基于区块链的数据资产保护与交易平台研究及应用

Research and Application of Data Asset Protection and Trading Platform Based on Blockchain

夏俊杰[1]，孙　晔[1]，杨海涛[1]，陈　昌[2]（1. 北京电信规划设计院有限公司，北京 100044；2. 西安纸贵互联网科技有限公司，陕西西安 710000）

Xia Junjie[1]，Sun Ye[1]，Yang Haitao[1]，Chen Chang[2]（1. Beijing Telecom Planning & Designing Institute Co.，Ltd .，Beijing 100044，China；2. Ziggurat Internet Technology，Xi'an 710000，China）

摘　要：

针对现有网络系统数据共享所面临的数据权属难确认、数据安全难保障、数据共享效率低等挑战，提出了一种基于区块链技术的数据资产保护与交易平台。通过引入区块链技术，可以有效确认数据权属，提升数据系统的安全性与可靠性，同时保证数据共享效率。经测试，平台可以支持每秒2 000次以上的数据操作；同时保证在1/3以下节点故障或遭到恶意攻击的情况下，维持整个系统的正常工作。基于区块链的数据资产保护与交易平台，为未来智慧城市、数字工程等系统构建了数据治理的底层平台。

关键词：

区块链；数据治理；安全访问控制；数据交易；数据确权

doi：10.12045/j.issn.1007-3043.2019.09.002

中图分类号：TP309

文献标识码：A

文章编号：1007-3043（2019）09-0005-05

Abstract：

Aiming at the challenges in the existing digital network system，a data asset protection and trading platform based on blockchain technology is proposed，such as data identification，data security and data sharing. By introducing blockchain technology，data ownership can be effectively confirmed，the security and reliability of the data system can be improved，and data sharing efficiency can be ensured. Experimental results show that the platform can support more than 2 000 data operations per second，while maintaining the normal operation of the entire system in the event of crash failure or malicious attack on less than one-third of the nodes. This blockchain-based data asset protection and trading platform will help to build the underlying data governance platform for future smart cities and digital engineering systems.

Keywords：

Blockchain；Data governance；Access control；Data transaction；Verification of data ownership

引用格式：夏俊杰，孙晔，杨海涛，等. 基于区块链的数据资产保护与交易平台研究及应用[J]. 邮电设计技术，2019（9）：5-9.

1 背景

1.1 区块链技术背景

区块链技术的诞生是记账方法演化到分布式场景下的天然结果。现代会计学通常采用的复式记账法最早在1494年提出，将每笔交易分别在来源方和目标方2个科目进行记录，引入对账验证功能。这本质上仍是中心化的记账方式，账本掌握在单个个体手中。随着计算机和网络技术的快速发展，记账数据量增大、记账个体增多，衍生出了以区块链为代表的分布式记账方法，用于解决众多个体共同维护同一个账本、合作完成记账的问题。

如图1所示，区块链是一种以区块为基本单位的链式数据结构，区块头中利用数字摘要对之前的交易历史进行校验，适合分布式记账场景下防篡改的需求。狭义上，区块链作为一个数据结构没有兼顾安全性、隐私、扩展性等需求，因此在实践中常常结合数字证书、加密等安全保护方法，同态、零知识等隐私保护方法。广义上，区块链指代基于区块链数据结构实现的分布式记账技术，包括分布式共识、隐私与安全保护、点对点通信、智能合约等。

