软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(8):2314−2336 [doi: 10.13328/j.cnki.jos.005764]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于区块链的分布式可信网络连接架构*

刘明达[1], 拾以娟[1], 陈左宁[2]

[1](江南计算技术研究所,江苏 无锡 214083)

[2](中国工程院,北京 100088)

通讯作者: 刘明达, E-mail: happyliumd@163.com

摘 要: 可信网络连接是信任关系从终端扩展到网络的关键技术.但是,TCG的TNC架构和中国的TCA架构均面向有中心的强身份网络,在实际部署中存在访问控制单点化、策略决策中心化的问题.此外,信任扩展使用二值化的信任链传递模型,与复杂网络环境的安全模型并不吻合,对网络可信状态的刻画不够准确.针对上述问题,在充分分析安全世界信任关系的基础上,提出一种基于区块链的分布式可信网络连接架构——B-TNC,其本质是对传统可信网络连接进行分布式改造.B-TNC 充分融合了区块链去中心化、防篡改、可追溯的安全特性,实现了更强的网络信任模型.首先描述B-TNC的总体架构设计,概括其信任关系.然后,针对核心问题展开描述:(1) 提出了面向访问控制、数据保护和身份认证的 3 种区块链系统;(2) 提出了基于区块链技术构建分布式的可信验证者;(3) 提出了基于DPoS 共识的的远程证明协议.最后,对 B-TNC 进行正确性、安全性和效率分析.分析结果表明,B-TNC 能够实现面向分布式网络的可信网络连接,具有去中心化、可追溯、匿名、不可篡改的安全特性,能够对抗常见的攻击,并且具备良好的效率.

关键词: 区块链;可信网络连接;信任模型;分布式网络;共识协议

中图法分类号: TP309

中文引用格式: 刘明达,拾以娟,陈左宁.基于区块链的分布式可信网络连接架构.软件学报,2019,30(8):2314−2336. http://www.jos.org.cn/1000-9825/5764.htm

英文引用格式: Liu MD, Shi YJ, Chen ZN. Distributed trusted network connection architecture based on blockchain. Ruan Jian Xue Bao/Journal of Software, 2019,30(8):2314−2336 (in Chinese). http://www.jos.org.cn/1000-9825/5764.htm

Distributed Trusted Network Connection Architecture Based on Blockchain

LIU Ming-Da[1], SHI Yi-Juan[1], CHEN Zuo-Ning[2]

[1](Jiangnan Institute of Computing Technology, Wuxi 214083, China)

[2](Chinese Academy of Engineering, Beijing 100088, China)

Abstract: Trusted network connection is the key technology for trust relationship to extend from terminal to network. However, TCG's TNC architecture and China's TCA architecture are both oriented to a strong identity network with central access. In actual deployment, there is a single point of access control and policy decision center. In addition, the trust extension uses the binary trust chain transfer model, which is not consistent with the security model of the complex network environment, and the portrayal of the trusted state of the network is not accurate enough. In response to the above issues, this study fully analyzes the trust relationship in the security world and then proposes a distributed trusted network connection architecture based on blockchain, called B-TNC, which is the transformation of TNC with blockchain essentially. B-TNC fully integrates the de-centralization, tamper-proof, and traceable security features of blockchain,

* 基金项目: 核高基国家科技重大专项(2013ZX01029002G001)
Foundation item: CHB National Science and Technology Major Project of China (2013ZX01029002G001)
本文由“面向自主安全可控的可信计算”专题特约编辑林璟锵教授推荐.
收稿时间: 2018-05-29; 修改时间: 2018-09-21; 采用时间: 2018-12-13; jos 在线出版时间: 2019-03-28
CNKI 网络优先出版: 2019-03-29 09:47:15, http://kns.cnki.net/kcms/detail/11.2560.TP.20190329.0947.015.html

and realizes a stronger network trust model. This paper first describes the overall architecture design of B-TNC, and summarizes its trust relationship. Then, the core problems are described: (1) proposing three blockchain systems for access control, data protection, and identity authentication; (2) proposing to build distributed trusted verifiers based on blockchain; and (3) proposing a remote attestation protocol based on DPoS consensus. Finally, this paper analyzes the correctness, security, and efficiency of B-TNC. The analysis shows that B-TNC can realize trusted network connection oriented to distributed network, with decentralization, traceability, anonymity, not tampered security features that are resistant to common attacks, with sound efficiency.

Key words: blockchain; trusted network connection; trust model; distributed network; consensus protocol

为了解决传统体系结构存在的安全问题,可信计算[1,2]应运而生.可信计算的目标是在计算体系中引入信任根,进而建立一条信任链[3],将信任关系从底层硬件扩展到上层应用,以增强计算系统的安全性.可信计算在保护终端安全方面发挥了重要的作用,目前已经成为了标准化的技术.

可信计算组织(TCG)于 2015 年发布了 TPM2.0 规范[4],成为 ISO/IEC 标准[5].另外,以 ARM Trustzone[6,7]和 Intel SGX[8,9]为代表的可信执行技术(trusted execution environment,简称 TEE)近年来也得到了广泛的关注.可信执行技术的核心思想是:以 CPU 作为信任根,建立从信任根直接到应用程序的信任链.TEE 目前存在侧信道攻击等安全问题[10],并未实现预期的强安全性,但是其思想是可以借鉴和值得研究的.我国可信计算技术走在世界的前列,已经进入了可信 3.0 的发展阶段[11],核心思想是建立一套主动免疫的计算机安全体系.无论是理论还是工程实践方面,都取得了可喜的成果.对于国家安全战略,复杂的网络安全环境中的关键信息基础设施必须要实现自主可控.然而自主不等于可控,自主也不等于安全,必须加入更多的安全防控手段.可信计算是实现自主可控的关键技术,尤其是在云计算大数据的背景之下,可信计算必须重点突破.

面对各种安全威胁和风险,只有终端计算环境的可信是不够的,还要把信任关系从终端计算环境传递到网络环境,可信网络连接技术应运而生[12].以 TCG 的可信网络连接(TNC)为例[13],在终端接入网络之前,TNC 对终端的身份状态和可信状态进行度量,只有身份合法,并处于安全运行状态的终端才可以接入网络环境.TNC 本质上是可信计算与网络接入控制机制的结合.研究可信网络连接,用可信计算的思想解决网络空间安全问题,本身具有重要的意义.

随着云计算大数据等新型计算模式的兴起[14−16],网络空间面临着复杂棘手的安全威胁,最为严重的是基础网络设备和 CPU 级的安全漏洞,典型漏洞见表 1.

Table 1 Vulnerability and attack

表 1 漏洞和攻击

名称	时间	影响设备	描述
CVE-2018-0171	2018.03	思科网络设备	攻击者可以远程控制网络设备
CVE-2018-0150	2018.03	思科网络设备	攻击者可以远程登录控制设备
BranchScope	2018.03	CPU	能够突破 SGX 安全架构
Meltdown 漏洞	2018.01	CPU	获取关键敏感数据
Spectre	2018.01	CPU	获取关键敏感数据
TPM 芯片漏洞	2017.10	英飞凌 TPM1.2 和 TPM2.0	生成不安全的 RSA 密钥

无论多么高明的网络安全防护手段,在部署的时候都要依托实际的软硬件系统,但是漏洞是客观存在的.尤其基础网络设备、CPU 和安全芯片的漏洞,会对基本的安全假设带来严重的挑战,使安全协议失效.与其他安全技术相比,可信计算更加偏向底层部件的安全,更接近安全的源头,在保护系统结构安全方面拥有不可替代的优势.周天明等人指出[17]:可信计算是一个保障体系,其目标是实现网络空间可信.广义上讲是解决如何将最基本的信任关系传递到整个网络空间,这并不意味着只局限于信任链的技术路线.

TNC 和 TCA 架构[18]都在一定程度上实现了信任向网络扩展,相关研究者在此基础之上展开了大量的研究工作,主要集中在远程证明、访问控制、匿名性和可信虚拟化,但是鲜有可信网络连接基础架构的研究.TNC 和 TCA 架构目前存在以下问题和挑战.

(1) 信任模型存在局限.网络空间安全状态复杂.安全是一个相对性的概念,单纯用二值化的可信判断标

准无法准确刻画实际的安全状态,信任关系难以传递到网络环境.因此,以信任链为基础的信任模型存在局限,需要进一步拓展.

(2) 访问控制单点化.在有中心的网络环境中,无论是实际的物理网络还是虚拟网络,最终都是由访问控制部件根据一定的访问控制策略来决定计算节点之间是否可以通信.访问控制部件可以是安全网关、单向隔离设备以及防火墙等.但是基础网络设备存在被攻破的风险,一旦发生安全问题,网络就会被操控.

(3) 策略决策中心化.在传统的可信网络架构中,会维护一个策略决策的服务端用于策略判断和生成访问控制规则.TCA 架构依托可信第三方进行策略管理,比 TNC 架构具有更强的安全性.但是在部署的时候,策略管理器作为可信第三方,实际上就成了整个网络的可信中心.策略管理器的实体必然是一个通用计算环境,也将面临上述安全威胁.

针对上述问题,本文结合目前网络环境的实际需求,提出了基于区块链的分布式可信网络连接架构.首先,本文对网络安全世界的信任问题进行深入的阐述,指出目前的信任模型存在的问题;然后提出可信网络总体架构,对信任关系、基础框架、区块链结构进行详细描述,并给出基本的安全假设;接着对可信网络的运行流程进行介绍,并对核心问题展开描述,提出了一种基于委托股权证明(deligated proof of stake,简称 DPoS)[19]的远程证明方法;最后,从正确性、安全性和效率等 3 个方面对架构进行分析.本文的主要贡献在于:

(1) 分析了网络安全世界的信任问题,在总结现有可信网络链接缺陷的基础上,提出了“网络环境依托信任契约,终端环境依赖可信计算”的信任扩展方法;

(2) 提出了基于区块链技术的可信网络链接架构,充分发挥区块链技术在分布式网络中构建可信契约的优势,解决了传统可信网络连接面临的访问控制单点化和策略决策中心化的问题;

(3) 提出了一种基于 DPoS 共识的远程证明协议,在充分保护隐私的情况下,实现了平台身份证明和完整性证明,将远程证明的决策从依托中心化的可信第三方变为依托信任契约.

本文第 1 节对相关问题和技术进行介绍.第 2 节介绍 B-TNC 总体架构和建立模型.第 3 节介绍 B-TNC 运行流程,并且提出关键问题的解决思路.第 4 节从正确性、安全性和效率这 3 个方面对架构进行分析.第 5 节总结全文并展望下一步工作.

1 相关问题

为了对基于区块链的分布式可信网络链接进行详细的阐述,首先对可信网络连接和区块链的基本原理进行描述,在此基础上,对安全世界的信任问题进行探讨,指出用区块链技术构建可信任网络的必要性和优势.

1.1 可信网络连接

可信网络连接是以TNC和TCA技术路线为代表.狭义上讲,可信网络连接是一种基于对平台身份和平台完整性状态的证明,从而决定终端是否可以接入网络环境的技术.但是随着云计算的发展,网络环境不再是单纯的终端连接的网络,有了更加丰富的组织形式.广义上讲,可信网络连接是将可信计算的信任关系传递到网络环境的过程.可信计算在云环境下的应用同样属于这一范畴,其核心技术是信任根的虚拟化问题.

传统的可信网络架构 TNC 和 TCA 的技术具有相似性,但是 TCA 架构克服了 TNC 的不足,是中国对可信计算的重要创新.以 TCA 架构为例,可信网络连接旨在构建一个三元对等的安全架构,引入一个可信第三方对参与网络连接的实体进行身份认证和平台运行状态的认证.TCA 对实体鉴别、访问控制以及各个部分之间的通信都制定了相应的标准,只有具备合法信任根的终端才能够参与到网络交互中,这就实现了信任关系传递到网络环境.

可信计算目前已经成为系统安全的重要技术,尤其是在自主可控领域,发挥了无法替代的作用.原因在于:可信计算能够接管 CPU 对计算环境安全的控制权,进而将安全掌握在自己手中.如何实现信任根 TPM 或 TCM 的虚拟化,将信任链从计算终端传递到虚拟网络环境,是可信云计算的关键问题[20−22].我们曾面向高安全的虚拟计算环境,提出一种基于 SR-IOV 技术构建硬件虚拟化 TCM 的方法[23],为每个虚拟节点提供硬件级的虚拟化

TCM,实现了虚拟机获取基于硬件的密钥保护和密码计算资源.但是这种信任扩展方式和云环境下动态灵活的网络特性互相矛盾,并不能展开大规模的部署和应用.信任关系如何向云环境传递,仍需展开更加深入的研究.

