基于区块链的远程证明模型

刘明达 拾以娟
(江南计算技术研究所 江苏 无锡 214083)

摘 要 远程证明是构建可信网络的核心。但是,当前的远程证明模型仅面向有中心的网络,存在网关中心化、决策单点化的问题,并不适用于去中心的场景。针对去中心分布式网络环境中计算节点无法进行远程证明的问题,借鉴区块链的思想,提出了一种基于区块链的远程证明模型(Remote Attestation Based on blockchain,RABBC),并重点描述了模型框架、区块链核心结构和协议过程。分析表明,RABBC 具有去中心化、可追溯、匿名、不可篡改的安全特性,并具备较高的效率。

关键词 区块链,远程证明,去中心化,可信网络
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.02.008

Remote Attestation Model Based on Blockchain

LIU Ming-da SHI Yi-juan
(Jiangnan Institute of Computing Technology,Wuxi,Jiangsu 214083,China)

Abstract Remote attestation is the core of constructing the trusted network. However,current remote attestation model only looks on centralized network,in which there are some problems,such as centralized gateway and decision by single point,causing that it is not suitable to use this model in decentralized situation. Aiming at the problem that the computing node cannot execute remote attestation in the environment of centralized distributed network,by drawing lessons from the thought of blockchain,this paper proposed a remote attestation model based on blockchain (RABBC),and focused on model frame,core structure of blockchain and protocol process. The analysis shows that RABBC has the safe characteristics of decentralization,traceability,anonymity,non-tampering,and it is efficient.

Keywords Blockchain,Remote attestation,Decentralization,Trusted network

1 引言

目前,可信计算[1-2]已成为增强计算机系统安全性的关键技术,其核心思想是基于可信平台模块(Trusted Platform Mo-dule,TPM),构建从底层到应用进而延伸到网络的信任链。远程证明[3]是可信计算的重要功能之一,是可信计算平台向外部实体证明自身可信的过程。相比于传统的身份认证,远程证明进一步扩展了认证的内容,使得验证双方能够进行更深层次、更细致的认证。远程证明的具体介绍参见 2.1 节。

随着云计算[4]、物联网[5]、区块链[6]、边缘计算[7]等新型计算模式的兴起,去中心的分布式网络环境以其动态灵活的特性得到了广泛的关注。在有安全需求的应用场景中,计算节点之间可证明、可感知的安全互信显得尤为重要。但是,目前的远程证明模型针对的是有中心的网络,实际应用场景中存在网关中心化和决策单点化的缺陷,如图 1 所示。在有中心的网络中,无论是虚拟网络还是物理网络,都是由网关根据一定的访问策略,控制内网计算节点之间以及内网计算节点和外部节点之间的通信。而访问策略由一个专门的服务器产生,这个产生策略的过程就是远程证明的过程。网关中心化指网关是整个访控安全的核心部件,一旦中心被攻破,整个网络就会被操控。无论是虚拟网关还是实际的网关设备[8],都不可避免地存在一些安全漏洞[9]。决策单点化是指,判定决策的执行和访问控制规则的生成,通常在认证服务器这一个节点完成,一旦认证服务器出现不稳定或者由于恶意攻击而出现错误,就有可能导致恶意节点入网。这两个问题也是有中心的系统面临的安全通病。

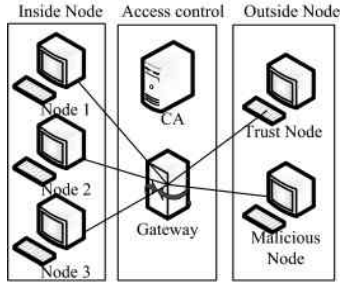

图 1 远程证明的典型场景

Fig. 1 Typical situation of remote attestation

由此可见,传统远程证明模型无法满足无中心分布式网

到稿日期:2017-11-27 返修日期:2018-01-08 本文受国家科技重点专项"核高基"(2013ZX01029002-001)资助。
刘明达(1991-),男,博士生,主要研究方向为计算机系统安全,E-mail:happyliumd@163.com;**拾以娟**(1977-),女,高级工程师,主要研究方向为可信计算和密码学,E-mail:14645789@qq.com(通信作者)。

