

基于区块链的铁路电子提单系统^①



肖梦雪¹, 左力¹, 徐志锬¹, 田金箫²

¹(西南交通大学 信息科学与技术学院, 成都 611756)

²(西南交通大学 计算机与人工智能学院, 成都 611756)

通信作者: 肖梦雪, E-mail: simmsxiao@foxmail.com

摘要: 提单是国际物流中的重要单证, 应用于铁路运输时将提高货物和资金流转效率. 现存的电子提单系统存在安全性低、公信力不足等问题, 难以保障各个参与方的权益. 本文在满足提单主要功能的基础上, 利用区块链去中心化、可溯源、可编程的特性, 确定了基于区块链的电子提单系统框架. 采用超级账本技术, 本文设计并实现了在区块链网络中多机构、多角色参与的电子提单发布、审核、质押等业务逻辑, 保证了电子提单安全、高效地流转. 经过区块链系统打包的交易数据, 凭借共识机制被锚定在链上, 实现了交易信息实时共享与查询, 有效地解决了物权争议与货物追踪问题.

关键词: 区块链; 铁路运输; 电子提单; 超级账本; 智能合约

引用格式: 肖梦雪, 左力, 徐志锬, 田金箫. 基于区块链的铁路电子提单系统. 计算机系统应用. <http://www.c-s-a.org.cn/1003-3254/8650.html>

Electronic Bill of Lading System Based on Blockchain

XIAO Meng-Xue¹, ZUO Li¹, XU Zhi-Kun¹, TIAN Jin-Xiao²

¹(School of Information Science and Technology, Southwest Jiaotong University, Chengdu 611756, China)

²(School of Computing and Artificial Intelligence, Southwest Jiaotong University, Chengdu 611756, China)

Abstract: As an important part of international logistics, the bill of lading can improve the efficiency of freight and capital circulation when applied to railway freight transportation. Faced with low security and insufficient credibility, the current electronic bill of lading system cannot guarantee the rights of participants. According to the decentralization, traceability, and programmability of blockchain, this study defines a framework of the electronic bill of lading system. Based on hyperledger fabric, the operation logic of electronic bill of lading, such as issuance, audit, circulation, and pledge is realized with multi-agency and multi-role participation in blockchain networks. The transaction information is stored on the chain and can be shared and queried in real time. In general, our work effectively solves the problems of property right and goods tracing.

Key words: Blockchain; railway freight transportation; electronic bill of lading; hyperledger fabric; smart contracts

铁路运输是国际贸易主要运输方式之一, 具有运量大、连续性高、风险小等优点. 传统的铁路物流票据是运单, 并不具有作为物权凭证的能力. 为确保货物贸易的顺利进行, 在跨境运输中采用具有物权凭证功能的多式联运“一单制”提单已成为必然趋势. 然而, 由于纸质提单存在流转成本高、速度慢、安全性低等问

题, 极大地影响了货物运输和资金流转的效率, 提单电子化已然成为提单发展的重要方向.

目前, 电子数据交换 (electronic data interchange, EDI) 技术^[1] 是提单电子化的主要途径, 然而, 基于 EDI 技术的电子提单系统存在以下弊端.

(1) 效率低. 数据信息的统计与分析都集中在 EDI

^① 基金项目: 成都市科技局技术创新研发项目 (2019-YF05-02059-GX)

收稿时间: 2021-11-26; 修改时间: 2021-12-22; 采用时间: 2021-12-28; csa 在线出版时间: 2022-05-31

网络中心进行,信息传输效率低。

(2) 安全性低.采用中心化的 B/S 或 C/S 架构,存在单点故障和数据篡改问题。

(3) 公信力低.文献 [2] 指出,EDI 系统中多机构、多地域间的信任只能依靠第三方机构建立,然而这类机构却很难在世界各地同时取得话语权与公信力.因此,在 EDI 系统中,提单不具有金融属性.这对电子提单跨机构、跨地域的审查和价值转移造成了阻碍。

而区块链技术具有去中心化、高透明度、去信任、不可篡改的特性,为上诉问题提供了有效解决方案.目前已经有学者对区块链技术应用于纸质提单电子化做了相关研究,如文献 [3,4] 都提出了在国际多式联运中使用电子提单的构想,阐明了基于区块链的电子提单系统的可行性.成都陆港公司推出了针对提单金融服务的区块链提单一点通,运用区块链的防篡改优势与金融机构银行等进行提单质押贷款交易,但仅限于公司与合作机构内部使用.因此,我们需要在此基础上拓展业务主体均使用的统一区块链电子提单,推动多式联运“一单制”的发展。