1.2 数据治理技术背景

数据作为现代企业的新型重要资产，往往未被充分利用，还会受到诸如数据安全事故、数据泄露、数据

收稿日期：2019-07-16

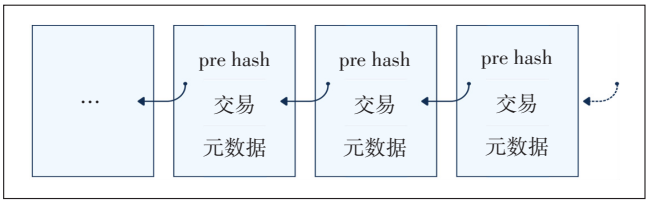

图1　区块链数据结构

造假、数据权属不明等问题困扰。针对这些问题，数据治理是将数据作为资产而展开的一系列具体化工作，是对数据的全生命周期管理，是企业实现数据价值的基础。

从数据生命周期的角度，数据治理需要解决三方面问题。

a）数据产生过程中，保障数据的真实性。既要从数据源头确保真实性，也要保证数据记录未篡改和可追溯。

b）数据交换和流通过程中，确保数据安全并保护隐私。数据开放、跨界共享是充分发挥数据潜能的大趋势，但安全的数据流通机制需要解决数据所有权如何确认、流通路径如何控制、如何避免数据被未授权使用、如何避免泄露隐私等问题。

c）对数据价值的有效实现。由于数据的价值具有时空相关性，且在动态变化，因此需要有衡量数据价值的有效手段。

2 区块链技术架构

2.1 整体架构

区块链系统的整体架构如图2所示，主要包括底层通信网络、区块链核心模块和上层接口3个部分。

底层通信网络是由多节点组成的点对点（P2P）网络，通过gRPC通道交互，通过Gossip协议进行数据同步。

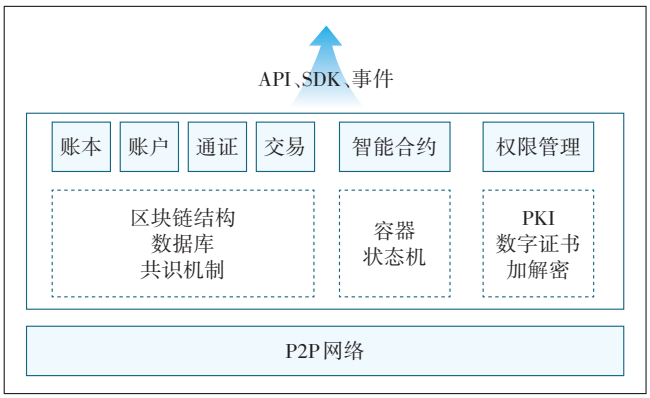

图2　区块链系统整体架构

底层之上为系统核心模块。账本、账户、通证、交易模块依赖区块链结构、数据库、共识机制等技术；智能合约依赖容器、状态机等技术；权限管理利用了公钥基础设施（PKI）、数字证书、加解密算法等安全技术。

上层是面向分布式系统和应用开发提供的应用程序编程接口（API），并设计实现访问和管理区块链资源的软件开发工具包（SDK）。此外，应用侧可以通过订阅和监听事件来获取交易执行、区块生成等信息。

2.2 核心模块

区块链系统的核心模块主要包括账本、账户、通证、智能合约、交易、共识机制等部分。

账本：包括区块链结构和多个数据库结构（包括状态数据库、历史数据库、索引数据库）。其中，区块链结构中的每个区块记录一段时间内发生的所有交易和状态结果，是对当前账本状态的一次共识；区块链结构由区块按照发生顺序串联而成，记录整个账本状态变更的历史；状态数据库记录变更的最终结果。

账户：账户由地址唯一标识。终端用户可自行生成唯一私钥，单向推导出公钥与地址。终端用户构造的交易需要指定发起账户，并用账户所属私钥签名，私钥保存在专有的安全硬件之中。每个账户可拥有多种通证，并记录在账本上。

通证：通证主要分为权限通证与权益通证2种类型。其中权限通证用于确定用户是否有权访问特定数据或获取数据服务，用户通过特定类型的权限通证，获取相应的数据或数据服务；权益通证是用户对数据资产保护与交易平台贡献度的衡量，通过提供数据或数据服务获得权益通证，通过消耗一定数量的权益通证获取数据或数据服务。

智能合约：由开发者编写的无状态的、事件驱动的代码。智能合约对外暴露若干接口，对应用发出的交易做出响应，执行代码逻辑，与账本进行交互。项目平台支持拥有权限的角色进行智能合约的升级。

