

基于改进 PBFT 算法的 PKI 跨域认证方案

钱思杰¹, 陈立全^{2,3}, 王诗卉²

(1. 东南大学信息科学与工程学院, 江苏 南京 210096;

2. 东南大学网络空间安全学院, 江苏 南京 210096;

3. 紫金山实验室, 江苏 南京 211100)

摘 要: 为解决现有公钥基础设施跨域认证方案的效率问题, 利用具有分布式和不易被篡改优点的区块链技术, 提出基于联盟区块链的跨域认证方案。一方面, 该方案对联盟链在传统实用拜占庭共识算法 (PBFT) 的基础上加入了节点动态增减功能; 改进了主节点选举方式; 将三阶段广播缩减为两阶段广播, 减少了通信开销。另一方面, 该方案设计了联盟链跨域认证协议, 给出了区块链证书格式, 描述了跨域认证协议, 并进行了安全和效率分析。分析表明, 在安全方面, 该方案具有抵抗分布式攻击等安全属性; 在效率方面, 与已有跨域认证方案相比, 该方案在计算开销上、通信开销上都有优势。

关键词: 跨域认证; 区块链; 拜占庭容错算法; 公钥基础设施

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020042

PKI cross-domain authentication scheme based on advanced PBFT algorithm

QIAN Sijie¹, CHEN Liquan^{2,3}, WANG Shihui²

1. School of Information Science and Engineering, Southeast University, Nanjing 210096, China

2. School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China

3. Purple Mountain Laboratories, Nanjing 211100, China

Abstract: In order to solve the efficiency problem of the existing public key infrastructure cross-domain authentication scheme, a cross-domain authentication model based on the consortium blockchain which has the advantages of distributed and difficult to be tampered with was proposed. On the one hand, the dynamic join and exit function was added to the practical Byzantine fault tolerant (PBFT) algorithm, the primary node election mode was improved, and the three-stage broadcast was reduced to two-stage broadcast for the reduction of communication overhead. On the other hand, the cross-domain authentication system architecture based on consortium chain was

收稿日期: 2019-09-04; 修回日期: 2019-12-19

通信作者: 陈立全, lqchen@seu.edu.com

基金项目: 国家自然科学基金 (61571110)

Foundation Item: The National Natural Science Foundation of China (61571110)

论文引用格式: 钱思杰, 陈立全, 王诗卉. 基于改进 PBFT 算法的 PKI 跨域认证方案[J]. 网络与信息安全学报, 2020, 6(4): 37-44.

QIAN S J, CHEN L Q, WANG S H. PKI cross-domain authentication scheme based on advanced PBFT algorithm[J]. Chinese Journal of Network and Information Security, 2020, 6(4): 37-44.

designed, the blockchain certificate format and the cross-domain authentication protocol were presented, the security and efficiency were analyzed. The results shows that in term of security, the proposed model has security attributes such as resisting distributed attacks. In terms of performance, the proposed model has advantages in both computational overhead and communication overhead when it was compared with the existing cross-domain authentication schemes.

Key words: cross-domain authentication, blockchain, Byzantine fault tolerant algorithm, public key infrastructure

1 引言

互联网的快速发展给人们的生活带来了极大的便利^[1]。但与此同时,如何在开放的互联网中建立信任关系并且保证信息的真实性、完整性、机密性以及不可否认性一直是互联网面临的最大难题^[2]。

针对上述问题,世界各国研究人员逐步设计出了一套完整的安全体系,即目前广泛使用的公钥基础设施(PKI, public key infrastructure)技术。PKI通过可信第三方证书颁发机构(CA, certificate authority)来管理公钥,它以证书的方式把用户的公钥信息和其他信息绑定在一起。在通信时,证书依赖一方会申请对方的证书链,申请成功后,利用自身签发的自证书CA来逐一地验证证书链的可靠性,这一体系使在互联网中的各用户可以验证对方的身份^[3]。

