文章编号：2095-2163(2023)01-0213-09 中图分类号：TP393.03 文献标志码：A

基于委员会轮换机制的跨链数据整合技术研究

许 倩[1]，翟健宏[2]
（1 哈尔滨工业大学 计算学部 哈尔滨 150001；2 哈尔滨工业大学 计算学部网络空间安全系，哈尔滨 150001）

摘 要：随着区块链技术的发展，区块链的应用场景也不断丰富和复杂，而能够进行高效安全的跨链操作是区块链技术大规模落地应用的必备条件，因为不同区块链网络可以拥有不同协议和架构，造成不同区块链之间难以跨链操作。本文在研究已有的跨链技术的基础上，结合信任度评价的思想，设计基于委员会轮换机制的跨链数据整合方案，为跨链技术的研究提供一个新的解决思路。方案设计动态信任模型，引入遗忘机制，对信任随时间的变化进行建模；以节点的信任度为标准选举委员会成员，作为跨链消息传输媒介；同时，本文参考 PBFT 共识算法的思想设计了基于距离的消息验证机制，委员会成员通过基于距离的消息验证机制对消息进行验证和签名，达成一致。

关键词：跨链技术；共识算法；遗忘机制；信任模型；委员会轮换机制

Research on cross-chain data integration technology based on committee rotation mechanism

XU Qian[1], ZHAI Jianhong[2]
(1 Faculty of Computing, Harbin Institute of Technology, Harbin 150001, China;
2 Department of Cyberspace Security, Faculty of Computing, Harbin Institute of Technology, Harbin 150001, China)

【Abstract】 With the development of blockchain technology, the application scenarios of blockchain are constantly enriched and complex, and a safe and efficient cross-chain operation is a prerequisite for the large-scale application of blockchain technology. However, because different blockchain networks can have different protocols and architectures, different blockchains are isolated from each other, making it difficult to perform cross-chain operations. Based on the research of existing cross-chain technologies, this paper proposes a new cross-chain consensus algorithm and designs a cross-chain data integration scheme based on committee rotation mechanism by combining the idea of trust evaluation, which provides a new solution for the research of cross-chain technology. This paper designs a dynamic trust evaluation model that introduces the forgetting mechanism, and the trust model over time. The committee members are elected as cross-chain message transmission mediums based on the dynamic trust degree of the network nodes. At the same time, this paper designs a distance-based message verification mechanism with reference to the idea of PBFT consensus algorithm. Committee members verify and sign messages through this message verification mechanism and reach a consensus.

【Key words】 cross-chain technology; consensus algorithm; forgetting mechanism; trust model; committee rotation mechanism

0 引 言

2009 年，比特币作为第一种虚拟货币诞生，标志着区块链技术在金融领域首次得到正式应用。比特币交易是建立在 P2P 网络的基础上，在比特币系统中，通过挖矿创建区块链，矿工将交易打包进区块，使得已付款的交易变成“确认”状态以获取信赖。依据其不同架构，区块链的发展可分为 3 个阶段：第一阶段是比特币区块链，该阶段以数字加密货币区为主要特征，旨在使任何两个区块链帐户能够顺利地进行节点对点的业务而无需第三方中介机构；第二阶段是以太坊区块链，该阶段以智能合约为主要特征，其特点是使用以太坊虚拟机（EVM）对区块链进行复杂算法的编程，通过编写智能合约使得区块链可以在电子货币之外的更丰富场景中得到应用；第三阶段是超越货币、金融范围的区块链应用，这一阶段区块链充分融入人们的生产和生活，可被称为区块链时代。

2021 年 10 月 28 日，在 Facebook Connect 大会上 Facebook 首席执行官马克·扎克伯格宣布将

作者简介：许 倩（2000-），女，本科生，主要研究方向：区块链技术、计算机应用技术；翟健宏（1968-），男，硕士，副教授，主要研究方向：网络内容安全、网络安全、云安全等。

收稿日期：2022-05-29

Facebook 更名为“Meta”,来源于“元宇宙”,称要在 5 年内转型成为一家元宇宙公司。2021 年 9 月 16 日,清华大学新闻与传播学院新媒体研究中心发布了《2020 年—2021 年元宇宙发展研究报告》,将“区块链”作为元宇宙的底层架构之一,在区块链框架下搭建社交平台、经济平台,并结合 UGC 搭建内容平台。这表明,在元宇宙元年的 2021 年,区块链将迎来一个发展的热潮。

由于区块链技术构建的是若干个彼此隔离、无法通讯的完全单独的网络,所以每个节点也无法全部处在同一个网络中。除了公共链是可以广泛共存的,私人链和联盟链可以支持各个组织都拥有各自的区块链,甚至在一个组织内部也能够同时运行多条区块链,所以这些区块链可以彼此独立,在单独属于自身的网络中工作。但是由于区块链技术应用场景不断丰富和复杂,各个区块链网络间往往彼此隔离,从而导致块链间无法有效跨链操作,这使得通过区块链技术实现全球价值互联甚至是全球范围内的“元宇宙”的愿望难以实现。目前学术界有许多跨链技术的设计方案,但大多都有中心化或易受到攻击等各种风险,很难将其在实际中应用。在区块链跨链技术尚未成熟的今天,距离达到区块链技术的大规模落地应用的目标还有一段距离。