络中远程证明的需求。为了解决这一问题，本文创新地将区块链技术应用于远程证明，将区块链去中心、不可抵赖、不可篡改和匿名的特性与远程证明的可信和安全相结合，得到了基于区块链的远程证明模型 RABBC。本文重点描述了 RABBC 模型的基本架构、区块链的构建和协议模型。分析表明，RABBC 模型满足去中心化、可追溯、匿名性和不可篡改等安全性需求，并具有良好的性能。

2　背景知识与威胁模型

2.1　远程证明

远程证明过程就是可信计算平台向外部实体证明自己拥有合法的 TPM，并且提供证据证明自身处于可信的运行状态。此时，在可信计算的安全模型里，外部实体相信这个平台是可信的，可以进行安全交互。为了实现这个目标，研究人员已进行了大量的研究工作，主要集中在两个层次。

1）平台身份证明：针对平台的身份进行可信认证，判断对方是否具备合法的背书密钥（Endorsement Key，EK）即合法的 TPM。其核心问题是，既要实现相互证明以确认身份，又要满足匿名性。平台身份证明主要有两种方案：TPMv1.1 标准下的 Privacy CA（Privacy Certification Authority）方案[10] 和 TPMv1.2 标准下的直接匿名证明（Direct Anonymous Attestation，DAA）方案[11]。

2）平台完整性状态证明：获取平台的可信状态信息，对平台的运行状态是否可信做出判断。主要分为基于二进制和基于属性两种方法。二进制证明是最基本的证明方法，会将平台的完整性信息全部发送给验证者验证，但是会暴露平台配置等隐私内容；基于属性的证明是对可信平台的安全属性进行提炼，将平台的完整性信息和安全属性进行映射，不需要暴露平台的具体信息就能够证明自身可信，但是需要第三方的介入。

在 RABBC 模型中，主要面临两个场景的远程证明：当新节点加入网络时，对这个节点能否加入网络进行判定；当网络中的两个节点进行通信时，节点之间进行快速的远程证明。

2.2　区块链

区块链技术源自于 2008 年出现的比特币[12]。区块链虽然来源于比特币，但却高于比特币，在近几年得到了飞速发展。目前有很多区块链的项目，其中最具有代表性的是以太坊（Ethereum）[13] 和 Hyperledger Fabric[14]。以比特币、以太坊和 Hyperledger 为例，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构成。目前已经有大量文献对区块链的具体原理和体系结构进行了介绍[15-16]，本文不再赘述。

RABBC 模型在本质上是一个联盟链，并不是一个开放型的区块链系统。它包含了相似的模型结构：1）网络层，在分布式网络中，网络节点之间的通信同样是 P2P 网络。2）共识层，RABBC 的共识层有两层含义：可信状态的判定标准，也就是提供的证据满足怎样的标准时，才能够说明身份可信和运行状态可信；如何选择记账节点。3）数据层，如何构造一个区块链的数据结构，使其能够在全网维护一个共享账本，账本上记录了各个计算节点的安全状态关系，并且不可伪造，可以追溯。4）智能合约层，对于不同的数据输入，执行不同的操作，这个过程是根据合约代码自动进行的。例如，节点 A 在区块链数据中获知节点 B 可信，那么就应该允许节点 A 和节点 B 进行通信。5）应用层，应用层实际上是分布式网络中处理的各项业务，可以是安全计算、金融服务等。

2.3　威胁模型

本文的目的在于证明基于区块链构建远程证明模型的可行性，这是一个新的研究方向，因此须给出安全假设并建立威胁模型。

存在一个证书签发机构（Certificate Authority，CA），其产生公私钥和直接匿名证明（DAA）的签名值，但不参与决策；TPM 是可信的，能够真实地报告平台信息；网络中的节点在刚加入网络时可信；可以通过加密来保证通信信道的安全。将共识机制抽象化，不具体实现共识方法。将智能合约抽象化，描述其功能但不具体实现智能合约。假设计算机系统中的 BIOS、OS、VMM、应用软件是不可信的；在网络运行过程中，可信节点的数目满足公示机制的理论要求，如工作量证明（Proof of Work，PoW）要求 51% 的节点可信。