经过三十多年的发展,PKI技术已经进入大范围实施部署阶段^[4]。在单一PKI域的情况下,可以轻松地完成证书认证路径的构造和验证。但在大范围PKI系统中,还是需要借助如交叉认证等方式才能实现跨域认证^[5]。文献[6]根据各信任域已有的PKI拓扑关系构建认证路径,但路径复杂、认证效率不高的问题突出。文献[7]提出了基于网格的PKI多信任域认证方案,但该方案无法抵抗伪造攻击。文献[8]结合传统单点登录技术和身份联盟技术设计了一种新的跨域认证方案,可以保证用户的匿名性,但缺点是认证效率低,每次跨域时都需要重新进行域间通信。综上所述,基于PKI/CA的跨域认证方案还远不成熟。

区块链技术作为比特币的底层技术,最早由中本聪提出^[9],其结合了诸多现代计算机技术,对数据进行存储、交换和处理,是一种安全性极高的分布式存储技术^[10]。

区块链技术的快速发展,使大量的研究人员

对区块链技术在身份认证领域的潜力越来越重视。文献[11]提出了一种新的PKI认证体系,该体系以比特币区块链系统为底层基础,使用Certcoin代替CA提供密钥查询和跨域认证功能,但是由于区块链账本记录了用户身份造成隐私泄露问题。文献[12]改进了Certcoin方案,在其基础上增加了隐私保护功能。文献[13]基于以太坊区块链架构设计了一种新的分布式PKI认证体系,该方案能够很好地解决传统PKI证书管理、撤销和查询通信量过大的问题。

本文提出了一种改进的实用拜占庭容错(APBFT, advanced practical Byzantine fault tolerant)算法,该算法引入了节点动态增减功能,并且为了降低通信开销对其共识机制进行了改进,同时改进主节点选举算法。在此基础上,本文提出了一种改进的PBFT算法的PKI跨域认证方案,该方案能有效应对传统PKI/CA跨域认证体系存在的单点失效、效率低、路径复杂等问题。方案分析表明,本文方案不仅能降低共识阶段节点间的通信开销,而且能减少跨域认证时的签名验证次数。

2 基于选举改进的PBFT共识算法

拜占庭容错(BFT, Byzantine fault tolerant)算法的研究最早起源于Lamport等1982年发表的论文“Polynomial Algorithms for Byzantine Agreement”^[14],它最早是用来解决在通信可靠的条件下,网络环境中若存在恶意节点或者故障节点时如何达成一致共识的问题^[15]。研究初期的拜占庭容错算法由于存在复杂度过高的缺点,一直停留在理论阶段。

真正使拜占庭容错算法在实际应用中变得可用是Castro和Liskov创新性地提出了实用拜占庭容错共识算法^[16],他们将算法复杂度从指数级别降为多项式级别。

原PBFT算法的设计初衷并不是针对区块链

设计的, 因此将其直接应用到区块链中存在一些缺点, 主要有以下几个方面。

1) 主节点选举策略过于简单。区块链安全的一大原因是区块的不断增长, 其攻击难度指数上升。然而原 PBFT 算法的主节点选取只考虑了视图编号, 没有完全利用区块链的优势。

2) 不能实现节点的动态增减。区块链基于点对点网络架构, 其架构需要支持节点的动态增减。然而原 PBFT 算法并不支持灵活的节点动态增减。

3) 预准备、准备、确认这三阶段的广播通信非常消耗带宽资源。假设节点总数为 N , 则在不考虑节点失效的情况下, 完成一次三阶段共识过程, 共需要进行传递的消息次数 $Z = 2N^2 - 2N$ 。若请求频率较高, 势必带来极大的消息传递成本。

本文主要研究基于区块链的跨域认证方案, 需要在区块链中存储身份认证相关的信息, 便于在认证时查询区块链账本并使用有关信息。针对上述问题, 本文提出了一种改进选举方式的 PBFT 共识算法, 简称 APBFT 算法。

2.1 算法创新点

(1) 实现节点动态增减机制

APBFT 在原 PBFT 算法主节点和从节点的基础上新增备份节点和代理节点, 并将主节点和从节点统称为共识域节点。其中, 共识域存储节点用符号 R_1 表示, 备份域节点用 R_2 表示, 代理域节点用 R_3 表示。

R_1 参与共识算法, 假设 R_1 能容忍的最大拜占庭节点个数为 f , 则 R_1 满足 $R_1 \geq 3f + 1$ 。

R_2 不直接参与共识算法, 而是作为 R_1 的缓冲区, 当 R_1 内发生节点淘汰时, 接收从 R_1 淘汰下来的节点, 通过基于 Raft 的选举机制选出新的代表节点进入共识域。假设 $R_2 = f$ 。