交易：一次对账本的操作，导致账本状态的一次改变。如转移通证、调用智能合约等。

共识机制：共识过程表示多个节点对于一批交易的发生顺序、合法性、对账本状态的更新结果达成一致的观点。

2.3 交易流程

无论是平台上数据的确权、访问控制还是共享，都会涉及到对底层区块链账本的操作。这种对账本状态的改变，被统称为交易。典型的区块链交易处理过程

如图3所示。

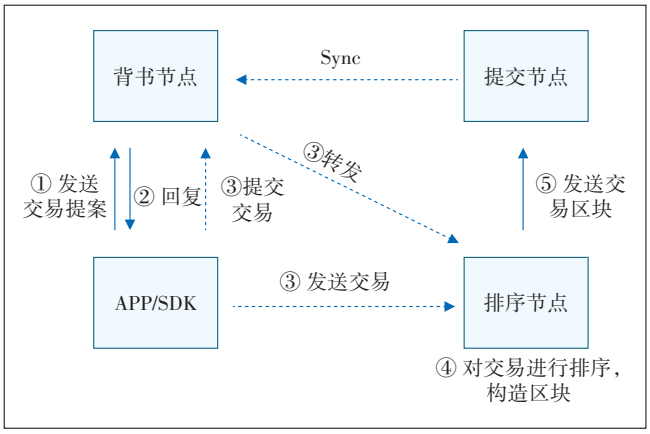

图3　典型区块链交易处理过程

上层平台系统对链的操作指令，通过SDK完成。SDK发送的交易提案（Signed Proposal）包含通道编号、智能合约和参数、提交方身份签名、发起用户签名。

背书节点收到交易提案后，需要校验提案结构完整性、提交方身份签名、交易编号合法性、是否满足通道要求、发起用户签名与计数器等，模拟执行交易（包括读写集和用于通证的转移集）并对结果签名，构造提案回复（Proposal Response）。

SDK需要校验收到的提案回复，并比对多个背书节点的回复结果，同时检查是否收集足够背书。收集足够背书后将构造完整交易结构，发送给排序节点。

排序节点新生成的区块中包含排好序的一批次交易。提交节点需要进行交易的逐个检查，并确定合法交易对状态的更新值。具体的检查包括交易结构完整性、签名、编号等；还需对交易的读集做验证，对转移集的转出方做余额检查。最后，根据所有合法交易更新账本状态。

3 平台介绍

基于上述的区块链相关技术及架构，开发了基于区块链的数据治理平台系统。系统体系架构分为5层，自下而上分别是基础设施层、网络层、合约层、服务层、展示层。体系架构如图4所示。

基础设施层提供系统运行的底层资源支持，包括物联网（IoT）设备、网络资源、存储资源、安全设备等硬件设备资源。其中，IoT设备负责数据的采集；网络资源可以根据实际部署情况采用互联网或者专网，对于有数据隐私要求的部署环境，可以采用专网；存储资源根据使用的服务器类型不同可以分为私有服务器和云

