面向区块链贸易系统的无管理者安全模型

黄龙霞[1]，王良民[1]，张功萱[2]
（1. 江苏大学计算机科学与通信工程学院，江苏 镇江 212013；2. 南京理工大学计算机科学与技术学院，江苏 南京 210094）

摘 要：针对传统集中式贸易系统中管理者滥用权力问题，提出面向区块链贸易系统的无管理者安全模型，同时解决去管理者的贸易系统由于管理员缺失导致的背书安全、贸易不及时、验证低效、动态低效等问题。所提安全模型基于区块链技术解决传统贸易系统中的中心化集权的问题，采用基于同态认证的公开审计技术实现了无管理者的安全背书、背书密钥更新及贸易的高效验证，引入基于信誉的激励机制保证了贸易的及时性。最后，通过安全证明与性能分析表明了所提安全模型的安全性和可靠性，通信和计算开销均低于 IPANM。

关键词：区块链；贸易系统；安全模型；无管理者；激励机制
中图分类号：TN918.1
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2020235

Security model without managers for blockchain trading system

HUANG Longxia[1], WANG Liangmin[1], ZHANG Gongxuan[2]
1. School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China
2. School of Computer Science and Engineering, Nanjing University of Science & Technology, Nanjing 210094, China

Abstract: In view of the abuse of power by managers in the traditional centralized trading system, a security model without managers for the blockchain-based trading system was proposed, which also solved the problems of unsafe endorsement, untimely trading, low auditing efficiency and dynamic inefficiency caused by the elimination of managers. The proposed security model realized decentralization based on the blockchain technology, by using homomorphic authentication-based public auditing to achieve the secure endorsement and key updating for non-manager groups and efficient verification for transaction information respectively, introducing the reputation-based incentive mechanism to ensure the timeliness of the transaction. Finally, the security and reliability of the proposed security model were demonstrated by security proof and performance analysis, and the communication and computing costs are both lower than IPANM.

Key words: blockchain, trading system, security model, non-manager, incentive mechanism

1 引言

随着各种电子钱包的发展，以数字货币为主体的贸易系统以不可阻挡的发展速度在生活中得到普及。传统的集中式贸易系统在解决智能服务贸易时赋予中心实体过高的权力，而权力集中会带来集

收稿日期：2020−08−07；**修回日期**：2020−10−25
通信作者：王良民，wanglm@ujs.edu.cn
基金项目：国家重点研发计划基金资助项目（No.2017YFB1400700）；江苏省自然科学基金资助项目（No.BK20200888）；国家自然科学基金资助项目（No.61702230, No.62002139）；中国博士后科学基金资助项目（No.2019M651738）；江苏省高等学校自然科学研究基金资助项目（No.19KJB510021）
Foundation Items: The National Key Research and Development Program of China (No.2017YFB1400700), The Natural Science Foundation of Jiangsu Province (No.BK20200888), The National Natural Science Foundation of China (No.61702230, No.62002139), The China Postdoctoral Science Foundation (No.2019M651738), The Natural Science Foundation of Jiangsu Higher Education Institutions (No.19KJB510021)

权者滥用权力的问题。但简单地从贸易系统中取消管理者，会使贸易系统因管理员的缺失而产生恶意贸易、处理不及时等情况[1]，进而导致贸易系统可靠性以及安全性受到威胁。因此，如何设计分布式分中心的服务贸易模型、突破分布式架构下的关键技术、确保贸易的可靠性和安全性成为亟待解决的问题[2]。

随着区块链技术的发展，越来越多的贸易系统引入该技术[3]。区块链是指一系列基于密码学原理而不基于中心节点的通用技术，具备去中心化、公开透明、去信任、匿名性和不可篡改性等属性[4]，用于在点对点的分布式网络中交换信息和数字资产。通过引入机制允许所有节点参与，对贸易进行一致性协商使贸易民主化，在如物联网、边缘计算、政府管理、云计算、金融、医疗和物流等领域均得到了广泛的应用[5-6]。

基于区块链技术建立贸易系统借助区块链的去中心化和去信任的属性，可以解决传统贸易系统中存在的中心化集权的问题[7]，但完全去中心的公有链无法满足企业的需求，同时在隐私和监管方面均存在不足，因而实际应用中企业往往选择具备部分去中心和提供隐私保护及监管的联盟链[8]。在联盟链中，买家发起的贸易需要网络中的背书节点进行背书签名，只有在管理者确认买家已收齐背书的情况下，买家才可以继续执行贸易提交的操作。在本文方案的无管理者贸易模型中，该环节的安全性与高效性由同态属性与双线性对[1]来保证。买家可自行验证是否收齐背书签名，且仅当收齐背书签名，买家在后续阶段中能够通过验证。

同态属性还可以实现大量信息的高效验证，鉴于区块链中区块的设置，每个区块存储的信息有限，因此需借助线上验证–线下存储的模式[9]。随着时间的推移，贸易系统会以不可预估的速度产生大量数据，因此需要考虑如何高效验证线下存储的贸易信息的正确性，同时还需要在验证过程中确保数据信息的隐私不被泄露。公开审计技术借助挑战–应答协议[10]，能实现大量数据的安全与高效验证，以及基于区块链的贸易系统的安全性与高效验证。为了提高验证效率并确保验证安全性，本文方案在贸易验证阶段引入了公开审计技术。

除了安全性，基于区块链的贸易系统中的部分去中心化带来的系统不稳定问题也亟须处理，系统中贸易处理不及时、参与者发布恶意贸易等问题均会降低贸易系统的可靠性。所以，基于区块链技术的贸易系统需要合理的激励机制[11]。虽然联盟链中的节点是被指定的或者为利益共同体，但是对买家的正确行为进行奖励以及对恶意行为进行惩罚，有利于减少恶意贸易出现的机会，使贸易系统良化。本文方案采取一种快速的判定方法，该方法根据实体行为对信誉值进行加分或减分，对信誉值高的买家所发起的贸易优先处理，确保系统稳定的同时鼓励实体执行正确操作。

本文方案中去管理者的贸易系统流程能够同时从可靠性和安全性两方面来提高基于区块链的贸易系统的质量。本文的贡献如下。

1) 实现了去管理者的安全背书认证，借助同态属性，使用户在收到所有背书节点的背书签名后可自行生成有效的背书签名，且支持高效密钥更新。

2) 实现了高效且安全的批量贸易验证，引入公开审计技术，实现验证阶段的批量高效签名验证，且不需要使用其他实体的私有信息。

3) 保证了贸易系统的可靠性，采用基于信誉的激励机制对任务进行排序，减少高信誉用户等待时间并周期性对所有节点的信誉值进行定量评估。

针对中心实体或者管理者所导致的权限集中与滥用权力的问题，公有链系统的结构采取完全去中心化[12]，开放性在带给用户获取链上数据权限的同时给隐私保护和监督带来威胁；私有链在解决如上问题时会引起信息孤岛的问题[8]。因而，兼具管理、认证、授权、监控、审计的联盟链成为贸易系统的首选，但为了适应无管理者安全模型，还需要引入新的技术来实现安全的去中心。

