面向大数据的区块链在清算系统中的应用

蔡维德[1,2,3]，郁莲[4]，袁波[2]，邓佑权[2]，李琪[1]，郭斌[1]
1. 北京航空航天大学数字社会与区块链实验室，北京 100191；2. 北京天德科技有限公司，北京 100080；
3. 亚利桑那州立大学，美国亚利桑那州 菲尼克斯 85287；4. 北京大学软件与微电子学院，北京 102600

摘要
介绍面向大数据的区块链在清算系统中的应用实践，内容涉及区块链共识、区块链交易数据安全传输、区块链数据存储、区块链数据查询、交易数据加解密以及清算核心业务等方面，重点分析了大数据版区块链在清算过程中对复合交易进行拆解合并的架构设计，并从大数据分析层面提出对区块链上的数据做风险决策与评估的潜在价值和重要意义。

关键词
大数据；区块链；共识机制；密码学；清算系统

中图分类号：TP31 文献标识码：A doi: 10.11959/j.issn.2096-0271.2018003

Big data-oriented blockchain for clearing system

TSAI Wei-Tek[1,2,3], YU Lian[4], YUAN Bo[2], DENG Youquan[2], LI Qi[1], GUO Bin[1]
1. Digital Society & Blockchain Laboratory, Beijing University of Aeronautics and Astronautics, Beijing 100191, China
2. Tiande Technologies Co., Ltd., Beijing 100080, China
3. Arizona State University, Phoenix 85287, USA
4. School of Software and Microelectronics, Peking University, Beijing 102600, China

Abstract
The big data oriented blockchain for trade clearing was introduced, including consensus, secure transmission of trading data storage, data search, encryption and decryption of trading data and trade clearing business. The analysis of the framework design on dismantlement and combination of the composite trading was emphasized, and the potential value and significant meaning of blockchain data on risk decision and assessment through the big data analysis were identified.

Key words
big data, blockchain, consensus mechanism, cryptography, clearing system

1 引言

2008年10月31日中本聪发表了比特币论文[①]，首次提出了区块链概念，伴随比特币的区块链技术在近年来得到了长足发展，研究和使用区块链技术已经成为行业创新和转型的重要驱动力。本文涉及的清算系统使用的是天德大数据版区块链，为了检验这套系统的可靠性与准确性，笔者与某清算所联合展开为期一个月的实地测试，共计使用原始脱敏交易数据33.34亿笔，产生200多亿笔原子交易，充分验证了整套系统的安全性、可靠性与正确性。

本文涉及的清算是指从交易到结算的所有活动，其中交易数据的清算逻辑采用实用拜占庭容错（PBFT）算法，不仅可以检测故障，同时可以检测作弊。清算数据可通过区块链进行溯源取证，清算过程和结果的真实性得到了保证。同时，在数据安全访问方面采用公钥私钥加密解密（RSA、ECC、SM2），SHA、ECDSA数字签名，CA数字证书等方式，保证数据传递和存储的安全。

笔者在后文结合天德大数据版区块链在清算系统中的应用案例，讨论和分析大数据版区块链在清算过程中对复合交易拆解、合并的设计方法以及将区块链数据持久化存储到大数据平台的过程，最后提出应从区块链大数据中发掘有价值信息，这为监管部门洞察交易数据提供了一个新的方向。

从2015年到2017年，世界上包括银行在内的许多机构、金融专家都认为清算是区块链的一个重要应用，可是一直没有机构做出来，或者即使做出来，结果也不甚满意。甚至到2016年底，部分金融专家开始改变说法："清算不是区块链的专长，区块链可能不适合做清算"[②]。然而，2017年4月，中国团队创建了大数据版的区块链，并成功应用在清算的实践中。

清算的困难在于：数据量庞大；分账、对账处理必须正确；隐私保护要求高；系统处理性能要求高；系统安全性要求高；记账方式复杂多样。

一般区块链（如比特币和以太坊区块链）不能高速地处理大规模海量数据，且性能慢（一秒处理不到20笔交易），不能保护隐私。目前大部分银行用余额记账，有些区块链用未花费的交易输出（unspent transaction output，UTXO）记账，余额查询复杂，不适用于银行业务。中国团队的成功有以下几个重要原因。