1.2 区块链基础

区块链[24,25]本质上是一个状态机副本协议,旨在建立一个去中心或弱中心化的数据库系统,实现分布式环境下安全高效的共识机制.除了在电子货币中取得的成果外,基于区块链可实现更广泛意义上的安全多方计算,因此,区块链技术可应用领域相对电子货币更加广泛.在区块链提出之前,类似的功能通常基于安全多方协同计算实现,例如通过著名的拜占庭协议[26]也可以实现多方参与者的共识.区块链技术的独特之处在于如下几方面.

(1) 区块链共识机制无需可信第三方参与.

无可信第三方参与意味着任何用户均可自由参与区块链系统,因此,区块链称为无许可系统.在传统的安全多方计算环境中,攻击者可注册足够数量的用户,则可实施女巫攻击(sybil attacks)[27].Barak 等人系统研究了无许可机制系统下的女巫攻击问题,区块链技术通过工作量证明机制有效抵抗了此类攻击[28].随着区块链技术的演进,从业务驱动的角度出发,又出现了有许可的区块链系统,即私有链或联盟链.节点必须提供可信的身份证据才能够参与到区块链中.

(2) 区块链共识机制运行效率极高.

传统的安全多方计算协议均较为复杂[29],通信复杂性及计算复杂性限制了其在大规模环境中的使用.区块链技术是第一种可在全球范围分布式部署的共识协议.区块链系统通过简单的无认证广播信道以及区块链长度竞争机制,实现了高效的共识.

典型的区块链系统由网络层、共识层、数据层、智能合约层和应用层组成[30].其中,网络层通常是基于 P2P 协议进行节点之间的通信;共识层实现共识协议,协议可以是根据实际场景自由选择,比如基于工作量证明 PoW,和基于权益证明 PoS;数据层是区块链的数据结构,其结构设计通常根据实际需要与应用场景紧密耦合,每一个计算节点负责维护自己的存储系统;智能合约层能够对于不同的数据输入执行不同的操作,这个过程依托代码自动执行,并在全网达成共识;应用层是区块链系统的各种基本业务,比如金融服务、数据溯源等.为了便于描述,本文将区块链系统进行抽象表示,如图 1 所示.

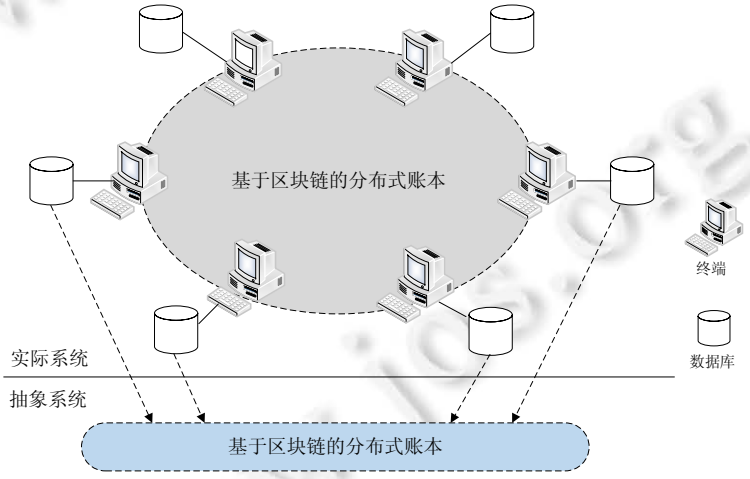

Fig.1 Abstractdescription of blockchain system

图 1 区块链系统抽象描述

1.3 安全世界的信任问题

安全世界的信任问题源自于人类社会的信任关系,而人类社会信任关系扩展模型与人类社会的组织关系是相对应的.信任是多元的,发生在不同主体的交互过程,是一个网状的拓扑结构.也就是说,如果没有信任的交

互,即便每个人都相信自己,也无法形成信任社会.人类社会发展至今,已经形成了比较完善的社会信任体系,根据信任体系参与者的数量不同,可以从两个维度去区分.

(1) 依托信任传递的“小团体”信任模型.

这种信任模式通常发生在较少的个体之间,最典型的模式为:*A* 信任 *B*,*B* 信任 *C*,进而 *A* 在某种程度上可以信任 *C*,这个过程是单向的.依托这种信任传递关系,能够实现两类信任场景:一种是家庭、家族甚至族群之间的互相信任,信任传递的路径短,信任在传递过程中的损耗相对比较低,但是难以扩展到更大的范围;另一种是对权威的信任,人们通常愿意相信权威人士或专家,类似于可信的第三方,但是这并不能解决普通成员之间的互信,并且权威并不是完全可信的.在小团体信任中,个体的信任失效有可能引发整个信任关系的失效.

(2) 基于信任契约的“大团体”信任模型.

随着人类社会的进步与发展,相互协作的团体规模越来越大,形成了城邦、国家或者企业集团,规章制度、法律法规就成了维系其运行的关键因素,这就是信任契约.信任契约的形成需要参与的实体达成共识,并且保证大部分的参与者遵守这一契约.在人类社会中,不可能所有的个体都能够严格遵守规章制度和道德法律,一定存在不遵守规则的个体,但是信任契约对此是可以容忍的.

可信计算以信任链技术为基础,将信任传递与体系结构高度融合,能够有效实现计算终端环境的可信.但是为了实现方便,可信计算在实际应用时采用的是二值化的信任判断模型,对于安全的刻画局限于安全或不安全,这与复杂的网络计算环境是不符合的.同样的安全状态,对于不同的业务应用场景是不同的,这涉及到复杂的等级保护问题,本文不再展开.

从最基本的原理而言,网络计算环境和社会环境具有极高的相似性,都是由多个主体构成,主体之间存在各种通信交互往来,存在恶意主体,都更强调整体性而弱化个体.可信计算在将信任关系传递到网络环境时,基本思想是:通过保证每一个计算终端的安全,进而保证网络环境的整体可信.但是基于上述讨论可知,个体安全并不能保证整体安全,并且保证所有的个体可信是困难的,一定存在一定比例的坏节点.本文认为,信任模型缺陷是限制信任关系向网络环境传递最大的制约因素,也是制约可信网络连接发展的重要原因.

回到可信计算发展的出发点,以人类社会基本的信任关系作为基点去探索安全世界的信任关系,我们可以得到这样的结论:信任链的信任传递模型能够有效实现终端环境的可信,但与网络环境不适应,需要建立信任契约来解决网络环境下的信任传递问题.

区块链可以看作可信的一种形态,与可信计算技术路线中集中式的信任根不同.区块链凭借巧妙的数据结构和共识机制,实现了一种分散式的信任根,以整体协同计算的方式为整个网络环境提供基本的信任支撑.集中式信任根的实现形式为 TPM/TCM/CPU,分散式信任根的实现形式为区块链,其对比见表 2.

Table 2 Centralized trust root and distributed trust root

表 2 集中式信任根和分散式信任根

名称	集中式信任根	分散式信任根
信任来源	物理安全,密码安全	密码安全,共识协议
信任根	TPM/TCM/CPU	共识协议
质疑部分	不相信其他部件	不相信单个节点
信任模型	以信任链为基础由点到面的信任结构	以概率为基础由面到面的信任结构
安全假设	安全假设不完全符合实际网络环境	安全假设与实际网络环境基本一致
信任传递	信任难以扩展到网络环境	建立网络世界的安全契约

综上所述,以区块链为基础的分散式信任根在信任模型构建、安全假设以及信任传递方面与实际网络环境更加贴合.这能够有效弥补传统可信计算在构建可信网络时存在的不足,将信任关系有效传递到网络环境中.为了实现这个目标,本文在对安全世界的信任问题的研究基础之上,探索如何基于区块链技术构建分散式信任根的方法,以整体的网络空间作为着眼点,实现网络空间的可信.

2 B-TNC 总体架构与模型构建

基于区块链的分布式可信网络连接架构 B-TNC 本质上是可信计算技术和区块链的融合.本节首先描述

B-TNC 中的信任传递关系,然后给出 B-TNC 的基础框架和总体架构.接着对其进行抽象化的描述,提出最基本的理论模型.在此基础之上,提出 B-TNC 的区块链结构设计方法,最后给出安全假设.

2.1 信任关系

根据信任来源不同,B-TNC 架构的信任关系从逻辑上可以分为网络可信和终端可信,如图 2 所示.

(1) 终端可信.终端计算环境的可信由可信计算保障,采用信任链的信任传递方法.信任根的可信由硬件安全保证.通常认为,基于硬件的安全防护强度要高于软件.在硬件设计中,要充分考虑信任根的物理安全,并且能够有效对抗常见的侧信道攻击,如能量分析[31].信任链的信任关系由密码安全保证,而密码体质的安全源自于数学原理.具体来说,只要密码学体制未被攻破,就能保证信任传递的真实性.

(2) 网络可信.根据第 1.3 节对安全世界信任问题的讨论,本文提出基于区块链实现网络层的可信.以密码安全和共识协议为基本手段,建立网络环境下的信任契约,重点对计算节点在网络环境中的连接行为进行管控.基于区块链的网络可信有两层含义:一方面是基于区块链的可信连接,核心是远程证明、访问控制和日志审计过程;另一方面是基于区块链构建可信第三方,提供 CA 服务,零知识证明以及可信验证等服务.

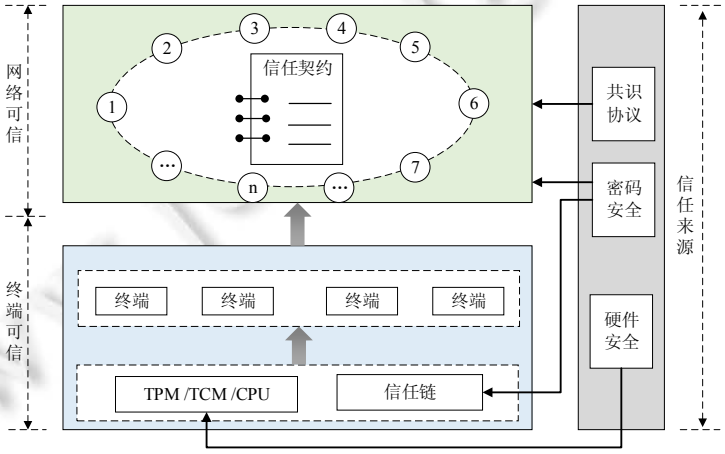

Fig.2 Trustrelationship in B-TNC

图 2 B-TNC 中的信任关系

终端可信和网络可信并不是完全独立的.终端可信是网络可信的基础,可信计算一方面能够为安全系统提供最基础的密码支持,另一方面能够增强终端计算环境的安全性,这对于区块链系统非常重要.因为区块链系统要满足大多数节点诚实这一基本的假设,终端可信恰好有助于此.同时,区块链弥补了可信计算在解决网络可信方面的不足,能够将信任关系有效地传递到网络环境当中.这样就构建了一种双层的信任关系.在这个基础之上,可以提出 B-TNC 的基础框架和总体架构.

2.2 基础框架

基于区块链的分布式可信网络连接架构的基础框架包含 3 个实际网络运行环境,分别是可信网络环境、分布式的可信第三方以及外部网络环境,如图 3 所示.

(1) 可信网络环境.可信网络环境是需要保护的网络环境,在本文的假设中具有去中心的特点.与信任关系相对应,每一个被允许加入可信网络环境的终端都必须具备合法的信任根 TPM/TCM.信任根一方面可以对计算终端安全提供可信支撑,另一方面为计算节点提供强身份认证.可信网络环境是一个依托区块链系统组成的逻辑环境,在网络中维护一个面向可信网络连接的区块链系统,提供访问控制、日志审计以及远程证明的服务功能.可信网络环境中存在两种节点:可信计算节点(trusted node,简称 TN),这是实际安全的节点,具有合法的 TPM;非可信节点(non-trusted node,简称 NTN),网络中实际可

能存在安全隐患的节点,但并不一定是恶意节点.