自2007年Ateniese等[13]基于RSA（Rivest-Shamir-Adleman）算法提出非可信存储环境中的可证明数据持有协议，使用了同态加密和双线性对技术。之后基于该协议，多种公开审计方案应用于云环境[1]、无线体域网[14]等领域以确保远程数据的正确性。文献[15]加强了原有完整性验证方法，解决了验证者使用收集的证明信息获取用户身份隐私或者数据隐私的问题。Wang 等[16]结合区块链技术和 RSA 签名实现高效的私有数据持有证明，系统管理者负责公有参数的设定与私有信息的分发。以上方法可提高贸易系统中的海量贸易信息的验证效率，同时批量验证允许验证者同时处理多个审计任务请求，大大降低验证开销[17]。为防止验证者在验证过程中通过线性结合收到的验证信息来恢复出信息，验证过

程中的隐私保护不容忽视，对此，文献[18]使用盲化技术对发送的信息进行保护，文献[1]使用联盟链对验证者进行管理与控制，文献[19]设计了一个基于物流行业的区块链应用与监管系统，用分级分层模式实现了具有隐私保护的可追溯。

联盟链为贸易系统提供管理、认证、授权、监控、审计等功能，但背书节点具备过于集中的权力。针对集权化问题，Fu 等[20]指出这种设置将导致权力滥用和诬陷等问题，并提出将单个管理者的身份认证权力分发给若干管理者共同维护，实现身份追溯权力的分发。Huang 等[1]借助秘密共享技术将权力分发给每个参与用户，直接取消管理者，但是由于全员参与的设定，该方案的计算与通信开销均较高，且每次的密钥更新均涉及所有参与实体，这导致不支持高效的成员动态。而贸易系统中的动态性也是不可忽视的，因此以上方法不能直接应用于无管理者的贸易系统。

现有的激励机制主要有基于互惠机制的方案、基于电子货币的机制和基于信誉的激励机制。基于互惠机制的方案根据用户的贡献度来匹配价值相当的服务[21]，但系统中的实体需要建立长期的互惠关系。最广为人知的激励策略是基于货币的机制，通过将记账节点获取的奖励定期减半[22]来鼓励矿工挖矿，但该激励机制基于公有区块链，无法直接应用于本文方案。基于电子货币的机制需要集权的可信中心，均不适用于无管理者贸易系统。基于信誉的激励机制评估用户的信誉值，信誉值高的用户可获得更好的服务。同时，根据参与实体的贸易表现及时地进行信誉更新也是很有必要的[23]。

2　预备知识

2.1　双线性对

群 G_1 和 G_2 代表 2 个 q 阶乘法循环群，g 是群 G_1 的生成元，双线性对 $e:G_1\times G_1\to G_2$ 具备如下特性。

1) 对于群 G_1 中每个元素 $u,v\in G_1$ 和素数域中每个元素 $a,b\in Z_q$，有 $e(u^a,v^b)=e(u,v)^{ab}=e(u^b,v^a)$。

2) 对于群 G_1 中的每个元素 $u_1,u_2,v\in G_1$，可得到 $e(u_1u_2,v)=e(u_1,v)e(u_2,v)$。

3) e 是可计算的且是不可解的，也就是说 e 是非退化的，即 $e(g,g)\neq 1$。

本文方案中密码算法安全性依赖于 2 个困难问题，具体如下。

1) DL（discrete logarithm）问题。给定循环群的生成元 g 和公钥 $Y=g^x\in G_1$，计算出私钥 $x\in Z_q$ 在计算上是困难的。

2) CDH（computational Diffie-Hellman）问题。给定元组 $(g,g^\alpha,g^\beta)\in G_1$，在未知 α,β 的情况下计算出 $g^{\alpha\beta}\in G_1$ 在计算上是不可行的。

2.2　区块链

比特币热潮之后，其背后的技术支持–区块链技术进入人们的视野，并在工业界与学术界均成为热点。从严格定义上来说，区块链分为 3 种类型：公有链、私有链和联盟链。公有链上的操作是公开的；私有链是比较封闭的局域网；联盟链由参与实体共同维护并提供对参与成员的管理、认证、授权、监控、审计等全套安全管理功能。联盟链是一种特定的区块链，具有多个预选节点，从而以适中的成本建立分布式共享数据库[24]。

2.3　公开审计技术

作为公开审计技术的核心内容，挑战–应答协议使用 4 个步骤完成第三方验证，借助挑战–应答协议，公开审计使验证者在不知道用户私钥的情况下使用公开信息对远程存储的信息进行完整性验证，且不需要下载所有存储的信息。公开审计模型如图 1 所示。

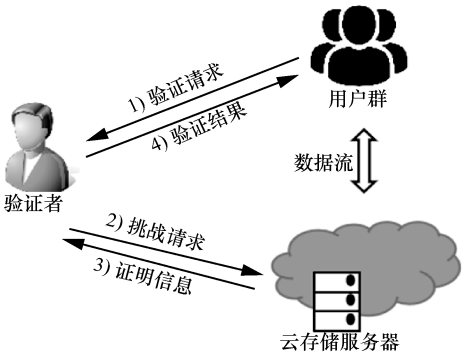

图 1　公开审计模型

如图 1 所示，用户群中的实体可自行存储/下载信息，可通过执行挑战–应答协议验证存储至云服务器的数据。首先用户给验证者发送验证请求；收到验证请求的验证者发送挑战信息给云服务器；云服务器根据挑战信息使用本身存储内容计算生成证明信息并返回给验证者；验证者在验证证明信息的正确性后将结果返还给用户。具体的过程可参考文献[10]。

2.4　同态认证技术

同态性在实现数据密文可计算的同时能保证

明文不可见，即某一信息先计算后加密与先加密后计算所得到的结果是相同的。同态认证技术便基于该属性，其是公开审计技术实现安全抽样验证的基础。该技术主要应用了同态性的 2 种属性：无块验证与不可延展性[14]。其中，无块验证利用了同态属性使验证者在验证文件完整性时不需要下载该文件；不可延展性可有效防止不良实体使用线性结合已有的信息生成组合文件的签名，除非该实体窃取了正确的签名私钥。

2.5　基于信誉的激励机制

在区块链贸易系统中，为了确保贸易系统的稳定性与及时性，需要加入激励机制以加速贸易的确认与打包。基于信誉的激励机制对积极参与的实体进行信誉奖励，信誉值高的实体能够在贸易打包过程中获取较高的优先级，以此激励实体执行正确的操作。

3　系统模型

3.1　安全交互模型

如图 2 所示，本文方案的安全交互模型包含 3 种实体：认证中心、贸易节点群和联盟链网络。认证中心负责所有参与者的注册与登录；贸易节点群由买家与卖家组成；联盟链网络中有 3 种节点，分别是背书节点、排序节点和记账节点，这 3 种节点分别负责贸易背书、贸易排序和贸易验证。

