基于以太坊的区块链金融数据安全研究与应用

——以保理融资问题为例

黄庆安[1]，黄文波[2]

（1. 福建开放大学 科研处，福州 350013；2. 南开大学 金融学院，天津 300350）

摘要：近年来，伴随着金融信息化的浪潮，金融业务活动中产生了海量的金融数据，其中许多不乏与金融消费者个人安全甚至国家安全息息相关的数据。结合我国现有的金融数据安全问题以及传统保理融资模式存在的不足，基于以太坊区块链技术，运用文献搜集法和理论剖析法，创建一个基于以太坊的保理融资（含合约拍卖）模型并根据其消息传输图设计对应算法。最后，运用在线集成开发环境 RemixIDE 和智能合约高级语言 Solidity 对合约拍卖算法进行实现，并综合分析所构建模型的有效性和适用度。

关键词：区块链；以太坊；金融数据；保理融资

中图分类号：F832 **文献标志码**：A **文章编号**：1671－1807(2023)17－0024－09

近年来，随着大数据信息时代的发展，产生了大量数据，关乎个人隐私、企业生存甚至国家安全。因此，国家越来越重视数据安全保护，将数据安全提升至国家安全层面。2020 年 4 月，国务院印发《关于构建更加完善的要素市场化配置体制机制的意见》，提出将数据从信息化资产进一步变为生产要素。

随着信息化发展，金融行业开始重视对金融数据的利用和保护。由于金融数据涵盖市场数据、行业指数和企业数据等重要指标，其安全性也成为人们关注的焦点。与此同时，具有去中心化、可信安全、开放透明的区块链技术已经被广泛应用于金融、医疗、物流等领域。在良好的市场监管体制下，利用区块链技术可以帮助金融机构解决金融数据安全问题，帮助其实现业务革新，完善金融信息服务质量。

与此同时，以太坊（Ethereum）作为一个可以直接部署和执行去中心化智能合约的开源平台，已经成为许多学者调试开发区块链相关模型的重要方法。如何借助以太坊解决金融数据安全问题逐渐成为一个国内外共同关注的热点问题。为此，基于以太坊来研究金融数据安全保护问题，设计一种基于以太坊的保理融资模型，以期为金融数据安全保护提供新的思路，也为政府机关、金融机构及金融企业提供理论参考与实践依据。

1 文献综述

国外的研究工作起步较早且较为成熟。2017 年，Weber 等[1]对区块链系统在处理金融交易时的可用性进行了研究，Rouhani 和 Deters[2]也研究了私有区块链中的以太坊交易性能。随后，Egelund-Muller 等[3]提出基于以太坊的分布式账本上的金融合同管理，并提供了可行的解决方案。

在保理融资领域，Kayal 等[4]针对参与发票保理和库存融资的利益相关者采用区块链技术的兴趣进行了探索性研究，但并没有进行实质性的模型构建。Nijeholt 等[5]提出了 Dec Reg，一个已在私有区块链上实现的基于区块链技术的框架，以解决保理中的“双融资”问题。尽管网络外的实体不能访问发票数据，但是 Dec Reg 网络内部仍然可以访问这些数据，并不能消除所有安全风险。Hofmann 等[6]在 Nijeholt 等[5]的基础上针对发票产生唯一的标识符，但没有提供实现各方相互作用的细节。Guerar 等[7]针对国际发票融资模式提出了基于公共区块链的发票融资平台，使用星际文件系统（inter planetary file system，IPFS）加密发票数据，并详细阐述了各方作用的相关细节。

在国内也有不少学者进行了关于区块链金融的相关研究。在电子货币方面，郭笑春等和汪寿阳[8]以

收稿日期：2023-05-10

基金项目：福建省高校以马克思主义为指导的哲学社会科学学科基础理论研究项目（JSZM2021086）。

作者简介：黄庆安（1969—），男，福建寿宁人，福建开放大学科研处，教授，管理学博士，研究方向为互联网金融、农村金融、信用担保；黄文波（1998—），女，福建寿宁人，南开大学金融学院，硕士研究生，研究方向为金融科技。

Libra为案例,探究了大型跨国企业发行的数字货币国际化所带来的影响;方燚飚和周创明[9]提出基于区块链智能合约的代币系统并利用以太坊进行系统测试与分析。除了货币应用之外,国内已经有不少学者研究关于区块链技术在金融场景中的实际应用。朱立等[10]针对上海证券交易所业务情形——"去中心化的主板核心交易系统"研究了属于高性能联盟区块链的优化算法。在保理融资领域,李言和郭建峰[11]以中国建设银行为例,提出一个简单的出口保理融资工作流程,但并没有从理论角度分析相关流程的效果与成因;邓爱民和李云凤[12]提出以区块链为基础的供应链"智能保理"的业务模式并从博弈论角度进行了分析,得出区块链可以优化主体方决策行为的结论,但没有对区块链的制约违约行为的原因进行分析;焦媛媛等[13]在区块链赋能视角下对保理融资三方演化博弈进行研究,并发现区块链赋能保理融资模式下的隐性价值损失是束缚核心企业与供应商违约的关键因素,但并没有针对保理融资模式进行详细的设计;胡卿汉和何娟[14]针对基于区块链的保理融资模式进行详细的设计与阐述,但是仅从博弈论角度进行模型分析,并没有实现算法设计和仿真测试。