3　模型架构

3.1　整体框架与定义

RABBC 的整体框架如图 2 所示。下面分别对参与模型的各部分进行定义。

TN：Trusted Node，可信计算节点，是分布式网络中实际安全的节点，具有合法的 TPM。

NTN：Non-Trusted Node，非可信节点，是分布式网络中实际可能存在安全隐患的节点，不一定是恶意节点，具有合法的 TPM。

MN：Malicious Node，恶意节点，是外部网络试图入网的恶意节点，不具备合法 TPM 或运行状态不可信。

AN：Accounting Node，记账节点，根据共识算法选举产生的记账节点，很大概率地属于 TN。

P2P：分布式的底层网络基础，各计算节点互相通信的基本信道，通信安全由 TPM 的密码功能保证。

A-BC：Attestation BlockChain，远程证明区块链，用于存储计算节点的安全和连接状态，为远程证明提供证据的分布式区块链系统。$A\text{-}BC:(B_1->B_2->\cdots->B_n)$。

CA：Certificate Authority，证书签发机构，为计算节点的 TPM 进行背书，并协助完成某些功能，但不参与任何决策，最大限度地保证去中心化。

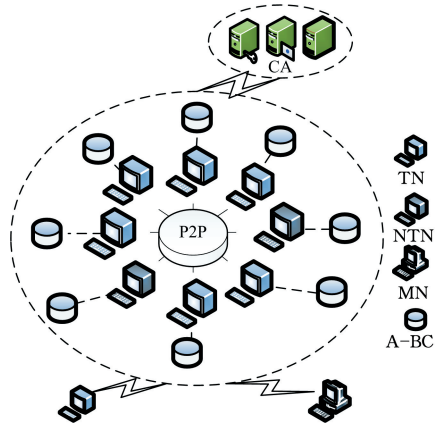

图 2　RABBC 的整体框架

Fig. 2　Overall framework of RABBC

下面给出系统的各项集合和基本操作的定义。

定义 1 将用户的身份证据集定义为 $P=\{P_{AIK},P_{Nonce},P_{Others}\}$。其中,核心是 P_{AIK},代表身份密钥(Attestation Identity Key,AIK);P_{Nonce} 是随机数,用于抗重放。将节点的完整性证据集定义为 $S=\{S_1,S_2,S_3,\cdots,S_n\}$,其中 n 为计算平台组件的数目。计算机平台组件主要包括可信度量根、BIOS、OS_Loader、OS、APP 等。

定义 2 定义计算节点的集合 $C=\{C_1,C_2,C_3,\cdots,C_n\}$,其中 n 表示分布式网络中已有的计算节点数目。定义计算节点的决策集合,$D_m=\{D_{1m},D_{2m},D_{3m},\cdots,D_{nm}\}$,这是一个布尔集,表示各节点对节点 C_m 的证明结果,1 代表可信,0 代表不可信。

定义 3 定义完整性度量函数 $F_{Measure}(C_m,P_m,S_m)$,计算平台 C_m 对自身的完整性进行度量,得到身份证据集 P_m 和完整性集 S_m。若 TPM 可信,则证据集无法伪造。

定义 4 定义完整性验证函数和规则:

1)$Verify_{Auth}(C_k,P_m,D\_auth_k)$,计算节点 C_k 根据身份证据集 P_m 对计算平台 C_m 进行平台身份证明,以验证其身份是否合法,得到结论 D_auth_k。

2)$Verify_{State}(C_kS_m,D\_state_k)$,计算节点 C_k 根据完整性集合 S_m 对平台 C_m 的完整性状态进行校验,以验证其没有被篡改,得到结论 D_state_k。

3)$Decision_{single}(D\_auth_k\&D\_state_k,D_{km})$,计算单节点 C_k 对节点 C_m 的决策结果 D_{km},由 1)和 2)中的结论得到。

定义 5 定义选取记账节点的共识算法 $PICK_{AN}(C,AN)$,在集合 C 中,选取记账节点 AN。

定义 6 定义全网决策函数 $Decision_{multiple}(AN,D_m,access,new\_block)$,其中 D_m 的定义参照定义 2,$C_m.Access$ 是最终的决策,new_block 是新的区块。AN 根据决策集合 D_m,按照"少数服从多数"的原则,得出节点 C_m 最终是否可以入网的决策 $access$,1 代表可入网,0 代表不可入网,并根据决策结果生成 new_block。

定义 7 定义区块链更新函数 $Re\text{-}Blockchain(AN,A\text{-}BC,C,new\_block)$,记账节点 AN 将新区块 new_block 广播给区块链系统 $A\text{-}BC$ 的所有节点集合 C。