- 做出大数据版的区块链，使用大数据平台处理清算中的海量数据（而不是用普通数据库），数据存储规模支持横向扩张，自动三备份，增强单点容错性，多服务器并发处理。
- 将一个复合交易分解为6个原子交易，而不是直接处理复杂、原始的交易，简化了清算流程。这项工作很重要，因为如果没有进行原子化交易的分解操作，区块链数据即使分片，也很难提高性能。一个交易可能会涉及6个及以上的账户，但这些账户可能会在不同分片上，如果一起处理，参与的分片可能要互相等待，导致分片后的区块链性能无法大幅提高。如果分开处理，每个原子交易就可以在一个分片上单独处理，每个分片不互相干扰，并且可以并行处理。这样就解决了以太坊没有解决的问题，因为以太坊提出的数据分片方法虽提高了性能，但未分解交易。在商品交易上，一个商品交易需要分解为6个原子交易，但信用卡等交易可能会涉及更多账户。
- 采用多链式架构（而不是用单链架构）保护隐私，并且简化区块链架构。
- 采用账户链—交易链（ABC-TBC）熊猫模型架构完成负载均衡的机制，保持

① https://www.bitcoin.org/bitcoin.pdf

② https://www.coindesk.com/nowhere-near-web-blockchain-adoption-sees-debate-mit-event/

系统的性能。

● 采用余额记账，与现有的银行账户系统兼容，方便与银行和金融机构对接服务。

2 大数据版区块链技术体系架构

本文涉及的区块链技术基于天德大数据版区块链技术体系架构，该架构共分5层，分别是：存储层、核心层、服务层、接口层和应用层③，如图1所示。

③ http://www.tdchain.cn/download/writepaper.pdf

④ http://www.tdchain.cn/download/jbcc.pdf

2.1 存储层

存储层包含区块链数据缓存、区块链数据存储和读写分离模块，本文主要介绍基于大数据平台的区块链数据存储。其内容包括区块数据、链式结构、HBase存储优化技术等。Hadoop框架是一个可靠、可扩展的分布式开源计算框架，HBase是基于Hadoop平台之上的一种分布式列式高维数据库，可扩展性高、吞吐量大、容错能力强、支持动态扩容、支持高并发高速读写，且可以根据业务需求方便地建立多级索引表，为检索区块链上的数据提供灵活的操作方式和良好的性能。

2.2 核心层

核心层包含建块预处理模块、共识机制模块、信誉机制模块、块同步模块、交易验签模块、节点签名验签模块、验证节点管理模块。

2.3 服务层

服务层包含账户链（ABC）、交易链（TBC）和链上代码，ABC负责存储和维护账户信息，TBC负责执行交易和维护交易历史。

2.4 接口层

Java区块链连接器（Java blockchain connector，JBCC）不仅是天德区块链（TDBC）对外服务的接口，也是行业应用与区块链之间的沟通桥梁。JBCC提供创建交易链、创建用户链、插入交易、查询链信息、查询交易信息、获取身份证书、获取交易证书等功能，目的在于提供一种区块链的统一接口标准，支持用户二次开发、高效使用区块链的功能④。

2.5 应用层

通过区块链接口层JBCC提供的服务，区块链可以快速对接传统应用业务，如版权登记、金融交易、清算、征信、保险、供应链金融及共享经济等领域。

3 清算系统技术体系架构

清算系统采用ABC-TBC双链式架构，将账户信息和交易信息分离，系统在可扩展性及负载均衡上有很大的优势。ABC只进行账户维护，TBC负责交易处理，ABC需要提供账户信息给TBC执行交易。因此，ABC可由一个机构管理，并保持完整的账户历史记录。TBC将多个ABC联系在一起，并通过交易软件进行交易和记录交易历史信息。TBC跟踪完整的交易记录，ABC的每一次变化都可以追溯到TBC的交易记录[1]。