综上所述,国内外区块链在金融方面已有许多研究与应用,针对国际保理融资已有不少研究,但尚未有学者使用以太坊平台针对国内的保理融资模式进行深入研究和完善。

2 相关理论基础

2.1 区块链概述

区块链是一个分布式的网络数据库,具有去中心化、开放可编程、安全可信的特征,可体现不断增长的记录列表,这种记录称为"区块"。不同的区块链接到一起,并使用密码加密,每个区块由区块头(Block Header)和区块体(Block Body)组成,区块头包含区块编号、前一区块的哈希值、本区块哈希值、时间戳、Nonce(用于工作量证明);区块体包含交易信息等,不同区块链表现不同。

每一个区块会拥有一个哈希值,这个哈希值会被包含在下一个区块中,这就形成了一个使得区块难以篡改的链式结构,全部节点共同参与确认与维护在区块链网络中进行的所有交易,交易与数据的安全性和有效性由区块链的共识机制来担保。

回溯区块链的版本升级过程,最初的区块链 1.0 技术主要有加密技术、分布式存储、P2P(peer-to-peer)的数据传输技术、共识机制等,这些形成了区块链底层技术。随后,基于以太坊的区块链 2.0 技术诞生了,计算机协议"智能合约"赋予了区块链更大的能力,用户可以通过"智能合约"写出更加丰富精确的协议。

2.2 以太坊概述

以太坊是一个开源的可编译、部署并执行去中心化智能合约的区块链平台,其通过加密数字货币以太币(Ether)在提供去中心化的以太坊虚拟机(Ethereum virtual machine,EVM)来处理这些合约。在虚拟机编译 Solidity 等高级语言之前,需要将其编译为 EVM 字节码(bytecode),才能在以太坊上运行。

以太坊的本质是一个基于交易的状态机,一系列的输入可以被状态机读取并输出新的状态。以太坊拥有一个保存代码和数据的存储器,使用区块链来跟踪这个存储器,区块链可以保存这些状态变化的结果。在创世纪状态的时候,状态机还没有任何输入。当交易被执行输入后,创世纪状态就会转变成最终状态,随时代表着以太坊当前的状态。

与通用计算机不同的是,共识机制控制了以太坊的状态转换,共享账本上记录了这些状态转换的信息。

2.3 智能合约

智能合约是 Solidity 等合约编程语言编写的计算机程序,开发者将其部署在平台上,最后经过编译器编译后形成合约部署的交易,随后打包进区块在以太坊节点之间多次分发与复制,最终以确定性方式运行在以太坊虚拟机(EVM)上。合约中的代码需要外部账户所创建的交易触发才可以执行,执行过程中发生的状态变化被记录在区块链上。

金融交易的本质是跨越时空的价值交换,而智能合约可信透明、安全公平、自动高效的特征可以满足金融交易的本质需求,提升了金融交易的交易效率,扩大了金融交易的范围。具体而言,智能合约在金融领域的应用涵盖了多个方面(表 1)。

表 1 智能合约金融场景及应用特点

金融场景	应用特点
跨境支付	快速交易,保证安全性
征信	挖掘数据蕴藏价值,实时更新征信情况,打破数据孤岛
供应链金融	确保交易数据的真实性和可靠性
资产证券化	提升发行与交易效率,保护个人隐私
保险理赔	提高责任认定、赔付处理效率
清算结算	缩短交易时间,提高计算准确率
金融审计	克服人为审计偏差

3 金融数据安全问题

3.1 我国金融数据安全发展现状

在大数据信息时代,数据对于人民生活、社会

进步乃至国家发展的重要性日益凸显。近年来，国家高度重视数据的安全保护工作，提出各项对数据安全保护的要求，并陆续发布相关法案。

2021年6月，全国人大常委会对《中华人民共和国数据安全法（草案）》进行了审议，将数据安全保护的工作要求提升至国家法律层面，要求各行业制定数据安全相关标准，采用分级分类的方式对数据进行保护。

作为国民生活中不可或缺的一部分，金融行业在国家发展中占重要位置，众多金融基础业务、核心流程、行业往来等过程中产生了大量金融数据并逐步以不同形式转化为数字资产。

为进一步提高金融行业数据安全管理水平，保证金融数据安全应用，2020年9月23日，金融行业标准《金融数据安全 数据安全分级指南》（JR/T 0197—2020）出台，针对金融数据安全分级的目标、原则和范围有了明确描述，同时详细阐述了数据安全定级的要素、规则和定级过程，并给出了典型的数据定级规则供金融业机构参考。随后，2021年4月8日，中国人民银行发布了《金融数据安全 数据生命周期安全规范》（JR/T 0223—2021），该文件明确了金融数据生命周期的安全原则、防护要求、组织保障要求以及信息系统运维保障要求。