基于国际铁路物流迫切的落地需求和区块链技术的优势,本文首先参考现有铁路运单与纸质提单的功能与制式,设计了一套电子提单数据结构;其次,依据 EDI 系统电子提单流转模式^[5]与当前国际贸易规则,制定了物权转移业务逻辑;最后,实现了一个多方监管共同维护的区块链电子提单系统。

1 相关领域及技术介绍

1.1 电子提单

电子提单不同于以纸面为媒介的传统提单,其内容以电子数据的形式存在,可通过电子计算机通讯的形式传输.文献 [6] 指出,电子提单在《海上货物运输公约草案》中被定义为“可流通性电子记录”,具有与纸质提单等价的功能,包括:货物交付、运输合同证明、承运人接收货物证明、物权凭证与提单流转、抵押贷款与单据交易。

目前,铁路电子提单发展停留在纸质提单电子化阶段,其流转模式和相关法制还不成熟,缺少一个完善的电子提单国际贸易平台。

1.2 区块链技术

区块链 (Blockchain)^[7] 本质是一个去中心化的、不可篡改的共享账本.使用区块链技术在不可信网络

环境中构建多方信任的分布式系统,将为企业和用户提供更低的沟通整合成本和更高的业务效率.除此之外,国家的支持为基于区块链技术的电子提单的实施提供了政策保障.2016 年工信部发布了区块链白皮书^[7],2019 年国家互联网信息办公室发布了《区块链信息服务管理规定》,目前,区块链已上升为国家战略。

与传统的电子提单流转平台 EDI 系统相比,区块链技术具有以下优势:一是去信任,能够在多地区、多机构之间建立信任关系;二是去中心,区块链中数据分布式存储,边缘数据访问效率高;三是不可篡改与可追溯,能够解决货物溯源与物权归属问题;四是高透明度,链上所有信息和业务规则能被参与方监督和验证,合法用户可凭借链式结构追溯订单本源。

1.3 超级账本

超级账本 (hyperledger fabric)^[8,9] 是一种模块化可插拔的区块链实施方案,从逻辑上结合了 3 个范畴,即成员管理、区块链和智能合约 (链码).成员管理功能在准入型区块链中实现权限控制,而合法的参与者只能通过智能合约记账.智能合约^[10] 是参与方之间必须执行约定内容的协议,执行过程不需要第三方干预,能够避免任何参与方欺诈。

2 基于区块链的电子提单系统方案

2.1 系统整体框架设计

电子提单系统整体框架,由下至上分为基础技术层、系统核心层和应用层,如图 1 所示。

在基础技术层中,P2P 网络协议实现了事务数据传输和区块同步;TLS 协议实现了对交易信息的验证以及安全保密通信;LevelDB 数据库和 CouchDB 数据库则用于数据存储。

在系统核心层中,联盟管理者 MSP (member service provider) 进行联盟成员证书以及权限管理;海关和监察部门对合约执行结果背书,生成相应事务信息;共识节点集群接受事务信息,通过共识协议实现对区块的更新和同步。

在应用层中,智能合约定义了系统的业务逻辑,以网页的方式向用户提供服务,包括账户登录/注册、提单发布、金融质押等.其中,用户分为普通用户 (托运人、承运人、收货人)、金融机构和海关 3 种角色.各个角色具体职能如下。

托运方:发起托运请求,提供货物信息,向海关提

交申请, 向金融机构贷款还款.

承运方: 运输货物, 提供运输信息.

收货人: 向提单持有方汇款获得货物支配权, 从承运人处提货结束提单, 以及向金融机构抵押赎回.

金融机构: 提供供应链金融功能, 包括资金暂存与金融质押.

海关和检查部门: 对线上信息和线下货物实体的一致性进行核实, 在系统中更新提单审核信息.