定义 8 $Refer(A\text{-}BC,C_m,P_{AIK\_m},C_m.Exist)$:查询拥有身份 P_{AIK_m} 的计算节点 C_m 在区块链系统 $A\text{-}BC$ 中是否合法,并得到查询结果 $C_m.Exist$。

定义 9 通信功能的相关定义如下:

1)$Send(N,Q)$,将内容 N 发送到节点 Q;

2)$Socket(A,B)$,节点 A 和节点 B 正式建立通信。

3.2 区块链的核心结构

3.2.1 数据结构

区块是区块链系统的核心数据结构。设计一个完善的区块链系统十分复杂,本节仅对 RABBC 区块的功能和特殊性进行描述。RABBC 区块链本质上是一个访问控制的决策账本,参与到计算网络中的计算节点以其 AIK 为标识,将其基本信息写入到区块链,并标记入网时间和有效时间。系统认定,保存在区块链中(AIK 和平台完整性状态)且在有效时间内的计算节点,就是已通过分布式网络中各个节点统一验证的节点,其安全状态显示可信。如果一个计算节点退出了网络,则会给这个节点标记退出时间,并更新其安全状态为不可信。区块链系统维护一个参数,记录每一个节点的信用值,用来标记该计算节点的可信程度。这个值在网络中是动态变化的,会根据节点在网络中的表现增加或减少。当某个节点信用值过低时,需要重新进行远程证明。根据不同的共识算法,可以灵活地决定记账节点的实现形式。区块的核心数据结构如图 3 所示。

AIK	入网时间	有效时间	平台完整性状态
退出时间	安全状态	信用值	是否为记账节点(可选)

图 3 区块的核心数据结构

Fig. 3 Core data structure of blockchain

3.2.2 股份授权证明机制

股份授权证明机制 DPoS[17],又称委托人机制,来自于比特股项目[18],其原理类似于政治活动中的议会制度。在规模为 N 的网络中,每一个计算节点 $\{C_1,C_2,C_3,\cdots,C_n\}$ 参与投票,产生 M 个代表,这 M 个代表拥有较高的信用值,按照时间顺序依次获取记账权限。DPoS 本质上是存在中心的,但是中心的产生由每个计算节点决定,如果代表未能履行职责或者本身出现了安全隐患,就会被新一轮的投票淘汰。DPoS 不是本文关心的重点,具体实现不再展开。实际上,共识机制的选择须结合实际应用场景,不可能通过一种机制解决所有问题。

3.3 协议模型

当计算节点 A 加入网络 $C=\{C_1,C_2,C_3,\cdots,C_n\}$ 时,需要对其进行可信证明,如果可信,则会形成 $C=\{C_1,C_2,C_3,\cdots,C_n,A\}$。该过程有两个核心步骤:1)$A$ 向网络 N 提供可信身份和完整性证明的证据;2)N 中的计算节点分别进行决策,记账节点汇总子结论,形成最终结果,并写入区块。

3.3.1 协议过程

协议过程如图 4 所示,具体描述如下:

Step1 $A->Send(apply\|AIKa,B)$

节点 A 向网络 N 中的计算节点 B 发送请求。

Step2 $B->Refer(A\text{-}BC,A,AIKa,A.Exist)$

节点 B 根据节点 A 的身份密钥 AIK_a 到区块链中查询,如果 $A.Exist$ 合法,则执行 Step3,否则执行 Step4。

Step3 $Socket(A,B)$

节点 A 和节点 B 正式建立通信,过程结束。

Step4 $PICK_{AN}(C,AN)$ then $B->Send(AN,A)$

在节点集合 C 中选取记账节点 AN,并将 AN 的信息发送给节点 A。

Step5 $F_{Measure}(A,P_A,S_A)$

节点 A 对自身进行完整性度量,得到身份证据集 P_A 和完整性集 S_A。

Step6 $A->Send(P_A\|S_A,AN)$

节点 A 将证明身份和完整性的证据发送给 AN,请求远程证明。

Step7　$AN->Send(P_A \| S_A, C)$

AN 将节点 A 的证据广播到整个网络中进行决策。

Step8　$Verify_{\text{Auth}}(C_k, P_A, D\_auth_k)$ and $Verify_{\text{State}}(C_k, S_A, D\_state_k), k \in \{1,2,\cdots,n\}$ then $Decision_{\text{single}}(D\_auth_k \& D\_state_k, D_{ka})$