3.2 我国现有的金融数据安全问题

3.2.1 金融业务活动中数据的虚假性问题

在传统的金融业务中，不论是以纸质还是电子形式记录的金融数据，如票据、表单、账本等都可能存在人为篡改的问题，以影响金融机构和金融活动者对这些金融数据的判断和认识，从而影响金融业务活动的正常开展。

3.2.2 金融数据记录的完整性问题

历史的金融活动数据往往可以反映一个个体或组织的信用程度和金融活动的偏好，可以帮助新开展的金融业务活动主体判断对方的信用程度和交易习惯，以此来帮助确定授信额度和业务方向。

3.2.3 金融数据的越权访问问题

部分存储在金融机构信息系统中的金融数据可能会面临被越权访问的风险。不论是合法人员对金融数据的未授权访问还是第三方机构与金融机构内部人员进行非法交易，导致客户的个人金融信息泄露，都会影响个人隐私甚至进行诈骗行为。

3.2.4 互联网对金融数据的窃取和攻击问题

在当前信息化时代，大部分金融机构的服务平台以及海量的金融数据已经在互联网上实现电子信息化，一方面，大大提高了服务效率并且优化了金融数据管理的形式，另一方面，许多黑客也通过窃取、破坏、篡改金融数据等方式实施网络攻击，导致大量金融数据泄漏事件。IBM Security在《2022年数据泄露成本报告》中指出，单个数据泄露事件给来自全球的受访组织造成平均高达435万美元的损失，创下该年度报告发布17年以来的最高纪录，全球数据泄露成本在过去两年上涨近13%。

4 基于以太坊的金融数据安全应用——以保理融资问题为例

4.1 传统保理融资模式存在的问题

保理融资指的是需要赊销商品的卖方申请将应收账款转移其保理商，并通过这种方式获得融资。传统的保理融资分为有追索权和无追索权两种。有追索权的情况下，卖方需要对买方的到期付款风险承担相应责任，在保理商要求下应该承担回购该应收账款或归还融资的责任。在无追索权的情况下，保理商需要承担应收账款的坏账风险。

传统保理融资业务工作模式（图1）为：①买方向卖方发出交易请求；②卖方同意交易请求并与买方签订贸易合同；③卖方需要向保理商提出应收账款转让的申请，双方签订合同，卖方发出融资申请；④保理商和卖方将保理融资的相关事务通知买方，并请求买方确认应收账款转让；⑤买方确认卖方和保理商的应收账款请求；⑥保理商向卖方支付部分款项，完成融资请求；⑦运输商向买方交付货物；⑧买方通知卖方、运输商、保理商货物已完成交付。

场景a：⑨买方在到期日向保理商付清应收账款；⑩保理商向卖方付清剩余款项；

场景b：⑪买方在到期日未向保理商支付应收账款的费用，保理商可以向其催收；⑫在拥有追索权的情况下，买方可以被要求回购应收账款或者退还融资；在无追索权的情况下，保理商需要承担坏账风险。

基于上述工作场景，传统保理融资存在的金融数据安全问题如下：

1）贸易交易数据的真实性与合法性风险。在保理申请的过程中，可能会存在卖方伪造发票数据、贸易合同等以骗取融资的情况，保理商面临贸易交易数据的真实性风险。

2）买方和卖方信誉数据的完整性风险。保理商在保理过程中还需要承担买卖双方的信誉风险，可能会因为无法得知买卖双方以往的信誉情况而承担一定的风险。在有追索权的业务中，保理商需要承担买方的未到期支付款项的信用风险，在无追

索权的业务中保理商需要为买方的坏账承担风险。

3)交易数据存在泄漏和非法篡改的风险。在传统的保理融资过程中产生的金融交易数据通常被记录在金融机构的信息系统中,一旦数据被泄露或者被篡改,就会影响业务的继续进行。除此之外,一旦某个金融主体呈现的金融数据存在非法篡改的情况,将导致其他金融主体面临欺诈的风险。