本文方案的安全交互模型包含 10 个步骤，具体如下。

步骤 1　用户向认证中心注册、登录，同时信誉值赋值。

步骤 2　买家向背书节点提交贸易提案。

步骤 3　背书节点基于信誉进行背书签名。

步骤 4　背书节点返回贸易模拟。

步骤 5　买家向排序节点提交贸易。

步骤 6　排序节点执行排序共识算法。

步骤 7　排序节点在全网广播区块。

步骤 8　记账主节点对贸易结果进行批量验证。

步骤 9　全网同步区块链信息。

步骤 10　记账主节点根据验证结果进行信誉减分及终止贸易，全网节点进行信誉反馈与更新。

3.2　设计目标

为了实现安全的去管理者贸易系统，本文方案需要实现以下目标。

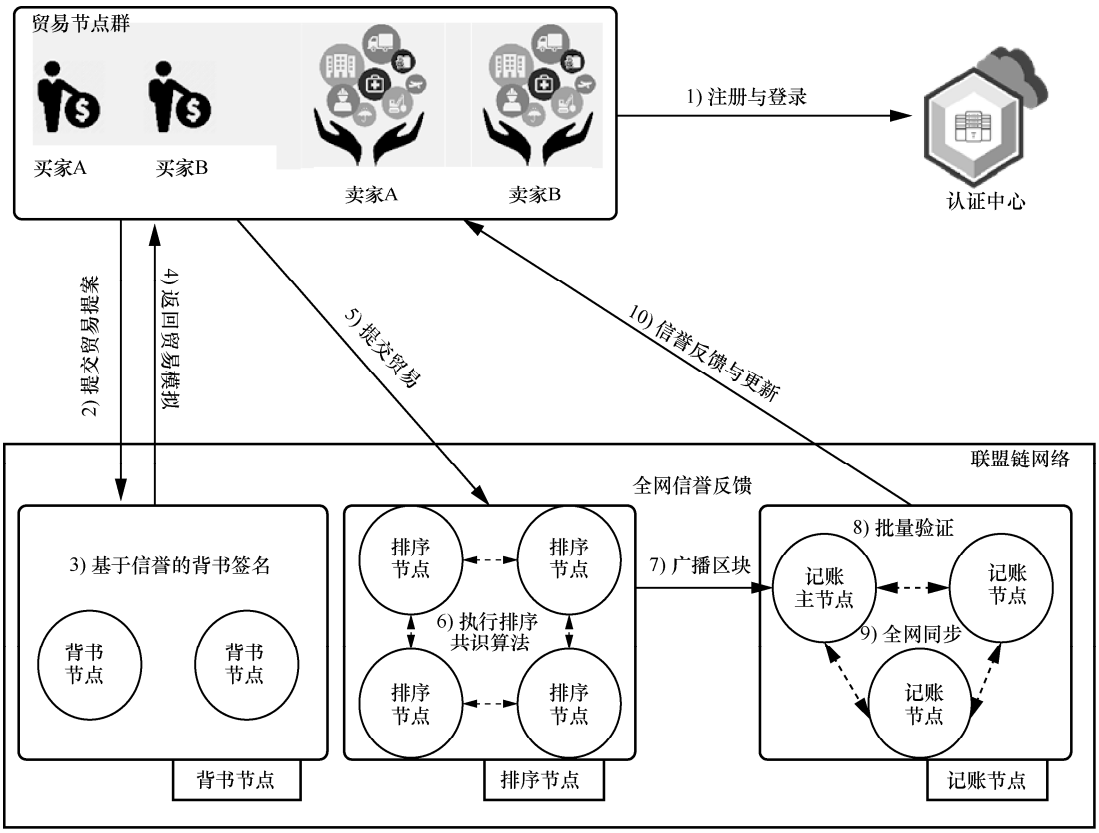

图 2　安全交互模型

1) 无管理者。在背书签名阶段，买家可自行生成有效的背书签名。

2) 正确性。若实体诚实地执行签名/协议，一定能够通过完整性验证。

3) 不可伪造性。在没有签名者的私钥的情况下，其他实体无法伪造正确的签名。

4) 抗重放攻击。在正确的数据块被损坏的情况下，存储实体无法进行重放攻击。

5) 隐私保护。在验证过程中，验证者无法从收到的验证信息中获取敏感信息。

6) 高效性。在验证贸易信息和判断事件成功时均能实现快速验证。

7) 动态性。当背书节点群发生变化时，系统能够快速实现密钥更新。

4 贸易系统的无管理者安全模型

本文基于区块链技术提出的贸易系统中的安全模型包含 3 个阶段：背书阶段、贸易阶段和信誉管理阶段，具体包含 8 个算法：用户注册与登录、贸易提案提交、基于信誉的背书、买家提交贸易、排序共识、贸易结果验证、不良贸易节点惩罚和信誉反馈与更新。为便于读者理解，本文所用符号及其含义如表 1 所示。

表 1 符号及其含义

符号	含义
G, Z_q	群，素数域
$(\mathrm{sk}_a, \mathrm{pk}_a)$	实体 P_a 的密钥对
θ_a	实体 P_a 的信誉值
tx_a	贸易提案的参数列表
r_m	模拟结果
$\{(r_m, \rho_e, P_e)\}_{e\in\Delta}$	贸易提案的模拟执行结果
v_j, Θ_j, β_j	排序值，贸易信誉值及权重
T_j, α_j	时间戳值及权重
$\{<\gamma, s_\gamma>\}_{\gamma\in I}$	挑战信息的集合
w_i	事件 e_i 对应的权重值
E, W, V	事件集合，权重集合，验证结果

4.1 背书阶段

算法 1 用户注册与登录。该算法由认证中心运行，输入为用户的身份信息，输出为买家用户的初始化系数。具体执行过程如下。

认证中心为系统中每个用户 P 随机从素数域中选取 $\mathrm{sk}\in Z_q$ 作为用户的私钥，使用循环群 G 的生成元 g 计算公钥 $\mathrm{pk}=g^{\mathrm{sk}}\in G$，公私密钥对 $(\mathrm{sk}, \mathrm{pk})$ 中的私钥 sk 通过安全通道发送给对应用户 P，公钥 pk 为系统公开信息；用户 P 的信誉值被初始化为 θ；每个背书节点 P_{e_ζ} 的私钥为 sk_{e_ζ}；集合 Δ 为背书节点的集合；背书签名的公钥为 $\mathrm{pk}_\Delta=\prod_{\zeta\in\Delta}\mathrm{pk}_\zeta=\prod_{\zeta\in\Delta}g^{\mathrm{sk}_\zeta}=g^{\sum_{\zeta\in\Delta}\mathrm{sk}_\zeta}$。

算法 2 贸易提案提交。该算法由买家实体运行，输入为买家的密钥信息和贸易信息，输出为贸易提案的参数列表 tx_a，具体执行过程如下。

首先，买家 P_a 通过连接到背书节点 P_{e_ζ} 来与区块链网络进行通信；然后买家 P_a 使用 sk_a 对贸易信息 m 加密生成客户端签名 σ_m，生成参数列表 $\mathrm{tx}_a=(\mathrm{ID}_a, \mathrm{SC}_a, m, T, \sigma_m)$，包含身份标识 ID_a，合约标识与方法 SC_a，贸易信息 m，时间戳 T，客户端签名 σ_m；最后买家 P_a 将贸易提案的 tx_a 发送给背书节点 P_{e_ζ}。

算法 3 基于信誉的背书。该算法由背书节点运行，输入为贸易提案和背书节点的密钥，输出为贸易提案的模拟执行结果，具体执行过程如下。

首先，背书节点 P_{e_ζ} 收到 tx_a 之后，通过判断买家的公钥 pk_a 与客户端签名 σ_m 的关系进行验证，若验证不通过则拒绝贸易；否则，使用合约标识与方法 SC_a 调用链码中的函数对上述贸易参数生成模拟结果 r_m。然后，背书节点 P_{e_ζ} 使用 sk_{e_ζ} 对该贸易的模拟结果 r_m 进行背书签名 $\rho_{e_\zeta}=(H(\mathrm{ID}_a)g^{r_m})^{\mathrm{sk}_{e_\zeta}}$，其中，$H(*)$ 表示哈希函数 $H:\{0,1\}^*\to G_1$，ID_a 表示贸易用户的身份标识。最后，P_{e_ζ} 完成贸易的背书，将贸易提案的初模拟执行结果 (r_m, ρ_{e_ζ}) 返回给 P_a，并附上背书节点 P_{e_ζ} 的身份标识，即返回 $(r_m, \rho_{e_\zeta}, P_{e_\zeta})$。