R_3 不参与共识算法, 只会同步共识域中的区块链账本数据。代理节点作为中间代理人的角色接收客户端的请求, 检验请求发起者的合法性, 并为之提供快速查询服务。

(2) 优化主节点选举策略

原 PBFT 算法主节点编号 p 与视图 v 的关系为 $p = v \bmod |R|$, 考虑到区块链中区块高度的增长, APBFT 重新设计主节点编号 p 与视图 v 的关

系为 $p = (h + v) \bmod |R_1|$, 其中, h 表示当前区块的高度。

(3) 缩减广播流程通信开销

原 PBFT 算法的三阶段中的确认阶段其实是对准备阶段的一种“确认”, 是为了防止某些节点在准备阶段之后发生视图切换导致的不一致性。但在区块链环境中, 需要保证的是节点具有相同的区块高度和视图号, 而这两者可以通过同步机制和视图切换协议保证。故本文 APBFT 算法取消三阶段中的确认阶段, 只保留预准备阶段和准备阶段。

2.2 一致性协议

本文算法确保了单个数据区块在唯一视图下的一致性, 故本文算法删除了确认阶段, 只保留预准备和准备阶段。具体算法流程如下。

1) 客户端 C 向代理节点 R_3 发起请求, 并附上交易者的签名。

2) R_3 收到请求后进行验证, 若验证通过, 则提交到共识域节点 R_1 主节点 p 。

3) 收到请求后先写入本地内存中缓存, 然后根据请求的时间顺序写入区块中, 将一段时间 t 内的请求信息构造成新区块。

p 在 t 时间后, 向从节点广播新区块的共识提案 $\langle \text{FAST-PROPOSAL}, v, h, p, \text{block} \rangle_\sigma$, 其中, v 表示当前的视图版本, h 表示区块链账本的高度, p 表示主节点, block 表示新生成的区块, 主节点生成预准备消息后附上其签名 σ 。

R_1 中的从节点 r_i 在收到 p 发来的预准备消息后, 对消息进行签名认证, 若验证通过, 则发送 $\langle \text{FAST-CONFIRM}, v, h, r_i, d(\text{block}) \rangle_\sigma$ 给 p 和其他所有从节点 r , 其中, r_i 是从节点, $d(\text{block})$ 表示新增区块的消息摘要; 若验证不通过, 从节点怀疑主节点, 以广播方式发起视图切换协议, 协议具体在下文中介绍。

当 R_1 中的任何节点收到 $2f$ 个验证通过的共识确认消息, 表示该新区块提案获得认可, 节点可以将其添加在区块链账本上, 开启下一轮共识。

2.3 选举加入制度

本文算法新增备份节点 R_2 , 以心跳包的方式与共识域节点 R_1 内主节点 p 保持连接, 当 p 发送拜占庭错误时, p 退出 R_1 , R_2 收不到 p 发来的心跳包,

故 R_2 从域内候选节点中选举出新的代表节点进入 R_1 中。选举方法参考 Raft 算法, 具体流程如下。

- 1) 任何备份域节点 R_2 都有资格成为代表节点, 在选举时, 向其他节点发出选举自己的请求。
- 2) 每个候选者在一个选举周期内有且只有一次投票机会, 它将把同意的选票发送给第一个收到选举请求的节点。
- 3) 每个候选者只要得到超过一半的选票就可以赢得此次选举, 成为代表节点。