本项目在研究已有的跨链技术的基础上,旨在提出一种新的跨链共识算法,结合信任度评价的思想,设计一个可行的跨链数据整合方案并对方案的实施进行实验分析,为跨链技术的研究提供新的解决思路和实践基础。

1 国内外研究现状

Ripple 实验室于 2012 年提出了 Interledger 协议,并在 2015 年 11 月发布 Interledger 白皮书[1]。Interledger 协议(ILP)作为跨链解决方案公证人机制的代表,解决了区块链不同账本之间的协同问题。ILP 协议支持账本之间的安全转移,并允许在两个账本上的任何账户成员之间创建连接。2013 年 Herlihy[2] 提出了原子交换的基本理念,原子交换是一种支持不同区块链网络之间资产快速交换的技术。“原子”代表了交易的一致性,因此原子交换将交易划分为两种类型:完全成功或完全失败。2014 年 BlockSream 提出了侧链机制,通过双向楔入技术,一笔资产进行交易时首先在主链上锁定,确认无误后在侧链上释放,以此实现价值的跨链转移。2016 年 Cosmos[3] 被提出,基于建立区块链互联网的构想,使用 Tendermint 共识引擎和 IBC 协议构建出一个支持异构区块链接入并进行互操作的网络。2017 年 Block Collider 项目构建了在多个区块链块集上的高速分布式账本,将这些链集成在一起并支持许多跨链功能。在区块生成上,BlockCollider 的每个块都引用每个桥接链的头块——这个元组被称为“基元组”,以此来统一每个桥接链上的最新区块,并在 PoW 的基础上设计了一种基于字符串编辑距离的 Proof of Distance 共识算法来提高挖矿效率。

虽然国内对区块链跨链技术的研究起步较晚,但是近几年也产生很多优秀的研究方案,给予了国内研究者很大的信心和鼓励。2018 年,张诗童、秦波和郑海彬[4] 基于哈希锁定技术提出了一个多方跨链协议,协议依据图的搜索策略设计了“边着色”自动撮合交易算法,同时提出一种价格磋商机制,解决了多方跨链资产的清结算问题;2019 年,赵涛等[5] 借鉴路由器特点,提出了一个基于聚类簇中心的共识跨链交换模型;李莎莎等[6] 针对主从多链,利用逻辑回归设计了基于信誉度的智能合约;2021 年戴炳荣等[7],通过改进 Google 用于网页重要性评价的 PageRank 算法,提出跨链公证人机制评价模型;同年,谢家贵等[8] 提出了一种基于星火区块链的跨链机制,设计了一种主链可以接入两种类型的子链:同构子链和异构子链的新型主子链架构,并通过骨干节点执行中继合约完成跨链通信;2020 年 10 月,杭州趣链科技有限公司联合浙江大学计算机科学与技术学院共同提出了兼容异构区块链的通用跨链协议 IBTP,并研发了一个基于侧链中继的异构区块链互操作平台 BitXHub[9]。

2 基于委员会轮换机制的跨链数据整合方案

2.1 基于委员会轮换机制的跨链数据整合方案总体设计

对区块链网络进行拓扑和建模,如图 1 所示。假设 i 为区块链编号,则集合 L_i 代表区块链账本中属于链 i 的一个节点集,$L_i = \{p_{i1}, p_{i2} \cdots, p_{in}\}$,其中 p_{in} 表示链 i 中的节点。图 1 中有 3 条区块链,其节点集为 $\{L_1, L_2, L_3\}$;区块链之间的跨链操作即节点集之间的互操作和数据访问,即 L_i 跨链向 L_j 发送或接受数据是可行的;集合 C 表示形成中继链的一组委员会节点,C 中的节点来自已有区块链;委员会 C 中蓝色节点来自区块链 1,绿色节点来自区块链 2,橙色节点来自区块链 3。

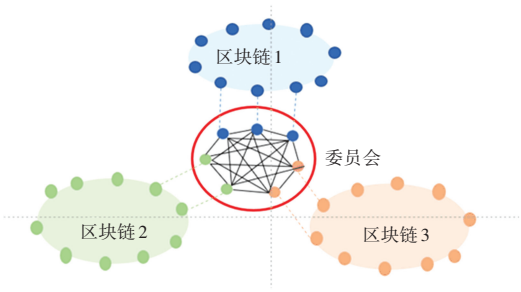


图 1　区块链跨链网络模型

Fig. 1　Blockchain cross-chain network model

跨链方案的核心分为两部分：节点信任度的动态评估和定期委员会轮换机制。

对于每条链，在时间 t 时，计算每个节点之间的信任关系，构建节点之间的信任关系矩阵 $\boldsymbol{D}^t$，并将信任度进行正则化处理，得到最终的信任关系矩阵 $\boldsymbol{C}^t$；为了充分考虑链中所有节点之间的信任和交互，根据间接节点的信任关系，计算节点之间的信任关系，得到信任的迭代公式 $\boldsymbol{T}_k^t = \boldsymbol{C}_k^t \boldsymbol{T}_{k-1}^t$；通过迭代得到全链节点的信任值矩阵 $\boldsymbol{T}^*_i$。

