

基于可信联盟的 P2P 网络身份认证机制

陈盈盈¹, 章峰¹, 蒋文保^{1,2}, 周旭²

(1. 北京信息科技大学信息管理学院, 北京 100089;

2. 中国科学院计算机网络信息中心, 北京 100190)

摘要: 为了有效解决传统 PKI 体系中存在的 CA 交叉认证及单点故障等问题, 提出了一种新的身份认证机制。首先, 基于区块链技术构建基本架构, 通过动态生成可信节点来构建可信联盟; 其次, 提出全网统一的唯一身份标识 ID 并采用 SRT 数据结构存储; 最后, 通过双层共识机制全网节点皆能进行统一身份标识认证。实验表明, 本机制能够满足海量用户身份信息的查询和管理, 并且能够保证身份认证过程中的高效与安全。

关键词: 区块链; 可信联盟; 身份认证; 双层共识

中图分类号: TN915.08

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020021

P2P network identity authentication mechanism based on trusted alliance

CHEN Yingying¹, ZHANG Feng¹, JIANG Wenbao^{1,2}, ZHOU Xu²

1. School of Information Management, Beijing Information Science and Technology University, Beijing 100089, China

2. Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190, China

Abstract: In order to effectively solve the problems of CA's cross certification and single point of failure in traditional PKI system, a new identity authentication mechanism was proposed. Firstly, this mechanism built the basic architecture based on blockchain, and built the trusted alliance by dynamically generating trusted nodes. Secondly, the whole network unified unique identity was proposed and used a new data structure, named SRT, to store. Finally, all nodes in the network could mutual authentication through the double layer consensus mechanism. Experiments show that this mechanism can meet the query and management of massive user identity information, and ensure the efficiency and security in the identity authentication process.

Key words: blockchain, trusted alliance, identity authentication, double layer consensus

收稿日期: 2020-01-15; 修回日期: 2020-03-25

通信作者: 蒋文保, jiangwenbao@bistu.edu.cn

基金项目: 科技创新服务能力建设-网络空间安全学科创新平台建设基金资助项目 (No.77F1910917); 国家重点研发计划基金资助项目 (No.2018YFB1800100)

Foundation Items: Capacity Building of Scientific and Technological Innovation Service-Construction of Innovation Platform for Cyberspace Security Discipline (No.77F1910917), The National Key R&D Program of China (No.2018YFB1800100)

论文引用格式: 陈盈盈, 章峰, 蒋文保, 等. 基于可信联盟的 P2P 网络身份认证机制[J]. 网络与信息安全学报, 2020, 6(2): 77-86.
CHEN Y Y, ZHANG F, JIANG W B, et al. P2P network identity authentication mechanism based on trusted alliance[J]. Chinese Journal of Network and Information Security, 2020, 6(2): 77-86.

1 引言

随着网络技术的快速发展,网络用户的数量不断扩增,与此同时,网络犯罪的手段不断升级。近几年,网络身份冒充、伪造虚假身份和非法身份欺骗等手段导致的网络攻击和网络诈骗事件不计其数,造成了严重的后果。网络身份是维护网络空间安全的基础,因此网络身份认证一直被大众关注,也是相关领域研究人员重点研究的课题与方向。基于研究背景,人们将总是习惯依附于一个中心化事物的思想逐渐转变为去中心化,而对网络身份认证技术的研究也形成了由基于公钥基础设施(PKI, public key infrastructure)技术的数字证书形式到基于区块链技术的身份认证方案的演变^[1]。

但目前基于区块链技术的身份认证方案仍存在不可控、缺乏安全验证以及用户信息泄露等问题。故在某些问题层面,完全去中心化的方式并不利于整体有效的管理,所以本文采用“局部中心化,整体去中心”的思想,结合区块链技术对P2P(peer to peer)网络中节点的身份进行安全有效认证。首先,在网络中根据节点的分布个体聚焦度确认可信节点,普通节点通过可信节点的安全认证得到唯一身份标识ID;其次,同一可信联盟中的可信节点通过共识协议对全部在册节点数据进行共享存储,在册节点可通过联盟内任意可信节点进行查询验证;最后,加入权威联盟生态的不同可信联盟之间通过共识协议对联盟间的在册节点数据进行共享存储,最终可达到认证数据全网统一,全网节点皆能通过全网任意可信节点互相认证身份。

2 相关工作

目前以公钥证书的形式将用户公钥和用户身份进行绑定,已形成解决网络安全问题的成熟方案^[2]。但是,PKI通过引入可信第三方CA进行身份认证,这带来了证书的管理、存储和计算上的代价。大规模密钥管理的问题一般是采用物理上增加CA的方法,而各个CA的用户之间还存在交叉认证和信任管理的问题。并且,导致提供商的中央服务器崩溃是黑客的主要目标,因此用户