2.4 同步机制

新选举出的代表节点在进入共识域节点 R_1 之前, 需要进行区块链账本数据同步, 具体流程如下。

- 1) 新选举出的代表节点向 R_1 发出同步请求 $\langle \text{SYN-REQUEST}, r_i, v, \text{vtid} \rangle_\sigma$, 其中, r_i 表示代表节点在共识域中的位置, vtid 表示其提交的最大事务号。
- 2) 同步阶段, R_1 中的各节点收到同步请求后, 先验证签名 σ 是否正确, 然后检查视图号 v 的合法性, 最后对比自己的区块链账本末尾区块编号与消息中的 vtid 是否一致。若都通过, 则向代表节点回复消息 $\langle \text{SYN-REPLY}, r_i, v, \text{blocks} \rangle_\sigma$, 其中 blocks 为存在差异的备份数据区块。
- 3) 验证阶段, 其他节点收到代表节点的备份数据区块后, 验证其合法性。如果合法, 则保存起来, 广播验证通过消息, 消息格式为 $\langle \text{SYN-ACK}, v_i, v, d(\text{block}) \rangle$, 其中, $d(\text{block})$ 为收到的备份数据区块中最后一个区块的摘要。
- 4) 收到 $2f+1$ 个含有相同 $d(\text{block})$ 的消息, 代表节点发送区块同步指令给那些相同 $d(\text{block})$ 的节点, 同步完成后重新计算本地区块链账本的哈希值, 若相等, 则表示同步正确。

2.5 视图切换协议

当共识域中的主节点 p 发生拜占庭错误时, 需要使用视图切换协议。具体流程如下。

2.5 视图切换协议

当共识域中的主节点 p 发生拜占庭错误时, 需要使用视图切换协议。具体流程如下。

- 1) 计算 $v_k = v + 1$ 。
- 2) 节点 r_i 向所有其他节点发送视图切换请求 $\langle \text{ChangeView}, h, r_i, v, k \rangle$ 。
- 3) 任意节点只要收到来自不同节点 r_i 关于 v 的视图切换请求数大于 $n-f$ 时, 就达成共识进行视图切换。令 $v = v_k$, 并且通过公式

$p = (h + v) \bmod |R_1|$ 重新计算出新的主节点。

- 4) 如果在经过时间 $2^k \cdot t$ 间隔后, 仍未能达成共识, 则重新开始这一轮的视图切换。

3 基于联盟区块链的根 CA 跨域认证方案

区块链主要分为三大类: 公有链、私有链和联盟链^[17]。其中, 联盟链中节点数是固定的, 联盟链只需极低的成本就能很好地做到节点间的连接, 具有交易速度快、交易费用低、扩展性强的优点。PBFT 是联盟链最常用的共识算法。

本节在 APBFT 的基础上提出一种由根 CA 作为联盟节点而建立的跨域认证方案。本方案的创新点如下。

- 1) 设计一种适用于联盟区块链下的根证书, 将根证书颁发记录保存在区块链账本上。由于在区块链中的节点互相信任对方, 可以取消根 CA 之间互相签发证书的步骤。
- 2) 使用区块链存储根 CA 之间的信任授权信息, 区块链账本上存储了多个信任域的根 CA 作为交易的发起方和接收方的信任授权信息。
- 3) 借鉴区块链分布式的思想, 将多个根 CA 作为共识节点建立联盟区块链方案, 同时保证原有 PKI 方案内的架构和认证方式不变。

3.1 方案简介

联盟链系统架构如图 1 所示, 多个根 CA 作为联盟区块链的验证节点将各个信任域之间的授权信息以及查询日志信息组装在区块中, 并且通过共识算法将其记录到联盟区块链账本中。为了提高区块链的扩展灵活性, 并且避免失效节点参与共识过程, 增加了备份节点作为共识节点失效后的缓冲。同时设置了代理节点作为身份验证查找使用, 代理节点不参加共识过程, 但是会同步联盟区块链账本中的数据, 方便证书颁发机构查询使用。

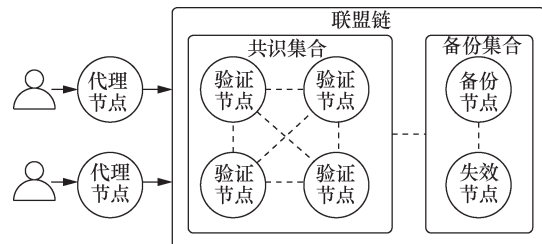


图 1 联盟链系统架构
Figure 1 Consortium blockchain system architecture

3.2 联盟区块链证书

本文设计一种针对联盟区块链场景的证书，由联盟区块链各节点达成共识后记入区块链账本中，该证书可作为授权域不可篡改的可信凭证。图2展示了传统的 X.509 证书与本文区块链证书的具体差别。