(2) 分布式的可信第三方.可信第三方是构建实际密码系统的基础,但是中心化的信任背书通常意味着更大的攻击威胁.近年来出现了基于区块链技术构建可信第三方的研究,如 Conner 等人提出的 Certcoin[32,33]、Chen 等人提出的 CertChain[34],都是将区块链技术用于实现一个更加安全高效的公钥基础设施(public key infrastructure,简称 PKI).除 PKI 外,可信网络连接架构需要可信验证和零知识证明两种第三方服务,其中,可信验证源自于基于属性的远程证明[35],能够根据完整性证据为通信双方提供可信判断服务;零知识证明被用于直接匿名证明(direct anonymous attestation,简称 DAA)[36],用于保护计算平台在参与网络通信过程中的匿名性.受到 Certcoin,CertChain 启发,分布式的可信第三方的构建具有可行性,但实现细节不作为本文的研究重点.

(3) 外部网络环境.外部网络环境从用户角度分为诚实用户和恶意用户,从终端可信角度分为可信终端、恶意终端和未知终端.未知终端的含义是:不具有恶意终端的恶意行为,但是可能存在潜在的安全风险.外部网络环境和可信网络环境与可信第三方的关系相同,都是获取证书服务、可信验证和零知识证明服务.外部网络和可信网络环境之间是远程证明、可信连接和访问控制.外部网络存在恶意节点(malicious node,简称 MN),是外部网络试图入网的恶意节点.

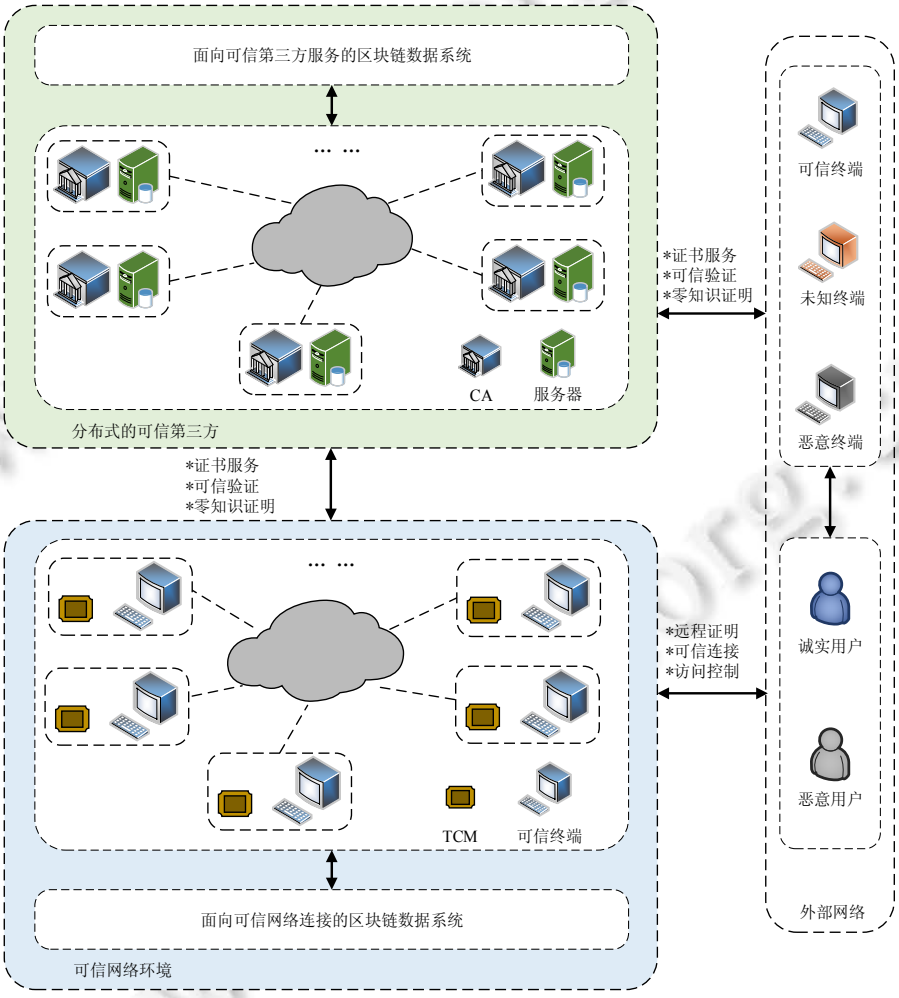

Fig.3 Basicframe of trusted network

图 3 可信网络基础框架

2.3 总体架构

B-TNC 的总体架构如图 4 所示,包括 4 个实体、3 个区块链系统、5 个层次和若干接口组件.该架构在传统可信网络连接层次上增加了区块链系统.B-TNC 将策略的执行由中心转移到各实体,将决策由分布式的可信第三方转移到分布式的可信第三方,实现了一种新型的可信网络连接架构.

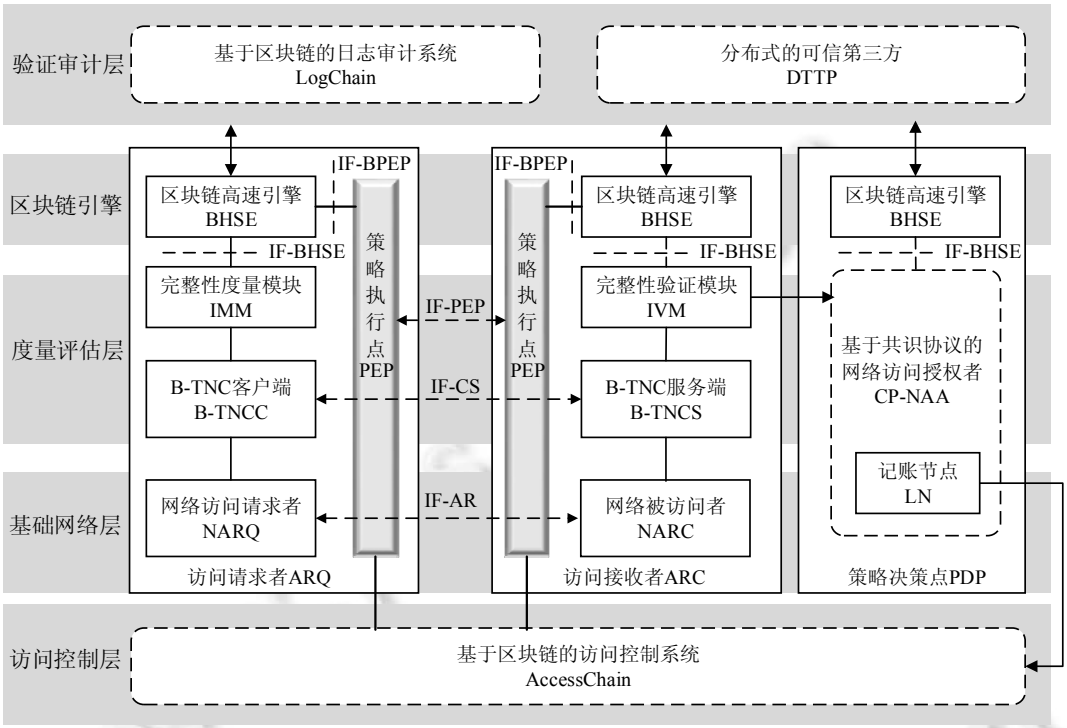

Fig.4 Overall architecture of B-TNC

图 4 B-TNC 总体架构

- 实体

4 个实体分别是访问请求者(access requestor,简称 ARQ)、访问接收者(access receiver,简称 ARC)、策略决策点(policy decision point,简称 PDP)和策略执行点(policy enforcement point,简称 PEP).其中,

- ARQ 位于外部网络,发出访问请求,收集平台完整性可信信息,申请与可信网络环境中的计算节点建立网络连接;
- ARC 位于可信网络环境,是被访问的计算节点,需要对访问请求进行处理,将 ARQ 的平台完整性信息转发到区块链系统进行可信验证;
- PDP 在组成结构上与传统可信网络连接不同:B-TNC 中,PDP 是一个由全网共同组成的逻辑实体,通过区块链数据库系统和共识协议维系.PDP 根据各计算节点的安全策略对 ARQ 的访问请求进行决策判定,判断的依据是 ARQ 的身份和完整性状态信息,并将判断结果写入的区块链系统;
- PEP 部署在 ARQ 和 ARC,负责执行访问控制策略.

ARQ 包括 4 个组件:网络访问请求者(network access requestor,简称 NARQ)发出访问请求,申请加入可信网络环境,建立网络连接.ARQ 的 B-TNC 客户端(B-TNC client,简称 B-TNCC)收集完整性度量模块(integrity measurement module,简称 IMM)的完整性度量信息,并将完整性度量信息向远端平台报告.完整性度量信息的内容和组成由可信度量的具体模型决定.IMM 和 TCM 协同度量 ARQ 各个组件的完整性.区块链高速引擎(blockchain high-speed engine,简称 BHSE)是实体与区块链系统之间的接口,一方面提供区块链读取写入查询等

基本功能,另一方面对区块链数据系统进行实时解析,在本地维护一个支持高速查询的区块链数据库.但是必须被可信网络接受以后才能够获得区块链上的数据.

ARC 包括 4 个组件:网络访问接收者(network access receiver,简称 NARC)接收外部节点 ARQ 的入网申请,发起对 ARQ 的可信度量.ARC 的 B-TNC 服务端(B-TNC server,简称 B-TNCS)接收 ARQ 发送的完整性度量报告,并提交到完整性验证模块(integrity verifier module,简称 IVM)进行验证.IVM 发起对 ARQ 的可信验证,将可信度量信息广播到可信网络环境的计算节点,等待验证.区块链高速引擎与 ARQ 中的作用相同,不再赘述.

PDP 包括两个组件:基于共识协议的网络访问授权者(network access authority based on consensus protocol,简称 CP-NAA)和区块链高速引擎.与 TNC 架构中的 NAA 不同,B-TNC 的 CP-NAA 并不是单一的物理实体,而是由运行在可信网络中的多个计算节点组成的逻辑实体.这些计算节点均产生 ARQ 是否可以加入可信网络的决策,并基于共识协议汇总决策,形成最终的共识.需要说明的是,共识协议多种多样,必须根据具体的共识协议设计合理的决策节点数目.在 CP-NAA 中,每次共识均选举产生一个记账节点(leader node,简称 LN),由 LN 作为区块链中的"矿工"将最终的结果写入区块链系统.本文提出了一种基于 DPoS 共识的方法,以验证其可行性,但并不仅局限于此.

- 区块链系统

3 个区块链系统分别是基于区块链的访问控制系统(access control blockchain,简称 AccessChain)、基于区块链的日志审计系统(log audit blockchain,简称 LogChain)和分布式的可信第三方(distributed trusted third party,简称 DTTP).在前期研究中,我们提出了基于区块链的远程证明模型[37],给出了访问控制和可信证据追溯的基本方法,两类功能都在同一个区块链上.但是访问控制和日志审计的数据量并不同,不能很好地满足实际需求.在此基础之上,本文提出了用 3 个区块链系统支撑可信网络连接的方法.AccessChain 用于记录访问控制策略,本质上是一个访问控制的决策账本,参与到可信网络环境的计算节点以身份密钥(attestation identity key,简称 AIK)作为标识.计算节点的基本信息被写入 AccessChain,并设置加入网络的时间和有效期.AccessChain 为 PEP 提供决策支撑.LogChain 记录可信网络运行的日志数据,为审计和追溯提供证据,主要是利用了区块链防篡改的特性.DTTP 是用区块链技术构建的可信第三方,提供 3 种服务:证书服务、完整性验证和零知识证明.CertChain 的研究已经证明,基于区块链构建分布式的可信第三方是可行的、高效的、安全的.如何具体实现不作为本文研究重点.

- 层次

5 个层次分别是访问控制层、基础网络层、度量评估层、区块链引擎和验证审计层:访问控制层运行 AccessChain;基础网络层支持传统的网络连接通信技术,如 P2P、Gossip 协议、VPN 等机制;度量评估层进行平台的度量认证,形成计算节点是否可以加入可信网络的决策;区块链引擎和其他部件交互,提供区块链服务;验证审计层由 LogChain 和 DTTP 组成,为可信网络提供验证和审计的支撑.