数据容易受到黑客攻击。电子身份eID^[3]是一种基于PKI技术的应用形式。而区块链的去中心化结构能够很好地解决传统的身份管理机制中存在的过分依赖第三方的问题,近几年,基于区块链的网络身份认证技术在不断探索研发中。有学者提出基于区块链的ID即服务(BIDaaS)^[4],旨在提供从BIDaaS提供商到其合作伙伴的身份和身份验证管理基础结构,但其没有防止合作伙伴滥用用户信息的有效机制。Lin等^[5]研究了基于区块链的身份管理系统(BIMS)中的成员身份验证要求,并为BIMS设计了一种新颖的可传递封闭无向图认证方案,但在该方案中存在用旧证书欺骗用户的风险。Ferdous等^[6]提出利用区块链技术来寻找自我主权身份,并使用数学模型对自主主权身份的概念进行了严格的分析,但未提出具体的系统实现方案。

uPort、ShoCard和Sovrin是3种具有代表性的基于分布式分类账技术(DLT, distributed ledger technology)的身份管理方案^[7],它们分别基于以太坊、比特币区块链和许可分类账。uPort是一个开源的去中心化身份框架,旨在提供“所有人的去中心化身份”。uPort没有中央服务器,并且不对uPortID的所有者进行身份验证,这会对未经授权访问用户移动设备上的本地身份验证造成风险。ShoCard是移动设备上的数字身份证,通过存储在比特币交易中的加密哈希,将用户标识符与现有的可信凭证(如护照或驾驶执照),以及其他身份属性绑定在一起。但ShoCard的中介角色为ShoCardID的纵向存在带来了不确定性,如果该公司不复存在,ShoCard的用户将无法使用已获得认证的系统。Sovrin是建立在许可的DLT之上的开放源代码身份网络,用于存储身份记录。用户必须依靠在Sovrin网络中代表其行事的代理机构以及维护分布式分类账的管理员。根据代理人的选择及实施,很多信息可能会由代理人掌握。可以看出,目前基于区块链技术的身份认证方案仍存在一些不足。因为区块链技术仍在发展中,所以不论是其底层技术还是有关应用层面都可以不断完善与扩充,可以有效利用其核心技术思想去创新,从而可以解决更多领域面临的一些问题,区块链技术具有十分广阔的应用前景^[8]。

综上所述, 本文提出一种基于可信联盟的网络身份认证机制, 该机制致力于解决传统 PKI 体系中存在的一些问题, 如由 CA 自身安全引起的单点故障问题以及 CA 之间存在的兼容性和可信度等问题。同时与现有基于区块链技术的身份认证方案进行比较, 期望能够在一定程度上避免其不足之处, 更好地实现在功能需求上的目标^[9]。根据国家有关部门提出的针对网络空间身份管理的相关意见^[10]及发展思路^[11], 本文提出唯一身份标识 ID, 其能够对网络身份进行统一管理^[12], 有效解决了各个不同领域身份认证不一致的问题。

3 基本架构

3.1 可信联盟

在 P2P 网络中, 每个节点都是独立的资源库, 但因为在现实生活中, 每个节点的社会属性有所不同, 所以网络中的节点也具有不同的属性。有的节点与其他节点的关联度很高, 则在社会中具有一定程度的重要性; 有的节点与其他节点的关联度正常, 那就意味着该节点属于社会中普通的一员。而人们往往对社会重要性高的人物具有一定程度的信任, 因此本系统通过计算网络中节点的重要性来确定可信节点, 并采用分布个体聚焦度来衡量网络中节点的重要性。可信联盟由具有相同可信等级的可信节点构成。去中心化可信联盟的基础架构如图 1 所示。

每个可信联盟内部达成共识如下。

- 1) 普通节点一旦与可信节点建立连接, 且通过可信节点的安全认证, 可信节点则赋予普通节点唯一身份标识 ID, 该标识被可信联盟内的所有可信节点认可, 此时普通节点成为在册节点。
- 2) 当普通节点与联盟内另一可信节点建立连接时, 可信节点可通过在自身维护的区块链中查询该普通节点提供的唯一身份标识 ID 来确认该普通节点的身份信息。
- 3) 普通节点与普通节点间建立连接时, 也可通过提供唯一身份标识 ID 来互相认证。
- 4) 普通节点未与任何可信节点建立连接或未通过安全认证, 则为游离节点。
- 5) 考虑到未加入可信联盟的可信节点, 如果通过该可信节点注册的普通节点长期无法与可信

联盟内其他在册节点取得身份认证, 那么会选择可信联盟中的可信节点进行重新注册成为在册节点, 而该可信节点则会降级直至成为普通节点。

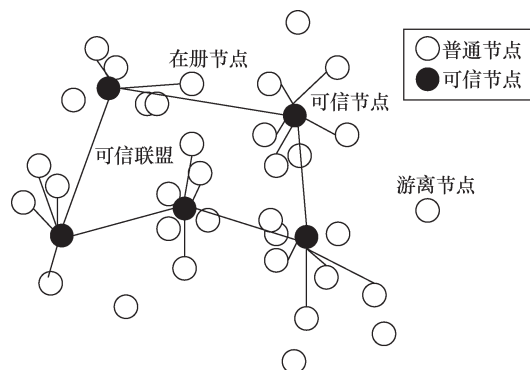


图1 去中心化可信联盟基础架构
Figure 1 Decentralized trusted alliance infrastructure

3.2 权威联盟

不同可信程度的可信联盟间可建立连接, 构成权威联盟生态。可通过权威节点将不同的可信联盟连接起来, 而权威节点是通过可信联盟内部随机选择某一个可信节点得到的, 可信联盟内部的每个可信节点都有机会成为权威节点, 但可信联盟内部同一时间只能存在一个权威节点。可信联盟内包含权威节点且与其他可信联盟建立了连接, 则可称该可信联盟为权威联盟, 如图 2 所示。