值得注意的是，若在同一时段，背书节点 P_{e_ζ} 收到来自若干买家 $P_a, P_b, \cdots, P_t$ 的若干贸易提案 $\mathrm{tx}_a, \mathrm{tx}_b, \cdots, \mathrm{tx}_t$，背书节点 P_{e_ζ} 按照买家 $P_a, P_b, \cdots, P_t$ 信誉值 $\theta_a, \theta_b, \cdots, \theta_t$ 的大小对所述贸易提案排序，依次进行贸易模拟和背书签名。其目的在于不被信誉低的恶意节点影响其他正常贸易的成功速度，同时也体现激励性，因为高信誉的节点发起的贸易在背书阶段具有较高的优先级。

4.2 贸易阶段

算法 4 买家提交贸易。该算法由买家运行，

输入为用户的身份信息与贸易模拟结果，输出为贸易签名信息，具体执行过程如下。

首先，买家 P_a 将背书节点群 Δ 里所有背书节点返回的贸易提案初模拟结果 $\{(r_m,\rho_{e_\zeta},P_{e_\zeta})\}_{\zeta\in\Delta}$ 进行整合，计算得到签名信息 $\rho_e=\prod_{\zeta\in\Delta}\rho_{e_\zeta}=(H(\mathrm{ID}_a)g^{r_m})^{\sum_{\zeta\in\Delta}\mathrm{sk}_{e_\zeta}}$，若未收集到足够的贸易提案初模拟结果，贸易失败；然后，买家 P_a 将包含贸易模拟结果、最终背书签名信息以及自身节点信息的贸易提案模拟结果 $\{r_m,\rho_e,P_a\}$ 上传至半可信云服务器[1]，云服务器验证 $e(\rho_e,g)=e((H(\mathrm{ID}_a)g^{r_{m_i}}),\mathrm{pk}_e)$ 是否成立，若成立则接收该信息进行存储；最后，买家 P_a 将贸易 m 相关信息提交给排序节点群中的排序节点 P_O，并附上排序节点的身份标识 id_O。

算法 5　排序共识。该算法由排序节点运行，输入为若干有效背书，输出为打包好的贸易区块，具体执行过程如下。

首先，排序节点 P_O 根据某一时段中来自贸易群组若干买家产生的共计 N 条贸易信息，即 N 条有效背书，记为 $\{r_{m_1},r_{m_2},\cdots,r_{m_N}\}$，使用式(1)对每个贸易信息的背书 r_{m_i} 进行验证，其中，pk_e 由 $g^{\sum_{\zeta\in\Delta}\mathrm{sk}_{e_\zeta}}$ 聚合而成。

$$e(P_{e_\zeta},g)=e((H(\mathrm{ID}_a)g^{r_{m_i}}),\mathrm{pk}_e) \tag{1}$$

其中，$H(*)$ 表示哈希函数，pk_e 表示背书节点 P_{e_ζ} 的公钥，g 表示循环群 G 的生成元，$e(\cdot)$ 表示双线性对运算；排序节点 P_O 计算排序值 $v_j=\alpha_jT_j+\beta_j\Theta_j$，其中，$T_j$ 表示贸易信息的时间戳值，Θ_j 表示贸易信誉值，α_j 表示共识算法中时间戳的权重值，β_j 表示共识算法里面贸易信誉值的权重值，α_j 和 β_j 均由系统按照实际需求设定；计算贸易的卖家 P_A 的信誉值 $\Theta_j=q\theta_a+(1-q)\theta_A$，其中，$q$ 表示贸易买家信誉权重值，由系统按照实际需求设定；θ_a 表示贸易买家 P_a 的信誉值；排序节点 P_O 将收到的所有贸易信息按照计算得到的排序值 v_j 的大小进行排序，完成贸易打包。最后，排序节点 P_O 将打包好的贸易区块发送给记账主节点 P_C，并附上记账节点身份标识 id_C。

算法 6　贸易结果验证。该算法由记账主节点运行，输入为打包好的贸易区块，输出为验证结果，具体执行过程如下。

记账主节点 P_C 为记账节点群选取的群组中信誉值最高的记账节点 P_C。首先，记账主节点 P_C 将排序节点发送的贸易区块中的信息进行验证，使用同态认证的同态特性对若干信息同时进行验证，即验证式(2)是否成立。验证分为 3 个步骤：1) 记账主节点 P_C 选取一个由 c 个随机数组成的集合 I 来定位本次验证向云服务器挑战的 c 个贸易，集合 I（即 I 为挑战贸易的下标集合）中每个元素选择随机数 $s_\gamma\in Z_q$ 生成内容为 $\{<\gamma,s_\gamma>\}_{\gamma\in I}$ 的集合 R，将集合 $R=\{<\gamma,s_\gamma>\}_{\gamma\in I}$ 发送给存储贸易的云服务器；2) 云服务器根据集合 R 和存储的信息计算 $S=\sum_{\gamma\in I}s_\gamma r_{m_\gamma}$ 和 $P=\prod_{\gamma\in I}\rho_\gamma^{s_\gamma}$，并将证明值 (S,P) 返还给记账主节点；3) 记账主节点根据收到的信息来验证式(2)。

$$e(P,g)=e(\prod_{\delta\in J,\gamma\in I}(H(\mathrm{ID}_\delta)^{s_\gamma})g^S,\mathrm{pk}_e) \tag{2}$$

其中，J 为集合 I 中每个下标对应贸易信息的买家的身份集合，ID_δ 为集合中买家的身份标识，r_{m_γ} 和 ρ_γ 分别为贸易背书及其签名。

4.3　信誉管理阶段

算法 7　不良贸易节点惩罚。该算法由记账主节点运行，输入为打包好的贸易区块，若验证不通过输出新的信誉值，具体执行过程如下。

记账主节点 P_C 丢弃验证不通过的贸易区块，根据无效信息对跟该贸易相关的买家、卖家、背书节点、排序节点进行信誉减分。设原信誉值 θ_i 为实体 P_i 与记账主节点 P_C 进行交互的事件集合为 $E=\{e_1,e_2,\cdots,e_n\}$，集合 E 中事件的权重集合记为 $W=\{w_1,w_2,\cdots,w_n\}$，集合 E 中事件成功与否的结果集合记为 $V=\{v_1,v_2,\cdots,v_n\}$，其中 $v_i\in\{0,1\}$，取 1 时表示成功，取 0 时表示失败；记账主节点 P_C 计算 $R=v_1\wedge v_2\wedge\cdots\wedge v_n$，若 $R=0$，则说明实体 P_i 进行了不良操作，因此需要对实体 P_i 进行信誉值减分，得到新信誉值 $\theta'_i=\theta_i-\sum_{i\in[1,n]}w_i(1-v_i)$，$w_i$ 表示事件 e_i 对应的权重值。然后，重复上述步骤直至所有参与实体完成信誉更新。

算法 8　信誉反馈与更新。该算法由记账主节点运行，输入为打包好的贸易区块，若验证不通过则输出为新的信誉值，具体执行过程如下。

首先，记账主节点 P_C 计算 $R=v_1\wedge v_2\wedge\cdots\wedge v_n$，若 $R=1$ 则说明实体 P_i 对所有贸易进行了诚实操作，实体 P_i 进行信誉值加分 $\theta'_i=\theta_i+i\in[1,n]\sum w_iv_i$；重复上述步骤直至所有参与实体完成信誉更新；全网