4.2 以太坊保理融资数据安全模型构建

本文构建一个基于以太坊的金融保理融资(含合约拍卖)数据安全模型。该模型增加了保理商的拍卖机制,卖方可以指定向所有保理商或部分保理商开放保理权的拍卖。

该模型中的具体实体作用如下。

1)卖方(Seller):指在平台上通过发票进行融资,需要向买方出售货物的企业。在智能合约上可以通过拍卖寻找平台上的投资者。

2)买方(Buyer):指在平台上需要向卖方购买商品,并可以通过保理融资延迟支付发票金额的企业。

3)保理商(Factor):指可以为买卖方提供保理业务的金融机构(如银行)。在该平台中指允许以拍卖形式以低于商品实际价值购买发票以获得利润的人或金融机构。

4)运输商(Transporter):运输商品并提供关于运输状况的相关信息。

拟议的保理融资数据安全模型(图 2)的总体概述为:①卖方将发票数据写入数据层,并在以太坊智能合约中创建合约并将其部署到以太坊智能合约中,其中包含了参与拍卖的最低金额以及发票的哈希值;②在确认卖方提供的发票是真实的情况下,买方接受发票;③运输商负责运输货物并将货物的最新状态更新到以太坊智能合约上;④卖方确认收到货物;⑤保理商审核发票的唯一性和真实性后,开始在平台上参与拍卖,并提出自己的报价,投资

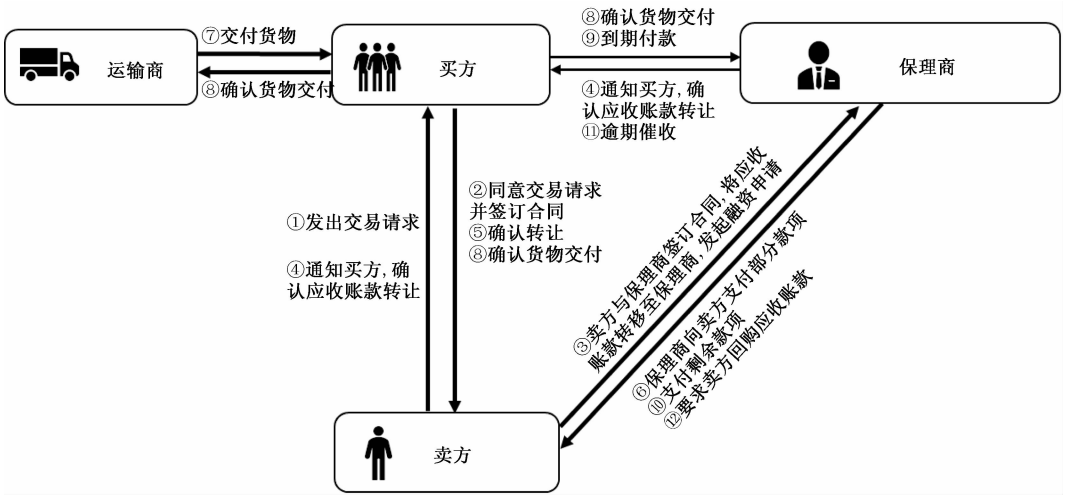

图 1 传统保理融资业务的工作模式

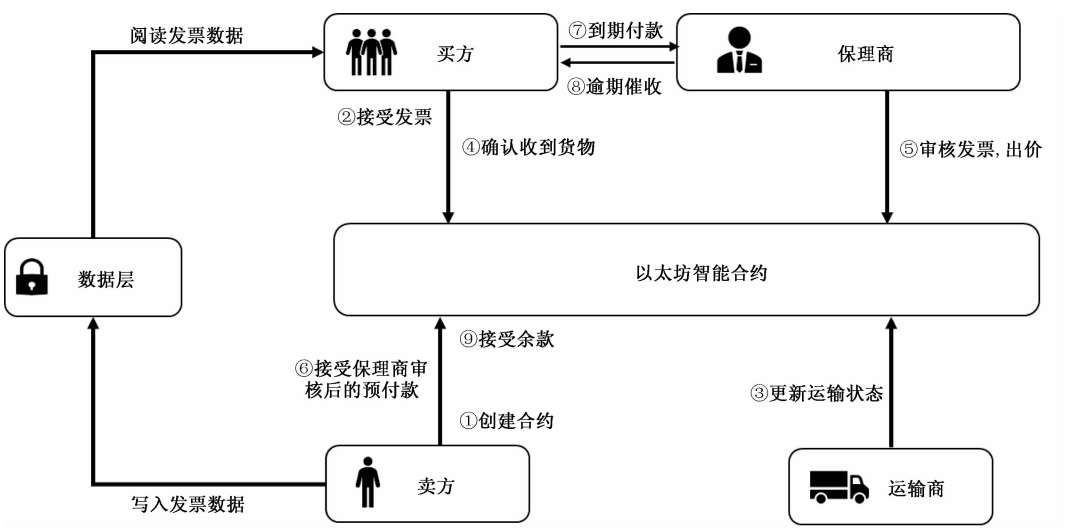

图 2 以太坊金融保理融资数据安全机制

者可以在以太坊平台查看买方的信誉记录；⑥卖方接受保理商的预付款，即融资成功；⑦买方到期向保理商付清款项；⑧若买方未及时付款，保理商向其催款，但保理商不享有追索权；⑨买方付清款项，保理商向卖方支付余款。