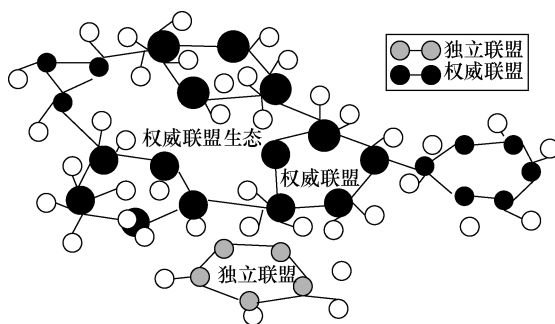


图2 权威联盟生态架构
Figure 2 Ecological architecture of authoritative alliance

权威联盟相互之间达成共识如下。

- 1) 一个可信联盟中的权威节点一旦与另一个可信联盟中的权威节点建立连接, 且双方互相关通过彼此的安全认证, 则都将对方的唯一身份标识 ID 存储在自身维护的区块链中。
- 2) 当权威联盟与权威联盟生态中的其他权威联盟建立连接时, 可通过提供唯一身份标识 ID

得到联盟间的身份认证,进而确认联盟中节点的身份信息。

3) 一个可信联盟没有与权威联盟建立连接或未通过权威联盟的安全认证,则为独立联盟,该联盟中的节点身份无法得到其他联盟的认证。

而在 Hyperledger Fabric^[13]中,默认 MSP 使用符合 X.509 标准的证书为身份,采用数字证书机制来实现对身份的鉴别和权限控制,CA 节点负责对网络中的成员身份进行管理,实现的是传统的 PKI 分层架构。在 MSP 中,CA 节点分为根 CA (RCA) 和中间 CA (ICA),客户端是从 CA 节点获取合法的身份证书来加入网络的应用通道,CA 节点在签发证书后,自身不参与网络中的交易过程。而本文中的可信节点具备去中心化特性,是根据节点的社会属性并结合实时的网络数据来动态生成的,且非独立于网络交易过程之外。与传统的 CA 节点不同,但皆具备认证功能。普通节点通过可信节点的认证后,与可信联盟内的其他在册节点间都可进行身份认证。为了保证交易的私密性,相互隔离的通道设计是 Fabric 的一个特点,每个通道维护一条私有的区块链。但本文中的可信联盟之间是可以进行数据共享的,这样设计是为了达到全网节点皆能通过全网任意可信节点互相认证身份。

4 关键技术

4.1 计算分布个体聚焦度

本文采用分布个体聚焦度来衡量节点的可信度。由于网络节点会因为国家差别、地域差别、个人偏好等导致分布性不同,而且这种分布性是呈动态变化的。因此,本文提出计算分布个体聚焦度的方案:首先计算出每个分布区域的个体数量,然后计算该分布区域内每个个体的聚焦度,从而确定区域内核心个体,达到分区计算、全局管理的目的。计算步骤如下。

1) 计算分布区域及个体数量:全网节点数量众多而且数据传播范围有所不同,因此合理地行分布区域的划分,是改善针对全网个体管理的有效方法。设 F 为分布区域数, g_f 为第 f 区域内个体数, F 可根据具体应用场景及应用范围进行设置,参考实际网络节点区域性分布特点, g_f 则

可以根据动态统计划分区域内实际网络在线节点数来确定。

2) 计算分布区域内个体聚焦度:采用网络分析中的指标——度中心性 (degree centrality) 来计算分布区域内个体聚焦度。度中心性是指网络中一个节点与其他节点相关联的程度,是一种能够直接描述节点中心性的度量指标^[14]。一个节点的节点度即该节点与其他节点的连边数,节点度越大就意味着这个节点的度中心性越高,该节点在网络中就越重要^[15]。计算该分布区域内个体节点与该分布区域内其他节点的关联程度即与其他节点的连边数,连边数越多表明聚焦度越大,该节点在该分布区域内就越重要。设 i, j 皆为区域 f 内节点, b_{ij} 为节点 i, j 之间存在的关联边,那么节点 i 的分布个体聚焦度可表示如下。

$$Dif_F(f_i) = \sum_{j=1}^{g_f} b_{ij} (i \neq j) \quad (1)$$

分布区域内进行标准化测量如式(2)所示。

$$Dif'_F(f_i) = \frac{Dif_F(f_i)}{g_f - 1} \quad (2)$$

分布个体聚焦度越大表示在该分布区域内,其他节点越认可该节点的重要地位,进一步表明,该节点是值得信任和依赖的。

4.2 可信等级划分

设 m 为分界点, m 的大小可根据全网节点的分布个体聚焦度的计算结果进行确定,将分布个体聚焦度值大于 m 的节点确定为可信节点,否则为普通节点。采用 K -means 聚类算法^[16]将可信节点进行等级划分。

1) 首先确定以哪些可信程度即分布个体聚焦度的值为等级标准,确定聚类中心。

2) 计算每个节点的分布个体聚焦度数据点到聚类中心的距离,距离哪个最近就划分到哪一类中。

3) 计算每一类中心点并将其作为新的中心点;