- 接口

B-TNC 架构存在多个实体,与 TNC 架构相同,实体之间同样有通信和互操作的需求.但是由于引入了区块链系统,导致架构中存在虚拟的逻辑实体,并且接口更加复杂.对其中比较重要的接口进行定义,从底层到上层包括 IF-AR,IF-CS,IF-PEP,IF-BHSE 和 IF-BPEP.其中,IF-AR 是 ARQ 和 ARC 之间的接口,实现双方的信息传输;IF-CS 维护 B-TNCC 和 B-TNCS 之间的通信,主要支持可信网络节点加入时的网络数据传输;IF-PEP 是 PEP 之间的根据访问控制策略形成的稳定的安全信道;IF-BHSE 是各个实体调用区块链系统的接口;IF-BPEP 是 PEP 获取区块链中存储的策略的接口.但是具体协议实现不作为本文研究重点.

2.4 抽象描述

给出 B-TNC 中各部件的定义,未定义的部分沿用第 2.3 节的描述.

定义 1. $P_i=\{P_{i\_AIK},P_{i\_Nonce},P_{i\_Others}\}$,参与节点 i 的身份证据集合,其核心是 P_{i_AIK},是用户的身份密钥,在可信系统中用于标识用户的身份;P_{i_Nonce} 是随机数,用于对抗重放攻击.对身份合法性的可信验证就是对 P_i 的验证.

定义 2. $S_i=\{S_{i\_1},S_{i\_2},S_{i\_3},\ldots,S_{i\_n}\}$,参与节点 i 的完整性证据集合,其中,n 为计算平台组件的数目.计算平台的

组件主要包括信任根、BIOS、内核、操作系统和应用程序.

定义 3. $T=\{T_1,T_2,T_3,\ldots,T_n\}$,可信网络中计算节点的集合,$n$ 为可信网络中计算节点的数目.外部节点集合定义为 $C=\{C_1,C_2,C_3,\ldots,C_n\}$.定义计算节点的决策集合 $D_m=\{D_{1\_m},D_{2\_m},D_{3\_m},\ldots,D_{n\_m}\}$,表示 T 中各节点对节点 C_m 的证明结果,1 代表可信,0 代表不可信.

定义 4. *AccessChain*:$(AC_1\rightarrow AC_2\rightarrow\ldots\rightarrow AC_n\rightarrow\ldots)$.

定义 5. *LogChain*:$(LC_1\rightarrow LC_2\rightarrow\ldots\rightarrow LC_n\rightarrow\ldots)$.

给出 B-TNC 中各基本操作的定义:

定义 6. $F_{Measure}(C_m,P_m,S_m)$,完整性度量函数.计算平台 C_m 对自身的完整性进行度量,得到身份证据集合 P_m 和完整性证据集 S_m.

定义 7. *Verify_Identity*(T_k,P_m,*Id_Result*),身份合法性验证函数.计算节点 T_k 根据 P_m 对平台 T_m 进行身份合法性校验,得到证明结果 *Id_Result*.

定义 8. *Verify_Integrity*(T_k,S_m,D_{k_m}),完整性验证函数.计算节点 T_k 根据 S_m 对平台 T_m 进行完整性校验,得到证明结果 D_{k_m}.

定义 9. *Pick*(*T*,*LN*),每个阶段记账节点的共识算法,在集合 *T* 中选取领导节点 *LN*.

定义 10. *Decision*(*LN*,D_m,*Access*,*AC_newBlock*),全网决策函数.领导节点 *LN* 根据决策集合 D_m 产生最终决策 *Access*,其中,1 代表可以入网,0 代表不可入网.进而根据决策结果生成 AccessChain 的新区块 *AC_newBlock*.

定义 11. *Re_Blockchain*(*LN*,*Blockchain*,*T*,*new_Block*),区块链更新函数.领导节点 *LN* 将 *new_Block* 广播到可信网络中所有节点 *T*.需要说明的是,根据实际需要,*Blockchain* 有两种:AccessChain 和 LogChain.与之对应,*new_Block* 包括 *AC_newBlock* 和 LogChain 的新区块 *Log_newBlock*.

定义 12. *Refer_AC*(*AccessChain*,P_{i_AIK},*AC_Result*),查询拥有身份 P_{i_AIK} 的计算节点在 AccessChain 中是否合法,并得到查询结果 *AC_Result*.

定义 13. *Refer_Log*(*LogChain*,P_{i_AIK},*Log_Result*),查询拥有身份 P_{i_AIK} 的计算节点在 LogChain 中是否有记录,并得到查询结果 *Log_Result*.

定义 14. *Refer_DTTP*(*DTTP*,P_{i_AIK},*DTTP_Result*),查询拥有身份 P_{i_AIK} 的计算节点在 *DTTP* 中是否有记录,并得到查询结果 *DTTP_Result*.

定义 15. 通信功能相关定义如下:

- *Send*(*Message*,*P*,*Q*),将内容 *Message* 从 *P* 节点发送到 *Q* 节点;
- *Connect*(*P*,*Q*,*time_begin*,*time_end*),*P* 和 *Q* 两个节点建立正式通信,有效期从 *time_begin* 到 *time_end*;
- *Disconnect*(*P*,*Q*,*time*),*P* 和 *Q* 从时间 *time* 开始断开连接.

2.5 区块链结构

B-TNC 中的 3 个区块链系统代表了区块链技术在信息安全领域的 3 个重要的应用方向,即访问控制、数据保护和身份认证[38].本节描述 3 种区块链系统的基本结构,对区块链系统的功能进行梳理,重点是说明可行性.

- AccessChain

访问控制是用户权限管理的重要技术手段,能够允许合法用户访问资源,并且拒绝非法用户的越权访问.区块链和访问控制的结合主要采用两种技术路线:基于交易进行策略/权限管理、基于智能合约进行访问控制.在 B-TNC 的架构下,AccessChain 属于前者.基于交易进行策略/权限管理的访问控制系统主要有 Damiano 机制[39]、Zyskind 机制[40]、FairAccess 机制[41−43]和 Dorri[44,45].其中,Zyskind,FairAccess 和 Dorri 面向的是移动应用或物联网环境,和 B-TNC 的应用场景不符.AccessChain 的可行性源自于 Damiano 系统.Damiano 面向泛化的应用场景,探索了使用区块链创建、管理、执行访问控制策略的可行性,对基于属性的访问控制模型 ABAC 进行了扩展.AccessChain 的数据结构如图 5 所示,是一个通用的区块链数据结构.每一条记录就是一个节点的访问控制信息,其中包括节点信息(AIK,IP,MAC 等信息)、入网时间、有效期、随机数等.本文在第 3 节参考 Damiano 系统的设计方法,对 AccessChain 的运行流程进行描述.但是 Damiano 面向的是公有链,和 B-TNC 有一定的不同.

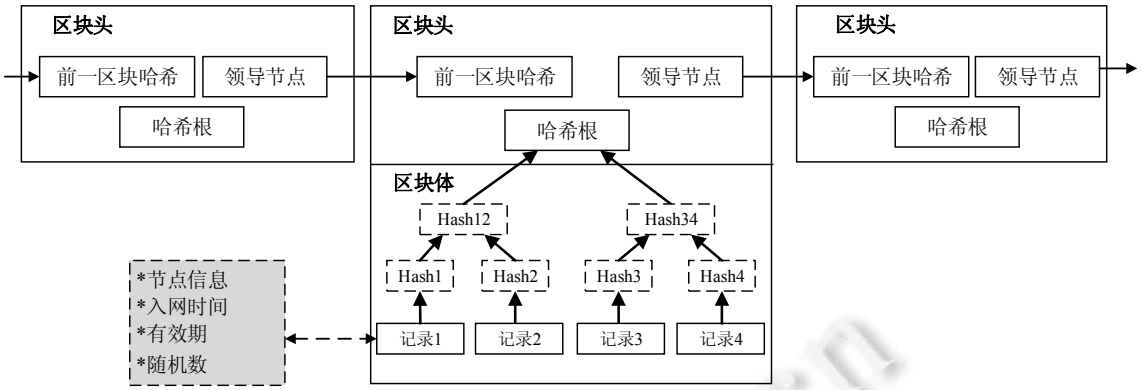

Fig.5 Data structure of AccessChain

图 5 AccessChain 的数据结构

- LogChain

区块链是一种分布式的共享数据总账,记录在区块链上的数据只可以增加,不可以篡改.这个特性可以用于实现信息系统全流程的监控,实现不可篡改的数据记录,适合于日志审计系统的构建,从数学原理上保证审计系统的安全性.Cucurull J 等人[46]使用区块链来实现不可篡改的安全审计日志,将区块链防篡改的特性与日志审计系统结合,实现了可信的日志审计系统,也为 LogChain 提供了理论和实践的支撑.在 B-TNC 架构中,可信网络中计算节点的日志信息由 LogChain 记录,网络运行中的重要行为都会被记录到链上.

在远程证明中,可信验证通常依托于可信第三方.但是在 B-TNC 中,LogChain 系统能够为可信验证的决策提供可靠的依据,增强可信系统的安全性.本文仅对 LogChain 基本功能进行梳理,不再展开设计工作.需要说明的是,与 AccessChain 相比,LogChain 对数据吞吐量的要求更高,记录的数据更多,但是对于共识时效性要求较低.

- DTTP

身份认证是可信第三方的一个重要功能,目前,相关研究者已经展开了基于区块链构建 PKI 的研究,为分布式可信第三方 DTTP 的创建奠定了基础.目前,PKI 系统在分布式环境下面临的最大的挑战是证书授权中心(certificate authority,简称 CA)不可信的问题.CA 不可信主要包括 3 种情况:1) CA 被黑客攻击,导致中间人攻击的问题;2) 用户无法验证 CA 签证的过程,导致证书不透明的问题;3) 中心化 CA 故障,导致所有证书不可用.为了解决上述问题,相关研究者展开了大量的研究.具有代表性的是麻省理工学者 Conner 提出的 Certcoin 系统和武汉大学学者 Chen 提出了 CertChain 系统.上述研究一方面证实了基于区块链构建 PKI 的可行性,另一方面证明了基于区块链构建 PKI 在安全方面的优势.

可信网络连接中涉及到 3 种可信第三方,除 PKI 系统外,还有 DAA 中零知识证明证据发布者以及基于属性的远程证明中可信验证者.零知识证明证据发布者可以依托 PKI 系统建立,在 TPM/TCM 身份注册或验证时生成证据,理论上不存在实现难度.但是分布式的可信验证者目前并没有可以参考的系统,本文提出了一种基于区块链的设计思路,具体描述见第 3.2 节.

2.6 安全假设

1. 敌手可以窃听、截获和篡改通信消息.
2. 底层密码算法是安全的,随机数和私钥均无法被分析攻破.
3. 可信网络在建立之初是可信的.
4. 网络中的节点在刚刚加入网络时可信.
5. 通信信道安全,可以通过加密保证.
6. 敌手无法控制 1/3 以上的节点,这个数字是由共识算法决定的.

3 B-TNC 运行流程

本节对 B-TNC 架构最重要的问题进行描述,包括 B-TNC 的基本流程、分布式可信验证者构建的方法和基于 DPoS 共识的远程证明机制.

3.1 基本流程

3.1.1 系统初始化

B-TNC 在运行之前需要进行基本的初始化操作,主要包括可信网络环境初始化、区块链系统初始化.

(1) $T=\{T_1,T_2,T_3,\ldots,T_n\}$.初始节点建立可信网络环境.

(2) AccessChain:($AC_1\rightarrow AC_2\rightarrow\ldots$).初始化 AccessChain,创建初始节点.

(3) LogChain:($LC_1\rightarrow LC_2\rightarrow\ldots$).初始化 LogChain,创建初始节点.

(4) 可信第三方 DTTP 开始提供可信第三方服务:证书服务、零知识证明和可信验证.

3.1.2 基本运行流程

假设 B-TNC 处于运行过程中,此时有外部计算节点 C_i 发起对可信网络 T 内部节点 T_j 网络申请,该过程的基本运行流程如图 6 所示.