对于得到信任值矩阵的链，根据其节点数目占所有链节点的比例进行委员会节点分配。在每条链上的可靠节点中，选择信任值排在前 c_i 的节点作为委员会节点。每条链选择出该链的委员会成员，共同管理委员会中继链。对于跨链的交互，当 $n_u \in L_x, n_s \in L_y, n_u$ 对 n_s 发送消息时，L_x 的委员会节点启动跨链消息传递进程，将消息打包成标准格式，在委员会成员中进行广播和验证。通过 L_y 的委员会节点进行背书请求和签名接受，最后完成跨链消息的验证，对消息进行保存。当委员会处理了 B 个消息后，所有链进行信任度的重新计算，委员会进行更新。

2.2　动态信任度计算模型

2.2.1　单个节点的信任关系计算

在网络中，信任度计算所需的信息可以从以下 3 方面进行收集[10]：

(1)态度：表示主体(发送方)对客体(接收方)持有的积极或消极看法，即是否愿意向客体发送消息；

(2)行为：表示客体对主体动作的反应行为，主体可以据此来确定对客体的信任程度；

(3)经验：是在一次交互中客体对主体行为的感知，会对信任度的确定产生影响。

对于上述 3 个因素，经验往往会影响态度和行为。因为过去的好的经验会促使客体对主体做出积极响应，同理过去不好的经验会促使主体对客体产生消极看法，进而影响两者的信任关系。因此本文选择并收集经验来进行之后的信任计算。

为了获得经验，固定主体(发送方)，设为 A，观测其他节点对主体节点动作的积极行为反应和消极行为反应，来收集在主体节点视角下客体节点的行为信息，此行为信息作为之后信任度评估的信任信息。对于观察者 A 来说，B 的积极行为数目用 a 来表示，a 初始化为 0；B 的消极行为数目用 b 表示，b 初始化为 0。当 A 观察到 B 是正常行为时，$a = a + 1$；当 A 观察到 B 是异常行为时，$b = b + 1$。对于时间 $t = n * \Delta t (n = 1,2,3,\cdots)$，得到第 n 个 Δt 的行为信息列表 $\{a_n, b_n, t_n\} (n = 1,2,3,\cdots)$。

基于观察者 A 收集到的 B 的积极行为和消极行为的信息，可以使用贝叶斯分布来对信任度进行计算。因为 beta 分布灵活且较为简单，且仅有两个参数，本文使用 *beta* 概率分布方程来刻画信任度，公式(1)：

$$beta(p \mid \alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\,\Gamma(\beta)} p^{\alpha-1} (1-p)^{\beta-1} \quad (1)$$

其中，α 表示正因子；β 表示负因子；$\alpha = a + 1$，$\beta = b + 1, 0 \leqslant p \leqslant 1, \alpha, \beta > 0$。

beta 分布概率的期望，公式(2)：

$$E(P) = \frac{\alpha}{\alpha + \beta} \quad (2)$$

使用期望来表示对于 A 来说 B 的信任度，公式(3)：

$$t_d = \frac{\alpha}{\alpha + \beta} = \frac{a + 1}{a + b + 2} \quad (3)$$

为了描述事件对信任度评估的动态影响，引入遗忘机制。因为过去观察结果对当前时间段的信任评估的影响会随着时间的增加而减弱，即过去的观察所占的权重低于近期观察的权重。由此，引入遗忘机制来模型化这个影响减弱的现象：在时间 t_1 时表现出 K 个积极行为和在时间 $t_2 (t_2 > t_1)$ 表现出 $K\beta^{t_2 - t_1}$ 个积极行为是等价的，其中 $\beta (0 < \beta \leqslant 1)$ 表示遗忘因子。

假设从 t_1 到 t_2，分别有 Δa 和 Δb 个新增的积极行为和消极行为，则在时间 t_2，a 更新为 $(a\beta^{t_2 - t_2} + \Delta a)$，$b$ 更新为 $(b\beta^{t_2 - t_2} + \Delta b)$。因为持续的积极行为会产生较好的声誉，因此当信任度大的时候，只有很少一部分坏的行为会破坏声誉，即信任度越大，遗忘因子越小，因此可以使 $\beta = 1 - t_d$。

在单个时间段内如何进行信任度评估的详细表述见表 1。

表 1 单个节点的每个时间段的信任计算算法

Tab. 1 Trust calculation algorithm for each time period of a single node

算法 1:对于单个节点每个时间段的信任计算算法(建议伪代码再伪点)

初始化:

设置遗忘因子 $\beta(0 < \beta \leqslant 1)$

令 a'_n, b'_n 表示在遗忘机制下在时间 $t_n = n \cdot \Delta t(n = 1,2,3,....)$ 时的积极行为数目和消极行为数目。初始化 $a'_1 = a_1, b'_1 = b_1$。