4) 重复上述步骤,直到每次迭代后类中心点的变化达到标准。

根据聚类结果,确定每个可信节点的可信等级,设可信等级为 R_i ,即同类中的节点具有同一个可信等级。

4.3 构建可信联盟

等级是通过网络计算得到节点的自身属性，节点本身不可更改。等级相同的可信节点间签订“共识协议”，则表明这些可信节点属于同一个可信联盟。

算法1 构建可信联盟

输入 关联边

输出 可信联盟

```

1) If 仿真时间运行至分布个体聚焦度计算
阶段 then
2) For 任意节点  $i, j \in gf$  do
3) If  $i \neq j$ , 且存在  $b_{ij}$  then
4) 将  $b_{ij}$  代入式(1)、式(2)求出  $Dif'_F(f_i)$ 
5) End if
6) End for
7) End if
8) If 仿真时间运行至可信等级划分阶段
then
9) For 任意节点  $i, j \in gf$ ,  $m$  为可信阈值 do
10) If  $Dif'_F(f_i) > m$  then
11) 采用  $K$ -means 对  $Dif'_F(f_i)$  进行聚类, 得
到可信等级  $R_i$ 
12) End if
13) If  $R_i$  等于  $R_j$  then
14)  $i, j$  签订“共识协议”, 归属同一个可
信联盟
15) End if
16) End for
17) End if

```

4.4 普通节点-安全认证

首先普通节点通过 RSA 算法^[17]在本地生成公私钥对，然后用私钥将个人身份信息进行签名并向可信节点发送认证请求。可信节点再用该普通节点的公钥对普通节点发送的个人信息进行验证，验证成功则表明该普通节点认证通过，否则不通过。认证通过后，可信节点将该普通节点的个人身份信息生成唯一身份标识 ID 并和该普通节点的公钥一一对应在区块链上进行存储。其他节点则可通过向可信节点提交身份标识查询请求，来认证节点身份信息，图3为具体的安全认证过程。分布式网络环境下密钥管理较为复

杂^[18]，此处采用数字签名为节点安全认证过程增加保障。

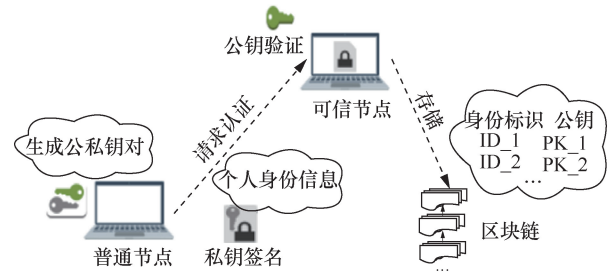


图3 安全认证过程

Figure 3 Safety certification process

另外，可信节点自身可向联盟中的其他可信节点进行安全认证，过程同上述普通节点认证一致，以此获得自身的唯一身份标识。

普通节点可以随时查询自己的身份标识和对应的公钥信息，通过判断该可信节点是否修改过自己的身份信息进而确定该可信节点是否真实可信。假设该可信节点是一个恶意节点并篡改了普通节点的个人身份信息，那么当普通节点发现后可选择其他可信节点进行重新注册。这样，该可信节点会逐渐失去与普通节点建立的联系，从而导致自身分布个体聚焦度的变化，最终成为普通节点。因此，在安全认证过程中存在一种隐形的对可信节点进行监督的机制。

获得唯一身份标识 ID 后，任意节点在向网络中其他节点进行签名验证的时候可提供此身份标识 ID，其他节点则可通过可信节点对该身份标识 ID 进行查询验证，从而确定该节点的身份是否真实可信。

4.5 数据存储-Struct Radix Tree

为了防止一人申请多个身份，可信节点必须对申请者的个人身份信息进行有效管理，本文采用 Struct Radix Tree 数据结构存储 ID 数据。Struct Radix Tree 是基于 Radix Tree（即基数树）的构造规则进行部分改进得到的一种数据结构。Radix Tree^[19]是以一个或多个字符叠加作为一个分支进行查找的。对于节点插入：当添加新的 Key 时，需要拆分原有的公共前缀分支。对于节点删除：当删除一个现有 Key 后，发现其父节点只有另外一个子节点 Key，则此子节点可以和父节点合并为一个新的节点，以此减少树的比较深度。而本

文中的 Struct Radix Tree 将按照不同的组织进行拆分, 数据结构如图 4 所示, 借鉴 Domain 方式进行构建的层级式命名方式, 方便管理。例如, 北京某所大学的某位学生 X, 可以将其 ID 命名为 cn.bj.bistu.X。

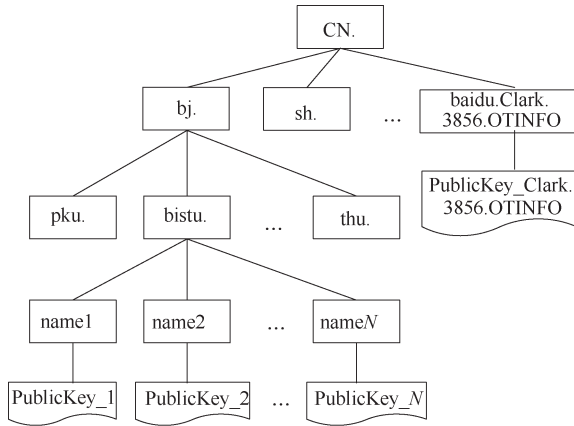


图 4 Struct Radix Tree 数据结构
Figure 4 Data structure of Struct Radix Tree

由于网络节点用户所属国家及分布区域的不同, 其可以形成不同的 Struct Radix Tree, 以不同的城市或者组织进行分级, 最终的叶子节点将会存储每个用户对应的公钥信息。