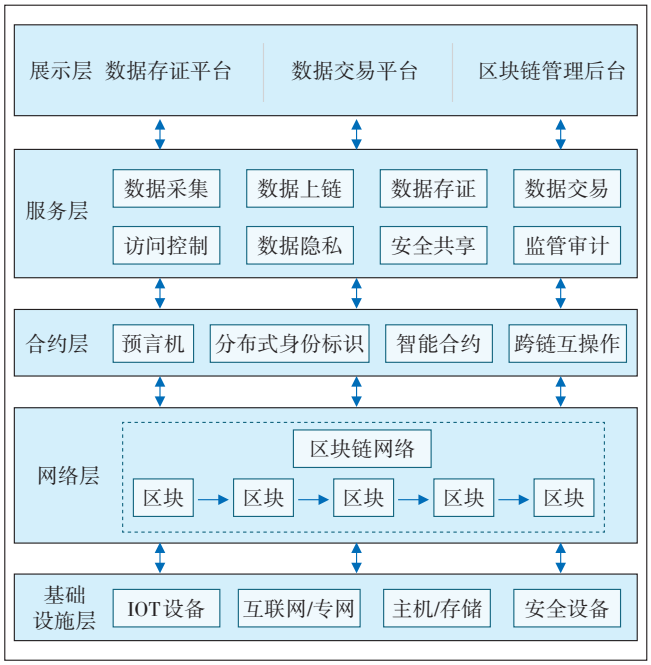

图4　区块链数据治理平台架构

服务器，区别同样在于数据隐私的要求程度。基础设施层还包括安全设备等其他硬件，用于保护底层网络系统的安全性。

网络层提供系统构建的基础区块链网络，区块链采用基于Hyperledger Fabric的联盟链网络方案，覆盖大部分业务场景的需求；区块链网络通过区块链适配器将不同底层的接口统一在同一协议框架下适配，通过向下兼容不同底层、向上提供统一接口的方式，节省上层业务服务的集成开发成本。

合约层通过智能合约实现上层应用对链上数据、业务的调用。主要包含的技术有预言机技术、分布式身份标识、跨链互操作等。

服务层为展示层提供相应的接口支持，提供一系列基于区块链技术的数据服务，包括数据采集、数据上链、数据存证、数据交易、访问控制、数据隐私、安全共享、监管审计等，实现数据从物理世界到区块链网络到全生命周期流转服务，保证整个流程中数据的真实性、安全性、隐私性、可审计。

展示层通过可视化界面的形式与平台使用者、网络管理员进行人机交互，主要包括数据存证平台、数据交易平台、区块链管理后台。数据存证平台用于数据的采集、上传、存证，并通过预言机技术生成验证证书，供相关审计工作使用；数据交易平台用于数据的交易与安全共享，基于区块链智能合约，实现跨主体之间的数据安全交易与协作，保证交易过程的不可篡改，保护

数据的隐私安全；区块链管理后台则用于管理链上网络状态，支持动态调整网络配置，监控网络节点运行状态等功能。

系统包括区块链网络管理员、数据管理员和超级管理员3类g角色。面向不同角色的系统功能架构如图5所示。

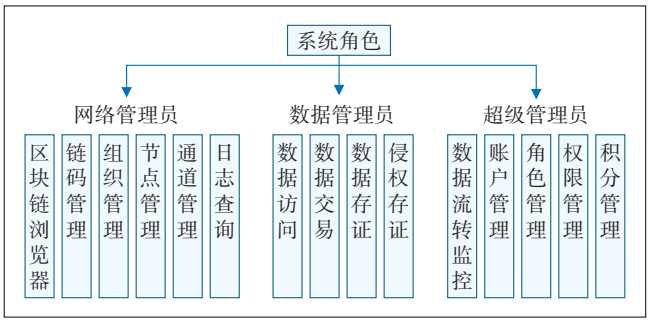

图5　系统角色架构

面向区块链网络管理员，系统支持区块链浏览器、链码管理、组织管理、节点管理、通道管理、日志查询功能。区块链浏览器用于监测区块链网络的整体配置情况以及区块链上的交易及区块详情；链码管理用于在区块链上安装、部署智能合约；组织管理用于新增、管理链上组织，每一个组织代表一个机构或企业实体，不同实体之间的文件、用户、积分等的数据互通均以组织为单位进行；节点管理用于新增、管理链上节点，支持动态查看节点的运行状态，对宕机节点及时进行故障维护；通道管理用于新增、管理链上的通道，每一个通道代表由多个组织组成的链上联盟，用于实现同一区块链上的数据隐私管理；日志查询支持常规的操作与运行日志查询。