迭代:

For $n = 1$ to N

If $n = 1$ then

$$T_{d,t_n} = \frac{a'_n + 1}{a'_n + b'_n + 2}$$

Else

$$a'_n = a'_{n-1}\beta^{\Delta t} + a_n, b'_n = b'_{n-1}\beta^{\Delta t} + b_n$$

$$T_{d,t_n} = \frac{a'_n + 1}{a'_n + b'_n + 2}$$

End if

$$\beta = 1 - T_{d,t_n}$$

End for

输出:

时间 $t_n = n * \Delta t(n = 1,2,3,....)$ 时的 B 的信任度 T_{d,t_n}

2.2.2 信任关系矩阵构建

由算法 1,得到在节点 A 视角下的不同时刻 $t_n = n * \Delta t$ 时节点 B 的信任度 T_{d_B,t_n}。对于任意节点 i,可以得到不同时刻 $t_n = n * \Delta t$ 下,对其他节点的信任度向量 $\boldsymbol{T}^{i,t_n}, \boldsymbol{T}^{i,t_n} = \{\boldsymbol{T}_{d_1,t_n}, \boldsymbol{T}_{d_2,t_n}, \boldsymbol{T}_{d_3,t_n}, \cdots\}$。

由此,构建节点间信任关系矩阵 $\boldsymbol{D}^{t_n}$, $\boldsymbol{D}^{t_n} = [\boldsymbol{T}^{1,t_n}, \boldsymbol{T}^{2,t_n}, \cdots, \boldsymbol{T}^{n,t_n}]^{\mathrm{T}}$。

$D_{ij}^{t_n}$ 表示在时间 t_n 时,节点 i 对节点 j 的信任关系;节点自身的信任度为 0,即 $D_{ii}^{t_n} = 0$;不存在交易和区块链交互行为的节点(即 $a = 0$,且 $b = 0$ 的一对节点)的信任关系为 0.5。

为了防止恶意节点给其他恶意节点较高的信任值,给正常节点较低的信任值,从而影响到最终信任代表节点的选取,故将节点之间的信任值进行正则化处理,得到最终的信任关系矩阵 $\boldsymbol{C}^t$, 公式(4):

$$\boldsymbol{C}_{ij}^{\ t} = \frac{D_{ij}^{\ t}}{\sum_j D_{ij}^{\ t}} \tag{4}$$

2.2.3 全链节点的信任值

节点可以通过检测其他节点的行为得到节点和其它节点之间的信任关系,但事实上节点还可以利用其他节点的信任信息,对该节点做进一步的信任评估。比如节点 A 对节点 D 的信任度,除了依据节点 A 与 D 的交互行为直接判断之外,还可以通过其相邻节点 B 和 C 进行间接计算。即对于任意节点 i,在时间节点 j 的信任度可以通过 i 的相邻节点作为间接节点进行计算,公式(5):

$$d_{ij} = \sum_k d_{ik}\, d_{kj} \tag{5}$$

其中,节点 k 是节点 i 的相邻节点; d_{ik} 表示节点 i 对节点 k 的信任度; d_{kj} 表示节点 k 对节点 j 的信任度。

为了充分考虑链中所有节点之间的信任和交互,本文根据间接节点的信任关系计算节点之间的信任关系。以此类推,最终利用全网节点的信任关系计算节点的信任值。其中迭代公式(6)为:

$$\boldsymbol{T}_k^t = \boldsymbol{C}^{\,t}\boldsymbol{T}_{k-1}^t \tag{6}$$

其中, $\boldsymbol{C}^t$ 表示上述信任关系矩阵; $\boldsymbol{T}$ 是一个 $n \times 1$ 的列向量; $\boldsymbol{T}_k^t$ 表示第 k 次迭代后的节点信任矩阵。

信任矩阵 $\boldsymbol{C}$ 中的每个元素表示节点之间的直接信任关系,信任度高的关系数值接近 1,信任度低的关系数值接近 0,节点之间交互很少的情况下为 0.5。初始化每个节点的信任值都是相同的,为 $\frac{1}{n}$,因此 $\boldsymbol{T}$ 初始值为一个值全为 $\frac{1}{n}$ 的列向量。假设收敛误差为 ε, 根据迭代公式不断迭代,直至收敛得到最终全链节点的信任值。节点信任值的计算算法见表 2。

表 2　全链节点的信任值计算算法

Tab. 2　Trust value calculation algorithm of full-chain nodes

算法 2：全链节点的信任值计算

输入： $\boldsymbol{C}, \boldsymbol{T}_0, \varepsilon$

输出： 最终信任值向量 $\boldsymbol{T}^*$

初始化：

$\boldsymbol{T}_0 = e/n$ and $k = 1$;

迭代：

Repeat

计算第 k 次迭代结果 $T_k^t = \boldsymbol{C}^t T_{k-1}^t$;

计算和上一次迭代结果之差 $\sigma = \| T_k^t - T_{k-1}^t \|$

Until($\sigma < \varepsilon$)

