Info、节点的状态信息Sys.Node Info和控制信息Control Info。节点信息用于维护信用节点评价指标体系，实现监督链节点相关数值的量化监控和评价，通过评价算法筛选合适节点构建节点候选集，实现节点的非交互、无感知、平滑地动态更新。控制信息包括授权信息和审计信息，用于监管链的扩容，提高系统吞吐量。

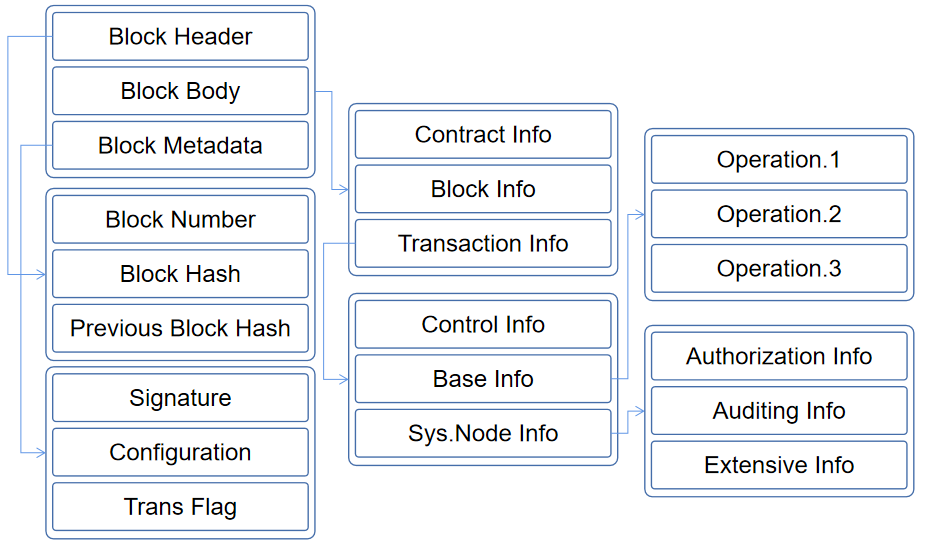


图 2-1 监管链区块结构基本设计思路

### 信用节点评价

以联盟链为基础的监管链摒弃了公共链通过PoW缓解拜占庭错误的方案，强化了权威节点的作用和能力。联盟链的权威节点通过了合法验证，降低作恶风险。本研究提出了信用节点评价指标，包括节点稳定度、节点联通度、数据合法性和哈希率。这四个指标综合反映了一个节点在审计链中的安全性、可靠性、稳定性和可用性。

### 信用节点分类

审计链的节点逻辑上分为三类：客户节点、中间节点和权威节点。通过强化权威节点保证审计链的工作效率，但权威节点并非一成不变。通过信用节点评价指标体系，对三类节点进行度量和评价。

### 节点动态更新

如图2-2信用节点分类与状态迁移，新加入的节点被认为是恶意节点，只有被评价指标体系认可的节点才能称为合法的节点，而且三种节点的身份可以相互转化。三种节点在功能上有重叠，权威节点拥有客户节点和中间节点所有的能力，中间节点具备客户节点的所有能力。

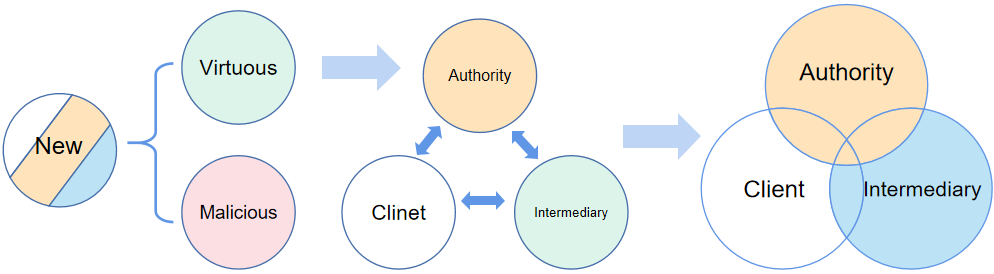


图 2-2 信用节点分类与状态迁移

### 非交互式选举

监管链通过非交互式选举方式实现权威节点的动态更新。通过2.2.2信用节点评价体系，构造权威节点候选集，并持续动态更新该集合。根据监管链的需要，权威节点通过候选集实时更新。被淘汰的节点失去权威节点身份，由候选集补充。权威节点之间通过内部协议达成快速共识。每次补充的权威节点在本次共识结束后加入网络。