图2 X.509 证书与本文区块链证书

Figure 2 X.509 digital certificate and blockchain certificate in this paper

本文设计的联盟区块链证书将传统的 X.509 证书中的发行者唯一标识与主体唯一标识更换为授权域唯一标识和被授权域唯一标识。在用户跨域认证生效后，认证域的根 CA 会生成区块链证书颁发给发起请求的用户，以便该用户再次访问时能够快速认证。

本文区块链证书取消了签名与签名算法模块。传统 PKI 使用数字签名的原因主要是增加不可抵赖性，但是区块链本身具有强不可抵赖性。与此同时，本文新增的代理节点专门负责查验多个域中的可行凭证，可代替证书签名的验证。

本文区块链证书取消了证书撤销检查服务功能。由于在区块链数据库中的数据无法修改，故传统的撤销服务在区块链中无法直接应用。为了解决该问题，本文重新设计了写入数据库的数据形式，把写入接口定义为 $\text{post}(\text{action}, \text{data})$ ，其中， action 表明用户对于数据想要执行的处理动作，在

本文中可以是 issue 或 revoke 两种状态， data 表明区块链交易数据；同时重新设计了读取数据库的数据形式，读取接口为 $\text{get}(\text{condition})$ 。 condition 表明要查询的条件，可以是某一区块的哈希值，也可以是区块中授权证书的哈希值^[18]。

3.3 跨域认证协议

在上述系统架构和区块链证书的基础上，本文提出了一种基于联盟区块链的跨域认证协议。假定联盟区块链完成初始化，即各个域的根 CA 区块链证书记录在区块链中。

假设 A 域中的客户端想要获取 B 域中的服务器的服务，故 A 域中的客户端需要获得 B 域中的服务器对其的信任。相关符号定义见表1，协议流程如图3所示。

表1 协议符号说明
Table 1 Description of scheme parameters

符号	含义
$A \rightarrow B : m$	A 向 B 发送消息 m
C_x	X 域客户端
S_x	X 域服务器
Cert_x	X 域非根 CA 的公钥证书
$\text{Sign}_{\text{sk}_x}(m)$	X 域客户端对消息 m 的私钥签名
RCA_x	X 域的根 CA 服务器
$\text{BcCert}_{\text{RCA}_x}$	X 域的根 CA 的区块链证书
PP	联盟链代理节点
CP	联盟链共识节点

A 域用户请求 B 域服务器服务的具体流程如下。

1) $C_A \rightarrow S_B$

A 域客户端 C_A 向 B 域服务器 S_B 发起请求，

申请服务器服务。

2) $S_B \rightarrow C_A : \{N_1\}$

S_B 向 C_A 发送随机数 N_1 。

3) $C_A \rightarrow S_B : \{N_1, \text{Cert}_A, \text{Sign}_{\text{sk}_A}(N_1)\}$

C_A 收到 N_1 后，用私钥对其进行签名得到 $\text{Sign}_{\text{sk}_A}(N_1)$ ，并将公钥证书 Cert_A 以及 N_1 一起发给 S_B 。