面向数据管理员，系统支持数据访问、数据交易、数据存证、侵权存证功能。数据访问功能会根据管理员的权限等级来显示密级不高于管理员权限的数据文件，支持管理员查看数据的名称、哈希值、描述、作者等相关信息。数据交易功能支持以积分形式购买数据文件以及对申请制的数据下载，数据交易完全在区块链上完成，交易结果记录在区块上，不可篡改。数据存证功能根据管理员不同的权限等级支持上传不同密级的数据，上传的数据会即时生成哈希值，并将哈希值保存在区块链上，生成存证信息，包括存证区块哈希等信息。侵权存证功能支持从侵权网站固化侵权证据，基于预言机技术完成侵权页面的存证、哈希上链以及证明文件生成。

面向超级管理员，系统支持数据流转监控、账户管理、角色管理、权限管理、积分管理功能。数据流转监控功能为管理提供全平台数据上传、存证、交易、下载等流程中用户的每一个操作的信息记录，用于监管操作的规范性与安全性。账户管理功能支持管理添加用户、审核并修改用户信息、为用户分配权限、为用户转账积分，提供对平台用户的完善管理工具。角色管理功能用于设置平台上角色，角色用于表明用户权限与身份，不同角色的权限需要管理员在平台配置。权限配置功能提供多个维度的平台使用权限细分，管理员根据实际需求将细分权限汇总成权限集合，再分配给角色作为该角色所具有的权限。积分管理功能主要实现对链上流转积分的总量、分配方式、增发方式等经济模型的宏观调控，保证积分的价值稳定。

系统基于Hyperledger Fabric联盟链搭建，同时搭载了Oracle预言机技术、DID分布式身份标识技术与跨链互操作技术，具备高安全、高并发、可扩展等特性，在资产登记和流转、共识优化、隐私保护、行为监管、跨链交互等方面具备先进优势。

4 平台测试结果

数据治理平台系统的测试主要从压力测试、高并发测试、低负载测试等方面展开，总体测试结果表明，在采用24C128G配置的服务器、万兆宽带网、Kafka共识机制和ECDSA密码学算法的情况下，压力测试持续运行1 h以上系统维持正常运行，高并发测试的tps均达到2 000以上，长期测试正常运行1个月，日均交易8 779笔。

a）压力测试：分别在4节点、8节点、16节点的压力测试场景（3种场景的配置如表1所示）下测试了治理平台系统的运行状况。在区块链平台测试环境中，持续保持未处理交易在1 000以上，系统持续运行1 h，未出现故障，且能正确处理性能范围内的交易。表2和表3列出了4节点情况下的具体测试结果，在测试过程中，共完成了359 976笔交易，吞吐量达到2 345 tps。

表1　压力测试系统配置

场景	共识节点数/个	背书节点数/个	提交节点数/个
4节点	4	2	2
8节点	8	4	4
16节点	16	8	8

b）高并发测试：在区块链平台测试环境下，在1 s内发送5万笔交易请求，交易包括不同的类型，包括数

表2　性能指标

名称	成功	失败	发送频率/tps	结果/tps
transfer	359 976	0	2 951	2 345

据存证、数据确权、数据交易、身份认证等。在高并发的情况下，吞吐量达到了2 235 tps，且对每一种交易类型的支持吞吐量较为平均。

c）长期运行测试：构建了常规的数据治理系统，由6节点组成，部署了2个链码，支持数据存证与数据交易2种常规功能，经过累积一个月的系统常规运行，共生成了412 019个区块，记录交易422 854笔，日平均交易约为8 779笔，在此期间，系统运行正常无宕机情况出现，低负载运行效果良好。