C 中各节点验证身份和完整性证据，并得到单节点对 A 是否可以入网的结论 D_{ka}。

Step9　$C_k->Send(D_{ka}, C), k \in \{1,2,\cdots,n\}$

各节点将结论 D_{ka} 广播到全网 C。

Step10　$PICK_{AN}(C, AN')$

选择一个新的记账节点 AN'。

Step11　$Decision_{\text{multiple}}(AN', D_m, access, new\_block)$

在 Step9 中，全网得到了决策集 D_m，AN' 根据决策集分析得出全网的认证结论，并生成新的区块 new_block。

Step12　$Re\text{-}Blockchain(AN', A\text{-}BC, C, new\_block)$

AN' 将新区块广播到全网，实现区块链数据库 $A\text{-}BC$ 的更新。

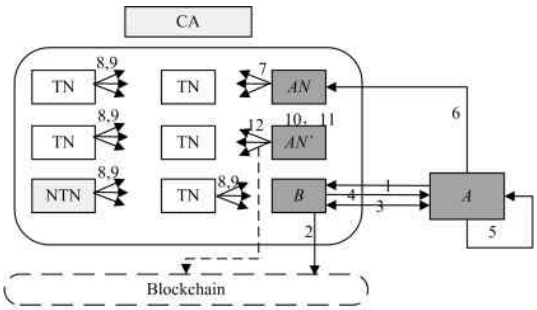

图 4　协议过程

Fig. 4　Protocol process

3.3.2　关键问题

问题 1　记账节点的选取问题

1）第一次选取 AN：在节点 A 申请入网时，整个网络无法保证节点 B 一定能够如实地反映节点 A 的真实可信状态，因此 Step4 选择了一个记账节点 AN，它可以被看作是一个可信的节点，能够将节点 A 的可信报告如实地公布到全网。

2）第二次选取 AN'：因为证据由 AN 发出，如果再由 AN 汇总结论，在节点 A 入网的这一次任务中，AN 实际上成为了全网的中心，这与去中心化背道而驰。

问题 2　信用值的作用

为了简化协议描述，3.2.1 节中提到的信用值并没有在协议中体现。信用值的引入有两方面起作用：

1）投票产生记账节点。在 DPoS 共识机制中，网络节点倾向于选择信用值高的节点作为记账节点，可以对投票数和信用值进行加权以获得最终票数。

2）信用降低与奖励。在 Step11 产生新区块时，如果一个节点的结论和整体结论相悖，那么就要降低这个节点的信用值。当一个计算节点的信用较低时，需要重新进行远程证明，而被选为记账节点的则可以获取信用值作为奖励。

一个 NTN 节点在实际运行中总会产生一些降低其信用值的行为，这也就降低了 NTN 成为记账节点的可能性。

3）CA 的作用。CA 在系统中是为 TPM 背书，也就是说，每个计算节点都可以通过 CA 颁发的证书证明对方拥有合法的 TPM。RABBC 模型本质上不是一个完全开放的区块链系统，而是一个联盟链。这里的去中心化体现为决策去中心化、访问控制去中心化、每个计算节点平等并可以参与到网络环境的安全决策中。

4）可信证据的追溯。区块链会如实地记录每一个参与到网络中的计算节点的行为，基于区块链的特性，这个记录不可篡改并且可以追溯。为了简化问题，RABBC 中仅包含了计算节点的身份和完整性状态，以及加入和退出的时间。存在以下两种情景：

①“节点 A 是可信的”这一结论被写入区块链，在节点 A 处理安全事务时，无须再进行复杂的远程证明，节点 B 只须在区块链中找到 A 节点可信的证据即可。

②“节点 A 是不可信的”这一结论被写入区块链，在有效的时间范围内，如果节点 A 发起与网内节点的安全交互，则会直接被拒绝。

当两个区块对一个节点的描述存在冲突时，以后置位区块中的信息为准，而无须遍历整个区块，提高了检索效率。

4　协议分析

4.1　安全性分析

基于区块链的远程证明模型 RABBC 应在继承区块链安全特性的基础上，保证远程证明的安全需求。安全需求主要包括去中心化、可追溯、匿名性和不可篡改。本文对安全性的分析基于 Dolev-Yao 威胁模型[19]，敌手可以窃听、获取和篡改协议消息，其本质上是一个合法的网络使用者；但是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 TPM 保证。