END

2.3　基于定期委员会轮换的共识算法

2.3.1　委员会的建立和迭代

委员会是从每条链中选择若干特殊节点经选举组成，委员会成员之间通过协议进行消息的传递和确认，并在规定时间进行委员会成员的重新选举。委员会的建立分为两方面：委员节点的分配和委员会成员的选举与更迭。

2.3.1.1　节点分配算法

设 $\bigcup_{i=1}^{n} L_i = L, c = |\boldsymbol{C}|, c_i$ 表示委员会 $\boldsymbol{C}$ 中属于 L_i 的节点的数目。$\boldsymbol{C}$ 容错为 $O = \dfrac{c-1}{3}$，则节点分配算法为：

(1) $\forall c_i^{'}, 1 \leqslant c_i^{'} \leqslant O$;

(2) 计算 $c_i^{'} = \dfrac{|L_i|}{|L|} \times c$;

(3) 若 $c_i^{'}$ 满足 ① 则 $c_i = c_i^{'}$，否则，额外的节点将被分配到其他更小的子集。通过上述算法，得到每条链 L_i 中应被选出的委员会节点的数目 c_i。

2.3.1.2　委员会成员选举与更迭

对于每个节点 $n_i \in L_i$，选择(IP,PK)[IP 地址和公钥]作为其识别。从链集合 $\{L_1, L_2, \cdots L_n\}$ 中分别选择 $\{C_1, C_2, \cdots, C_n\}$ 节点作为委员会节点构成中继链，其中 $|C_i| = c_i$。

在算法 2 中，得到了在全链节点的信任值向量 $\boldsymbol{T}^*$。为了使链中被选举称为委员会的节点能够被其他节点充分信任，同时也为了提高整体信任度，在链的所有节点中，选择信任值最大的前 c_i 个节点作为委员会成员。

在本文的跨链数据传输中，委员会成员是中间枢纽和核心，起到至关重要的作用。为了防止委员会成员中心化，从每条链中选举出大于 1 个委员会成员；同时，委员会成员也很难维持其信任度一直处于较高水平，因此在一定时间后，需要重新竞争委员会节点，选出新的委员会成员。对于算法 2 得到的信任矩阵 $\boldsymbol{T}^*$，每次委员会一轮工作结束后，重新进行计算得到新的信任矩阵，进行委员节点的更迭。

2.3.2　协议设计

对于不同链来说，发送消息没有统一的格式，为了方便委员会节点进行消息的收发和确认，本文定义一种统一的消息格式，并通过消息中间件对即将在委员会节点中进行跨链传递和确认的消息进行加工。定义消息的符号为 $Mag_{u,s}^*$，表示链 L_* 的节点 u 向其他链的节点 s 发消息，数据结构见表 3。

表 3　消息数据结构

Tab. 3　Message data structure

$Mag_{u,s}^*$	
符号	描述
IP	发送节点 u 的 ip 地址
PK	发送节点 u 的公钥
ID	在委员会构建的继承链中，目标节点所在区块链的编号，由 s 确定
$view$	视图编号
$hash(Data)$	数据的 $hash$ 值(用 SHA256 散列成)
$Data$	数据

在委员会成员之间进行消息交互时，委员会集合 $\boldsymbol{C}$ 中的节点将使用第一个字段来验证消息发送者的身份，如果不是 $\boldsymbol{C}$ 中的成员，则视为非法交易。

对于委员会 $\boldsymbol{C}$，将对信息 $Mag_{u,s}^*$ 进行验证以达成共识。对于传统的 PBFT 共识方法，当信息被 $2 \times f + 1$ 个节点确认后，就可以被视为可信的。但是，传统 PBFT 算法在委员会机制中将会引起委员会的串通欺骗行为。假设一个委员会集合 $\boldsymbol{C} = \{a:1, b:2, c:3, d:3, e:1\}$，即分别有 1,2,3,3,1 个节点来自链 a,b,c,d,e。则对于链 c 和 d，其被选为委员会的

成员数目最多且都为 3,有可能串通起来进行欺骗。为了解决上述问题,本文提出一个基于距离的消息验证机制。

首先定义区块链之间的距离。设 $D_{i,j}$ 为区块链 L_i 和 L_j 之间的距离,定义 $D_{i,j}=||L_i|-|L_j||$,如果 $|L_i|=|L_j|$ 且 $i\neq j$,则 $D_{i,j}=1$。

由此得到委员会之间的距离矩阵,设委员会有 n 个成员,则 $\boldsymbol{D}=[D_1,D_2,\cdots D_n]^{\mathrm{T}}$,其中,$D_i$ 是对委员会节点 i 来说的距离向量,$\boldsymbol{D}_i=[D_{i,1},D_{i,2},\cdots D_{i,n}]$。

对委员会节点 i 与节点 j, 之间的权重为 W_{ij}, 公式(7):

$$W_{ij}=\xi\left(\frac{\sum_{k=1}^{j}D_{ik}}{D_{ij}}\right) \tag{7}$$

其中,$\xi(*)$ 是标准化函数。

若 i,j 是被选自于同一条链的,则 $W_{ij}=1$。通过上述方式计算委员会节点之间的权重,因为若两个集合之间的区别越小,则权重的影响越大,交流和信任越强。

