摘要（研究内容、研究方法、研究结论各提供1-2句话概括，总字数100字以内）

本研究提出监管链共识算法的设计需求，完成算法的技术实现。通过划分网络节点、构建节点评价指标体系、设计权威节点选举机制算法，实现了信用节点候选集构建和信用节点非交互式动态更新。本研究将有效支撑下一阶段PBFT算法改进、吞吐量提高、应用共识解耦等工作。

关键字（1-2个）

共识算法； 指标体系

# 引言

课题X总的研究目标是。（不用写）

本年度，课题的研究内容主要包括以下2个方面。（各任务描述各自合同规定的阶段或年度研究任务的目标、内容、方法等要点。）

研究监管链共识算法的设计需求：以联盟链为基础，基于实用拜占庭容错、POA等算法，提出了满足满足监管需求的区块链设计，保证监管链安全可信、提升吞吐量、避免网络风暴、增强网络扩展性。

研究监管链共识算法的技术实现：以实用拜占庭容错、POA等算法为基础，通过优化事务元数据提取、并行化交易背书验证、角色权限动态调整、应用共识解耦等技术手段，设计满足目标需求的监管链原型。

完成2021年年度《技术进展报告》1篇。

# 研究概述

## 研究背景及意义（不用写）

。

## 课题四与其它课题的关系（不用写）

。

## 课题四研究内容

### 拟解决的关键科学与技术问题（各写1-2个）

设计满足监管需求，安全可信、吞吐量高、易扩展的监管链；并以实用拜占庭容错[1]、POA[2]等算法为基础，通过优化事务元数据提取、并行化交易背书验证、角色权限动态调整、应用共识解耦等技术手段，设计满足目标需求的监管链原型。

### 拟开展的主要研究内容（任务研究内容）（一段话）

研究联盟链环境下的新型共识算法，设计基于实用拜占庭容错（PBFT）[3]等基础算法的快速共识方法，探索交易元数据提取与优化、交易背书与验证并行化、节点角色动态调整[4][5][6]、节点信用分级与排序等机制，解决固定功能节点易遭攻击、大规模交易高并发造成的网络风暴等问题，提高监管链的安全性与效率。

### 研究技术路线（任务技术路线）（文字+至少1张图）

监管链的新型共识机制拟采用联盟链的拜占庭容错算法为基础架构，拟通过抽取交易的基础元数据重建交易的排序流程，并优化验证协议以充分实现背书策略验证等操作的并行化，大幅提高系统的吞吐率；拟构建节点候选集，利用可验证随机函数等密码学技术设计非交互式选举协议，实现背书节点等重要角色的动态更新，并引入信用模型对节点进行分级排序，实现应用层的信任机制同底层共识协议的解耦，提高系统的安全性与可扩展性。

如图1.1，本研究基于基础区块链数据结构和密码学原理[7]，扩展了区块的数据结构，满足监管链共识算法数据层要求。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。共识算法包括优化验证流程和评价指标体系两部分。

优化验证流程改进事务元数据，重构事务排序，并利用事务数据缓存和并行验证的方法提升网络吞吐量[8][9]。评价指标体系根据节点功能划分节点类型，建立节点演进模型，支撑建立节点信用评价。量化信用节点关键指标，基于演进模型、网络性能、安全需求、扩展能力，设计信用节点评价算法，以非交互、无感知、平滑地方式实现节点动态更新。

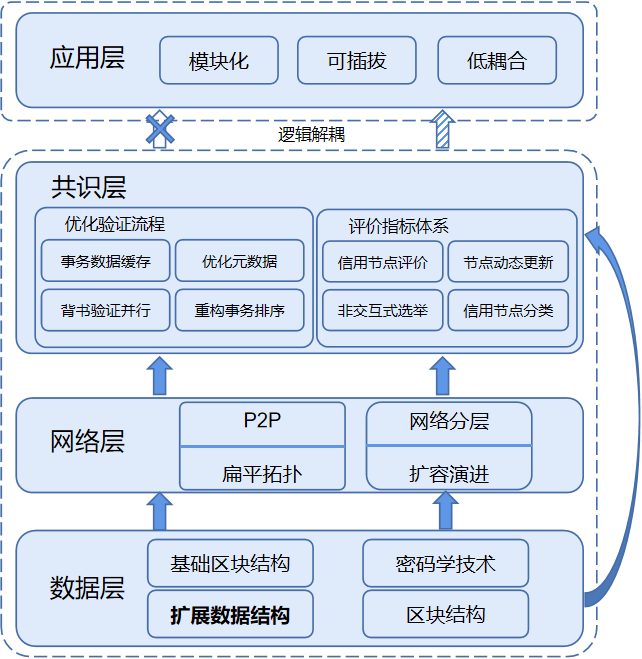


图1.1 监管链共识算法技术路线图

# （各任务阐述**阶段研究的过程、技术内容、进展或阶段成果，提供必要的数据图表）**

# “以链治链”架构下的监管链共识算法（各任务名字）

## 阶段性研究内容

研究监管链共识算法的设计需求：以联盟链为基础，基于实用拜占庭容错、POA等算法，提出了满足满足监管需求的区块链设计，保证监管链安全可信、提升吞吐量、避免网络风暴、增强网络扩展性。