权威节点的选择通过2.3成果展示的信用节点评价指标体系通过全网选举产生，选举活动和节点更新动作是异步的，不会造成阻塞，因此更新将非交互、无感知、平滑的完成。

### 网络扁平设计

监管链的三种节点组成立体扁平P2P网络结构。根据节点类型设计整体分层网络，局部扁平P2P网络，分层结构实现网络低成本扩容与演进。如图2-3所示，低层级节点向高层级节点汇聚，节点之间组成P2P的扁平拓扑结构。不同层级的组网自下而上，组成立体网络，并保持去中心化结构。

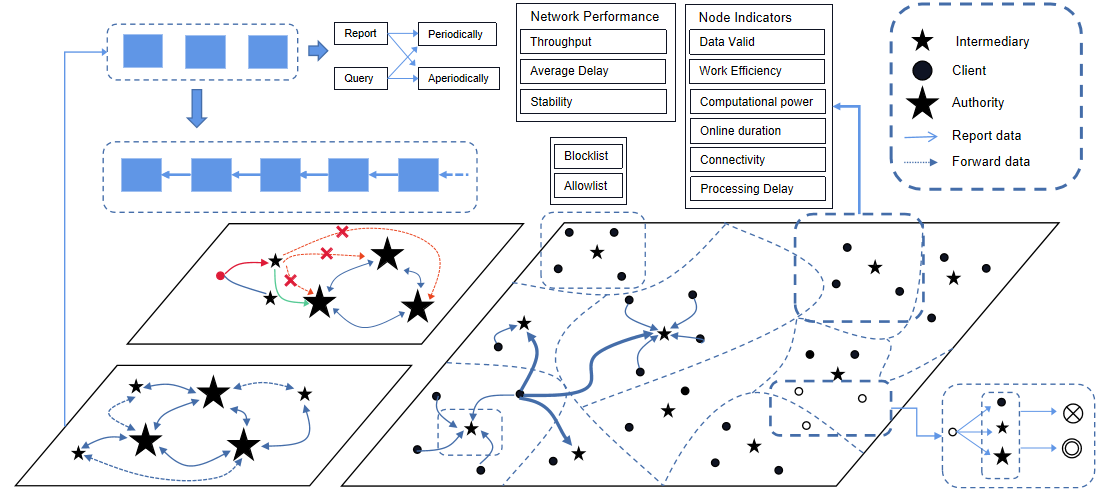


图 2-3 监管链分层扁平网络结构

## 阶段性成果

本研究扩展了区块链基本块结构，提出了监管区块的设计。将监督链节点划分为客户节点、中间节点、权威节点三种类型。提取三种节点的共性指标，对其量化描述，依据信用节点评价指标体系构建节点演进算法从而构建候选集。依赖候选集通过非交互式地进行节点的动态更新。

### 信用节点评价指标

在2.2.3中将节点分为三类。权威节点是可信、稳定的，同时应当具备一定算力。本研究提出了多项指标评估一个节点是否具备能力担任权威节点角色，从节点的在线时长、联通度、误码率、算力等方面考量。

Stability Value(SV)：稳定度反映了一个节点在网络中的稳定在线时长。只有SV超过预设特定阈值的节点才有资格成为核心节点。

网络所有节点组成的网络拓扑结构是动态变化的，有的节点稳定在线，有的节点频繁的上线和下线。假设网络核心节点在一个时间片段*t*内数量是固定的，*a*代表网络平均核心节点算力，*n*代表网络核心节点数量。当前网络的总算力*s* = *a·n*。算力*s*刚好满足当前网络处理数据的要求。但是比例*m*的节点在线时间不稳定，为了保证网络的业务处理最低能力，只能保守地把全网算力降为s = *(1-m)·a·n*。对应的，需要降低区块的目标难度。

显然，网络的整体算力变化应该处于一个合理的区间，所以网络中提供算力的节点就需要稳定在线。一个刚加入网络的节点*n*，在时间片段*t*内，在线时长*t1*，离线时长*t2*，离线次数*Toff*，网络要求在线时长*td*。

Degree Value(DV)：节点度是指和该节点相关联的边的条数，又称关联度。网络鼓励节点与更多的节点通信，避免网络出现割边或割点。网络的平均DV提高后，一方面提高网络的稳定性，另一方面减少矿池的出现和私自挖矿等攻击。因此节点的*DV*越高，越可信。低*DV*的节点被认为是孤立的节点。

假设节点*n*在时间片段*t*内与*m*个节点通信，那么节点*n*的*DV*为

假设若干个节点之间相互通信，组成矿池。网络认为这几个节点也是逐渐变为孤立点，其*DV*值逐渐弱化，网络设定衰减系数，新增节点*m*个，表示为：

Validity Value(VV):数据有效性主要衡量两个指标，一方面是衡量节点在规定时间内数据传输精确性。另一方面衡量节点在规定时间内数据的有效性。精确性体现在一个节点如果转发和确认的数据与原数据有差异，可以认为数据被修改。有效性体现在一个节点如果转发和确认的数据已经存在于区块链上，可以认为数据是无效的。*VV*保证了数据的正确性，避免数据被窜改。*VV*也避免了数据重复被确认，造成网络资源的浪费。