4.3　以太坊保理融资数据安全模型消息工作流程

在下文对工作流程的数据传输描述中，为了简化描述过程，假设卖方仅授权两个保理商（A 和 B）。卖方首先需要将自己的发票数据写入区块链中，加密过程是：①卖方通过随机数法生成一个会话密钥；②使用买方、A 和 B 的公钥加密这个会话密钥，以保证买方、A 和 B 可以验证发票的真实性，并参与整个保理融资过程。

在以太坊上金融保理融资数据传输过程（图 3）

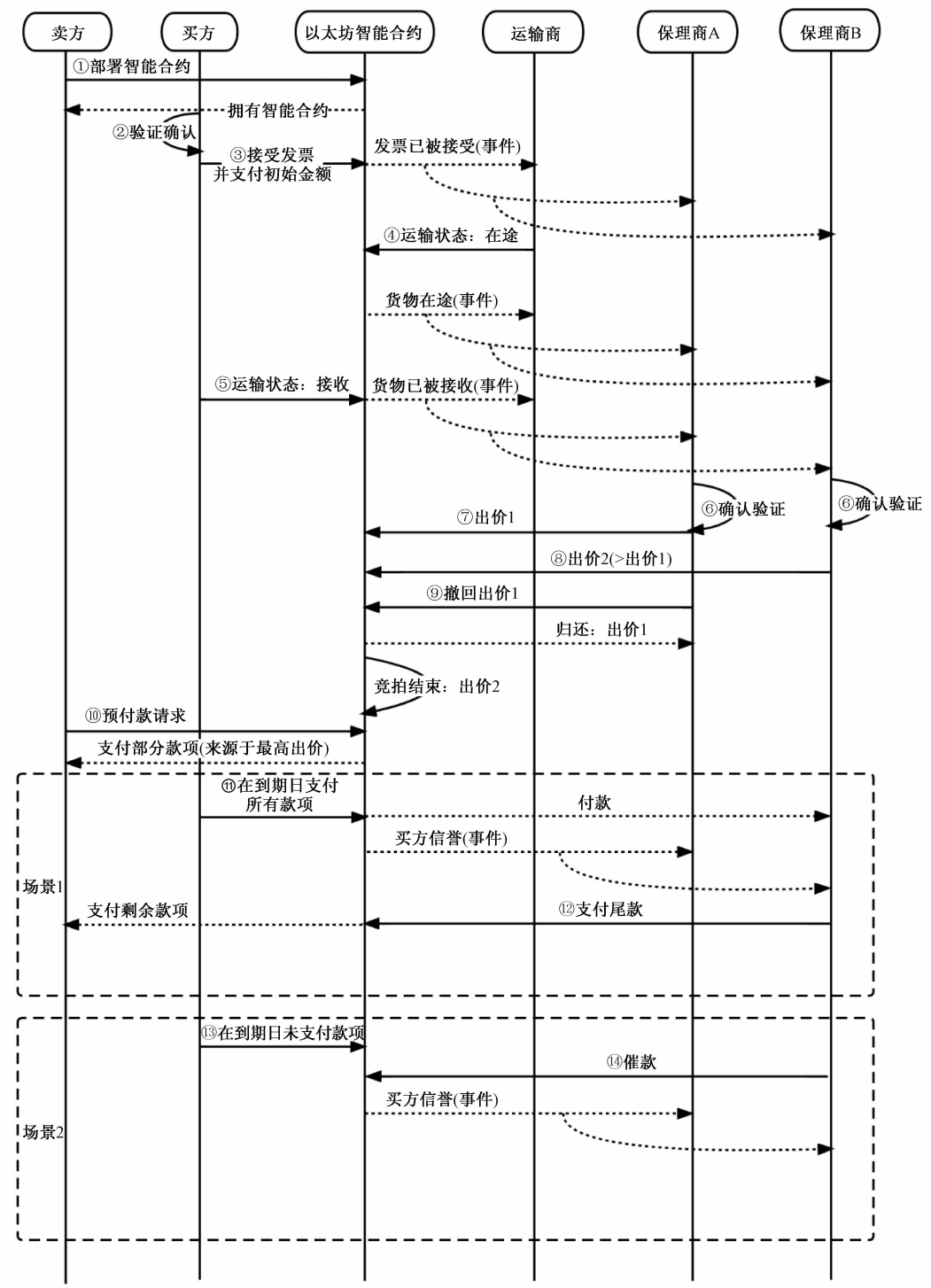

图 3　以太坊金融保理融资数据传输工作过程

为:①卖方创建一个智能合约并将其部署在以太坊平台上,其中涉及到最低出价;②买方使用自己的私钥和卖方的公钥解密存储在数据层中的发票的随机密钥,验证发票数据。若发票数据真实,则接受发票并支付一定的以太币,智能合约持有该以太币;③智能合约更新状态为发票已被接受;④运输商、保理商 A、保理商 B 可以在智能合约上看到发票已被接受,运输商在收到货物后,将智能合约上的运输状态改为在途;保理商 A 和保理商 B 可以在智能合约上看到运输的最新状态;⑤买方收到货物,智能合约将最新运输状态更新为已接收;⑥保理商 A 和保理商 B 通过用私钥和卖方的公钥对发票数据进行解密,可以查看到货物已被买方接收;⑦保理商 A 给出价格 1(大于最低出价);⑧保理商 B 给出价格 2(大于出价 1);⑨保理商 A 要求撤回出价 1,智能合约向保理商 A 发送其投标金额。该步骤可以避免以太币被自动发送至未赢得拍卖的保理商所产生的以太坊气浪费或者由以太币被发送到未知地址所产生的的安全漏洞;⑩卖方向智能合约提出预付款请求,智能合约向卖方支付来源于最高出价的部分金额。根据买方是否支付尾款,分为场景 1 和场景 2。

场景 1:⑪买方在到期日支付所有款项,智能合约将该金额支付给保理商 B,事件“买方信誉”被触发,买方信誉被记录在智能合约上,并通知所有人;⑫保理商 B 通过智能合约向卖方支付剩余款项。

场景 2:⑬买方在到期日未支付款项;⑭保理商 B 通过智能合约向买方催款,事件“买方信誉”被触发,买方声誉被记录在智能合约上,并通知所有人。

5 以太坊保理融资数据安全模型算法设计

Solidity 中有一组变量,称为全局变量,用于提供有关区块链的通用实用程序函数。因此,预定义保理融资智能合约实施的全局变量见表 2。

保理融资的过程定义了一些状态变量,这些变量被永久地存储在合约中,由卖方通过构造函数将其初始化。构造函数仅在合约部署时被调用一次,主要的状态变量见表 3。

表 2 全局变量

全局变量名称	解释
msg. sender	发起合约调用的以太坊地址
msg. value	调用中发送的以太币数量
msg. data	调用合约时传入的数据
Now	包含当前的时间戳

表 3 状态变量

状态变量名称	解释
InvoiceID	发票的唯一标识符的哈希值
DueDate	买方应当支付全部发票金额的日期
TotalCost	买方在到期日必须支付的金额
InitialCost	买方接受发票需要支付的初始金额
MinimumPrice	卖方接受的最低出价
BiddngTme	拍卖的持续时间
StartofAuction	拍卖的开始时间,使用当前时间戳进行初始化

主要的核心算法如下:

1)接受发票并支付费用:AcceptInvoiceAndPayInitialCost()。

算法 1:Accept Invoice And Pay Initial Cost

```
if msg. sender = BuyerAddress&&msg. value = InitialCost&&InvoiceAccepted=false then
    InvoiceAccepted ←true;
    InvoiceStatus("Invoice Accepted");
else
    Revert();
end
```

在算法 1 中,合约消息的发送方是买方且支付的 wei 数量为买方接受发票所需要支付的初始金额,并交付智能合约。当买方发送合约消息并且支付了初始金额后,发票的状态变为已接收并广播通知所有人。

2)货物发出:DispatchGoods()。

算法 2:Dispatch Goods

```
if
msg. sender = TransporterAddress&&InvoiceAccepted = true&&GoodsStatus=Warehousing then
    GoodsStatus ←InTransit;
else
    Revert();
end
```

在算法 2 中,合约消息的发送方是运输商,且货物的状态是已入库。在收到发票已被买方接收后,货物开始运输。

3)货物交付:GoodsDelivered()。

算法 3:Goods Delivered

```
if msg. sender=BuyerAddress&&GoodsStatus=InTransit then
    GoodsStatus ←Delievered;
    Send(TransporterAdress,Contract's Balance)
else
    Revert();
end
```

在算法 3 中,买方需要从运输商那里接收货物,确保货物状态是中转的且在收到货物后,将货物的

状态更新为已交付并由智能合约向运输方支付初始金额(即运费)。

4)合约拍卖:AuctionBidding()。

```
算法 4:Auction Bidding
Initialization=NewBid;
if msg. sender ≠ SellerAddress&&GoodsStatus = Delivered&&SrartofAuction ≤ Now ≤ StartofAuction + BiddngTme then
    NewBid ←Bids[msg. sender];
    if NewBid > MinimumPrice&&NewBid > HighestBid then
        Bids[msg. sender]←NewBid;
        HighestBid ←NewBid;
        HighestBider ←msg. sender;
    else
        Revert();
    end
else
    Revert();
end
```

在算法 4 中,卖方作为发票的持有者不能参与竞价。当且仅当货物显示已经交付并且处于拍卖进行时间,保理商才能参与竞价。所有人的出价都应该高于最低出价,大于所有出价的出价最高者将获胜。