1）去中心化

RABBC 模型的去中心化体现在两个方面：①无中心网关。区块链系统实际上就是将传统安全网关中的访问控制的决策列表以分布式数据的方式存储在每一个计算节点中，从而将安全风险分散，降低整个网络被攻破的可能性。②共同决策。以 DPoS 模型为例，记账节点本身就是通过投票产生的，每一个节点都拥有投票的权利。同时，一个外部节点能否入网的决策也是由所有计算节点共同产生的。

定理 1　若共识机制是可靠的，则 RABBC 模型具有去中心化的特性。

证明：假设敌手 MN 试图成为网络 C 的中心节点，当 $PICK_{AN}(C, AN)$ 可靠时，记账节点的选取具有随机性，并且大概率地属于可信节点，除非 MN 能够控制多数节点，否则攻击失败，这显然是困难的。考虑两种场景：

场景 1　MN 不属于网络 C。此时，MN 首先要进行远程证明，使网络 C 承认 MN 的合法身份，并写入区块链。若 MN 不具备合法 TPM 或 MN 本身处于不可信运行状态，则 Step5 得到的证据不合法，此时 MN 加入网络失败。若 MN 具备合法 TPM 并处于可信运行状态，则加入网络成功，此时 MN 也仅是一个普通节点。

场景 2 MN 已属于网络 C。与场景 1 相似，MN 是否能成为中心节点仍然是一个小概率事件。即便 MN 在计算中侥幸成为记账节点，也仅此一次；并且，如果 MN 在 Step10 和 Step11 中写入了与全网结论相悖的内容，其他节点是可以感知到的，这会降低 MN 的信用值，使其下次更难当选为记账节点。

2)可追溯

区块链是一个链状的数据结构，从网络运行开始，所有想要记录的行为均能够被记入区块链，只要沿着区块链进行搜索，就能够找到所有的历史记录。

定理 2 若网络行为已被写入区块链 A-BC，则该网络行为是可追溯的。

证明：可追溯具有双重含义，即写入区块链的证据最终都能够检索到，追溯到的证据具有可信性，不可抵赖。分别考虑如下两种典型场景。

场景 1 C 中的节点 C_m 由于受到攻击，被模型判定为恶意节点 MN。此时，网络中的计算节点可以在区块链中追溯 C_m 节点的网络行为，进而能够在分析行为的基础上做出安全响应。

场景 2 C_a 和 C_b 进行安全计算，由于某些利益驱动，节点 C_a 妄图删除审计日志，不再承认曾经与 C_b 发生过的交互行为。由于 RABBC 模型中区块链能够完整记录行为，并且是一个分布式的存储，因此节点 A 的抵赖是无效的。

3)匿名性

在远程证明的模型中，匿名认证是重点和难点。而对于一个开放的区块链系统，隐私保护同样是一个重要的问题，必须要保证区块链中的身份和数据隐私[20]。用身份密钥 AIK 来代表平台的身份去进行认证，这本身就是可信计算为了增强匿名性做出的设计。两者的结合能够有效地保证 RABBC 模型的匿名性。

定理 3 若 TPM 的密钥是安全的且底层采用匿名的 DAA 认证协议，那么 RABBC 模型也具有匿名性。

证明：假设 TPM 的密钥是安全的，则外部实体仅能够获取身份密钥 AIK 的证书，无法获得背书密钥 EK，也就无法获得平台与 TPM 的对应关系。而在 DAA 认证协议中，基于零知识证明的原理，外部实体只能知晓其身份的合法性，而不能知晓其具体身份。因此，RABBC 模型具有匿名性。

4)不可篡改

不可篡改是区块链的一个重要的安全特性。攻击者如果想篡改数据库，就必须控制网络中大多数的节点，这在实际应用场景中是十分困难的。

定理 4 若敌手无法控制区块链系统中的大部分节点(视共识算法而定)，则 RABBC 模型具有不可篡改的特性。

证明：假设敌手 MN 试图对区块链系统 A-BC 中的某一块 B_m 进行修改。区块链是一个具有强关联性的链式结构，一个区块稍作改动，其哈希散列值就会发生改变，因此必须对 B_m 后面的所有区块进行修改。区块链是一个分布式数据库系统，需要通过对在大部分节点上储存的数据进行修改才能生效，这与定理的安全假设相悖。因此，RABBC 模型具有不可篡改的特性。