可信节点将普通节点用户的 ID 以及公钥信息全部存储到区块中, 新接入区块的时候, 将可以自动读取区块中的数据, 并存储到 Struct Radix Tree 数据结构中。区块链会记录数据的每一次更改, 方便后期对系统的审计, 也可对出现的问题进行追踪溯源。本文采用 Struct Radix Tree 数据结构可以提高用户 ID 及公钥信息的存储效率, 满足海量用户身份信息的查询和管理。

4.6 一层共识

Gossip 协议是 P2P 领域的常见协议, 用于进行网络内多个节点之间的数据分发或信息交换。由于其设计简单、容易实现, 同时容错性较高, 而被广泛应用到分布式系统。本文通过在每个可信联盟内部采用基于 Gossip 协议的拜占庭共识算法 (GBC, Gossip protocol-based Byzantine consensus algorithm)^[20]来达到可信联盟内的一层共识。在每个可信联盟内部, 可信节点通过 Gossip 协议将本地存储在册的节点更新信息发送给联盟中其他可信节点进行存储备份。具体流程

如下。

1) 设 A、B 为同一可信联盟中的两个可信节点, 由于网络动态变化, A、B 在某一时刻都会存在一定程度的数据更新, 只要有数据更新便可发起信息交换。

2) 假设 A 先发起信息交换, 向 B 发送自己更新的数据, B 收到信息后更新比自己新的数据。

3) B 再将本地比 A 新的数据发送给 A, A 更新本地数据。

这样, 可信联盟中的可信节点间便可以达到数据状态同步。GBC 算法是将数据共分为 3 种: 本地数据 (LD)、全局数据 (GD) 和共识数据 (CD)。本文的 LD 数据指可信节点自身认证通过的身份认证数据, GD 数据指与其他可信节点 Gossip 后得到的所有身份认证数据, CD 数据则可通过计算 GD 数据中超过半数的一致元素来得到。和其他共识算法不同的是, GBC 算法的提案由参与共识的节点轮流提出, 即由可信联盟内所有可信节点轮流提出。那么在可信联盟中选取提案节点的方法为

$$q = (l - s) \% N \quad (3)$$

其中, q 为提案节点的编号, l 为当前区块链的长度, N 为参与共识的总节点数即该可信联盟内可信节点总数, s 表示当前区块链长度下共识过程中的轮数, $\%$ 为求余符号。当有新的区块加入时, s 将重置为 0。提案内容包括交易、 l 、 s 和上一个区块提交的 GD 数据。

本文在每个可信联盟内部维护着一条区块链, 每当有新的节点身份认证消息时, 可信节点将该节点的唯一身份标识 ID 及公钥信息全部存储在区块中, 签名后广播给可信联盟内其他可信节点进行确认, 认证通过后便将该消息存入共同维护的区块链中。

4.7 权威节点-安全认证

可信联盟中的权威节点向其他可信联盟中的权威节点请求安全认证的过程与上述普通节点请求安全认证的过程基本一致。不同的是权威节点可向另一权威节点提供已获得的唯一身份标识 ID, 安全认证通过后另一权威节点直接将该权威节点提供的唯一身份标识 ID 以及对应的公钥信

息在自身所维护的区块链中进行存储。

由于可信联盟之间在未互相认证之前无法查询到彼此的安全身份标识信息，所以当可信联盟中的可信节点在自身所处的可信联盟中查询失败的情况下，该可信联盟中的权威节点应向具有该安全身份标识信息的另一个可信联盟中的权威节点先进行上述的安全认证过程。且可信联盟之间的认证必须为双向认证，即被请求安全认证的权威节点需要向请求安全认证的权威节点请求安全认证。

4.8 二层共识

各可信联盟中的权威节点将自身可信联盟内存储在区块链上的数据采用 Gossip 协议进行传播。在一层共识的基础上，分别存储在各个可信联盟中的权威节点之间达成二层共识，在权威节点之间即在各个可信联盟之间共同维护着一条新的区块链，这条链上存储着权威联盟生态的所有身份认证数据。联盟中及联盟间达成双层共识的算法如算法 2 所示。

算法 2 联盟中及联盟间达成双层共识算法

输入 提案

输出 新的区块链

- 1) For 任意可信节点 $i, j \in gf$ do
- 2) If R_i 等于 R_j (联盟中) then
- 3) 由式(3)选择提案节点
- 4) 提案节点广播提案
- 5) 其他可信节点验证提案节点和提案，不通过，则进入 $i+1$ 轮共识，重复步骤 3)
- 6) 由 Gossip 过程计算出 CD
- 7) 检查是否达成共识，若达成且结果正确，则发布完整区块，否则重复步骤 3)
- 8) 将区块加入区块链
- 9) 输出新的区块链
- 10) End if
- 11) If R_i 不等于 R_j (联盟间) then
- 12) If 节点 $i, j \in$ 权威节点 then
- 13) 执行上述步骤 3)~9)
- 14) End if
- 15) End if
- 16) End for