同步信誉积分后，新的信誉值 θ'_i 作为该节点 P_i 下次贸易成功的预测值。

5 安全证明和性能分析

5.1 安全性证明

为了证明本文方案的安全性，本节从正确性、不可伪造性、抗重放攻击、隐私保护、安全密钥更新方面进行证明。

1) 正确性。按照背书算法生成的签名能够通过签名验证，正确存储了文件信息的云能够通过验证。

证明 在排序共识阶段，已知贸易信息的背书为 r_m，贸易信息背书的签名为 $\rho_e=(H(\mathrm{ID}_a)g^{r_m})^{\sum_{\zeta\in\Delta}\mathrm{sk}_{e_\zeta}}$，背书的签名公钥为 pk_e，因此，有式(3)成立。

$$\begin{aligned}&e(\rho_e,g)=e(\prod_{\zeta\in\Delta}\rho_{e_\zeta},g)=\\&e((H(\mathrm{ID}_a)g^{r_m})^{\sum_{\zeta\in\Delta}\mathrm{sk}_{e_\zeta}},g)=\\&e(H(\mathrm{ID}_a)g^{r_m},g^{\sum_{\zeta\in\Delta}\mathrm{sk}_{e_\zeta}})=\\&e(H(\mathrm{ID}_a)g^{r_{m_i}},\mathrm{pk}_e)\end{aligned}\tag{3}$$

由此可知，式(1)成立，即说明按照背书算法生成的背书签名能够通过签名验证。

在贸易结果验证阶段，根据收到的挑战信息集合 $R=\{<\gamma,s_\gamma>\}_{\gamma\in I}$ 和本身存储的贸易信息与签名信息，云存储服务器计算 $S=\sum_{\gamma\in I}s_\gamma r_{m_\gamma}$ 和 $P=\prod_{\gamma\in I}\rho_\gamma^{s_\gamma}$，其中，贸易信息 r_{m_γ} 的签名为 $\rho_e=(H(\mathrm{ID}_\delta)g^{r_{m_\gamma}})^{\mathrm{sk}_e}$，可以得到式(4)。

$$\begin{aligned}&e(P,g)=e(\prod\nolimits_{\gamma\in I}\rho_\gamma^{s_\gamma},g)=\\&e(\prod_{\delta\in J,\gamma\in I}((H(\mathrm{ID}_\delta)g^{r_{m_\gamma}})^{\mathrm{sk}_e})^{s_\gamma},g)=\\&e(\prod_{\delta\in J,\gamma\in I}(H(\mathrm{ID}_\delta)g^{r_{m_\gamma}})^{s_\gamma},g^{\mathrm{sk}_e})=\\&e(\prod_{\delta\in J,\gamma\in I}(H(\mathrm{ID}_\delta)^{s_\gamma}g^{r_{m_\gamma}s_\gamma}),\mathrm{pk}_e)=\\&e(\prod_{\delta\in J,\gamma\in I}(H(\mathrm{ID}_\delta)^{s_\gamma})g^{S},\mathrm{pk}_e)\end{aligned}\tag{4}$$

由此可知，式(2)成立，即说明云服务器正确存储了相关信息。

证毕。

2) 不可伪造性。除了合法的背书节点，其他实体无法生成有效的背书签名。

证明 假设算法 A 是一个 (t',ε') 算法，元组 (t',ε') 表示算法 A 以优势 ε' 伪造能够通过验证的签名的运行时间是 t'。敌手一共最多可以执行 q_H 次哈希查询和 q_S 次签名查询。算法 B 是一个 (t,ε) 算法，即算法可在时间 t 内以优势 ε 解决 CDH 问题，其中 $t\leqslant t'+(q_\mathrm{H}+q_\mathrm{S}+1)t_{G_1}$，$\varepsilon\geqslant\dfrac{\varepsilon'}{[e(1+q_\mathrm{S})]}$，$e=\lim_{q_\mathrm{S}\to\infty}\left(1+\dfrac{1}{q_\mathrm{S}}\right)^{q_\mathrm{S}}$，其中，$t_{G_1}$ 是幂运算的时间。

给定元组 (g,g^a,g^b)，算法 B 为敌手模拟安全游戏，过程如下。

算法 B 使用元组构造公钥，为了生成签名，敌手借助算法 B 使用算法 A 进行哈希查询和签名查询。对于每个贸易背书信息 r_{m_i} 的哈希查询，算法通过掷硬币，以 p_x 概率掷出 0。如果掷出 0，算法 $\mathrm{Exp}_{G_1}+(|\Delta|-1)\mathrm{Mul}_{G_1}$ 则选取随机数 $o\in Z_p$ 并返回 $h=H(i)g^{r_{m_i}}=g^og^b$；否则返回 $h=g^o$。因为随机数 o 也是从域 Z_q 随机选取出的，所以算法无法区分掷硬币的结果。

针对敌手的每次签名查询，算法均进行掷硬币，签名查询的掷硬币结果与哈希查询的掷硬币结果是相互独立的。 如果掷硬币结果为 0，则说明敌手要哈希查询的结果来攻击公钥，那么算法 B 退出；否则，算法 B 返回签名查询结果 $\rho_i=(h')^a$，其中 $h'=g^bg^o$。

游戏结束时算法 B 拥有 2 个信息 $\rho_i'=(g^bg^o)^a$ 和 $\rho_i=(g^a)^o$，那么通过计算 $\dfrac{\rho_i'}{\rho_i}=\dfrac{(g^bg^o)^a}{(g^a)^o}$ 可以输出 g^{ab}。也就是说，敌手在算法 $\mathrm{Exp}_{G_1}+(|\Delta|-1)\mathrm{Mul}_{G_1}$ 的帮助下解决了 CDH 问题，在这一过程中，在每次签名查询中掷硬币结果必须为 0 且最后一次的哈希查询结果为 1。因此敌手挑战成功的概率为 $p_x^{q_\mathrm{S}}(1-p_x)\varepsilon'$，当 $p_x=\dfrac{q_\mathrm{S}}{q_\mathrm{S}+1}$ 时，概率值取最大值为 $\dfrac{1}{e(q_\mathrm{S}+1)}$。由于在每次哈希查询和签名查询中执行了一次幂操作并在输出时执行了一次幂操作，因此运行时间为 $t'+(q_\mathrm{H}+q_\mathrm{S}+1)t_{G_1}$。

由于 CDH 问题是难解，因此算法 B 中的优势概率 ε 是极低的，也就是说敌手在未知私钥的情况下无法伪造正确的签名。

证毕。

3) 抗重放攻击。本文方案能够抵抗重放攻击。

证明　云存储服务器只有在使用本身存储的正确的信息并按照挑战−应答协议计算出证明信息的情况下，才能够通过贸易结果验证阶段的验证。

一旦被挑战的信息块 r_{m_l} 出现损坏，式(2)就无法成立，记账主节点判定验证不通过。假设云服务器想通过执行重放攻击以通过验证，那么云服务器需要使用不同于正确的贸易信息及其签名 r_{m_j},ρ_j 的集合提交给记账主节点。那么，云服务器生成的证明信息分别为 $S'=s_j r_{m_l}+\sum_{\gamma\in I,\gamma\neq j} s_\gamma r_{m_\gamma}$ 和 $P'=\rho_l^{s_j}\prod_{\gamma\in I,\gamma\neq j}\rho_\gamma^{s_\gamma}$。