4) $S_B \rightarrow \text{RCA}_A : \{N_2\}$

S_B 验证收到的消息，首先验证 N_1 是否有效，然后验证 C_A 的签名是否有效，最后通过证书链逐

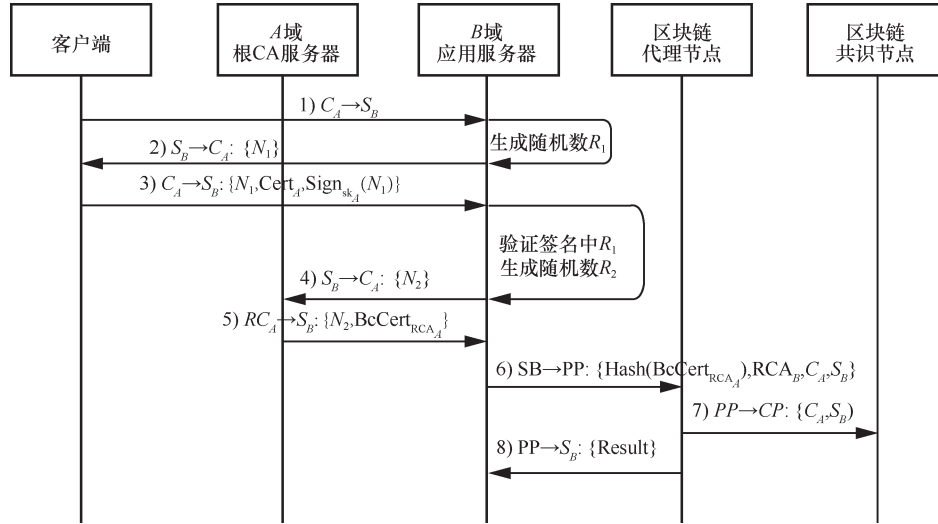


图3 X.509 协议流程

Figure 3 X.509 protocol process

步验证公钥证书 Cert_A 的有效时间并且找到 A 域根 CA 机构 RCA_A ; S_B 向 RCA_A 发送随机数 N_2 , 申请得到 A 域的区块链授权证书 $\text{BcCert}_{\text{RCA}_A}$ 。

5) $\text{RCA}_A \rightarrow S_B: \{N_2, \text{BcCert}_{\text{RCA}_A}\}$

RCA_A 收到 N_2 后, 将区块链授权证书 $\text{BcCert}_{\text{RCA}_A}$ 以及 N_2 一起发给 S_B 。

6) $S_B \rightarrow \text{PP}: \{\text{Hash}(\text{BcCert}_{\text{RCA}_A}), \text{RCA}_B, C_A, S_B\}$

S_B 收到消息后, 首先验证 N_2 是否有效, 然后验证 $\text{BcCert}_{\text{RCA}_A}$ 有效时间是否满足, 若满足, 则计算其哈希值 $\text{Hash}(\text{BcCert}_{\text{RCA}_A})$, 并将其与 B 域根 CA 机构 RCA_B 身份信息, C_A 信息和 S_B 信息一起发给区块链代理节点 PP 。

PP 通过 $\text{Hash}(\text{BcCert}_{\text{RCA}_A})$ 和 RCA_B 信息查询在区块链账本上查找信息, 若有查询信息, 则进一步查询区块链的具体授权信息, 若是 issue 状态, 则证书有效, 若是 revoke 状态, 则授权信息已被撤销。

7) $\text{PP} \rightarrow \text{CP}: \{C_A, S_B\}$

不管此次跨域认证是否成功, PP 都会将此次跨域认证双方的身份信息 (C_A, C_B) 记录到区块链共识节点中。

8) $\text{PP} \rightarrow S_B: \{\text{Result}\}$

PP 将跨域授权结果返回给 S_B , 若结果为已授权, 则 C_A 向发起的跨域请求成功。

4 方案分析

4.1 安全性分析

(1) 防止重放攻击

本文协议在信息传递的过程中使用随机数来保证传输的实时性, 即挑战应答的方式。具体来说, 服务器在接收到请求时会随机数发给客户端, 并且在本地记录该随机数, 在验证客户端发回来的消息时, 会验证消息中的随机数与在本地记录中的随机数是否相同, 进而防止恶意攻击者劫持消息后进行重放攻击。

(2) 抵抗分布式拒绝服务攻击

区块链是一种具有单点失效保护措施的分布式系统。具体来说, 每一个区块链节点上都会保存一份完全的数据复制, 所以当某几个节点失效时, 区块链也有保护措施以确保交易可以继续运行, 并不会影响整个区块链的数据安全, 进而解决单点失效问题。

(3) 双向实体认证

在跨域的时候, 授权服务器通过请求获得被授权客户端所在信任域的根 CA 区块链证书, 对其做哈希运算后在区块链上查找授权相关数据, 进而建立信任关系。进一步, 如果两个信任域之间互相颁发信任授权证书, 则可以实现域之间的客户端与客户端、客户端与服务器之间的双向认证。

4.2 性能分析

(1) 通信开销分析

假设共识域节点数为 $n(n > 3)$, 可以利用共识算法计算出一次完整的 PBFT 共识需要的通信次数, 计算范围只包括预准备阶段、准备阶段和确认阶段 3 个主要阶段。同时假设视图切换概率为 p (p 表示每隔 $\frac{1}{p}$ 次共识发生一次视图切换)。同理, 本文提出的一次完整的 APBFT 共识需要的通信次数也可以计算得到。具体通信开销对比见表 2。