5)融资请求:FinancingRequest()。

```
算法 5:Financing Request
Initialization:FundStorage
if msg. sender = Seller&& Now > StartofAuction + BiddngTme then
    FundStorage ←HighestBid;
    Send(Seller,0. 8FundStorage);
    FundStorage ←0. 2FundStorage;
else
    Revert();
end
```

在算法 5 中,卖方向智能合约请求融资,当且仅当拍卖结束,且拥有最高出价的情况下,智能合约向卖方发送 80%的资金(来源于最高出价),并留存 20%的资金待到期日决定是否给予卖方。

6)到期支付:PaidOnDueDate()。

```
算法 6:Paid on Due Date
if Now > StartofAuction + BiddngTme&&Now ≤ DueDate&&msg. sender=Buyer&&msg. value=TotalCost then
    BuyerPaidOnDueDate ←true;
    BuyerReputation(BuyerAddress,"Buyer paid on due date");
    Send(HighestBidder,msg. value);
else
    Revert();
end
```

在算法 6 中,在拍卖结束后,且到期日之前,卖方向智能合约发送总金额对应的以太币,则卖方按期支付发票。卖方信誉根据地址被记录在以太坊上,智能合约向最高竞价者发送对应的金额。

7)到期未支付:UnpaidOnDueDate()。

```
算法 7:Unpaid on Due Date
if msg. sender = HighestBidders&&Now > StartofAuction + BiddngTme&&Now > DueDate&& BuyerPaidOnDueDate = false then
    RefundRequest(msg. sender,"Refund request");
    BuyerReputation(BuyerAddress,"The Buyer unpaid on due date")
else
    Revert();
end
```

在算法 7 中,买方在到期日后未支付还款,保理商(最高竞价者)向智能合约发送催款请求,买方信誉根据其地址被记录在以太坊上。

6　安全性能分析

以太坊上的金融保理融资的数据安全模型相对于传统的保理融资模式有一些优点,可以有效规避传统保理融资模式的金融数据安全问题。

6.1　保证所有参与者的信誉数据公开透明

在以太坊平台中,所有参与者所发生的一切金融交易和行为都被记录在区块链上,其中包括信誉数据。保理商可以通过查看买卖方以往的信誉记录来确定竞价的最高值,以降低坏账风险。在本文的保理融资模型中,买方是否在到期日付款所导致的信誉结果,将会被记录在区块链上,买方为了保证自身在平台中长期获取他人信任,及时付款的能动性大大增加,减少了欺诈的可能性。此外,基于以太坊公开透明的特点,一旦卖方提交新的发票,所有人都可以访问得到这个行为,卖方不能通过一张发票进行二次融资。

6.2　保证发票数据的完整性和机密性

在本文的模型中,发票数据会被写入数据层并存储在区块链中,一旦发票数据遭到修改,其对应的哈希值就会发生变化,与原来的保理融资合同中的哈希值不匹配,就无法进行接下来的保理活动。与此同时,发票数据是被严格加密的,在卖方上传发票之前,会通过随机数生成会话密钥,并通过这个会话密钥对发票进行加密。随后,卖方会将买方和授权的保理商的公钥与这个会话密钥进行加密,这样只有合格的投资者才可以使用他们的私钥来解密会话密钥,随后使用会话密钥解密发票数据。

6.3 保证交易数据的完整性和可追踪性

在本文的模型中,交易的历史记录随时存储在智能合约的日志中,由于区块链的共识机制,没有人可以更改这些数据,这样可以确保交易记录的完整性。除此之外,该模型的算法可以有效保证数据的可追踪性。例如,若货物不在已交付的状态下,则拍卖算法就不能继续执行。通过消息传递时间顺序来控制进程并有效追踪数据,这样同样也保护了保理商的权益。

6.4 保证交易数据的公平性

在本文的保理融资模型中,添加了合约拍卖这一个机制,由算法 4 可以得知,该模型可以保证出价最高者获得保理的资格,有效规避由于买卖方私人因素而导致作弊行为,以保证交易的公平可信。

7 总结与展望

当前,金融数据的安全问题已经成为全球数据治理的重中之重,保理融资在国内金融市场以及国际金融市场中是非常重要的业务活动。本文首先总结了国内外现有的以太坊金融应用和研究现状,重点阐述了保理融资业务的以太坊区块链金融应用与研究。随后,针对区块链和以太坊进行了相关概念和工作原理的阐述,并描述了金融数据的基本概念和安全分类。

现有的金融数据存在虚假性风险、缺乏完整性、越权访问以及网络攻击等安全问题,而传统的保理融资模式也存在上述问题。为了改善传统的保理融资模式所存在的金融数据安全问题,本文提出了一个基于以太坊的保理融资(含合约拍卖)数据安全模型,以消息工作的时间顺序,设计了相应的算法,完善了数据的存储形式,并且利用智能合约来保证金融数据的可追踪性、保密性和完整性,大大降低了欺诈风险,并提高了保理融资的效率和可靠性,有效解决了传统保理融资模式所存在的金融数据安全问题。