使用如上结果根据式(2)计算可得式(5)。

$$\begin{aligned}
&e(P',g)=e(\rho_l^{s_j}\textstyle\prod_{\gamma\in I,\gamma\neq j}\rho_\gamma^{s_\gamma},g)=\\
&e(((H(\mathrm{ID}_{\delta'})g^{r_{m_l}})^{\mathrm{sk}_e})^{s_j}\cdot\\
&\prod_{\delta\in J,\gamma\in I,\gamma\neq j}(((H(\mathrm{ID}_\delta)g^{r_{m_\gamma}})^{\mathrm{sk}_e})^{s_\gamma},g)=e((H(\mathrm{ID}_{\delta'})g^{r_{m_l}})^{s_j}\cdot\\
&\prod_{\delta\in J,\gamma\in I,\gamma\neq j}(H(\mathrm{ID}_\delta)g^{r_{m_\gamma}})^{s_\gamma},\mathrm{pk}_e)=e((H(\mathrm{ID}_{\delta'})g^{r_{m_l}})^{s_j}\cdot\\
&\prod_{\delta\in J,\gamma\in I,\gamma\neq j}(H(\mathrm{ID}_\delta)^{s_\gamma})g^{S-s_j r_{m_l}},\mathrm{pk}_e)=e(H(\mathrm{ID}_{\delta'})^{s_j}\cdot\\
&\prod_{\delta\in J,\gamma\in I,\gamma\neq j}H(\mathrm{ID}_\delta)^{s_\gamma}g^{S'},\mathrm{pk}_e)
\end{aligned}\tag{5}$$

如果式(5)能够通过验证则说明式(6)成立，也就是说 $H(\mathrm{ID}_{\delta'})^{s_j}=H(\mathrm{ID}_\delta)^{s_j}$，这与哈希函数具有抗碰撞性相违背。因此，一旦存储信息出现错误，云存储服务器无法通过贸易结果验证阶段的验证。

$$H(\mathrm{ID}_{\delta'})^{s_j}\prod_{\delta\in J,\gamma\in I,\gamma\neq j}H(\mathrm{ID}_\delta)^{s_\gamma}=\prod_{\delta\in J,\gamma\in I}(H(\mathrm{ID}_\delta)^{s_\gamma})\tag{6}$$

证毕。

4) 隐私保护。记账主节点在验证贸易信息的正确性时无法从验证信息中获取贸易信息。

证明　在贸易结果验证阶段，记账主节点选取的挑战信息为 $R=\{<\gamma,s_\gamma>\}_{\gamma\in I}$，其中 s_γ 为随机数；记账主节点从服务器得到的证明信息 (S,P)，其中 $S=\sum_{\gamma\in I}s_\gamma r_{m_\gamma}$，$P=\prod_{\gamma\in I}\rho_\gamma^{s_\gamma}$。

挑战集合的大小为 $|I|$，假设贸易信息所在域包含 q 个元素，如果使用穷举法从证明信息中获取贸易信息和背书签名需要来验证 $q^{|I|}$ 次。而域的大小是一个大素数，随机集合 I 中随机数个数的选取决定了破解的难度，在文献[10]中详述了集合个数的选取原则，在此不做累述。在性能分析阶段，本文方案选取 300 或者 460 个随机数进行挑战，在 q 为大素数的基础上，穷举法的选项接近无穷大，因此，本文方案在贸易验证阶段确保记账主节点无法在验证过程中获取贸易信息。

证毕。

5) 安全密钥更新。当背书节点加入或者退出贸易系统时，背书签名密钥的更新是安全的。

证明　设原背书节点群为集合 Δ，每个背书节点 P_{e_ζ} 的私钥为 sk_{e_ζ}，背书签名的公钥为 $\mathrm{pk}_\Delta=\prod_{\zeta\in\Delta}\mathrm{pk}_\zeta$。若新节点 $P_{e_t},t\notin\Delta$ 加入背书节点群更新为 Δ'，那么新的背书签名的验证公钥 $\mathrm{pk}_{\Delta'}=\mathrm{pk}_\Delta\mathrm{pk}_t=\mathrm{p}k_\Delta g^{\mathrm{sk}_t}$，买家需要聚合集合 Δ' 中所有节点的子签名，生成的聚合背书签名即可使用新的验证密钥进行验证；若之后有旧背书节点 $P_{e_{t'}},t\in\Delta'$ 退出，背书节点群更新为 Δ''，那么新的背书签名的验证公钥 $\mathrm{pk}_{\Delta''}=\dfrac{\mathrm{pk}_{\Delta'}}{\mathrm{pk}_{t'}}=\dfrac{\mathrm{pk}_{\Delta'}}{g^{\mathrm{sk}_{t'}}}$。

证毕。

5.2　性能分析

本节首先分析本文方案的计算和通信开销，然后通过与 IPANM（incentive public auditing scheme for non-manager）方案对比来评估本文方案的性能，此外本节还对比了普通验证与批量验证的性能。为了方便读者阅读，表 2 列出了本节中所用符号的含义。

表 2　密码运算符号的含义

符号	含义
Exp_X，Mul_X	群和域中的幂、乘操作
hash，Hash	域和群中的哈希操作
Pair	对操作
$\|A\|$	元素 A 的大小

5.2.1　计算开销

计算开销主要集中在贸易方法中算法 4 当中的背书签名的合成与算法 6 贸易结果的验证。在背书签名合成阶段，买家将收集的来自各个背书节点的签名进行整合计算，所需开销为 $(|\Delta|-1)\mathrm{Mul}_{G_1}$。因为验证背书签名时使用的验证公钥也需要计算开销，即为 Exp_{G_1}，所以背书签名的合成的总计算开销为 $\mathrm{Exp}_{G_1}+(|\Delta|-1)\mathrm{Mul}_{G_1}$。

在贸易结果验证阶段，云服务器计算证明信息所需开销为 $c\mathrm{Exp}_{G_1}+(2c-1)\mathrm{Mul}_{G_1}$，验证者验证该证明信息的计算开销为 $2\mathrm{Pair}+c\mathrm{Exp}_{Z_q}+\mathrm{Exp}_{G_1}+c\mathrm{Mul}_{G_1}$。

如表 3 所示，所以，最终算法 6 中贸易结果验证的总开销为 $2\text{Pair}+c\text{Exp}_{Z_q}+(c+1)\text{Exp}_{G_1}+(3c-1)\text{Mul}_{G_1}$。

表 3　　计算开销

方案阶段	计算开销	
背书签名阶段	$\text{Exp}_{G_1}+(\lvert\Delta\rvert-1)\text{Mul}_{G_1}$	
贸易验证阶段	证明生成	$(\text{ID}_a,\text{SC}_a,m,T,\sigma_m)$
	证明验证	$2\text{Pair}+c\text{Exp}_{Z_q}+\text{Exp}_{G_1}+c\text{Mul}_{G_1}$
	合计	$2\text{Pair}+c\text{Exp}_{Z_q}+(c+1)\text{Exp}_{G_1}+(3c-1)\text{Mul}_{G_1}$