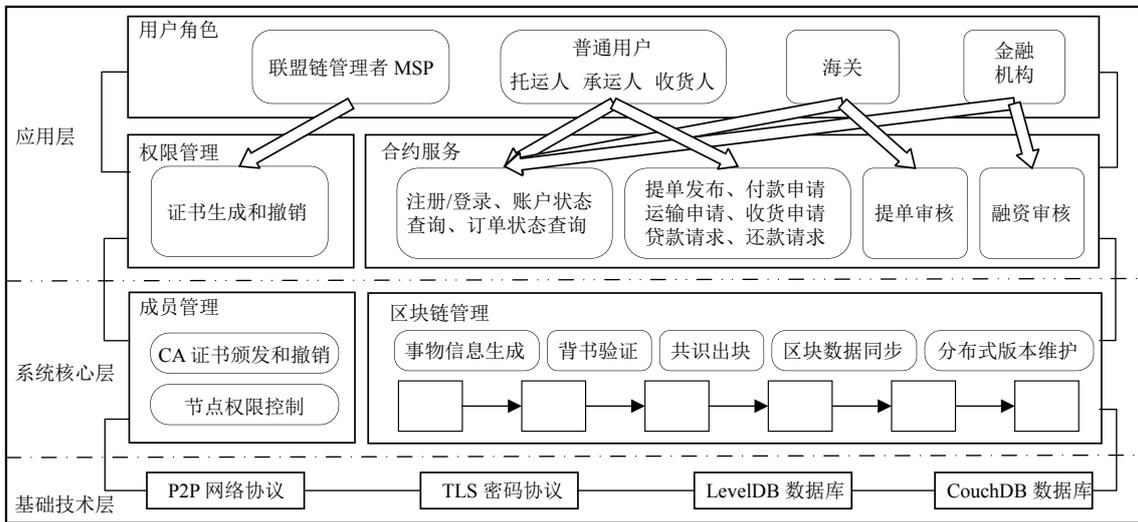


图1 电子提单系统整体框架

2.2 数据结构及业务逻辑设计

2.2.1 数据结构设计

参考《铁路货物运输国际公约》与《国际铁路货物联运协定》, 本系统设计了一套流通于电子提单平台的数据结构, 包括账户和提单两个部分.

(1) 账户用于保存用户信息, 其内容如表1所示. 系统为每个用户记录了一个账户, 内容包括用户ID、角色、货物质量、货运能力、资金以及身份证书的哈希值. 其中货运能力、货物、剩余资金等信息用于背书节点验证交易是否可被执行; 证书的哈希值用于验证交易发起者是否是资产持有人.

表1 账户数据结构

属性名	描述
UserID	用户标识符
Role	角色 (common、custom、banks)
Goods	货物质量
CarryCapacity	货运能力
Cash	资金
Hash	证书散列值

(2) 电子提单数据结构记录了交易的参与者、货物所需运力以及提单持有人的信息. 此外, 还记录了提单当前状态、审核状态和贷款抵押状态, 以及这些状态对应账户. 提单签发后, 用户可根据货物状态对提单

内容修改和更新, 提单操作将作为交易被打包上传至区块链, 具体结构如表2.

表2 提单数据结构

属性名	描述
BillID	提单编号
Shipper	托运人
Carrier	承运人
Consignee	收货人
Bank	金融机构
Goods	货物质量
DemandedCapacity	所需运力
Price	价值
CreationData	创建日期
ClosingDate	截单日期
AuditStatus	审核状态 (0未审核; 1已审核)
LoanApplications	贷款申请
LoanStatus	贷款状态
MortgageApplications	抵押申请
MortgageStatus	抵押状态
MortgageUser	抵押人
LoanUser	借贷人
FinishStatus	提单状态 (0发起; 1汇款; 2发货; 3运输; 4收货; 5银行结款, 正常结束; 9超时, 非正常结束)

2.2.2 物权转移业务逻辑设计

根据实际运输场景和物权转移流程, 基于区块链

与功能描述.

- 1) 首页: 实时更新区块, 提供区块查询功能.
- 2) 用户注册页面: 初始化账户.
- 3) 普通用户业务办理页面: 提供提单发布、付

款、发货、运输以金融质押等业务.

- 4) 海关审核页面: 提单审核. 海关以及检查部门在完成货物审核后, 通过该页面使提单生效.
- 5) 银行处理页面: 审核贷款、抵押业务.