研究监管链共识算法的技术实现：设计满足监管链需求的区块结构，支撑监管链共识算法实现。设计监管链共识算法，利用事务数据缓存[10]和并行验证[11]的方法提升网络吞吐量。构建信用节点评价指标体系，实现节点非交互式动态更新。

## 研究技术路线（技术实现方法）

### 监管链区块设计：

本研究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。

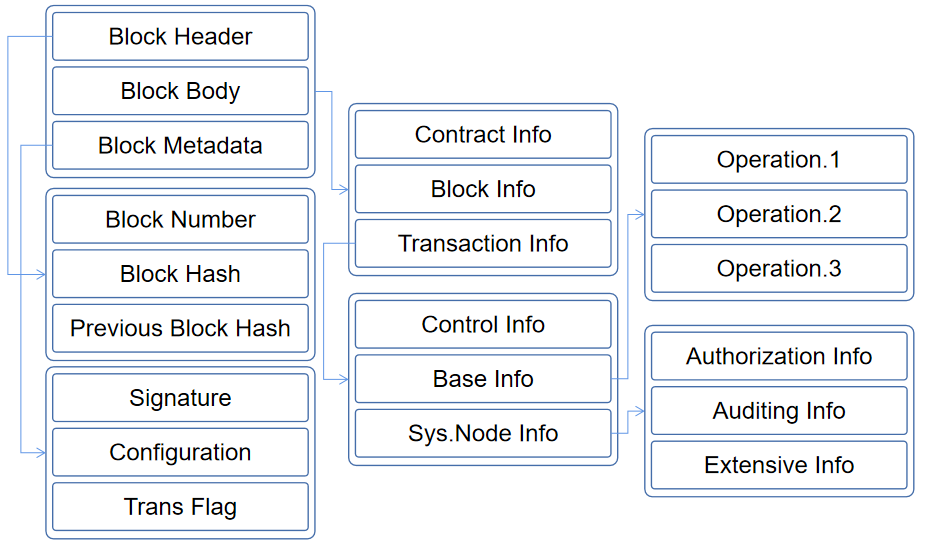


图2.1 监管链区块结构基本设计思路

### 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[12]缓解拜占庭错误的方案[13]，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。