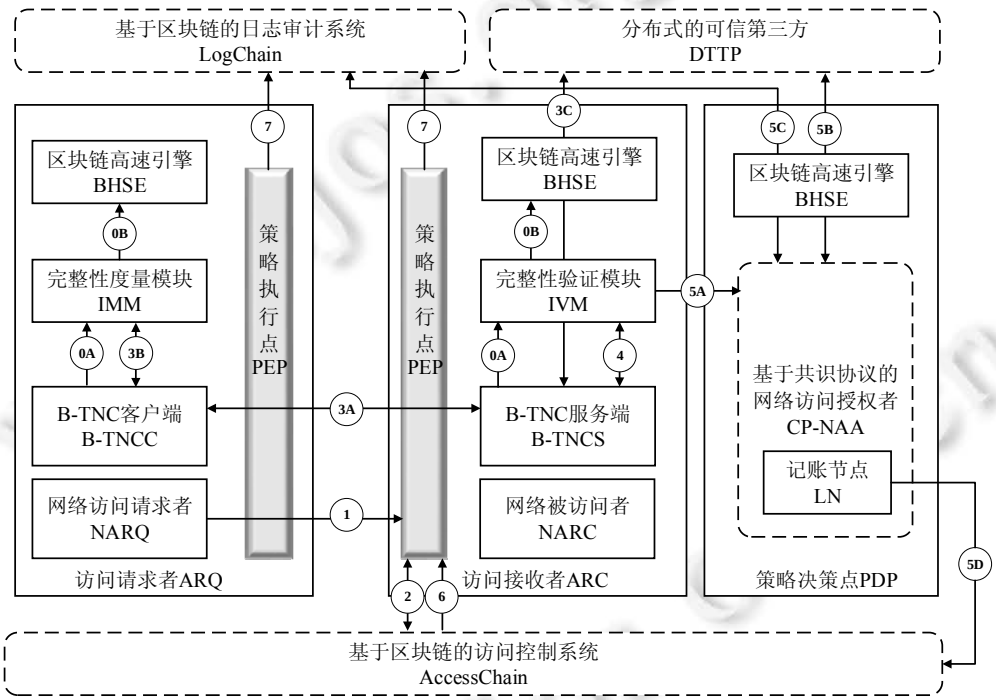

Fig.6 Work process of B-TNC

图 6 B-TNC 的工作流程

0a. 在进行网络连接和平台完整性验证之前,B-TNCC 需要对 IMM 进行初始化.同理,B-TNCS 要对 IVM 进行初始化.

0b. BHSE 对 AccessChain 和 LogChain 进行实时解析,在本地存储区块链数据库,实现高速查询.

1. $Send(P_{i\_AIK},NARQ,ARC.PEP)$.

当有连接请求发生时,NARQ 向 ARC 的 PEP 发送连接请求,其节点身份用 P_{i_AIK} 进行标识.

2. $ARC.PEP\rightarrow Refer\_AC(AccessChain,P_{i\_AIK},AC\_Result)$.

如果验证合法,*Connect*(*ARQ*,*ARC*,*time_begin*,*time_end*).

ARC 的 PEP 向 AccessChain 查询,判断 P_{i_AIK} 是否被认可,并得到结果 *AC_Result*.若验证合法,则 ARC 的 PEP 根据验证后的策略执行访问控制操作,建立通信连接;若验证不合法,则启动可信网络连接的身份验证和完整性状态验证.

3a. B-TNCC 和 B-TNCS 对平台身份的合法性发起验证.

3b. *ARQ.IMM*→$F_{Measure}$(C_i,P_i,S_i) then *Send*($P_i||S_i$,*B-TNCC*,*B-TNCS*).

ARQ 的 IMM 对平台进行度量,得到身份证据集合 P_i 和完整性证据集合 S_i,然后把证据集发送到 B-TNCS,等待验证.

3c. *Verify_Identify*(*ARC*,P_i,*Id_Result*).

ARC 对身份证据集合进行校验,得到身份合法性的验证结果.具体的过程是向使用可信第三方 DTTP 的证书服务或零知识证明服务,对 P_{i_AIK} 的合法性进行校验,以证明远端平台具备合法的 TPM/TCM.身份验证的实施比较灵活,对于隐私要求高的场景可以使用直接匿名证明 *DAA* 协议.若身份验证通过,则启动完整性验证过程.

4. B-TNCS 将完整性证据集发送到 ARC 的 IVM 进行处理,准备发起完整性证明.在这个过程中,若完整性信息不足,则要继续进行收集.

5a. *Send*($P_i||S_i$,*ARC.IVM*,*CP-NAA*).

ARC 的 IVM 将身份证据 P_{i_AIK} 和完整性证据 S_i 发送到 CP-NAA 请求决策.需要说明的是,CP-NAA 是由多个计算节点组成的,需要合作产生对证据验证结果.

5b. *Verify_Integrity*(*CP-NAA*,S_i,*D*).

CP-NAA 调用 DTTP 的可信验证服务,对完整性证据进行验证,得到验证结果的决策集合 *D*.可信验证服务的实现方法在第 3.3 节进一步阐述.

5c. *CP-NAA*→*Refer_Log*(*LogChain*,P_{i_AIK},*Log_Result*).

CP-NAA 向 LogChain 查询和 P_{i_AIK} 有关的审计日志,追溯该节点是否有恶意行为.

5d. *Decision*(*LN*,D_m,*Access*,*AC_newBlock*) **then** *Re_Blockchain*(*LN*,*AccessChain*,*T*,*AC_newBlock*).

领导节点根据 CP-NAA 得到的决策集合得出最终结论,并生成新的区块.进而将新区快广播到可信网络的所有节点,更新 AccessChain.领导节点的选取过程将在第 3.3 节详细描述.

6. *ARC.PEP* 此时可以在 AccessChain 中检测到可信证明的结果,执行访问控制策略.

7. *Re_Blockchain*(*PEP*,*LogChain*,*T*,*Log_newBlock*).

在可信网络运行过程中,PEP 会将执行访问控制决策的日志信息记录到 LogChain.计算节点在网络中的行为都会记录下来,并且是不可抵赖的.

3.2 分布式的可信验证者

可信验证方是基于属性远程证明的重要部分,在传统可信网络的体系中,实际扮演了可信第三方的角色.但是在 B-TNC 的架构中,如果仍旧采用中心化的验证方法,就会无法避免单点化和中心化的问题.本节提出一种建立分布式可信验证者的方法,假设用 5 台验证节点组成分布式的可信验证者.验证节点的数量可以根据实际需求灵活选择,本文仅以 5 为例.如图 7 所示.

5 个验证点组成一个私有链,具有强身份标识,无法被恶意节点伪装.验证者的主要任务是对平台可信报告进行分析和验证,其中包括完整性证据和平台属性证据.5 个节点共同维护一个区块链账本,存储验证策略和可信计算节点的完整性证据集合.在执行验证任务时,验证发起方会随机访问不同的验证节点,可以指定随机策略使每个验证节点被访问的频率大致相同.从分布式可信验证者建立到运行的过程描述如下.

1. Setup:完成可信验证方的初始化过程.

(1) 建立验证策略,将策略写入可信验证者的区块链系统.若策略变更,5 个节点运行共识协议共同更新.

(2) 从 CA 中心获取合法 TPM/TCM 注册时的完整性状态信息,写入可信验证者的区块链系统.

2. Verify:验证证据合法性的过程.以 T_m 请求验证 C_k 节点为例.

(1) T_m 随机选择一个验证点,与之建立通信.假设选择验证点 2.

(2) 验证点 2 发布智能合约,迅速共识到整个区块链系统.

(3) 假设这一阶段的记账节点是验证点 3.

(4) 验证点 3 访问区块链上的验证策略和 C_k 节点的完整性信息:若区块链上没有 C_k 节点的信息,则执行第(5)步;若有,则执行第(6)步.

(5) 验证点向 CA 中心请求更新数据,查询是否具有 C_k 节点的相关信息:若仍旧没有,则返回 C_k 节点非法;若有,则更新区块链,然后执行第(6)步.

(6) 验证节点将收到的完整性证据与区块链上的完整性进行比对,判断是否被修改:若没有被修改,执行第(7)步;若被修改,则返回完整性证据验证不通过.

(7) 根据验证策略对安全属性信息进行决策,判断待入网的节点安全配置是否符合要求,得出结论,并写入区块链系统.

(8) 验证点 3 在得出结论之后执行两个操作:一是将验证结论发送回验证请求点;二是将验证操作和结论写入到验证者的区块链系统,供其他验证者进行审计.

这种设计方法避免了可信证据只由单一的决策者的判断,从概率学的角度提高了整个验证判断过程的安全性.CP-NAA 是由多个节点构成的,在进行完整性验证的时候,这些节点会随机选择不同的验证点去进行验证.若某一个验证点被攻击,得出错误的结论,也无法对整体验证结论形成影响.并且验证结果在验证点之间是可查可审可追溯的,恶意的验证点能够迅速被发现清理.

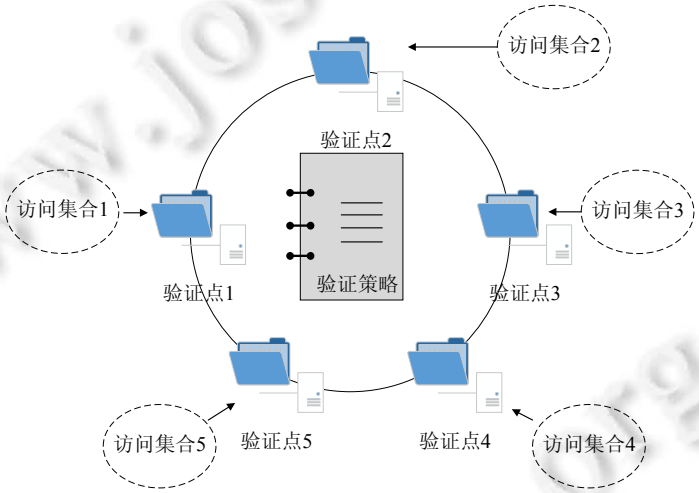

Fig.7 Distributed trusted verifier

图 7 分布式的可信验证者

3.3 基于DPoS共识的远程证明

3.3.1 DPoS基本原理

股份授权证明 DPoS 是 EOS 项目最早发布的共识机制,旨在消除比特币公式算法 PoW 资源消耗过大、算力过于集中的问题.DPoS 的基本思想是:选举出一定数量的节点,由这些节点作为代表协作轮流记账.这个思路类似于政治活动中的议会制度,选举出合适的代表,代替更多的节点行使权利.

以 EOS 的 DPoS 的部署为例,所有 EOS 的持有者根据持有的数量按照 1:1 获得选票,选出 21 个区块产生者,也叫做见证人.由这 21 个见证人相互协作,按照一定的顺序轮流记账,以 3s 为间隔产生区块.DPoS 有不可逆原则,一旦某个区块后面跟随了超过 2/3 见证人数量的区块,区块就进入了不可逆状态,也就是常说的该区块被确认了.在 21 区块产生节点的模型中,15 个区块(15/21>2/3)进入不可逆状态的时间(即交易 100%安全)为 45s.在

EOS 最新的版本中,引入了拜占庭容错机制,实现了秒级的确认性能.总之,EOS 的实践证明了 DPoS 的优势:解决了能耗的问题;共识节点少,共识效率高;不会产生硬分叉;安全性更强,只有控制超过 2/3 数量的节点才能够改变区块链;确认速度快.

从原理上分析,DPoS 本质上是存在中心的,如果见证人节点存在恶意行为,或者未能履行职责,就会在下一个投票阶段被淘汰.本文借鉴了 DPoS 的基本思想设计远程证明协议,描述了证明协议的基本过程.由于 DPoS 本身算法比较成熟,具体实现方法也不是本文重点,所以不对算法细节进行展开.需要说明的是,B-TNC 并不要求一定采用 DPoS 的共识机制实现 CP-NAA,能够实现多个计算节点共识产生共同决策的共识算法都是可以的.

3.3.2 远程证明过程

远程证明是 B-TNC 区别于传统可信网络连接最核心的部分,能够以集体决策的方式产生访问控制策略.在 EOS 中,DPoS 是根据掌握数字货币的数量来分配选票的,货币是利益所在.但是 B-TNC 中计算节点的利益在于能否被可信网络环境认可,并没有掌握数字货币.为了减少对 DPoS 算法的修改,本文提出可以选用节点在可信网络中的活跃时间代替数字货币.比如某计算节点在可信网络中的活跃时间为 T_{sum},单位时间为 T,那么拥有选票的数目 $Ticket=T_{sum}/T$.T 的选择要根据实际网络运行状况确定.假设 B-TNC 的见证者同样设置为 21 个,这些节点共同组成了图 4 中的网络授权者 CP-NAA.基于 DPoS 的远程证明过程核心是两个部分:(1) 基于 DPoS 选取验证节点,组成 CP-NAA;(2) 基于多方决策的平台可信证明.证明过程如图 8 所示.为了便于描述,将图中的节点数目进行了缩减.