本文构建的双层共识机制如图 5 所示。

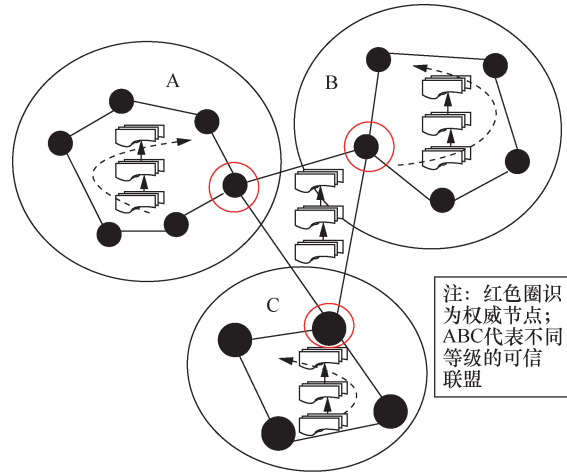


图5 双层共识机制

Figure 5 Double layer consensus mechanism

5 实验及分析

5.1 分布个体聚焦度仿真实验

本文采用 NetLogo 仿真实验软件对分布区域网络中的 1 004 个节点进行模拟测试分布个体聚焦度，得到图 6 所示结果。由于节点之间存在偏好，故每个节点与网络中其他节点的关联边数存在差别，图中节点的大小会随着分布个体聚焦度的变化而改变，分布个体聚焦度越高，则节点越大。上述节点的颜色是根据节点的大小进行区分的，节点颜色相同，则表明分布个体聚焦度大致处于同一个级别。

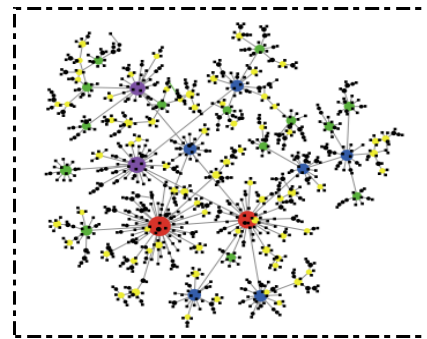


图6 模拟社交网络测量节点分布个体聚焦度

Figure 6 Simulate social network to measure Dif of nodes

图 7 是采用 K-means 算法对节点分布个体聚焦度进行精确划分的结果，共分为 6 个结果空间：[0.001 0~0.002 0]、[0.002 0~0.005 0]、[0.005 0~0.010 0]、[0.011 0~0.018 9]、[0.018 9~0.041 9]、[0.041 9~0.054 8]；6 个中心：0.001 2、0.003 3、

0.006 5、0.014 9、0.030 4、0.048 4。此处取分界点 m 的值为 0.005 0，那么分布个体聚焦度大于 0.005 0 的节点可确定为可信节点，进一步表明，由 1 004 个节点组成的分布区域网络中共存在 4 个不同等级的可信联盟。

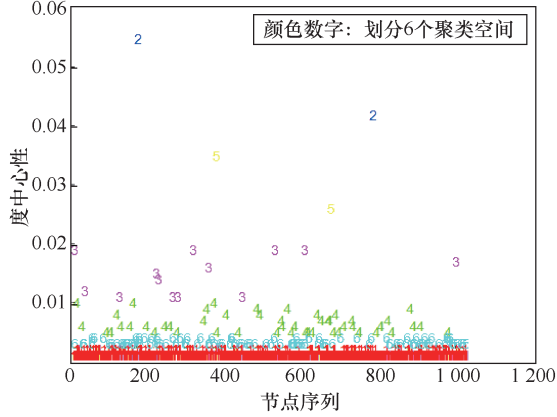


图7 可信联盟划分
Figure 7 Trusted alliance division

5.2 数据存储性能分析

将本文采用的 Struct Radix Tree 数据结构与层次化、扁平化的数据结构进行对比，数据查询与数据更新的实验结果分别如图 8、图 9 所示。

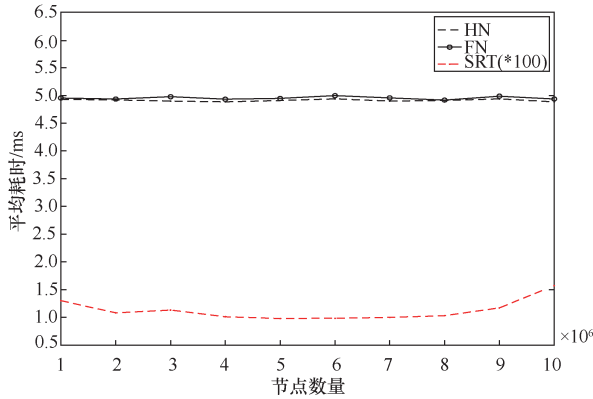


图8 数据查询
Figure 8 Data query

其中，HN 表示层次化数据结构，FN 表示扁平化数据结构，SRT 为本文中的 Struct Radix Tree 新型数据结构。将 SRT 平均耗时扩大 100 倍，可以很明显看出本文采取的 Struct Radix Tree 数据结构在进行节点身份信息的查询与更新时，耗时远远低于层次化数据结构和扁平化数据结构所用耗时，大大提高了数据存储效率。

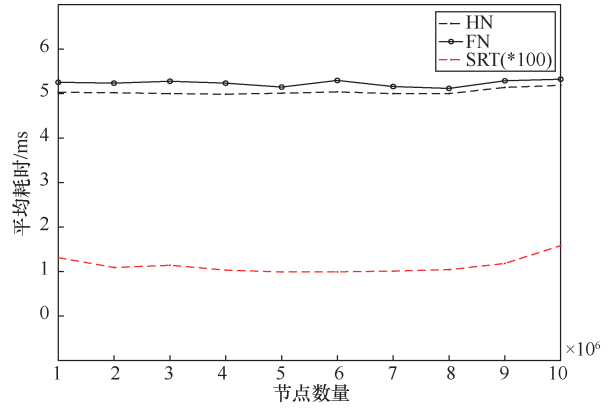


图9 数据更新
Figure 9 Data update

5.3 消息一致性性能分析

可信联盟中节点间采用的是 Gossip 协议，为了能够对可信节点间消息的一致性进行有效分析，作以下假设：

- 1) 网络中共 $n+1$ 个节点均匀分布；
- 2) 每对节点间建立连接发送消息的概率是 β , $0 < \beta < 1$ ；
- 3) 处于网络运行时间中某一时刻的节点，接收消息状态为 1（表示接收）和 0（表示未接收）；
- 4) 节点由 0 状态转化为 1 状态后，则保持 1 状态。