委员会维护一个交易数据池 τ, 来对消息进行统计,并根据消息个数来发送更改视图的要求,进行委员会的更新。每次委员会更新也意味着数据池的清空。设 B 为交易数据池的界限,即 $0\leqslant|\tau|\leqslant B$;$C$ 中异常节点的数目是 $\theta(\theta\leqslant\frac{2*(c-1)}{9})$。建立一个对链的映射 $R(L_i)=\{p\mid p\in\boldsymbol{C}\cap p\in L_i\}$,即 $R(L_i)$ 为委员会中属于链 L_i 的成员。验证机制流程如下:

(1)请求阶段:$n_u\in L_x$,$n_s\in L_y$,n_u 对 n_s 发送消息,则找到节点 $n_r\in R(L_x)$, 通过消息中间件打包消息为 $Mag_{r,s}^{y}$, 并和节点对其他委员会节点的权重向量 $\boldsymbol{W}_{x*}{}^{\mathrm{T}}$ 一起发送;

(2)请求背书阶段:$n_z\in R(L_y)$ 获得数据,将背书请求根据权重 $W_{x*}{}^{\mathrm{T}}$ 从大到小发送给其他节点,权重越大,优先权越高;

(3)验证签名阶段:在委员会中除了 $R(L_y)$ 的所有节点收到背书的请求后,验证数据。如果节点证实了信息,用自己的私钥对消息进行签名 $sig(v,m)$, 发送验证的消息和自己的签名 sign;

(4)广播和提交:收到 $2\times\theta+1$ 个背书签名后,n_z 记录消息 $T_{us}^{m}=(m,sig(u,k),k)$,并将交易数据提交给 n_r, 并广播给所有节点,同时同步到委员会的内存池,以便在循环结束将消息进行封装打包成块;

(5)委员会节点 n_z 和 n_s 位于统一条链,n_z 将对 n_s 进行链内的消息传递和验证。

在步骤 3 中委员会节点验证通过后,将使用自己的私钥对消息进行签名。使用 $sig(v,m)$ 表示节点 v 使用私钥对数据 m 进行签名(标记)。$\{sig(v_1,m),sig(v_2,m),\cdots,sig(v_i,m)\}$ 表示数据 m 被一组节点 $\{v_1,v_2,\cdots,v_i\}$ 赋予的验证签名,使用 $k=\mathrm{SUM}(sig(v_1,m),sig(v_2,m),\cdots,sig(v_i,m))$ 表示给予签名的节点数目。定义 $T_{us}^{m}=(m,sig(u,k),k)$ 为最终交易的结果,该交易是由 u 发送给 s 的。当 T_{us}^{m} 被证实,将这个数据存储到交易数据池 $T_{us}^{m}\Rightarrow t_i$。在一个委员会迭代周期中,$\tau=\{t_1,t_2,\cdots,t_B\}$。当 τ 的数量达到 B 时,进行委员会的重组。

3 实验测试

3.1 功能测试

本文测试环境:操作环境为 Windows 11,项目环境为 Maven 3.5.3、Java 1.8,编码工具为 IntelliJ IDEA 2020.1.3 x64。

首先,对 3 个关键模块——信任度计算模块、委员会选举模块和共识机制模块进行功能测试。

(1)信任度计算模块测试。在信任度计算模块测试中,设置 3 个节点,链内消息传递。根据算法,每次交易后,节点更新自己用于计算的信任因素 Δa,Δb, 在时间从 $n\Delta t$ 到达下一个时刻 $(n+1)\Delta t$ 时,节点的信任信息进行更新,见表 4。

表 4 节点信任关系向量的更新

Tab. 4 Update result of node trust relationship vector

消息	信任关系向量		
	Node1	Node2	Node3
0(初始化)	[0,0,0]	[0,0,0]	[0,0,0]
1:Node1→Node2	[0,0.5,0]	[0.5,0,0]	[0,0,0]
2:Node2→Node3	[0,0.5,0]	[0.5,0,0.5]	[0,0.5,0]
3:Node1→Node3	[0,0.5,0.5]	[0.5,0,0.5]	[0.5,0.5,0]
4:Node1→Node2	[0,0.667,0.5]	[0.667,0,0.5]	[0.5,0.5,0]
5:Node2→Node3	[0,0.667,0.5]	[0.667,0,0.667]	[0.5,0.667,0]
6:Node1→Node2	[0,0.7,0.5]	[0.7,0,0.667]	[0.5,0.667,0]
7:Node1→Node3	[0,0.7,0.667]	[0.7,0,0.667]	[0.667,0.667,0]

(2)委员会选举模块测试。当进行委员会选举时,首先对每个网络更新该网络的信任关系矩阵和信任向量,根据信任向量中每个节点的信任值从大到小进行委员会的选举。在本实验中,在网中设置 4 个节点,选择 3 个节点作为委员会节点。