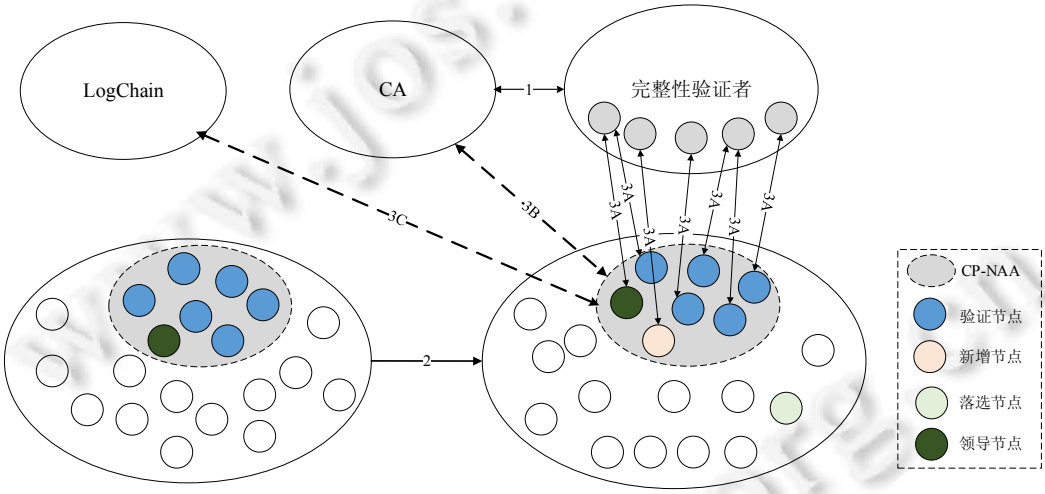

Fig.8 Remote attestation based on DPoS

图 8 基于 DPoS 的远程证明

1. Initialize:完成第 3.2 节中分布式可信验证者的初始化过程.

2. Select:选举产生 21 个 DPoS 见证人.若网络中节点不足 21 个,则网络中节点都作为见证人.

(1) 可信网络中的每一个计算节点 $Ticket=T_{sum}/T$,确定自己掌握的选票的数目.

(2) 假设以 2 小时为时间间隔,运行投票算法,选出 21 个超级节点作为见证人.在这个过程中,有可能存在节点落选、新节点补增的情况.

(3) $Pick(T,LN)$.超级节点之间共识产生一个随机数,用于对节点进行编号.然后按照编号的顺序,轮流担任领导节点 LN.可以按照 3 分钟的时间间隔轮换,但具体间隔需要结合实际网络规模进行分析.

3. Verify:对身份和完整性证据进行验证.

(1) 21 个见证人随机选择完整性验证节点,并将完整性信息和属性信息发送到相应的节点进行验证.验证过程参照第 3.2 节.

(2) 见证人根据自己的判断策略,灵活选择是否查询 LogChain,追溯待验证节点是否曾经存在恶意行为.

(3) 见证人根据自己的判断策略,灵活选择是否对待验证节点的身份进行进一步核验.

(4) 21 个见证人将自己得出的判断结论和判断依据广播给其他节点.需要说明的是,由于每个计算节点的判断策略由自己掌握,如果结论的得出既包含了完整性验证,也包含了恶意行为追溯和身份核验,那么这个结论显然是更加有说服力的.所以将判断依据一起广播出去,领导节点能够对最终结论进行综合考量.

(5) 领导节点对其他见证人的判断进行综合,若超过 2/3 见证人认为待验节点是可信的,那么就得出最终的结论,允许待验节点加入可信网络.并将结论写入到 AccessChain.

可信远程证明的方法模型有多种,但是其基本流程是相似的,即“连接申请、证据提交、可信判决、决策执行”.本文的远程证明和 TNC 架构相比,最本质的区别在于:对中心化的可信判决和决策执行进行了分布式的改造,能够提高分布式网络系统抵抗安全威胁的能力,增强系统容错性.其核心优势在于两个方面:1) 将判决点分散,能够有效抵抗单点故障或者中心被攻破的问题;2) 所有的决策产生过程在链上记录,可信可查可追溯,让恶意的判决点无所遁形.

3.4 激励机制

激励机制是区块链技术领域的重要研究方向,合理的激励机制能够保证更多的节点参与到区块链系统中,从而增强区块链系统的安全性.区块链分为公有链、私有链和联盟链.公有链一般是通过发行代币来解决激励问题.一个节点在区块链系统中越活跃,做出的贡献越多,就能获取更多的代币,如以太币、比特币.代币能够在链下换取更多的经济权益.而对于私有链或者联盟链系统,一般不会设计代币机制.在无代币区块链系统中,比如政府的各个部门、银行的各个机构,参与共识的节点本身通常是有利益协作的,所有合法节点都希望系统安全可靠高效运行,愿意参与到区块链系统中.所以,私有链或联盟链不需要链上经济的激励,但可以采取链上权益、数据权益等激励.

判断区块链系统类型的重要依据是,节点能否自由加入区块链系统.B-TNC 架构引入了 3 个区块链系统:访问控制系统、日志审计系统和分布式的可信第三方,均属于带准入控制的区块链系统,节点无法随意加入.和传统的可信网络连接单点化的架构相比,3 种区块链的引入上会增加系统构建的成本,带来更多的计算和存储开销.为了保证系统的良好运行,必须建立合适的激励机制.然而激励机制通常和具体的业务应用场景紧密相关,设计通用的激励机制是困难的.本文以一个具体的应用场景为例,提出激励机制的设计思路.

- 场景假设

应用场景:某大型科研系统,共有 5 个研究所,研究所下属总计 50 个研究室,总共包含 2 000 个科研人员.每一个研究所和研究室都有不同规模的数据中心,每一个科研人员拥有多个计算机终端.数据中心和计算终端之间互联互通.

- 激励措施

(1) 基于业务需求驱动,研究所和研究室必须按照网络配置要求提供相关设备,组成各功能区块链系统.可作为业务考核的标准.

(2) 根据参加区块链业务的活跃程度,计算季度或年度的贡献值,对贡献大的单位进行表彰或奖励.

(3) 对于所有可信节点,网络是否安全可信是他们的共同利益.在更加相信自己的基础之上,他们愿意贡献一部分计算和存储能力.

(4) 恶意节点在网络中的行为是完全可查可追溯的.恶意行为会降低其他节点对他的信任,很难被选为超级节点.

4 架构分析

4.1 安全性

在 Dolev-Yao 威胁模型下进行安全分析,攻击者可以窃听、获取和篡改协议消息,能够伪装成一个合法的主

体参与协议的运行.底层密码算法是安全的,随机数和私钥无法被攻破,这一点可以由信任根保证,但是系统对信任根仍旧保持一定的怀疑态度.假设2/3以上的计算节点是诚实可信的,攻击者无法控制1/3以上的节点.诚实可信一方面是节点行为可信,另一方面是节点的信任根可信.B-TNC继承了可信计算和区块链的安全特性,具有去中心化、可追溯、不可伪造、不可篡改并具备良好的匿名性.本文重点分析去中心化后最突出的安全特点.

1) 去中心化

B-TNC架构的去中心化体现在4个方面.

(1) 访问控制去中心.AccessChain将访问控制列表用区块链数据库的方式维护在每一个网络参与者,将访问控制决策执行权限分散,能够降低整个网络由于网关被攻破而崩溃的风险.

(2) 策略决策去中心.本文提出在DPoS共识下,超级节点组成共同的网络访问授权者,进而对节点的入网请求共同决策.少量非法节点即便参与到了决策中,也无法对最终结果产生实质的影响.

(3) 审计追溯去中心.基于区块链技术构建计算机日志审计系统是可行的,这一点毋庸置疑.安全可信防篡改的日志系统是安全审计的基础,大量的安全服务都是基于行为日志展开.基于区块链的日志审计系统不仅能够提供更强的防篡改特性,更能够提供一个全网视角下的日志审计视图,以便于联合审计挖掘.

(4) 可信第三方去中心.相关研究已证明,基于区块链技术构建分布式的PKI系统是具有可行性的.和集中式相比,分布式架构的PKI能够更加有效得解决单点信任中心存在的固有问题.本文也提出了分布式可信验证者的设计思路,能够提供更加安全的第三方验证服务.

总之,B-TNC架构从多个角度实现了去中心化的特性,解决了中心化网络判决模型的固有问题.

威胁场景假设:假设恶意节点*MN*试图成为领导节点,将非法的访问控制规则写入AccessChain.共识机制是可信的,领导节点的选取具有随机性,并且大概率属于可信节点.*MN*必须能够控制大多数节点,才能实现对访问控制规则的任意修改,但这显然是困难的.考虑3种攻击场景.

- 场景1:*MN*不属于可信网络.此时,*MN*首先要完成可信验证的整个流程,骗取可信网络承认自己的身份,将自己的信息写入AccessChain.若*MN*不具备合法的TPM/TCM,或者没有运行在可信状态,此时*MN*加入网络必然是失败的;若*MN*本身具备合法的TPM/TCM,并且也处于安全的运行状态,*MN*可以加入网络.但此时只是一个普通的节点,距离成为领导节点还有很大距离.
- 场景2:*MN*属于可信网络.在区块链系统中,*MN*是否可以成为可信节点仍然是小概率事件.首先要经过投票机制被选举为见证人之一,并且要在特定时间段才具有记账权限.在基于权益的共识协议中,运行在可信网络中的时间越长,当选为见证人的可能性越大.因为审计机制的存在,所有节点的行为都被记录在区块链日志系统中,只有可信节点才有可能长期运行在可信网络中.如果*MN*被选举为见证人,并且成为某一时间段的领导节点,那么就会在第3.1.2节的5D步骤中,写入与事实相悖的结论.这就会导致其他节点对*MN*的失信,使其下一阶段难以当选见证人.
- 场景3:*MN*对可信第三方展开攻击,试图成为可信第三方服务节点.可信第三方本身的安全防护强度高,攻克难度大.若*MN*发起对CA的攻击,并且成功,根据CertChain的安全证明,攻击能够快速被检测修复.并且身份验证过程会随机选择CA节点,不一定会访问到被攻击的节点.若*MN*发起对可信验证者的攻击,成功控制一个验证节点,那么这对于最终验证结论同样不会产生较大的影响:一方面,节点访问验证点具有随机性,单个验证节点的结论在最终结论中只占有1/5;另一方面,验证节点之间能够根据异常判定结果及时发现被攻击的节点.

2) 可追溯

传统可信网络连接针对安全接入后的防护能力不足,此时,基于区块链的分布式信任关系模型就能够对此进行很好的补充.恶意节点往往伴随恶意行为,可信的审计能够暴露恶意行为,进而发现恶意节点.区块链是一种以哈希为标志的链式存储结构,数据一但写入区块链,就能够沿着区块链追溯到历史记录.可追溯具有两个层面的含义:写入区块链的证据最终能够被检索到、检索到的数据是可信的并且不可抵赖的.

本文认为,信任根作为安全部件,在实际的设计与生产过程中,客观上是有可能存在安全隐患的.所以在安全假设中,本文假设安全的信任根是完全可信的,但在实际网络环境中,对信任根仍旧保持一定怀疑态度.区块链可追溯的特性就是很好的补充.

威胁场景假设,考虑 3 种共计场景.