本文中还利用在线编辑器 RemixIDE 和智能合约编程语言 Solidity 针对合约拍卖模型进行仿真实验测试并成功执行相关合约,并对整个模型进行了安全性能分析,得出了基于以太坊的保理融资(含合约拍卖)数据安全模型可以改善传统保理融资模型的金融数据安全问题的结论。

在大数据时代,以太坊应用开发的热潮重塑了人们对数据安全保护方式的认知。在不同金融场景的以太坊应用层出不穷,可以解决很多传统金融场景的金融数据安全问题。尽管本模型完善了金融数据的保密性、完整性、可追踪性等问题,并降低了欺诈的风险,但本模型仍然存在一些不足。下一步研究需要进一步完善模型,并提高算法的复杂性,使用 Dapp 完成对项目的开发应用。

在未来,以太坊的区块链应用仍然会是金融科技领域研究的重中之重。2019 年,《金融科技(FinTech)发展规划(2019—2021 年)》(中国人民银行印发)中提到将智能合约、数字签名、共识机制等技术应用到金融活动中,简化交易环节,提升金融交易信息的真实性、保密性和完整性,以便随时追溯金融交易过程。因此,以太坊在金融数据安全方面的研究前景广阔。

参考文献

[1] WEBER I, GRAMOLI V, PONOMAREV A, et al. On availability for blockchain-based systems[C]//2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS). Hong Kong: IEEE, 2017: 64-73.

[2] ROUHANI S, DETERS R. Performance analysis of ethereum transactions in private blockchain[C]//2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS). Beijing: IEEE, 2017: 70-74.

[3] EGELUND-MÜLLER B, ELSMAN M, HENGLEIN F, et al. Automated execution of financial contracts on blockchains[J]. Business & Information Systems Engineering, 2017, 59(6): 457-467.

[4] KAYAL A, YAO J, REDI J, et al. Financing small & medium enterprises with blockchain: an exploratory research of stakeholders' attitudes [J]. Blockchain Economics, 2019, 1: 65-83.

[5] NIJEHOLT H L À, OUDEJANS J, ERKIN Z. Decreg: a framework for preventing double-financing using blockchain technology[C]//Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. Abu Dhabi: ACM, 2017: 29-34.

[6] HOFMANN E, STREWE U M, BOSIA N. Discussion: how does the full potential of blockchain technology in supply chain finance look like? [M]. Berlin: Springer, 2018: 77-87.

[7] GUERAR M, MERLO A, MIGLIARDI M, et al. A fraud-resilient blockchain-based solution for invoice financing [J]. IEEE Transactions on Engineering Management, 2020, 67(4): 1086-1098.

[8] 郭笑春,汪寿阳. 数字货币发展的是与非:脸书 Libra 案例[J]. 管理评论,2020,32(8):314-324.

[9] 方燚飚,周创明. 基于区块链智能合约的代币系统[J]. 计算机应用研究,2020,37(12):3686-3690,3698.

[10] 朱立,俞欢,詹士潇,等. 高性能联盟区块链技术研究[J]. 软件学报,2019,30(6):1577-1593.

[11] 李言,郭建峰. 区块链技术在出口国际保理业务中的运

用及效果:基于中国建设银行的案例[J].对外经贸实务,2020(9):59-62.
[12] 邓爱民,李云凤.基于区块链的供应链"智能保理"业务模式及博弈分析[J].管理评论,2019,31(9):231-240.
[13] 焦媛媛,闫鑫,杜军,等.区块链赋能视角下保理融资三方演化博弈研究[J].管理学报,2023,20(4):598-609.
[14] 胡卿汉,何娟.区块链保理融资主体间信任机制研究[J].物流科技,2021,44(4):133-138.

Research and Application of Blockchain Financial Data Security Based on Ethereum: Taking factoring financing as an example

HUANG Qingan[1], HUANG Wenbo[2]
(1. Research Department of Fujian Open University, Fuzhou 350013, China;
2. School of Finance, Nankai University, Tianjin 300350, Chian)

Abstract: In recent years, with the wave of financial informatization, massive amounts of financial data have been generated in financial business activities, many of which are closely related to the personal security of financial consumers and even national security. Combined with the existing financial data security issues in China and the shortcomings of traditional factoring financing models, based on the Ethereum blockchain technology, literature collection method and theoretical analysis method are used to create an Ethereum-based factoring financing (including contract auction) model and the corresponding algorithm is designed according to its message transmission diagram. Finally, the online integrated development environment RemixIDE and the high-level smart contract language Solidity are used to implement the contract auction algorithm, and the validity and applicability of the model constructed are comprehensively analyzed.

Keywords: blockchain; ethereum; financial data; factoring financing