5.2.2 通信开销

本文方案的通信开销来自算法 2 中贸易提案的提交、算法 3 中背书签名的汇总、算法 4 中买家提交贸易和算法 6 中贸易验证阶段中协议交互。如表 4 所示，算法 2 最后提交贸易提案 $\text{tx}_a=(\text{ID}_a,\text{SC}_a,m,T,\sigma_m)$，其中，$\text{ID}_a,\text{SC}_a,T$ 的长度均为|id|，信息 m 的长度为$|Z_p|$，签名σ_m的长度为$|G_1|$，故算法 2 的通信开销为$3|\text{id}|+|Z_q|+|G_1|$。

表 4　　通信开销

算法	通信开销	对应内容
算法 2	$3\lvert\text{id}\rvert+\lvert Z_q\rvert+\lvert G_1\rvert$	$(\text{ID}_a,\text{SC}_a,m,T,\sigma_m)$
算法 3	$\lvert\Delta\rvert(\lvert\text{id}\rvert+\lvert Z_q\rvert+2\lvert G_1\rvert)$	$(r_m,\rho_{e_\zeta},P_{e_\zeta})$
算法 4	$\lvert\text{id}\rvert+\lvert Z_q\rvert+2\lvert G_1\rvert$	$\{r_m,\rho_e,P_a\}$
算法 6	$2c\lvert Z_q\rvert+c\lvert G_1\rvert$	$\{<\gamma,s_\gamma>\}_{\gamma\in I},(S,P)$

算法 3 中若干背书节点产生的签名$(r_m,\rho_{e_\zeta},P_{e_\zeta})$需要传输给买家，其中模拟结果$r_m$的长度为$|Z_q|$，子背书签名$\rho_{e_\zeta}$的长度为$|G_1|$，身份信息$P_{e_\zeta}$的长度为|id|。最终背书签名的合成需要$\Delta$个子背书签名，所以算法 3 的通信开销为$|\Delta|(|\text{id}|+|Z_q|+2|G_1|)$。

买家在运行算法 4 之后需要提交信息$\{r_m,\rho_e,P_a\}$提交，其中模拟结果r_m的长度为$|Z_q|$，背书签名ρ_e的长度为$|G_1|$，身份信息P_e的长度为$|\text{id}|$。所以算法 4 的通信开销为$(|\text{id}|+|Z_q|+2|G_1|)$。

在实现贸易结果验证的算法 6 中，涉及通信开销的有两步：挑战信息发送和证明信息发送。挑战信息为集合$R=\{<\gamma,s_\gamma>\}_{\gamma\in I}$，需要的通信开销为$2c|Z_q|$，证明信息$(S,P)$长度为$2|G_1|$。因此算法 6 的通信开销为$2c|Z_q|+c|G_1|$。

5.2.3 实验结果

在实验仿真中，本文方案使用 PBC（pairing based cryptography）[25]库来模拟所有方案中的密码操作，所有的实验均在 Ubuntu 系统中进行，实验次数不少于 1 000 次，该系统配置为 Intel Core i7 3.40 GHz。为了确保检测概率高于 99%，可以在应用时设置挑战块数 c = 460。本文将$|Z_q|$和$|G_1|$的长度设置为 160 bit，|id|的长度设置为 40 bit，n 为参与实体的总个数，根据秘密共享的最低安全性要求，设置门限值 $t=\frac{3}{n}$。为解决管理者集权带来的问题，IPANM[1]将管理员的权限分发给每个普通用户，由若干用户共同完成管理员的工作，从而取消管理员。本文方案受 IPANM 的启发，在联盟链中实现多背书节点子签名的安全高效聚合。

背书签名的生成。本文方案中为了贸易系统的安全性，采取多背书节点对同一贸易进行背书的方法，并且取消管理者进行背书聚合，以避免权力集中的管理者滥用权力。本文方案中，买家在收集齐所有背书节点的背书之后，自行聚合成最终背书签名，保证系统安全与背书签名安全的同时会产生的计算额外开销。

本文方案中背书签名生成的计算开销随背书节点个数的增加呈线性增长，但是额外开销的单位为微秒（μs），考虑到该方案区块链环境下不需要搜索确认背书签名是否收集齐，该部分开销是在可接受范围内的，尤其在网络环境不佳的情况下。如图 3 所示，本文方案的计算开销明显优于 IPANM 方案，原因是在密钥协商阶段，每个用户均需参与并进行 3 轮计算。

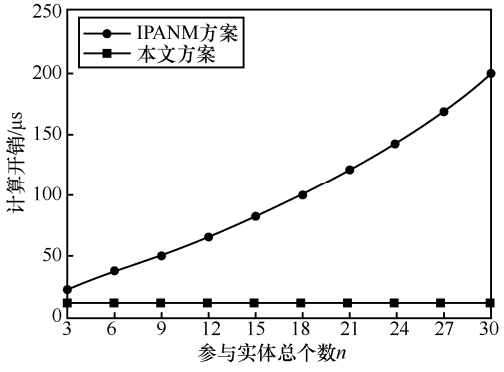

图 3　签名聚合阶段的计算开销对比

买家自聚合所产生的通信开销包含汇总背书子签名的通信开销$|\Delta|(|\text{id}|+|Z_p|+2|G_1|)$，如图 4 所示，与 IPANM 方案相比，本文方案在通信开销上具备明显优势，如图 5 所示，IPANM 方案在密钥生成阶段的通信开销特别高，原因在于 IPANM 方案中的密钥协商需要进行 3 次交互。

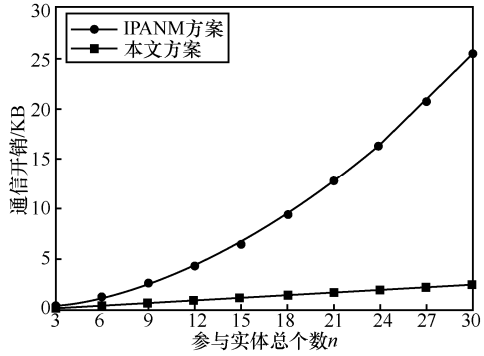

图 4　签名聚合阶段的通信开销对比

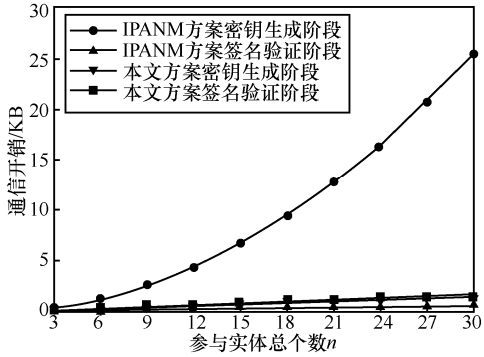

图 5　签名聚合分阶段的通信开销对比

高效验证。基于双线性对的属性，本文方案中的贸易验证可实现聚合验证，即批验证，因此比普通验证的一一验证节省了可观的计算开销。

如图 6 所示，相比于普通验证，批验证具备明显的优势。当挑战块数 c = 460 时，错误检测率可达至少 99%，对应普通验证的计算开销为 5.737 12 ms，批验证的计算开销为 0.035 458 ms，仅为普通验证的 0.6%。主要原因是执行双线性对计算的开销过大，普通验证执行的双线性对次数与挑战块数成正比，而批验证中的双线性对计算次数独立于挑战块数。

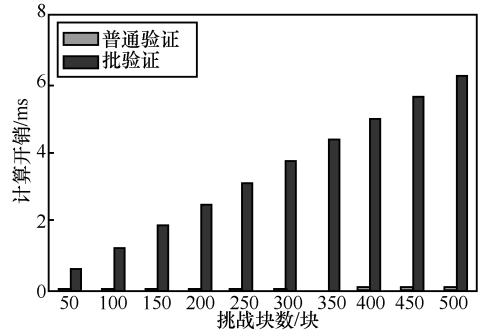

图 6　贸易验证阶段的普通验证与批验证对比

6　结束语

在传统的集中式贸易系统中，集中式管理者拥有过高的权力，本文提出面向区块链贸易的去管理者安全模型，同时解决因去管理者所造成的不安全背书、贸易时延以及贸易低效等问题。基于信誉的激励机制保证了诚实用户贸易的及时性，安全分析证明引入同态加密和公开审计技术的无管理者安全贸易模型具备正确性、不可伪造性、抗重放攻击、隐私保护和安全密钥更新。性能分析表明了本文方案在计算开销与通信开销上均具有明显优势。综上，本文方案实现了贸易系统的安全性和可靠性。

参考文献：

[1] HUANG L X, ZHOU J L, ZHANG G X, et al. IPANM: incentive public auditing scheme for non-manager groups in clouds[J]. IEEE Transactions on Dependable and Secure Computing, 2020, doi: 10.1109/TDSC.2020.3004827.