- 场景 1:可信网络 T 中的可信节点 T_m 受到网络攻击,变成恶意节点.如果恶意节点在网络接入的有效期内没有恶意行为,那么对网络的危害较小.有效期过了以后,需要重新运行可信连接的过程,对该节点的安全性进行分析.此时,如果恶意节点的关键数据被修改,或安全配置不足,就无法通过可信验证,被踢出可信网络.如果恶意节点在网络接入的有效期内有恶意行为,那么网络访问的日志信息会被写入 LogChain,其他节点能够通过对日志的审计及时发现异常行为.这就通过节点行为可追溯保证了网络的整体安全性.
- 场景 2:可信网络 T 中的 T_a 和 T_b 进行安全通信,协同完成某项计算任务.受到利益驱动,T_a 存在恶意行为,并试图删除网络日志文件,否认网络交互行为.但是由于日志审计系统是分布式的,LogChain 能够被存储于所有节点,所有的日志文件都是可以被你追溯的.单节点的日志删除最终是无效的,T_a 无法抵赖自己的行为.
- 场景 3:可信芯片存在底层的高危漏洞,攻击者能够伪造了一个合法的 TPM/TCM 参与到网络中.需要说明的是,此类攻击虽然客观存在,但是发生的可能性低,攻击难度很大.由于恶意节点的所有行为都是被记录在区块链系统中的,一旦有恶意行为,就会被迅速检测到.去中心化部分已经说明了单个节点的行为难以对整个系统安全产生决定性的影响.所以,在 2/3 节点可信的安全假设之下,即便信任根也存在安全隐患,网络整体的可信同样是可以保证的.

3) 不可篡改

不可篡改是区块链能够用于构建分布式信任根的重要安全特性.攻击者如果想对区块链数据库进行篡改,就必须控制网络中的大多数节点,而这与本文的安全假设不符.假设敌手试图对 B-TNC 中涉及到的区块链系统中的某一个区块进行修改,那么区块的哈希值就会发生改变,就必须对该区块后面的所有区块均进行改变.而区块链是分布式的数据库系统,只有在大多数节点上都进行相应的修改,攻击才能生效.因此,B-TNC 具有不可篡改的安全特性.

4) 抗合谋攻击

合谋攻击[47]指的是 2 个或 2 个以上的恶意节点相互串联,以破坏正常网络行为的攻击.合谋攻击有几个典型的特征:(1) 互相担保,协助攻击节点看似合法的节点;(2) 互相伪造,能够建立一个非法的通信链路;(3) 做伪证陷害合法节点.B-TNC 的远程证明和访问控制具有去中心化的特性,这将导致少量恶意节点的合谋难以对全局的安全决策产生决定性的影响,合谋攻击难以展开.

女巫攻击(sybil attack,简称 SA)指的是在对等网络中,单一节点具有多个身份标识,通过控制系统的大部分节点来削弱冗余备份的作用,女巫攻击是一种特殊的合谋攻击.而在 B-TNC 中,节点身份分布式的可信第三方授权,节点身份密钥由信任根保护,伪造大量身份本身具有难度.而控制多数节点在区块链的安全假设下是困难的,女巫攻击难以展开.

4.2 效率分析

区块链系统的引入会增加系统开销、增加网络系统的运行成本.但是为了获取更大的安全收益,一定开销是必然的,也是值得的.本节对系统运行成本和效率进行分析.为了更加直观,本节采用第 3.4 节的场景假设,在一个实际的应用场景中进行分析.

- 应用场景

某大型科研系统,共有 5 个研究所,研究所下属总计 50 个研究室,总共包含 2 000 个科研人员.每一个研究所和研究室都有不同规模的数据中心,每一个科研人员拥有多个计算机终端,假设一共 6 000 台计算终端.数据中心和计算终端之间互联互通.

- 网络配置

(1) 5 个研究所各贡献 1 台服务器,组成分布式的 CA 系统.

(2) 5 个研究所各贡献 1 台服务器,组成分布式的可信验证者.

(3) 5 研究所和 50 个研究室各贡献 1 台计算终端,用于组成分布式的日志审计系统.科研人员也可根据实际需求,选择是否加入日志系统.

(4) 5 研究所和 50 个研究室各贡献 1 台计算终端,用于组成访问控制系统.科研人员也可选择加入.

(5) 所有接入网络的计算终端安装区块链客户端软件.

- 数据存储

(1) 由研究所和研究室维护的服务器和终端,都要保存完整的区块链数据.

(2) 研究人员的计算终端可以选择保存完整数据,也可以选择性保存部分数据,如区块链的哈希根.

(3) 假设区块大小为 1MB.

- 运行频率

(1) 假设入网的有效期为 4 天,超过 4 上天就要进行可信证明,重新入网.

(2) 平均每 1 分钟有 1 台终端需要进行可信证明:6000÷(4 天×24 小时×60 分)≈1.

4.2.1 运行成本

区块链系统的运行成本通常包括 3 个部分:算力开销、网络开销和存储开销.

- 算力开销

区块链起源于比特币系统,其共识机制采用的是工作量证明 PoW,需要进行大量的哈希运算,寻找满足要求的随机数,俗称挖矿.为了解决这一问题,基于权益证明机制 PoS 被提出,从此规避了计算资源的浪费.而 DPoS 是在这基础上的升级,通过选举合适的代表,组成共识机构,实现高速的共识协议.

因此,在 B-TNC 并不会消耗过多的计算能力,仅需要通用的计算平台即可完成目标.每个研究所数据中心贡献 2 个服务器、2 个计算终端、每个研究室贡献 2 个计算终端,就能够实现.DPoS 协议是可扩展的,增加计算平台就能够实现网络的扩容.

- 网络开销

区块链系统的网络开销主要取决于两个方面:一是区块数据的大小,二是交易规模和频率.金融行业追求大吞吐量,要求每秒的交易能够达到 1 000TPS,甚至 10 000TPS 以上.在区块大小相对固定的情况下,网络性能主要受到交易规模和频率的制约.

但是 B-TNC 中,大规模的共识和通信主要在研究所和研究室之间.其中,CA 系统、分布式的可信验证者分别由 5 台服务器组成,访问控制由 21 个超级节点组成.根据运行频率的假设,每分钟进行 1 个终端的可信验证,区块大小 1MB.每分钟的网络开销为:1MB×21×1=21MB/min=0.35MB/s.公式的含义是:区块产生方把新区快传播给所有的超级节点.科研内网的网络带宽通常比较大,网络开销是可以容忍.

- 存储开销

根据网络开销部分的分析,访问控制链每分钟增加 1MB,一年增加约 513GB.存储量是比较大的.但是对于一个研究所或者研究室的数据中心,每年扩容一个约 5 000GB 的硬盘用于存储区块链数据,这本身的难度并不大.再加上日志审计系统,以及分布式的可信第三方,数据量约为 2TB.

4.2.2 效率分析

1) 共识机制

共识机制本身和应用场景的关联性很大,需要根据共识节点数目、链上数据量等要素来决定.

本文针对 AccessChain 和 CP-NAA 提出了基于 DPoS 的共识方法.在 EOS 项目实践中,DPoS 能够在公链上实现 3s 出块、45s 确认的性能.如果部署在 B-TNC 这种私有链架构中,必将带来更大的性能提升.这完全满足访问控制链中,1 分钟进行一次可信证明的要求.综合考虑,DPoS 共识用于远程证明是能够满足效率要求的.需要说明的是,提升区块链共识性能是一个重要的研究方向,相关研究者已经做出了大量的工作.B-TNC 并不要求具

体的共识机制,能够满足效率和安全性要求的共识机制都是可以的.对于可信第三方,以 CertChian 为例的 PKI 系统使用的是基于 PoS 的共识[48],并且其研究者已经证明了用区块链构建 CA 系统效率是足够的,能够提供毫米级的证书验证服务.本文提出的分布式可信验证者在设计中只需要 5 个节点,常见的 PBFT 等共识协议在目前已经主流的区块链基础平台上都能够实现每秒 1 000 笔级别的共识效率,完全可以适用.对于 LogChain,日志更加追求的是不可篡改的特性,对于共识效率的要求相对较低.但是日志本身的数据量大,数据产生的参与方多,可以考虑基于有向无环图 DAG 的共识协议构建大规模分布式网络的日志系统.但共识机制的选取和实际应用场景密切相关.

2) 远程证明

B-TNC 中的远程证明过程比传统的可信网络连接远程证明的过程更加复杂.远程证明的性能损失来自于两个方面:一是共识协议本身的运行速度,二是 DPoS 中的 21 个见证者分别运行可信验证的过程.上一节已经说明了共识机制本身的性能是足够的,能够在秒级完成验证确认.验证过程的性能开销主要来自于可信验证者对完整性证据的确认以及 CA 对于身份的确认.21 个见证者可以执行并行化的认证,时间开销并不是一个 21 倍的关系.并且领导节点只要收到 2/3 节点的通过验证的消息就能够认定验证通过,不需要等待所有节点结束.所以,即使有恶意节点故意拖延验证时间,也无法同时控制 2/3 的节点同时撒谎.所以和传统可信网络连接架构相比,基于区块链的远程证明带来的效率损耗不大,主要取决于对于证据的验证过程,这和 TNC 架构是相同的.假设完成证据验证的时间是 10s,那么远程证明过程的效率约为 3s+10s=13s.由于共识效率是高于网络通信频率的,所以不会产生交易堆积的情况,只要有证明需要,就可以立即运行证明过程.

3) 访问控制

区块链作为分布式数据存储,其数据量本身很大,可以达到 TB 级.但是在数据查询的时候,并不是直接面对整个数据.区块链数据库的增长速度约为 1MB/s,在 B-TNC 中的每一个节点都维护一个区块链高速引擎,能够实时解析区块链数据库,以结构化的方式存储在本地.区块链数据更新后,系统会根据新区块的内容及时更新本地的访问控制列表,以实现快速的数据查询.在本文的设计中,一个平台的最新状态总会被保存在后面的区块中,并且区块是经常更新的,那么这一过程在最新的一部分区块中就能较快地完成.对于普通的计算终端,并不需要维护全部的区块链数据,只需要去超级节点申请数据更新访问控制列表即可.所以当计算节点之间进行网络通信时,能够在秒级的时间开销内完成访问控制决策过程.

5 结束语

本文在对安全实际信任问题的分析基础之上,提出了基于区块链构建分布式信任根的思想,进而提出了基于区块链的分布式可信网络连接架构.其核心思想是:用区块链对可信网络中的中心化认证部件进行分布式改造,主要包括可信第三方、访问控制和日志审计.分析表明,B-TNC 能够有效解决传统架构下面临的访问控制单点化、策略决策中心化的问题.基于区块链的结构能够将二值化的信任模型扩展为网状的整体信任模型,更加符合实际的网络运行环境.本文在提出总体架构设计、抽象描述和运行流程的基础之上,对核心问题展开描述.最后进行了正确性,安全性和效率分析.

下一步工作将从两个方面展开:一是研究更加适合分布式环境下的可信验证模型,进一步弱化二值化信任判断模型的约束;二是原型系统的设计与实现,由于工作量较大,需要展开更广泛的合作.

References:

[1] Shen CX, Chen XS. Construction of the information security infrastructure based on trusted computing. Journal of Sichuan University, 2014,46(1):1−7 (in Chinese with English abstract).

[2] Feng DG, Qin Y, Wang D, Chu XB. Research on trusted computing technology. Journal of Computer Research & Development, 2011,48(8):1332−1349 (in Chinese with English abstract).

[3] Tan L, Xu ZW. Development of the transitive trusted chain based on TPM. Computer Science, 2008,35(10):15−18 (in Chinese with English abstract).

[4] Chen L, Li J. Flexible and scalable digital signatures in TPM 2.0. In: Proc. of the ACM Conf. on Computer and Communications Security. 2013. 37−48. [doi: 10.1145/2508859.2516729]

[5] Zhao S, Xi L, Zhang QY, *et al*. Security analysis of SM2 key exchange protocol in TPM2.0. Security & Communication Networks, 2015,8(3):383−395. [doi: 10.1002/sec.987]

[6] Winter J. Trusted computing building blocks for embedded linux-based ARM trustzone platforms. In: Proc. of the ACM Workshop on Scalable Trusted Computing. DBLP, 2008. 21−30. [doi: 10.1145/1456455.1456460.]