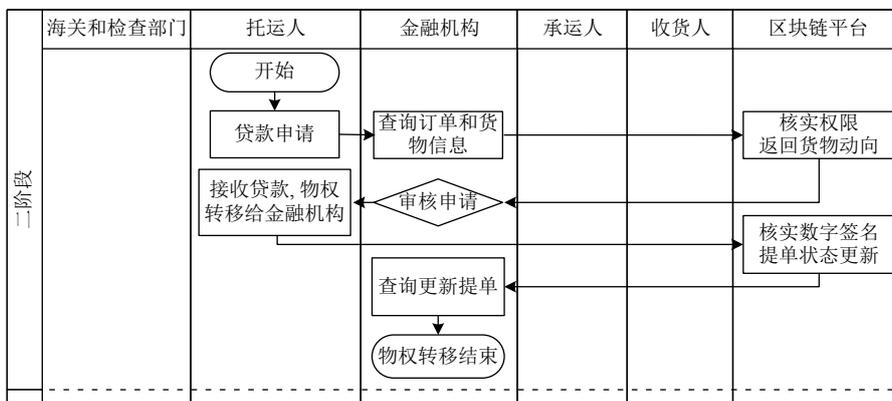


图4 金融质押流程图

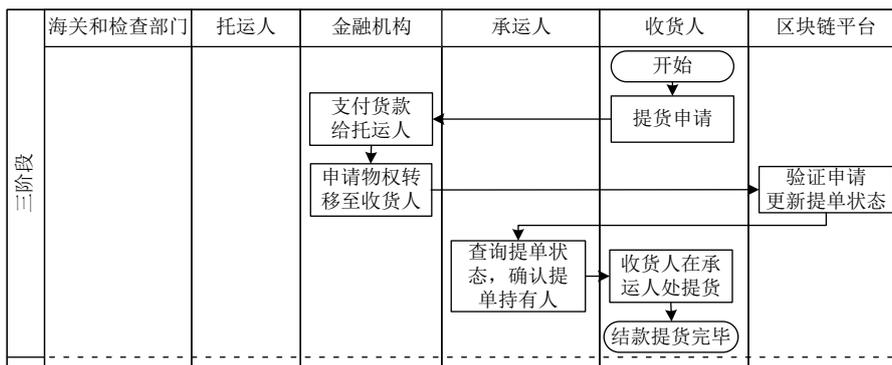


图5 结款提货流程图

(2) 基于区块链的电子提单系统后端

电子提单系统后端由 Gin 框架实现, Gin 是一个轻量级 HTTP Web 框架, 作用是创建路由引擎. 当网页发送请求某个路径时, 后端执行相应处理函数, 并返回结果至页面中. 其函数接口描述如表 3 所示.

表 3 后端函数接口描述

函数名称	功能描述	函数名称	功能描述
Install()	安装链码	InitCAAdmin()	创建管理员标识
Instantiate()	实例化链码	Register()	注册用户
QueryAccount()	查询账户信息	HistoryQuery()	查询区块记录
QueryBill()	查询提单信息	BlockQuery()	查询区块信息
IssueBill()	发起新提单	FinishBill()	结束提单

(3) 区块链网络

电子提单系统运行在一组经过认证的参与者之间,

每笔交易都包含发起者的证书, 区块链管理者可凭此进行交易追溯. 故系统的可监管性强, 参与者带来的风险较低. 基于此情况, 本论文考虑构建部分同步通信模型, 要求系统能够容忍故障错误. 具体的软件环境配置信息如表 4 所示, 在实现时, 使用超级账本提供联盟链网络, 底层配置为 Raft 共识算法、Gossip 数据分发协议以及 LevelDB 数据库. 在应用层, 通过编写智能合约, 实现电子提单系统的业务逻辑, 智能合约函数接口描述如表 5 所示.

在数据交互方面, 区块链网络、后端与前端之间的数据传输如图 6 所示. 前端网页发送请求参数至服务器, 服务器提交参数至区块链网络中的系统链码、Fabric CA 或用户链码, 并将请求结果返回给前端.