[2] LUO F L, DONG Z Y, LIANG G Q, et al. A distributed electricity trading system in active distribution networks based on multi-agent coalition and blockchain[J]. IEEE Transactions on Power Systems, 2019, 34(5): 4097-4108.

[3] 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述：原理、进展与应用[J]. 通信学报, 2020, 41(1): 134-151.
ZENG S Q, HUO R, HUANG T, et al. Survey of blockchain: principle, progress and application[J]. Journal on Communications, 2020, 41(1): 134-151.

[4] 刘哲, 郑子彬, 宋苏, 等. 区块链存在的问题与对策建议[J]. 中国科学基金, 2020, 34(1): 7-11.
LIU Z, ZHENG Z B, SONG S, et al. Problems and countermeasures of blockchain[J]. Bulletin of National Natural Science Foundation of China, 2020, 34(1): 7-11.

[5] XIE J F, TANG H L, HUANG T, et al. A survey of blockchain technology applied to smart cities: Research issues and challenges[J]. IEEE Communications Surveys & Tutorials, 2019, 21(3): 2794-2830.

[6] KANG J W, XIONG Z H, NIYATO D, et al. Toward secure blockchain-enabled Internet of vehicles: optimizing consensus management using reputation and contract theory[J]. IEEE Transactions on Vehicular Technology, 2019, 68(3): 2906-2920.

[7] 王明生, 曹鹤阳, 李佩瑶. 基于区块链的去中心化信贷系统及应用[J]. 通信学报, 2019, 40(8):169-177.
WANG M S, CAO H Y, LI P Y, et al. Decentralized credit system based on blockchain and its application[J]. Journal on Communications, 2019, 40(8):169-177.

[8] 曹兆磊. 一种适用于联盟链的共识机制[J]. 网络空间安全, 2019, 10(1): 96-101.
CAO Z L. A consensus mechanism for the consortium blockchain[J]. Cyberspace Security, 2019, 10(1): 96-101

[9] ZYSKIND G, ZEKRIFA D M S, ALEX P, et al. Decentralizing privacy: using blockchain to protect personal data[C]// IEEE Security & Privacy Workshops. Piscataway: IEEE Press, 2015: 180-184.

[10] HUANG L, ZHANG G, YU S, et al. SeShare: secure cloud data sharing based on blockchain and public auditing[J]. Concurrency and Computation: Practice and Experience, 2019, 31(22): e4359.

[11] TAO D, WU T Y, ZHU S, et al. Privacy protection-based incentive mechanism for mobile crowdsensing[J]. Computer Communications, 2020, 156: 201-210.

[12] KHORASANY M, MISHRA Y, LEDWICH G. A decentralized bilateral energy trading system for peer-to-peer electricity markets[J]. IEEE Transactions on Industrial Electronics, 2020, 67(6): 4646-4657.

[13] ATENIESE G, BURNS R, CURTMOLA R, et al. Provable data possession at untrusted stores[C]// ACM Conference on Computer and Communications Security. New York: ACM Press, 2007: 598-609.

[14] HE D B, ZEADALLY S, KUMAR N, et al. Anonymous authentication for wireless body area networks with provable security[J]. IEEE Systems Journal, 2017, 11(4): 2590-2601.

[15] TIAN H, NAN F, CHANG C, et al. Privacy-preserving public auditing for secure data storage in fog-to-cloud computing[J]. Journal of Network and Computer Applications, 2019, 127: 59-69.

[16] WANG H Q, WANG Q H, HE D B. Blockchain-based private provable data possession[J]. IEEE Transactions on Dependable and Secure Computing, 2019, doi: 10.1109/TDSC.2019.2949809.

[17] 刘云飞, 王勇军, 付绍静. 面向云端群组数据的轻量级完整性验证方案[J]. 通信学报, 2016, 37(S1): 140-146.
LIU Y F, WANG Y J, FU S K. Lightweight integrity verification scheme for cloud based group data[J]. Journal on Communications, 2016, 37(S1):140-146.

[18] 田俊峰, 李天乐. 基于TPA云联盟的数据完整性验证模型[J]. 通信学报, 2018, 39(8): 113-124.
TIAN J F, LI T L. Data integrity verification based on model cloud federation of TPA[J]. Journal on Communications, 2018, 39(8): 113-124.

[19] 余春堂, 韩志耕, 李致远, 等. 基于区块链的众包物流分级多层智能服务交易监管架构[J]. 网络与信息安全学报, 2020, 6(3): 50-58.
YU C T, HAN Z G, LI Z Y, et al. Blockchain-based hierarchical and multi-level smart service transaction supervision framework for crowdsourcing logistics[J]. Chinese Journal of Network and Information Security, 2020, 6(3): 50-58.

[20] FU A M, YU S, ZHANG Y Q, et al. NPP: a new privacy-aware public auditing scheme for cloud data sharing with group users[J]. IEEE Transactions on Big Data, 2017, doi: 10.1109/TBDATA. 2017.2701347.

[21] GONG X, CHEN X, ZHANG J, et al. Exploiting social trust assisted reciprocity (STAR) towards utility-optimal socially-aware crowd sensing[J]. IEEE Transactions on Signal and Information Processing over Networks, 2015, 1(3): 195-208.

[22] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. Bitcoin, 2008.

[23] 李沓, 田有亮, 向康, 等. 委托计算下基于区块链的公平支付方案[J]. 通信学报, 2020, 41(3): 80-90.
LI T, TIAN Y L, XIANG K, et al. Block-based fair payment scheme under delegation computation[J]. Journal on Communications, 2020, 41(3): 80-90.

[24] LI Z, KANG J, YU R, et al. Consortium blockchain for secure energy trading in industrial Internet of things[J]. IEEE Transactions on Industrial Informatics, 2018, 14(8): 3690-3700.

[25] LYNN B. PBC: the pairing-based cryptography library[DB]. The PBC Libary, 2011.

[作者简介]

黄龙霞（1991− ），女，江苏泰州人，博士，江苏大学讲师，主要研究方向为信息安全、云存储安全、区块链安全等。

王良民（1977− ），男，安徽潜山人，博士，江苏大学教授、博士生导师，主要研究方向为密码学与安全协议、物联网安全、大数据安全等。

张功萱（1961− ），男，江西景德镇人，南京理工大学教授、博士生导师，主要研究方向为云计算、无线传感网、可信计算等。