表 2 通信开销对比
Table 2 Comparison of communication overhead

方案	共识阶段	共识阶段 (视图切换)
PBFT	$2n(n-1)$	$2n(n-1) + pn(n-1)$
APBFT	$n(n-1)$	$n(n-1) + p(3n^2 - 4n + 1)$

首先, 考虑不发生视图切换的情况。两个方案的通信开销之比 $I = \frac{2n(n-1)}{n(n-1)}$, 其值恒等于 2, 故不发生视图切换的情况下, 本文提出的 APBFT 通信开销比原 PBFT 减少了 50%。

然后, 考虑发生视图切换的情况。此时 PBFT 的通信开销之比 $I = \frac{2n(n-1) + pn(n-1)}{n(n-1) + p(3n^2 - 4n + 1)}$, 通求导可知, 当 $p=0.5$ 时, I 值趋近于 1, 两个方案的通信开销相等; 当 $p < 0.5$ 时, 本文提出的 APBFT 通信开销更小, 进一步, 考虑到实际情况中视图切换的概率是极小的, 故在实际情况中 APBFT 的通信开销接近原 PBFT 算法的一半。综上所述, APBFT 算法可以有效降低联盟区块链中共识阶段通信开销。

(2) 计算开销分析

本小节主要将本文方案中密码学计算开销与文献[19]、文献[20]进行比较。本文假设共识节点数为 2, 不考虑备份节点。表 3 表示 3 种不同方案的计算开销。

由表 3 可以看出, 本文方案与文献[19]方案相比, 大量减少了数字签名验证的次数。文献[19]的方案是基于椭圆曲线密码的, 所以数字签名验证的次数会随着盟员的加入呈现线性上升趋势; 而本文方案是基于联盟链的, 所以理论上数字签

名验证的次数不会受盟员加入的影响, 但是为了维护区块链集体账本, 客观上也会产生大量的哈希计算。总体来看, 在节点数较少的情况下, 本文方案不管是数字签名验证的次数还是哈希运算次数都比文献[19]有显著的优势。

表 3 计算开销对比
Table 3 Comparison of computation overhead

方案	公钥加解密次数	数字签名验证次数	哈希运算次数
文献[19]	0	12	4
文献[20]	2	4	10
本文	0	4	2

本文方案与文献[20]方案相比, 减少了 2 次公钥加解密, 这是因为文献[20]方案为了保证隐私性, 对签名信息进行了加密, 故只有认证客户端和认证服务器才有资格验证签名。而本文方案由于会将查询记录在区块链账本中, 并不提供隐私性, 故并没有使用公钥加解密。但本文方案使用哈希运算的次数会随着盟员数的增长随之增加。不过由于哈希算法的计算效率本身远高于公钥算法, 同时实际环境中根 CA 的数量不会过多。故在多域联盟的环境下, 本文方案的跨域认证效率仍优于文献[19]和文献[20]。

5 结束语

本文提出了一种改进的算法方案 APBFT, 增加了节点动态增减功能, 改进主节点选举方式, 将三阶段广播缩减为两阶段广播, 降低了通信开销。与此同时, 本文提出了一种基于联盟区块链的跨域认证方案, 该方案不仅能实现跨域认证, 而且能提供证书查询功能。与现有跨域认证方案相比, 本文方案在保证安全的前提下, 有效提升了跨域认证效率, 可扩展性强。

参考文献:

- [1] 郭锐. 匿名通信系统流量伪装技术研究[D]. 北京: 北京邮电大学, 2018.
GUO R. Traffic camouflaging in anonymous communication system[D]. Beijing: Beijing University of Posts and Telecommunications, 2018.
- [2] 张琰, 王瑾璠, 齐竹云, 等. 基于动态累加器的去中心化加密搜索方案[J]. 网络与信息安全学报, 2019, 5(2): 23-29.
ZHANG Y, WANG J F, QI Z Y, et al. Decentralized searchable en-