[7] Santos N, Raj H, Saroiu S, Wolman A. Using ARM trustzone to build a trusted language runtime for mobile applications. In: Proc. of the Int'l Conf. on Architectural Support for Programming Languages and Operating Systems. 2016. 67−80. [doi: 10.1145/2541940.2541949]

[8] Jain P, Desai S, Kim S, Shij MW, Lee J, Choi C, Shin Y, Kim TS, Kang BB, Han D. OpenSGX: An open platform for SGX research. In: Proc. of the NDSS. 2016. [doi: 10.14722/ndss.2016.23011]

[9] Schwarz M, Weiser S, Gruss D, Maurice C, Mangard S. Malware guard extension: Using SGX to conceal cache attacks. In: Polychronakis MZ, ed. Proc. of the Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 2017). New York: Springer-Verlag, 2017. 3−24. [doi: 10.1007/978-3-319-60876-1_1]

[10] Moghimi A, Irazoqui G, Eisenbarth T. CacheZoom: How SGX amplifies the power of cache attacks. In: Proc. of the Int'l Conf. on Cryptographic Hardware and Embedded Systems; Fischer W, ed. Proc. of the Cryptographic Hardware and Embedded Systems (CHES 2017). New York: Springer-Verlag, 2017. 69−90. [doi: 10.1007/978-3-319-66787-4_4]

[11] Shen CX, Zhang DW, Liu JQ, Ye H, Qiu S. The strategy of TC 3.0: A revolutionary evolution in trusted computing. Engineering Sciences, 2016,18(6):53−57 (in Chinese with English abstract). [doi: 10.15302/J-SSCAE-2016.06.011]

[12] Zhang HG, Chen L, Zhang LQ. Research on trusted network connection. Chinese Journal of Computers, 2010,33(4):706−717 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2009.00706]

[13] Luo AA, Lin C, Wang YZ, Deng FC, Chen Z. Security quantifying method and enhanced mechanisms of TNC. Chinese Journal of Computers, 2009,32(5):887−898 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2009.00887]

[14] Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 2009,25(6):599−616. [doi: 10.1016/j.future.2008.12.001]

[15] Chen M, Mao S, Liu Y. Big data: A survey. Mobile Networks and Applications, 2014,19(2):171−209. [doi: 10.1007/s11036-013-0489-0]

[16] Lazer D, Kennedy R, King G, *et al*. The parable of Google Flu: Traps in big data analysis. Science, 2014, 343(6176):1203. [doi: 10.1126/science.1248506]

[17] Zhou MT, Tan L. Progress in trusted computing. Journal of University of Electronic Science & Technology of China, 2006,35(4):116−127 (in Chinese with English abstract).

[18] Li M, Li Q, Zhang GQ, Yan X. The implementation and application of trusted connect architecture. Journal of Information Security Research, 2017,3(4):332−338 (in Chinese with English abstract). [doi: 10.3969/j.issn.2096-1057.2017.04.007]

[19] Yuan Y, Ni XC, Zeng S, Wang FY. Blockchain consensus algorithms: The state of the art and future trends. Acta Automatica Sinica, 2018,44(11):2011−2022 (in Chinese with English abstract). [doi: 10.16383/j.aas.2018.c180268]

[20] Berger S, Caceres R, Goldman KA, Perez R, Sailer R, Doorn LV. vTPM: Virtualizing the trusted platform module. In: Proc. of the Conf. on Usenix Security Symp. USENIX Association, 2006. 305−320.

[21] Danev B, Masti RJ, Karame GO, Capkun S. Enabling secure VM-vTPM migration in private clouds. In: Proc. of the 27th Computer Security Applications Conf. DBLP, 2011. 187−196. [doi: 10.1145/2076732.2076759]

[22] Jin X, Chen XS. Rapid restoration of migrated trusted chain between physical machines. Journal of Wuhan University, 2016,62(2):103−109 (in Chinese with English abstract). [doi: 10.14188/j.1671-8836.2016.02.001]

[23] Liu MD, Cao HY, Shi YJ, Ma LY. Building trusted virtual environment by TCM hardware virtualization based on SR-IOV. Journal of Wuhan University, 2017,63(2):117−124 (in Chinese with English abstract). [doi: 10.14188/j.1671-8836.2017.02.004]

[24] Eyal I, Gencer AE, Sirer EG, Renesse RV. Bitcoin-NG: A scalable blockchain protocol. In: Proc. of the 13th Usenix Conf. on Networked Systems Design and Implementation. USENIX Association Berkeley, 2015. 45−59.

[25] Vukolić M. the quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In: Camenisch J, ed. Proc. of the Int'l Workshop on Open Problems in Network Security. New York: Springer-Verlag, 2015. 112−125. [doi: 10.1007/978-3-319-39028-4_9]

[26] Castro M, Liskov B. Practical Byzantine fault tolerance. In: Proc. of the 3rd Symp. on Operating Systems Design and Implementation. ACM Press, 1999. 173−186. [doi: 10.1145/571637.571640]

[27] Douceur JR. The sybil attack. In: Druschel P, ed. Proc. of the Int'l Workshop on Peer-to-Peer Systems. Springer, Berlin, Heidelberg, 2002. 251−260. [doi: 10.1007/3-540-45748-8_24]

[28] Barak B, Canetti R, Lindell Y, Pass R, Rabin T. Secure computation without authentication. Journal of Cryptology, 2011,24(4): 720−760. [doi: 10.1007/s00145-010-9075-9]

[29] Yoshida M, Obana S. On the (in)efficiency of non-interactive secure multiparty computation. In: Proc. of the Designs Codes & Cryptography. 2018. 1−13. [doi: 10.1007/s10623-017-0424-7]

[30] Blockchain. https://en.wikipedia.org/wiki/Blockchain

[31] Messerges TS, Dabbish EA, Sloan RH. Examining smart-card security under the threat of power analysis attacks. IEEE Trans. on Computers, 2002,51(5):541−552. [doi: 10.1109/tc.2002.1004593]

[32] Fromknecht C, Velicanu D. CertCoin: A NameCoin based decentralized authentication system. Technical Report, Massachusetts Institute of Technology, 2014.

[33] Fromknecht C, Velicanu D. A decentralized public key infrastructure with identity retention. IACR Cryptology ePrint Archive, 2014:803, 2014. https://eprint.iacr.org/2014/803.pdf

[34] Chen J, Yao SX, Yuan Q, He K, Ji S, Du RY. CertChain: Public and efficient certificate audit based on blockchain for TLS connections. In: Proc. of the IEEE INFOCOM. 2018. 1−9.

[35] Kuhn U, Selhorst M, Stuble C. Realizing property-based attestation and sealing with commonly available hard- and software. In: Proc. of the 2007 ACM Workshop on Scalable Trusted Computing. Alexandria, 2007. 50−57. [doi: 10.1145/1314354.1314368]

[36] Brickell E, Camenisch J, Chen L. Direct anonymous attestation. In: Proc. of the ACM Conf. on Computer and Communications Security. New York: ACM Press, 2004. 132−145. [doi: 10.1145/1030083.1030103]

[37] Liu MD, Shi YJ. Remote attestation model based on blockchain. Computer Science, 2018,45(2):48−52,68 (in Chinese with English abstract). [doi: 10.11896/j.issn.1002-137X.2018.02.008]

[38] Liu AD, Du XH, Wang N, Li SZ. Research progress of blockchain technology and its application in information security. Ruan Jian Xue Bao/Journal of Software, 2018,29(7):2092−2115 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5589.htm [doi: 10.13328/j.cnki.jos.005589]

[39] Maesa DDF, Mori P, Ricci L. Blockchain based access control. In: Chen L, ed. Proc. of the IFIP Int'l Conf. on Distributed Applications and Interoperable Systems. New York: Springer-Verlag, 2017. 206−220. [doi: 10.1007/978-3-319-59665-5_15]

[40] Zyskind G, Nathan O, Pentland AS. Decentralizing privacy: Using blockchain to protect personal data. In: Proc. of the IEEE Security and Privacy Workshops. Washington: IEEE Computer Society, 2015. 180−184. [doi: 10.1109/SPW.2015.27]

[41] Ouaddah A, Abou Elkalam A, Ait Ouahman A. FairAccess: A new blockchain-based access control framework for the Internet of things. Security & Communication Networks, 2016,9(18):5943−5964. [doi: 10.1002/sec.1748]

[42] Ouaddah A, Mousannif H, Elkalam AA, Ouahman AA. Access control in the Internet of things: Big challenges and new opportunities. Computer Networks, 2017,112:237−262. [doi: 10.1016/j.comnet.2016.11.007]

[43] Ouaddah A, Elkalam AA, Ouahman AA. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In: Rocha Á, ed. Europe and MENA Cooperation Advances in Information and Communication Technologies. 2017. 523−533. [doi: 10.1007/978-3-319-46568-5_53]

[44] Dorri A, Kanhere SS, Jurdak R, Gauravaram P. Blockchain for IoT security and privacy: The case study of a smart home. In: Proc. of the IEEE Int'l Conf. on Pervasive Computing and Communications Workshops. Washington: IEEE Computer Society, 2017. [doi: 10.1109/PERCOMW.2017.7917634]

[45] Dorri A, Kanhere SS, Jurdak R. Blockchain in Internet of things: Challenges and solutions. Technical Report, University of NewSouth Wales (UNSW), 2016.

[46] Cucurull J, Puiggalí J. Distributed immutabilization of secure logs. In: Barthe G, ed. Proc. of the Int'l Workshop on Security and Trust Management. Cham: Springer-Verlag, 2016. 122−137. [doi: 10.1007/978-3-319-46598-2_9]

[47] Cai YQ, Zhang E, He JY. (*t*,*n*) threshold signature scheme withstanding the conspiracy attack. Journal of Beijing University of Technology, 2011,37(8):1231−1235 (in Chinese with English abstract).

[48] Kiayias A, Russell A, David B, Oliynykov R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In: Katz J, ed. Proc. of the Int'l Cryptology Conf. New York: Springer-Verlag, 2017. 357−388. [doi: 10.1007/978-3-319-63688-7_12]

附中文参考文献:

[1] 沈昌祥,陈兴蜀.基于可信计算构建纵深防御的信息安全保障体系.四川大学学报(工程科学版),2014,46(1):1−7.

[2] 冯登国,秦宇,汪丹,初晓博.可信计算技术研究.计算机研究与发展,2011,48(8):1332−1349.

[3] 谭良,徐志伟.基于可信计算平台的信任链传递研究进展.计算机科学,2008,35(10):15−18.

[11] 沈昌祥,张大伟,刘吉强,叶珩,邱硕.可信 3.0 战略:可信计算的革命性演变.中国工程科学,2016,18(6):53−57. [doi: 10.15302/J-SSCAE-2016.06.011]

[12] 张焕国,陈璐,张立强.可信网络连接研究.计算机学报,2010,33(4):706−717. [doi: 10.3724/SP.J.1016.2009.00706]

[13] 罗安安,林闯,王元卓,邓法超,陈震.可信网络连接的安全量化分析与协议改进.计算机学报,2009,32(5):887−898. [doi: 10.3724/SP.J.1016.2009.00887]

[17] 周明天,谭良.可信计算及其进展.电子科技大学学报,2006,35(4)::116−127.

[18] 李明,李琴,张国强,颜湘.可信网络连接架构 TCA 的实现及其应用.信息安全研究,2017,3(4):332−338. [doi: 10.3969/j.issn.2096-1057.2017.04.007]

[19] 袁勇,倪晓春,曾帅,王飞跃.区块链共识算法的发展现状与展望.自动化学报,2018,44(11):2011−2022. [doi: 10.16383/j.aas.2018.c180268]

[22] 金鑫,陈兴蜀.可信链跨物理主机迁移及快速恢复方法.武汉大学学报(理学版),2016,62(2):103−109. [doi: 10.14188/j.1671-8836.2016.02.001]

[23] 刘明达,曹慧渊,拾以娟,马龙宇.基于 SR-IOV 的 TCM 硬件虚拟化构建可信虚拟环境.武汉大学学报(理学版),2017,63(2):117−124. [doi: 10.14188/j.1671-8836.2017.02.004]

[37] 刘明达,拾以娟.基于区块链的远程证明模型.计算机科学,2018,45(2):48−52,68. [doi: 10.11896/j.issn.1002-137X.2018.02.008]

[38] 刘敖迪,杜学绘,王娜,李少卓.区块链技术及其在信息安全领域的研究进展.软件学报,2018,29(7):2092−2115. http://www.jos.org.cn/1000-9825/5589.htm [doi: 10.13328/j.cnki.jos.005589]

[47] 蔡永泉,张恩,贺警阳.抗合谋攻击的(*t*,*n*)门限签名方案.北京工业大学学报,2011,37(8):1231−1235.

刘明达(1991－),男,山东齐河人,博士生,主要研究领域为信息安全,区块链.

陈左宁(1957－),女,博士,中国工程院院士,博士生导师,CCF 会士,主要研究领域为软件理论,操作系统,信息安全.

拾以娟(1977－),女,博士,副研究员,主要研究领域为信息安全,区块链,系统安全.