在消息传递下,该模块的执行结果见表 5。每

次选举网络信任向量进行更新，并选择信任值最大的前 3 个节点作为委员会节点。

表 5　委员会选举结果

Tab. 5　Committee Election Results

委员会选举次数	网络信任向量	委员会节点(节点编号)
0(初始化)	[0.25,0.25,0.25,0.25]	[0,1,2]
1	[0.286,0.25.0.214,0.25]	[0,1,3]
2	[0.289,0.215,0.211,0.285]	[0,3,1]
3	[0.275,0.196,0.225,0.204]	[3.0,2]
4	[0.274,0.224,0.226,0.276]	[3,0,2]
5	[0.274,0.257,0.226,0.243]	[0,1,3]

(3) 共识算法模块测试。在本模块测试中，构建 3 个网络，每个网络 6 个节点，委员会成员数目为 6，消息数据池限制为 5，$\theta = 1$，至少需要 $2\theta + 1 = 3$ 个节点签名。

测试消息共 20 条，其中 8 条为跨链消息，12 条为链内消息。根据算法，当 5 条跨链消息得到验证后，消息数据池满，进行一次委员会更迭。此时，交易数据池中已经完成验证等待进一步打包成区块的消息见表 6，迭代后的新委员会成员见表 7。

表 6　数据池满载消息

Tab. 6　Datapool full message

pool				
sender:ws://127.0.0.1:7002	sender:ws://127.0.0.1:8001	sender:ws://127.0.0.1:7001	sender:ws://127.0.0.1:9004	sender:ws://127.0.0.1:7005
receiver:ws://127.0.0.1:9003	receiver:ws://127.0.0.1:7002	receiver:ws://127.0.0.1:8003	receiver:ws://127.0.0.1:8002	receiver:ws://127.0.0.1:8005
data:stand up	data:sit down	data:byebye	data:thank you	data:i love you
signs:10273,234123,4213123,	signs:10273,23127,4213123,	signs:10273,12837,4213123,	signs:32946,870324,4213123,	signs:10273,12837,4213123,
signNodeNumber:3	signNodeNumber:3	signNodeNumber:3	signNodeNumber:3	signNodeNumber:3

表 7　委员会成员

Tab. 7　Committee members

Committee members		
Net1	Net2	Net3
nodeid: 1	nodeid: 0	nodeid: 1
nodeip:ws://127.0.0.1:7002	nodeip:ws://127.0.0.1:8001	nodeip:ws://127.0.0.1:9002
nodeid: 3	nodeid: 1	nodeid: 0
nodeip:ws://127.0.0.1:7004	nodeip:ws://127.0.0.1:8002	nodeip:ws://127.0.0.1:9001

3.2　性能测试

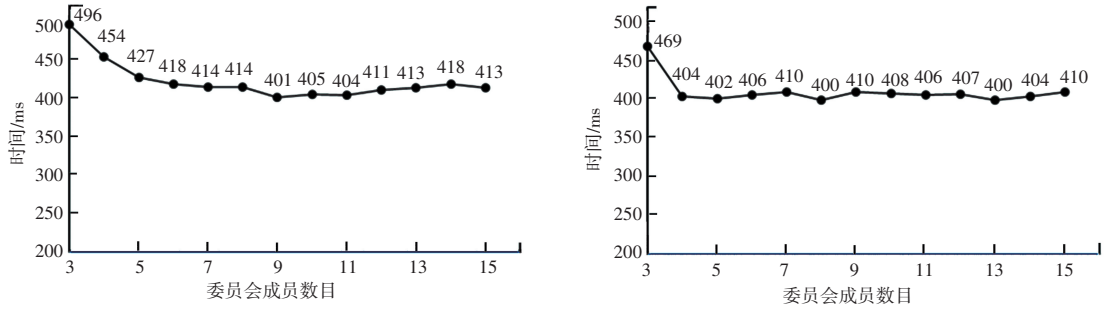
对本文提出的基于委员会轮换机制的跨链数据整合方案执行时间进行测试，主要观察委员会成员个数和数据量两者对消息跨链传递时间的影响。

3.2.1　委员会成员个数对跨链消息传递时间影响

在上文对共识算法的分析中，每条跨链消息需要 $2 \times \theta + 1$ 个节点的验证签名，而 θ 又与委员会成员个数相关，因此可以推测跨链的事件与委员会成员个数有关。

为方便测试，构造 3 个网络，对每个网络添加 6 个节点和 8 个节点的情况进行分别实验。

实验一　通过控制台输入来进行单一消息的发送。改变委员会成员数目，得到在不同委员会成员数目时跨链传输消息的时间，如图 2 所示。可以看到，当委员会成员数目增加时，跨链消息传输时间显著降低。