- crypton scheme based on dynamic accumulator[J]. Chinese Journal of Network and Information Security, 2019, 5(2): 23-29.
- [3] VACCA J R. Computer and information security handbook[M]. Boston: Elsevier, 2009.
- [4] 彭博, 刘进, 龚智, 等. 一种树型桥 CA 跨域信任传递方案研究[J]. 舰船电子工程, 2017, 37(3): 66-69, 113.
PENG B, LIU J, GONG Z, et al. Cross-domain trust model based on bridge CA[J]. Ship Electronic Engineering, 2017, 37(3): 66-69, 113.
- [5] PERLMAN R. An overview of PKI trust model[J]. IEEE Network, 1999, 13(6): 38-43.
- [6] ROUBAH K, OULD-ALI S. Dynamic data sharing and security in a collaborative product definition management system[J]. Robotics and Computer Integrated Manufacturing, 2006, 23(2).
- [7] 杨斌, 陈国庆, 孙永红. 一种新的基于身份的多信任域认证方案研究[J]. 计算机安全, 2010(8): 15-18.
YANG B, CHEN G Q, SUN Y H. Research of a new identity-based authentication model for multi-domain[J]. Computer Security, 2010(8): 15-18.
- [8] CHAN Y Y, FLEISSNER S, LIU J K, et al. Single sign-on and key establishment for ubiquitous smart environments[C]//International Conference on Computational Science and Its Applications. Berlin: Springer, 2006: 406-415.
- [9] 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, XUN 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.
- [10] 刘亚辉. 基于区块链的可信电子券系统的设计与实现[D]. 北京: 北京邮电大学, 2018.
LIU Y H. Design and implementation of trusted electronic coupons system based on block-chain[D]. Beijing: Beijing University of Posts and Telecommunications, 2018.
- [11] SUN Y, YU Y, LI X, et al. Batch verifiable computation with public verifiability for outsourcing polynomials and matrix computations[C]//Australasian Conference on Information Security and Privacy, 2016: 293-309.
- [12] GARG S, GENTRY C, HALEVI S. Candidate multilinear maps from ideal lattices[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2013: 1-17.
- [13] BONEH D, GOH E J, NISSIM K. Evaluating 2-DNF formulas on ciphertexts[C]//Theory of Cryptography Conference, 2005: 325-341.
- [14] LAMPORT S, PEASE M. The byzantine generals problem[M]. IEEE Computer Society Press, 1995.
- [15] 王娜. 无线传感网节点信任检测量化方案与方法研究[D]. 上海: 华东师范大学, 2015.
WANG N. Research on quantitative trust detecting method and model for nodes in WSNs[D]. Shanghai: East China Normal University, 2015.
- [16] CASTRO M, LISKOV B. Practical Byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems (TOCS), 2002, 20(4): 398-461.
- [17] 沈鑫, 裴庆祺, 刘雪峰. 区块链技术综述[J]. 网络与信息安全学报, 2016, 2(11): 11-20.
SHEN X, PEI Q Q, LIU X F. Survey of block chain[J]. Chinese Journal of Network and Information Security, 2016, 2(11): 11-20.
- [18] 蔡维德, 郁莲, 王荣, 等. 基于区块链的应用系统开发方法研究[J]. 软件学报, 2017, 28(6): 1474-1487.
CAI W D, YU L, WANG R, et al. Blockchain application development techniques[J]. Journal of Software, 2017, 28(6): 1474-1487.
- [19] 张文芳, 王小敏, 郭伟, 等. 基于椭圆曲线密码体制的高效虚拟企业跨域认证方案[J]. 电子学报, 2014, 42(6): 1095-1102.
ZHANG W F, WANG X M, GUO W, et al. An efficient inter-enterprise authentication scheme for VE based on the elliptic curve cryptosystem[J]. Acta Electronica Sinica, 2014, 42(6): 1095-1102.
- [20] 罗长远, 霍士伟, 邢洪智. 普适环境中基于身份的跨域认证方案[J]. 通信学报, 2011, 32(9): 111-115, 122.
LUO C Y, HUO S W, XING H Z. Identity-based cross-domain authentication scheme in pervasive computing environments[J]. Journal on Communications, 2011, 32(9): 111-115, 122.

[作者简介]



钱思杰 (1995—), 男, 浙江嵊州人, 东南大学硕士生, 主要研究方向为区块链和公钥密码学。



陈立全 (1976—), 男, 广西玉林人, 博士, 东南大学教授、博士生导师, 主要研究方向为信息系统安全、移动安全、区块链安全。



王诗卉 (1995—), 女, 江苏如皋人, 东南大学硕士生, 主要研究方向为隐私保护和密码学。