4.2 效率分析

1)共识机制

RABBC 不限制使用任何共识机制，DPoS 是目前比较适合的方案。DPoS 在产生之初，就是为了弥补工作量证明 PoW 固有的低效和高能耗缺陷，本身就已具有更好的效率。这也是 RABBC 在理论上能够获得良好效率的基础。在远程证明的应用场景中，需要的是快速认证，而不是金融行业要求的高交易吞吐量，计算节点的加入和退出虽然频繁，但也远远没有达到金融业万/秒的程度。目前，研究人员正在进行大量的共识机制方法的研究，从中选取一个适合应用场景的共识机制来保证模型的正确运行即可。

2)认证效率

在传统的远程证明模型中，两个“互相不认识”的节点在进行安全通信前，都要进行远程证明，并完成一系列复杂的步骤。而在 RABBC 中，完成这一步骤只需要在区块链中检索即可，这显然会带来巨大的性能提升。区块链作为一个分布式数据库，其数据量并不大。对于 RABBC 模型而言，其并不会产生大量的数据存储，因此在进行区块链检索追溯时，面对的不是一个大的数据量，这就能够在一定程度上保证模型的认证效率。同时，一个平台最新的状态总会被存储在后面的区块中，区块是经常更新的，因此这个检索过程在最新的一部分区块中就可以完成。

结束语 针对远程证明模型固有的缺陷，本文提出了基于区块链的远程证明模型，并对模型架构、区块链的核心结构和协议模型进行了定义和描述。分析表明，RABBC 模型具备良好的安全性和效率。远程证明是可信网络[21]的重要技术，但是本文的研究仅着眼于远程证明这一个点，与实现完整的去中心的分布式可信网络还有一定的距离，未来将进一步研究基于区块链的可信网络构建技术，并实现原型系统。

参 考 文 献

[1] ZHANG H G, HAN W B, LAI X J, et al. Survey on cyberspace security[J]. Science China(Information Sciences), 2016, 46(2): 125-164. (in Chinese)
张焕国，韩文报，来学嘉，等. 网络空间安全综述[J]. 中国科学(信息科学)，2016，46(2)：125-164.

[2] PEARSON S. Trusted Computing Platforms: TCPA Technology in Context[M]. Prentice Hall PTR, 2003: 206-208.

[3] 张焕国，赵波. 可信计算[M]. 武汉：武汉大学出版社，2011：23-25.

[4] HAYES B. Cloud computing[J]. Communications of the Acm, 2008, 51(7): 9-11.

[5] GUBBI J, BUYYA R, MARUSIC S, et al. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions [J]. Future Generation Computer Systems, 2013, 29(7): 1645-1660.

[6] YUAN Y, WANG F Y. Blockchain: The State of the Art and Future Trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494. (in Chinese)
袁勇，王飞跃. 区块链技术发展现状与展望[J]. 自动化学报，2016，42(4)：481-494.

(下转第 68 页)

参 考 文 献

[1] TAN K C,TEOH E J,YU Q,et al. A hybrid evolutionary algorithm for attribute selection in data mining[J]. Expert Systems with Applications,2009,36(4):8616-8630.

[2] HALL M A. Correlation-Based Feature Selection for Machine Learning[D]. Hamilton:The University of Waikato,1999.

[3] HONG Q,YANG Y. On Sampling-and-Classification Optimization in Discrete Domains[C]// IEEE Congress on Evolutionary Computation. IEEE,2016.

[4] ALMUALLIM H,DIETTERICH T G. Learning Boolean concepts in the presence of many irrelevant features[J]. Artificial Intelligence,1994,69(1-2):279-305.

[5] ALMUALLIM H,DIETTERICH T G. Learning with many irrelevant features[C]// National Conference on Artificial Intelligence. AAAI Press,1991:547-552.

[6] PUDIL P,NOVOVI,KITTLER J. Floating search methods in feature selection[J]. Pattern Recognition Letters,1994,15(11):1119-1125.

[7] ZHU W,SI G,ZHANG Y,et al. Neighborhood effective information ratio for hybrid feature subset evaluation and selection [J]. Neurocomputing,2013,99:25-37.

[8] GHAEMI M,FEIZI-DERAKHSHI M R. Feature selection using Forest Optimization Algorithm[J]. Pattern Recognition,2016,60:121-129.