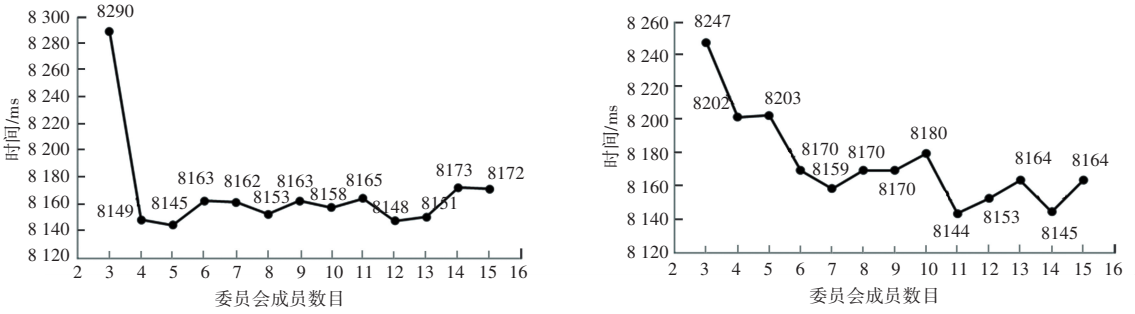


(a) 每个网络 6 个节点　　(b) 每个网络 8 个节点

图 2　单一数据时在不同委员会节点下的执行时间

Fig. 2　Execution time under different committee nodes for a single data

实验二 通过文件导入,发送批量数据。数据个数为 20 条,其中 10 条链内传输数据,10 条为跨链数据,实验结果如图 3 所示。



(a) 每个网络 6 个节点 (b) 每个网络 8 个节点

图 3 批量数据时在不同委员会节点下的执行时间

Fig. 3 Execution time under different committee nodes with large amounts of data

如图 3 所示,网络中共有 18 个节点的,当委员会成员数目为 5 时,执行时间最少;网络中共有 24 个节点的,当委员会成员数目为 11 时,执行时间最少。在两种网络中传输批量数据时,随着委员会成员数目的增多,数据传输的总时间均减少。当委员会成员数目为 3 个时,也就是占节点总数的比例很小时,数据传输的总时间最大,且远远大于其他情况。

因此,需要根据委员会总数来选择委员会成员数目,当网络中节点总数很大时,委员会成员的数目也应相应较大,以避免增加执行时间。

3.2.2 在不同数据量下的跨链消息传递时间

维持在同一区块链内的交易数据为 10 条不变,改变跨链交易时数据个数,能够看到当数据量增加时,执行时间也相应增加,基本成线性变化,变化趋势如图 4 所示。可以推测在委员会成员数目固定时,数据量是影响算法执行效率的最主要因素,且在本算法中,执行时间与数据量大致成线性变化趋势。

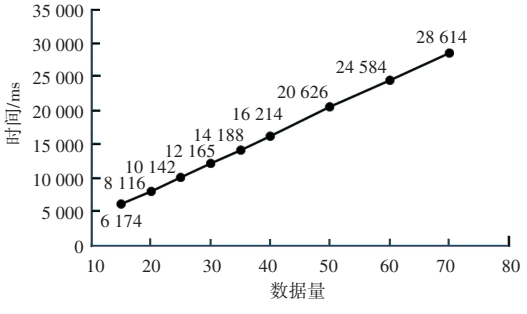


图 4 不同数据量下的执行时间

Fig. 4 Execution time with different amounts of data

4 结束语

本文针对不同区块链之间无法跨链传输数据的问题,设计并实现了一个基于委员会定期轮换机制的跨链数据整合方案,为区块链跨链技术的研究提供了新的解决思路和实践基础。本文的研究成果包含以下几个方面:

(1)设计了一个动态信任评估模型。充分考虑到区块链网络是 P2P 网络,具有高可变性,因此将节点的信任值视为动态变化的,引入遗忘机制刻画节点信任值的演化过程。

(2)设计了委员会选举和迭代算法。本文将节点的信任值作为委员会选举的标准,为了避免单一委员会节点造成中心化问题,选取信任值最大的一些节点而不是某个节点作为该链的委员会成员。同时,为了防止委员会成员之间串通欺骗,委员会不是固定的,在一个工作周期后,将对节点信任度进行重新评估,对委员会进行更新。

(3)设计了一个基于距离的消息验证机制。借鉴了 PBFT 共识算法思想,提出适用于属于不同链的委员会成员之间的消息验证机制。在该机制中,委员会成员通过链之间的距离得到权重向量,并根据权重向量的大小进行背书请求,当节点收到一定数目的来自其他节点的背书签名后,委员会节点之间达成共识,完成跨链消息的传输。

参考文献

[1] THOMAS S, SCHWARTZ E. A protocol for interledger payments [J]. https://interledger. org/interledger.pdf, 2015:25.

[2] NOLAN T. Alt chains and atomictransfers[EB/OL].[2020-10-06].https://bitcointalk.org/index.php? topic=193281.0.

[3] KWON J, BUCHMAN E. A Network of Distributed Ledgers Cosmos [EB/OL]. https://static.coinpaper.io/files/whitepapers/atom-cosmos_whitepaper.pdf.

[4] 张诗童,秦波,郑海彬. 基于哈希锁定的多方跨链协议研究[J]. 网络空间安全,2018,9(11):57-62,67.

[5] 赵涛,张凌浩,赵其刚,等. 基于聚类簇中心的共识跨链交换模型[J]. 计算机科学,2019,46(S11):557-561,566.