表 4 软件环境配置信息

软件环境	详细信息
OS	Ubuntu 16.04
Hyperledger Fabric	1.4.4
Docker	19.03.1
Docker-Compose	1.25.0-rc2
Go	1.12

表 5 智能合约函数接口描述

函数名称	功能描述	函数名称	功能描述
Invoke()	智能合约入口	PutAccount()	数据上链
Register()	账户注册	Deliver()	更新状态为发货
QueryAccount()	查询账户信息	Loan()	贷款申请
QueryBill()	查询交易提单信息	Payload()	还款申请
IssueBill()	发起新的提单	Transport()	更新状态为运输中
Remit()	更新状态为已汇款	Receipt()	更新状态为已收货
Mortgage()	抵押申请	Paymortgage()	赎回申请
CheckBill()	审核订单	CheckLoan()	银行业务审核
FinishBill()	更改订单为结束	CheckRole()	验证用户身份

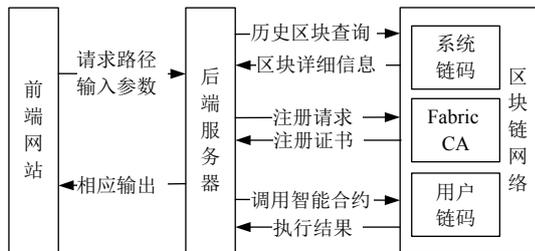


图 6 系统数据交互图

图 7 为提单发布页面, 托运人需提供托运人 ID、承运人 ID、收货人 ID、货物信息等, 提交成功后系统将返回该提单 ID。图 8 为海关审核页面, 海关提供提单 ID 与自己的用户 ID 完成货运提单的审核。其他页面操作与海关审核页面类似, 使用提单 ID 和账户 ID 即可完成交易与查询。

3.2 系统测试与分析

(1) 测试环境及配置

该系统中节点可分为对等节点 (Peer)、排序服务节点 (Orderer)、以及证书颁发机构 (CA)。其中 Peer 节点负责交易的执行、背书与验证; Orderer 节点采用 Raft 协议保持一致性, 组成共识集群, 负责交易的打包与排序; CA 节点负责证书颁发。为实现物流信息数据共享及物权价值多方认可, 在实际中, 节点分布于多地区, 其中 Orderer 节点由海关和检查机构管理。

在系统的可用性及交易处理能力测试中, 使用 Docker 集群部署 Peer 与 Orderer 两类节点, 并为这些节点配置了证书。此外, SDK 为上层应用, 能够调用智能合约。具体部署情况如表 6 所示。

BILL

Please fill all the texts in the fields.

User:

Shipper:

Carrier:

Consignee:

Bank:

Goods:

CarryCapacity:

Cash:

图 7 用户注册页面

CHECK BILL

Please fill all the texts in the fields.

User:

Bill ID:

图 8 海关审核页面

表 6 性能测试环境

服务器地址	CPU×内存 (GB)	运行服务
192.168.1.104	56×64	Orderer0
192.168.1.105	56×64	Orderer1 Peer.Org0 SDK
192.168.1.107	56×64	Orderer2 Peer.Org1

同时, 为满足实际应用需求, 限制区块所含最大交易数为 100, 单个交易最大为 98 MB, 出块时间不超过 2 s。

(2) 测试内容及测试结果

在容错能力方面, 共识集群采用 Raft 协议, 可容忍的故障共识节点数为总共识节点数的 50% 以内, 用户读写具有强一致性, 符合应用需求。

在性能方面, 测试内容为提单发布 (Invoke) 业务性能与账户查询 (Query) 业务性能, 指标包括每秒交易数 (TPS)、每秒查询数 (QPS) 与平均响应时间 (ART)。

可见, 随着并发数增加, 平均响应时间增长, TPS、QPS 增加。如图 9, 当并发数为 1200 时, 系统 TPS 最大, 为 182.1 s⁻¹; 当并发数为 1000 时, 系统 QPS 最大, 为 6310.3 s⁻¹, 符合一般业务场景对并发数的需求。在最大