[9] YU Y,QIAN H. The sampling-and-learning framework:A statistical view of evolutionary algorithms[C]// Evolutionary Computation. IEEE,2014:149-158.

[10] SUTTON A M,NEUMANN F. A Parameterized Runtime Analysis of Evolutionary Algorithms for the Euclidean Traveling Salesperson Problem[C]// AAAI Conference on Artificial Intelligence. 2012:595-628.

[11] HU Q,CHE X,ZHANG L,et al. Feature evaluation and selection based on neighborhood soft margin[J]. Neurocomputing,2010,73(10-12):2114-2124.

[12] MOUSTAKIDIS S P,THEOCHARIS J B. SVM-FuzCoC:A novel SVM-based feature selection method using a fuzzy complementary criterion[J]. Pattern Recognition,2010,43(11):3712-3729.

[13] HUANG J,RONG P. A Hybrid Genetic Algorithm for Feature Selection Based on Mutual Information[J]. Pattern Recognit. Lett.,2007,28(13):1825-1844.

[14] TABAKHI S,MORADI P,AKHLAGHIAN F. An unsupervised feature selection algorithm based on ant colony optimization [J]. Engineering Applications of Artificial Intelligence,2014,32(6):112-123.

[15] XUE B,ZHANG M,BROWNE W N. Particle swarm optimisation for feature selection in classification:Novel initialisation and updating mechanisms [J]. Applied Soft Computing,2014,18(C):261-276.

(上接第 52 页)

[7] SHI W S,SUN H,CAO J,et al. Edge Computing-An Emerging Computing Model for Internet of Everything Era[J]. Journal of Computer Research and Development,2017,54(5):907-924. (in Chinese)
施巍松,孙辉,曹杰,等. 边缘计算:万物互联时代新型计算模型[J]. 计算机研究与发展,2017,54(5):907-924.

[8] XU R,GUO J,DENG L. A database security gateway to the detection of SQL attacks[C]// International Conference on Advanced Computer Theory and Engineering. IEEE, 2010: 537-540.

[9] MURRAY A T,MATISZIW T C,GRUBESIC T H. A Methodological Overview of Network Vulnerability Analysis[J]. Growth & Change,2008,39(4):573-592.

[10] CHADWICK D W,BASDEN A. Evaluating Trust in a Public Key Certification Authority[J]. Computers & Security,2001,20(7):592-611.

[11] BRICKELL E,CAMENISCH J,CHEN L. Direct anonymous attestation[C]// ACM Conference on Computer and Communications Security. ACM,2004:132-145.

[12] ZOHAR A. Bitcoin[J]. Communications of the Acm,2015,58(9):104-113.

[13] Ethereum[EB/OL]. https://www.ethereum.org.

[14] LI W,SFORZIN A,FEDOROV S,et al. Towards Scalable and Private Industrial Blockchains[C]// ACM Workshop on Blockchain,Cryptocurrencies and Contracts. ACM,2017:9-14.

[15] UNDERWOOD S. Blockchain Beyond Bitcoin[J]. Communications of the Acm,2016,59(11):15-17.

[16] HE P,YU G,ZHANG Y F,et al. Surveyon Blockchain Technology and Its Application Prospect[J]. Computer Science,2017,44(4):1-7. (in Chinese)
何蒲,于戈,张岩峰,等. 区块链技术与应用前瞻综述[J]. 计算机科学,2017,44(4):1-7.

[17] DPoS[EB/OL]. http://8btc.com/article-3759-1.html.

[18] Bitshares[EB/OL]. http://www.btsabc.org.

[19] DOLEV D,YAO A. On the Security of Public Key Protocols [J]. IEEE Transactions on Information Theory,1983,29(2):198-208.

[20] ZHU L H,GAO F,SHEN M,et al. Survey of block chain privacy protection[J]. Journal of Computer Research and Development,2017,54(10):2170-2186. (in Chinese)
祝烈煌,高峰,沈蒙,等. 区块链隐私保护研究综述[J]. 计算机研究与发展,2017,54(10):2170-2186.

[21] LIN C,PENG X H. Research on trusted network[J]. Chinese Journal of Computers,2005,28(5):751-758. (in Chinese)
林闯,彭雪海. 可信网络研究[J]. 计算机学报,2005,28(5):751-758.