记 t 时刻处于 1 状态的节点数为 y_t ，处于 0 状态的节点数为 x_t ，则有 $y_0 = 1$, $x_0 = n$ ，且在任意时刻 $x_t + y_t = n+1$ 。那么，考虑网络连续运行时间，可知 $\frac{d_x}{d_t} = -\beta xy$ ，得到 $x = \frac{n(n+1)}{n + e^{\beta(n+1)t}}$ ， $y = \frac{n+1}{1 + ne^{-\beta(n+1)t}}$ 。当 $t \rightarrow \infty$ 时， $x \rightarrow 0$, $y \rightarrow (n+1)$ ，表明只要经过足够的时间，所有节点都将接收到消息。

设 $\beta = \frac{b}{n}$ ，令 $t = c \log(n)$ ，可得到 $y \approx (n+1) -$

$\frac{1}{n^{cb-2}}$ ，表明通过 Gossip 消息传递到所有节点需要的时间复杂度为 $O(\log(n))$ 。

而本文在每个可信联盟中以及可信联盟间采用 Gossip 协议进行数据传播，采取的是双层共识机制，以仿真实验 1 004 个节点为例：设 4 个不同等级的可信联盟中节点数量分别为 n_1 、 n_2 、 n_3 、 n_4 ，那么 4 个可信联盟中的节点分别达到数据一

致性的时间复杂度为 $O(\log(n_1))$ 、 $O(\log(n_2))$ 、 $O(\log(n_3))$ 、 $O(\log(n_4))$ 。由于网络运行的时间同步, 设 n_i 为可信联盟中节点数量最多的, 且已知可信联盟的数量远小于可信联盟中节点的数量, 则联盟间 Gossip 的时间复杂度必定小于 $O(\log(n_i))$, 因此, 本文中采取的 Gossip 策略使所有节点达到数据一致性时所需的时间复杂度为 $O(\log(n_i))$, 因为 n_i 是 n 的子集, 故 $O(\log(n_i))$ 必定小于 $O(\log(n))$ 。

可得出结论: 在网络节点总量相同的情况下, 本文所采取的双层共识机制下的 Gossip 策略可以提高网络节点达到数据一致性的效率。

5.4 安全分析

对本文机制中安全认证过程的安全性分析如下。

(1) 防抵赖

普通节点向可信节点请求个人身份认证时, 使用自身的私钥对消息进行签名处理, 如果在普通节点与可信节点间存在攻击者, 即使截获了该请求消息, 也不会造成任何影响, 普通节点的身份仍可得到验证, 无法抵赖。

(2) 预防 Sybil 攻击

全网节点进行身份认证后, 每个节点有且仅有一个全网唯一的身份标识 ID, 无法被假冒、篡改, 因此可以有效防止 Sybil 攻击。

(3) 不存在分叉现象

本文机制可以实现分布式存储节点身份认证数据, 达到全网节点身份可统一查询认证的目的, 由于确保数据最终一致性可避免区块链技术中存在的分叉现象, 不会发生由分叉引起的相关问题。

6 结束语

本文通过衡量网络中节点的社会属性来动态生成不同可信等级的可信节点, 可以消除传统 PKI/CA 体系中存在的 CA 交叉认证及单点故障等问题, 并为网络节点生成全网唯一身份标识 ID, 有利于网络空间身份的安全有效管理。本文通过采用双层共识机制实现了全网节点统一安全身份认证, 提高了节点达到消息最终一致性的效率。采用的 SRT 新型数据结构可以提高用户 ID 及公钥信息的存储效率, 满足海量用户身份信息的查

询和管理。在能够实现区块链技术的去中心化思想的同时能有效避免现有基于区块链技术的身份认证方案中存在的用户信息泄露、缺乏安全验证以及身份欺骗等问题。希望通过不断地改进, 本文机制能够最终优化为可以应用于多种认证场景的基础认证架构。

参考文献:

- [1] 周致成, 李立新, 李作辉. 基于区块链技术的高效跨域认证方案[J]. 计算机应用, 2018, 38(2): 316-320.
ZHOU Z C, LI L X, LI Z H. Efficient cross-domain authentication scheme based on blockchain technology[J]. Journal of Computer Applications, 2018, 38 (2): 316-320.
- [2] 杨小东, 安发英, 杨平, 等. 云环境下基于代理重签名的跨域身份认证方案[J]. 计算机学报, 2019, 42(4): 756-771.
YANG X D, AN F Y, YANG P, et al. Cross-domain authentication scheme based on proxy resignature in cloud environment[J]. Chinese Journal of Computers, 2019, 42 (4): 756-771.
- [3] 曹守启, 孙青, 曹莉凌. 动态 ID 多因素远程用户身份认证方案的改进[J]. 计算机工程与科学, 2019, 41(4): 633-640.
CAO S Q, SUN Q, CAO L L. An improved identity authentication scheme of dynamic ID multifactor remote users[J]. Computer Engineering & Science, 2019, 41(4): 633-640.
- [4] LEE J H. BIDaaS: blockchain based ID as a service[J]. IEEE Access, 2018, 6: 2274-2278.
- [5] LIN C, HE D, HUANG X, et al. A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems[J]. IEEE Access, 2018, 6: 28203-28212.
- [6] FERDOUS M S, CHOWDHURY F, ALASSAFI M O. In search of self-sovereign identity leveraging blockchain technology[J]. IEEE Access, 2019, 7: 103059-103079.
- [7] DUNPHY P, PETITCOLAS F A P. A first look at identity management schemes on the blockchain[J]. IEEE Security & Privacy, 2018, 16(4): 20-29.
- [8] 章峰, 史博轩, 蒋文保. 区块链关键技术及应用研究综述[J]. 网络与信息安全学报, 2018, 4(4): 22-29.
ZHANG F, SHI B X, JIANG W B. Review of key technology and its application of blockchain[J]. Chinese Journal of Network and Information Security, 2018, 4(4): 22-29.
- [9] 董贵山, 陈宇翔, 张兆雷, 等. 基于区块链的身份管理认证研究[J]. 计算机科学, 2018, 45(11): 52-59.
DONG G S, CHEN Y X, ZHANG Z L, et al. Research on identity management authentication based on blockchain[J]. Computer Science, 2018, 45(11): 52-59.
- [10] 杨明慧, 邹翔. 美国电子身份指南评析[J]. 计算机工程与应用, 2019, 55(23): 22-28, 34.
YANG M H, ZOU X. Evaluation of US electronic identity guide[J]. Computer Engineering and Applications, 2019, 55(23): 22-28, 34.
- [11] 胡传平, 陈兵, 方滨兴, 等. 全球主要国家和地区网络电子身份

- 管理发展与应用[J]. 中国工程科学, 2016, 18(6): 99-103.
- HU C P, CHEN B, FANG B X, et al. Development and application of network electronic identity management in major countries and regions around the world[J]. Strategic Study of CAE, 2016, 18(6): 99-103.
- [12] 张富友, 王琼霄, 宋利. 基于生物特征识别的统一身份认证系统研究[J]. 信息安全学报, 2019(9): 86-90.
- ZHANG F Y, WANG Q X, SONG L. Research on unified identity authentication system based on biometrics[J]. Netinfo Security, 2019(9): 86-90.
- [13] ANDOLA N, RAGHAV, GOGOI M, et al. Vulnerabilities on Hyperledger Fabric[J]. Pervasive and Mobile Computing, 2019, 59: 101050.
- [14] 闫泓任, 马国帅, 钱宇华. 基于节点度中心性的无监督特征选择[J]. 数据采集与处理, 2019, 34(2): 312-321.
- YAN H R, MA G S, QIAN Y H. Degree centrality based feature selection[J]. Journal of Data Acquisition and Processing, 2019, 34(2): 312-321.
- [15] 刘彩虹, 刘强, 祁瑞华. 一种邻近 H-index 的社会网络关键节点识别技术[J]. 中国科技论文, 2019, 14(3): 296-302.
- LIU C H, LIU Q, QI R H. Vital node identification technology of social networks using neighbors' H-index values[J]. China Science Paper, 2019, 14(3): 296-302.
- [16] 马福民, 逯瑞强, 张腾飞. 基于局部密度自适应度量的粗糙 K-means 聚类算法[J]. 计算机工程与科学, 2018, 40(1): 184-190.
- MA F M, LU R Q, ZHANG T F. Rough K-means clustering based on local density adaptive measure[J]. Computer Engineering & Science, 2018, 40(1): 184-190.
- [17] BHATTACHARJYA A, ZHONG X, LI X. A lightweight and efficient secure hybrid RSA (SHRSA) messaging scheme with four-layered authentication stack[J]. IEEE Access, 2019, 7: 30487-30506.
- [18] 戴千一, 徐开勇, 郭松, 等. 分布式网络环境下基于区块链的密钥管理方案[J]. 网络与信息安全学报, 2018, 4(9): 23-35.
- DAI Q Y, XU K Y, GUO S, et al. Blockchain-based key management scheme for distributed networks[J]. Chinese Journal of Network and Information Security, 2018, 4(9): 23-35.
- [19] LEIS V, KEMPER A, NEUMANN T. The adaptive radix tree: ARTful indexing for main-memory databases[J]. IEEE Computer Society, 2013, 1: 38-49.
- [20] 张仕将, 柴晶, 陈泽华, 等. 基于 Gossip 协议的拜占庭共识算法[J]. 计算机科学, 2018, 45(2): 20-24.
- ZHANG S J, CHAI J, CHEN Z H, et al. Byzantine consensus algorithm based on Gossip protocol[J]. Computer Science, 2018, 45(2): 20-24.

[作者简介]



陈盈盈 (1994—), 女, 河南信阳人, 北京信息科技大学硕士生, 主要研究方向为区块链技术、可信网络、信息安全。

章峰 (1994—), 男, 江苏宿迁人, 北京信息科技大学硕士生, 主要研究方向为区块链技术、信息安全。

蒋文保 (1969—), 男, 湖南永州人, 北京信息科技大学教授, 主要研究方向为可信网络、区块链、网络安全监测。

周旭 (1976—), 男, 四川成都人, 中国科学院计算机网络信息中心研究员, 主要研究方向为未来网络架构、5G、区块链。