假设节点*n*在时间片段*t*内的接受到数据，转发正确数据，打包数据*，*确认有效数据*，*网络的合法性最小值是，*VV*的计算如下：

Computational Power(CP):算力（也称哈希率）是网络处理数据能力的度量单位。即为计算机（CPU）计算哈希函数输出的速度。网络必须为了安全目的而进行密集的数学和加密相关操作。在某一时间段t内，网络处理段数据量是一定的。网络在*t*内处理这些数据需要算力*m hash/s*，全网符合要求的核心节点数量为*n*，则单节点的算力为

网络的数据处理能力需要不断提升，所以核心节点的数量和核心节点的算力也要提升。算力可以作为限制条件排除一些低算力的节点，算力也可以作为竞争指标增强节点的可信度。如果存在一个节点*x*，其算力，网络平均算力为，且有：

节点*x*将在网络中占据主导地位。因此本研究限制节点的算力不可无限膨胀，网络规定底数，以为底的对数作为算力度量值。在鼓励节点增加算力的同时，限制节点进行算力攻击。如下：

### 多维权威节点选举机制

本研究提出了多维度指标描述节点的各项性能。这些指标综合体现一个节点的可信度。节点x的可信度表示如下：

,,和表示节点x的稳定度、联通度、数据有效性和算力在可信度中的权重。根据TSN对各个指标需求，各项权重可以调整，且满足

### 区块与数据结构

本研究扩展了区块的事务消息内容，包括基本的操作信息Base Info、节点的状态信息Sys.Node Info和控制信息Control Info。节点信息包括2.3.1提出的信用节点评价指标，这些指标用于维护信用节点评价指标体系，实现监督链节点相关数值的量化监控和评价，通过2.3.2多维权威节点选举机制筛选合适节点构建节点候选集，实现节点的非交互、无感知、平滑地动态更新。

如图2-4是区块结构和数据结构设计，区块数据结构的设计目标是实现对被监管链审计的同时，实现网络的可扩展性。审计链在主链存储对被监管链审计的事务，随着网络扩展，主链从传统事务链平滑演进为控制链。区块将从初始区块、过渡区块、控制区块动态演进。控制链存储对扩展子链的控制信息。同时通过叔区块存储网络中的争议和分歧，并通过激励机制鼓励节点同步叔区块，并在主链侄节点存储叔区块相关信息。

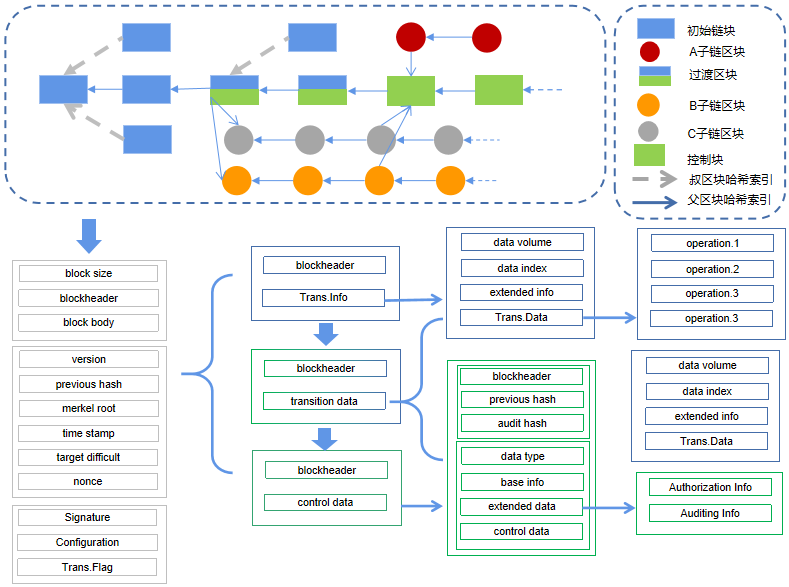


图 2-4 监管链区块与数据结构

## 结论

现阶段工作已完成监管链数据结构和网络结构的初步设计思路（2.3.3），建立了实现节点分级的信用节点评价指标（2.3.1），并依据评价指标设计了多维权威节点选举算法（2.3.2）。

本阶段的工作围绕节点动态更新和候选集构建开展，缺乏对系统安全性、吞吐量和扩展性的整体思考和系统设计。

下一年度的工作将重点围绕PBFT性能问题，5000tps吞吐量挑战等方面展开。同时应用层和共识层的信任机制解耦需求迫切，本研究将提出应用共识解耦的具体方案。在候选集构建、节点动态更新、PBFT改进等方面形成高质量SCI论文1篇、专利1个、软件著作权1项。