表3　资源消耗

类型	名称	内存(最大)	内存(平均)	CPU(最大)/%	CPU(平均)/%
Process	node local-client.js(avg)	148.2 MB	133.0 MB	98.28	73.12
Docher	192.168.1.128/multiplehos...com_1	7.9 MB	7.3 GB	211.12	150.98
Docher	192.168.1.130/multiplehos…com 1	7.7 GB	7.2 GB	185.68	133.20
Docher	192.168.1.127/multiplehos…com 1	9.9 GB	9.0 GB	946.98	713.61
Docher	192.168.1.125/multiplehos…com 1	10.0 GB	9.2 GB	1 000.33	761.74
Docher	192.168.1.121/multiplehos…ka1 1	999.3 MB	999.1 MB	1.75	0.79
Docher	192.168.1.121/multiplehos…er1 1	644.8 MB	641.0 MB	14.84	0.87
Docher	192.168.1.120/multiplehos…ka0 1	404.7 MB	404.6 MB	0.80	0.37
Docher	192.168.1.120/multiplehos…er0 1	573.6 MB	562.6 MB	16.85	0.93
Docher	192.168.1.122/multiplehos…ka2 1	9.0 GB	8.4 GB	172.22	122.51
Docher	192.168.1.122/multiplehos…er2 1	393.0 MB	390.0 MB	7.17	0.40
Docher	192.168.1.126/multiplehos…com 1	10.1 GB	9.3 GB	937.56	723.27
Docher	192.168.1.126/multiplehos…ca1 1	18.7 MB	18.7 MB	0.00	0.00
Docher	192.168.1.124/multiplehos…ca0 1	5.8 MB	5.8 MB	0.00	0.00
Docher	192.168.1.124/multiplehos…com 1	9.8 GB	9.1 GB	854.39	640.52
Docher	192.168.1.123/multiplehos…ka3 1	440.4 MB	440.4 MB	0.86	0.42

上述测试表明，基于区块链的数据资产保护与交易平台，在高负载、高并发、长期运行等条件下，均能够正常、安全工作，且系统性能满足上层应用的需求。

5 未来展望

基于区块链的数据资产保护与交易平台，为智慧城市、数字工程等系统构建了数据治理的底层平台。在实际的应用过程中，该平台一方面需要进一步完善其功能，构建数据采集、传输、存储、确权、访问控制、交易、隐私保护、安全共享与监管等全生命周期的数据治理能力；另一方面需要与实际应用场景紧密结合，在电子政务、商品溯源、供应链管理、数据监管等领域，发挥更大的作用。

参考文献：

[1] PACIOLI L. Summa de Arithmetica geometria proportioni：et proportionalita[M]. Paganino de paganini，1994.

[2] 杨保华. 账本科技演化录[J]. 清华金融评论，2018(2)：97-99.

[3] 李兴欣. 区块链技术在我国银行支付清算应用研究[D]. 北京：北京邮电大学，2018.

[4] 杨保华，陈昌. 区块链原理，设计与应用[M]. 北京：机械工业出版社，2017.

[5] 顾芳，刘旭峰，左超. 大数据背景下运营商移动互联网发展策略研究[J]. 邮电设计技术，2012(8)：21-24.

[6] 韩晶，张智江，王健全，等. 面向统一运营的电信运营商大数据战略[J]. 电信科学，2014，30(11)：154-158.

[7] 朱洁，罗华霖. 大数据架构详解-从数据获取到深度学习[M]. 北京：电子工业出版社，2016.

[8] CACHIN C. Architecture of the hyperledger blockchain fabric[C]// Workshop on distributed cryptocurrencies and consensus ledgers，2016：310.

[9] Decentralized Identifiers(DIDs)：Data Model and Syntaxes for Decentralized Identifiers[EB/OL]. [2019-03-29]. https://w3c-ccg.github.io/did-spec/.

作者简介：

夏俊杰，毕业于南京邮电大学，北京电信规划设计院副院长、总工程师，长期从事互联网、国际国内标准化研究、技术研发以及咨询设计等工作；孙晔，毕业于伦敦帝国理工学院，北京电信规划设计院综合业务部创新业务总监，硕士，主要从事区块链解决方案的设计与其在智慧城市，智慧园区等场景的落地应用工作；杨海涛，毕业于北方交通大学，高级工程师，主要从事智慧城市顶层设计、移动通信网络规划等工作；陈昌，毕业于清华大学，纸贵科技有限公司CTO，硕士，负责金融区块链技术解决方案的架构设计和实施。