并发数下, 提单发布业务与账户查询业务的平均响应时间分别为 5.616 s 和 0.517 s, 处于用户普遍可容忍等待时间内, 满足提单业务办理的普遍要求。

并且, 随着并发数的增加, 系统 CPU 占用率与内存占用率皆 < 20%, 在正常范围内, 区块链电子提单系统能够在订单量突增情况下正常处理业务办理请求。

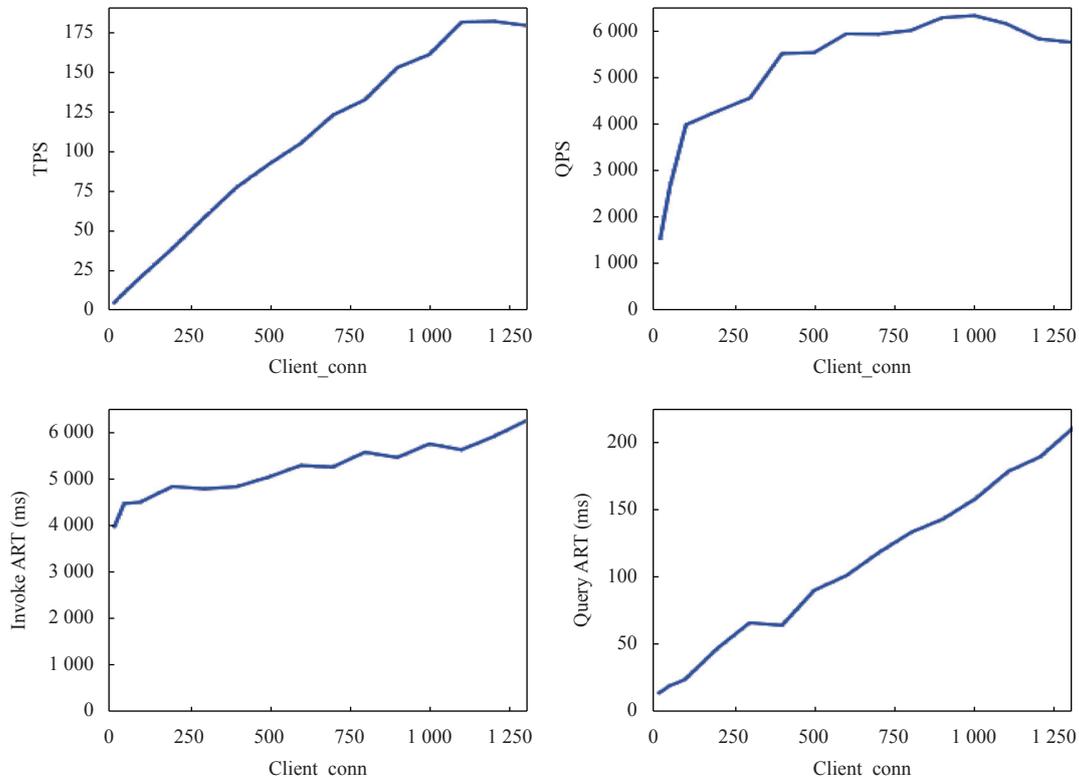


图9 性能测试结果

4 结语

区别于传统电子提单系统, 本文设计并实现了具有去信任、防篡改、可溯源特性的电子提单平台, 使用统一制式实现了电子提单“一单制”。该平台中的电子提单具有物权属性, 提供了一套适用于区块链的提单流转与质押流程。此外, 经测试该系统性能满足铁路货运需求。

本文着重研究基于区块链的电子提单系统基础性设计与实现方案, 旨在为当前多机构、多地域的铁路运输业务提供技术支撑。同时, 这也是对未来电子提单系统进一步发展的前沿性探索。

参考文献

- 李俊, 吴国新. 基于 EDI 的单证交换系统. 计算机应用, 1997, 17(6): 24-27.
- 马连良. 电子提单在国际贸易中存在的问题与对策. 对外经贸实务, 2018, (10): 62-65. [doi: 10.3969/j.issn.1003-5559.2018.10.015]
- 邢虎松, 邓元慧. 区块链技术在提单电子化领域的应用研究. 生产力研究, 2019, (6): 77-83. [doi: 10.19374/j.cnki.14-

1145/f.2019.06.012]

- 刘昱刚, 王添碧, 王海玥, 等. 基于区块链技术的多式联运电子提单研究. 交通运输系统工程与信息, 2018, 18(S1): 74-79. [doi: 10.16097/j.cnki.1009-6744.2018.Sup.1.011]
- 纪臻. 电子提单流转模式之对比研究 [硕士学位论文]. 济南: 山东大学, 2013: 1.
- 王传丽. 国际贸易法. 北京: 中国政法大学出版社, 2009.
- 周平. 中国区块链技术和应用发展白皮书. 北京: 工业和信息化部, 2016.
- Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. Proceedings of the 13th EuroSys Conference. Porto: ACM, 2018. 30. [doi: 10.1145/3190508.3190538]
- Cachin C. Architecture of the hyperledger blockchain fabric. Workshop on Distributed Cryptocurrencies and Consensus Ledgers. 2016.
- Szabo N. Smart contracts: Building blocks for digital markets. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html, 1996.

(校对责编: 牛欣悦)