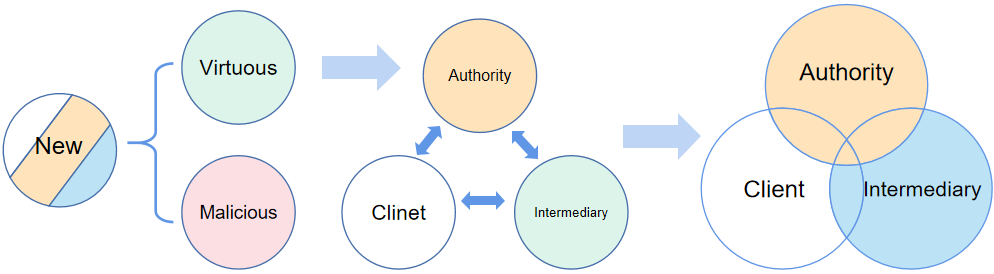


图2.2 信用节点分类与状态迁移

### 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[14]。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。

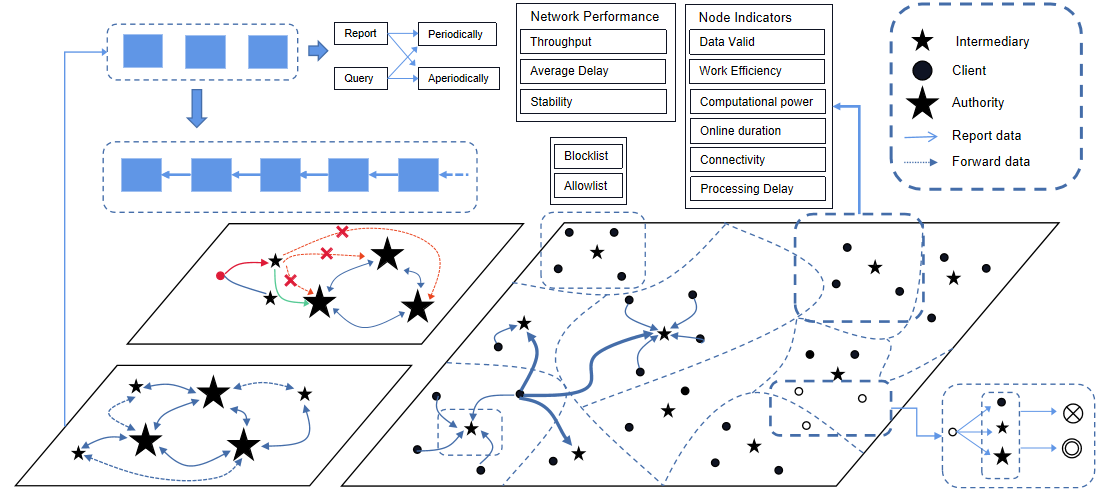


图2.3 监管链分层扁平网络结构

## 进展或阶段性成果

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。我们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。我们从节点的在线时长、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。我们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。

我们假设节点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。

我们假设节点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。因此我们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

我们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。

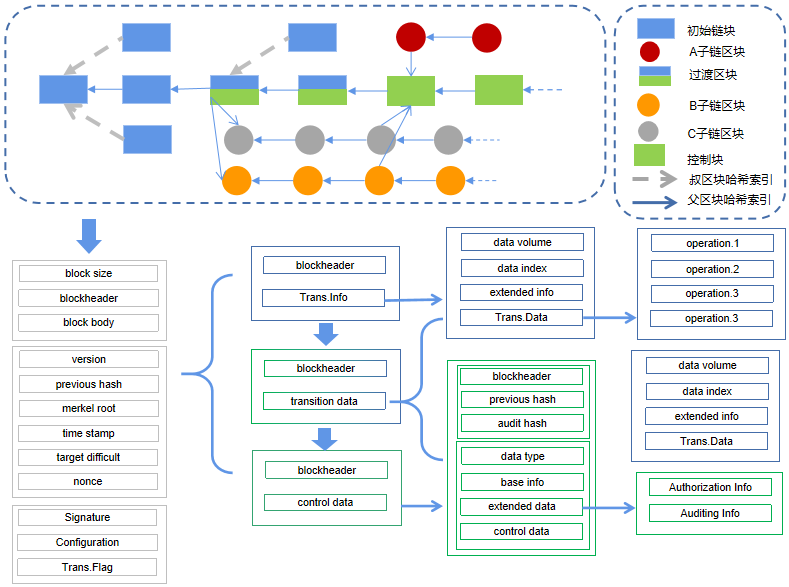


图2.4 监管链区块与数据结构

## 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。

（阶段研究工作完成情况、经验和教训、下一年度或下一阶段的工作计划和建议）

参考文献

（参考文献的著录遵照GB/T 7714《文后参考文献著录规则》 的规定执行。）

[1]Miguel, Castro, Barbara, et al. Practical byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4):398-461.

[2]OpenEthereum. Proof of Authority[EB/OL]. [2021.10.15]. https://github.com/paritytech/parity/wiki/Proof-of-Authority-Chains

[3]Dinh T, Wang J, Chen G, et al. BLOCKBENCH: A Framework for Analyzing Private Blockchains[J]. 2017.

[4]Christian Cachin. Architecture of the hyperledger blockchain fabric[EB/OL]. 2016[2021]. https://www.zurich.ibm.com/dccl/papers/cachin\_dccl.pdf.

[5]Corda. R3 Corda[EB/OL]. [2021]. https://github.com/corda/corda/.

[6]Gideon Greenspan. Multichain[EB/OL]. [2021]. https://www.multichain.com/.

[7]Bitcoin: A Peer-to-Peer Electronic Cash System[J]. Social Science Electronic Publishing.

[8]Bessani A, Sousa J, Vukoli M. A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform[C]// the 1st Workshop. IEEE Computer Society, 2017.

[9]Yin M, Malkhi D, Reiter M K, et al. HotStuff: BFT Consensus in the Lens of Blockchain[J]. 2018.

[10]Nathan S, Thakkar P, Vishwanathan B. Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform[C]// 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS). IEEE, 2018.

[11]Gorenflo C, Lee S, Golab L,et al. FastFabric: Scaling hyperledger fabric to 20000 transactions per second[J]. International Journal of Network Management, 2020, 30(5).

[12]Garay J, Kiayias A, Leonardos N. The Bitcoin Backbone Protocol: Analysis and Applications[C]// Springer Berlin Heidelberg. Springer Berlin Heidelberg, 2015.

[13]Vukoli M. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication[C]// International Workshop on Open Problems in Network Security. Springer International Publishing, 2016.

[14]Cachin C, Guerraoui R, Luís Rodrigues. Introduction to reliable and secure distributed programming[M]. 6. Springer, 2011 :281-339.