一个传统的区块链需要同时进行账户和交易信息的维护，所以它不可能轻易地分裂。天德多链式区块链架构通过将账户信息和交易信息分离为ABC和TBC，可以

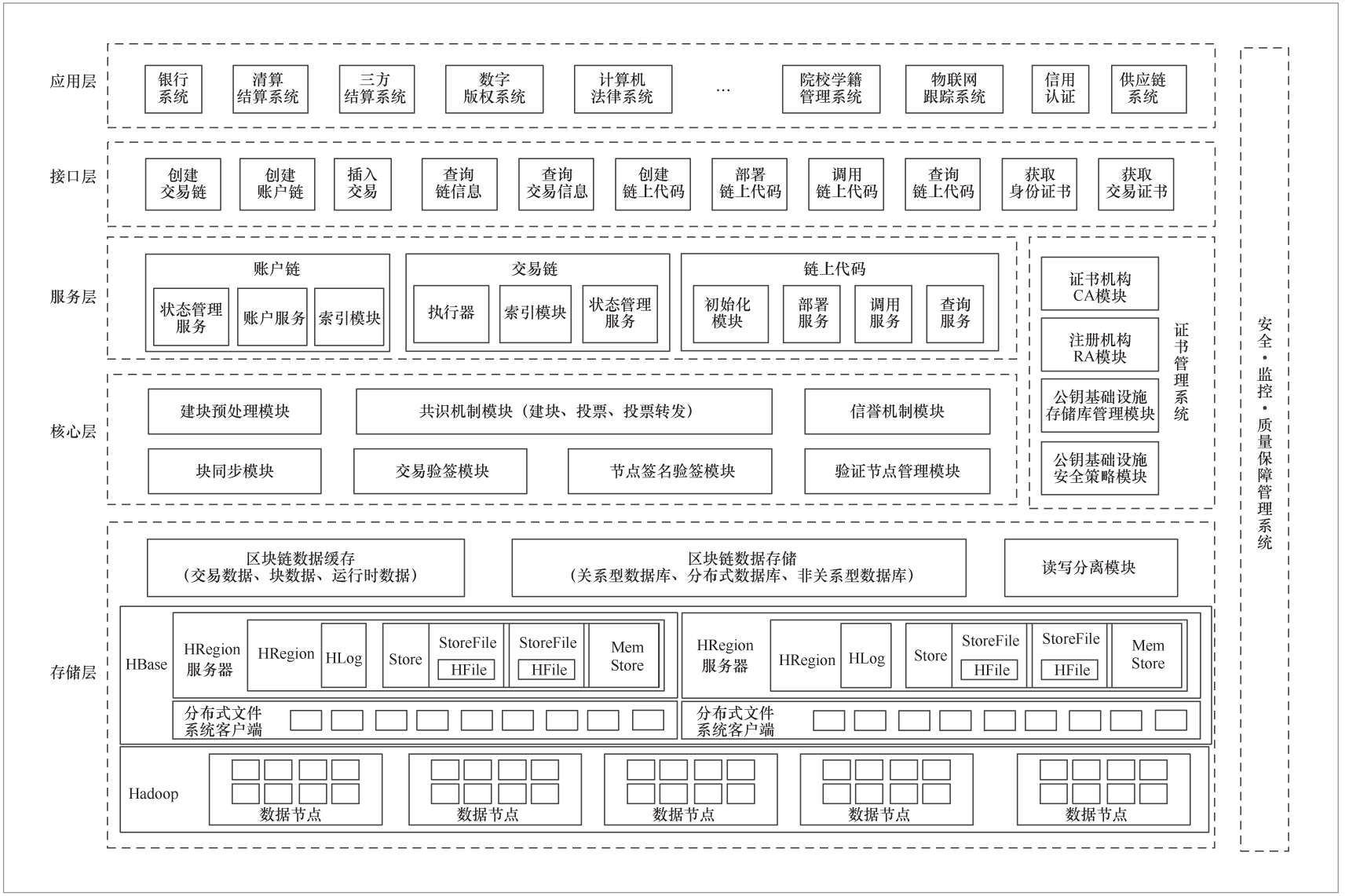

图1　天德大数据版区块链技术架构

从许多方面进行优化。具体来说，可以提升系统整体的可扩展性，从而实现负载平衡，因为ABC可以分片成多个子ABC，每个子ABC负责一组账户，而且TBC可以根据工作负载需要进行扩展。当一个ABC被分成多个具有独立账户的子ABC时，由于每个账户仅存在于一个子ABC中，并且任何ABC不处理交易活动，因此子ABC之间互不干扰。在这种情况下，每个子ABC可以并行运行在不同的处理器上，以加速计算，而不需要任何子ABC之间的交互。在分离成ABC和TBC模型之后，区块链可被分割、合并，从而实现横向可扩展[2]。随着工作负载的增加，可以通过添加更多的服务器，使整个系统保持高性能。

基于前面的讨论，本清算系统提出了采用负载均衡的双链式区块链架构，如**图2**所示。

该架构具有以下主要特点。

- 交易所：每个交易所至少有一个ABC存储有关客户账户及其交易历史的信息，可能还有多个处理交易的TBC。每个交易所都用ABC存储交易所的所有账户信息和余额，并使TBC更新。
- 清算中心：有一个区块链大账本和多个TBC。一套TBC在交易所与ABC进行交互以接收交易信息，另一套与银行进行互动，以更新银行的账户信息。
- 银行：每家银行至少有一个ABC，可能还有多个TBC。银行使用ABC存储账户信息及其余额，并使用TBC跟踪与账户相关的交易活动。
- 监管机构：监管机构可以访问存储在区块链上的大账本，但是需要参与银行、清算中心相关的区块链基础设施的建设。由于区块链大账本包含所有账户的完整交易历史记录，因此监管机构可以查看每笔交易，包括所有交易详情，如交易金额、交易类型、交易日期和时间等[3]。

4 双链式清算系统的账务处理流程设计

原始交易根据清算业务自定义的数据结构实现，一笔正常的原始交易数据需要

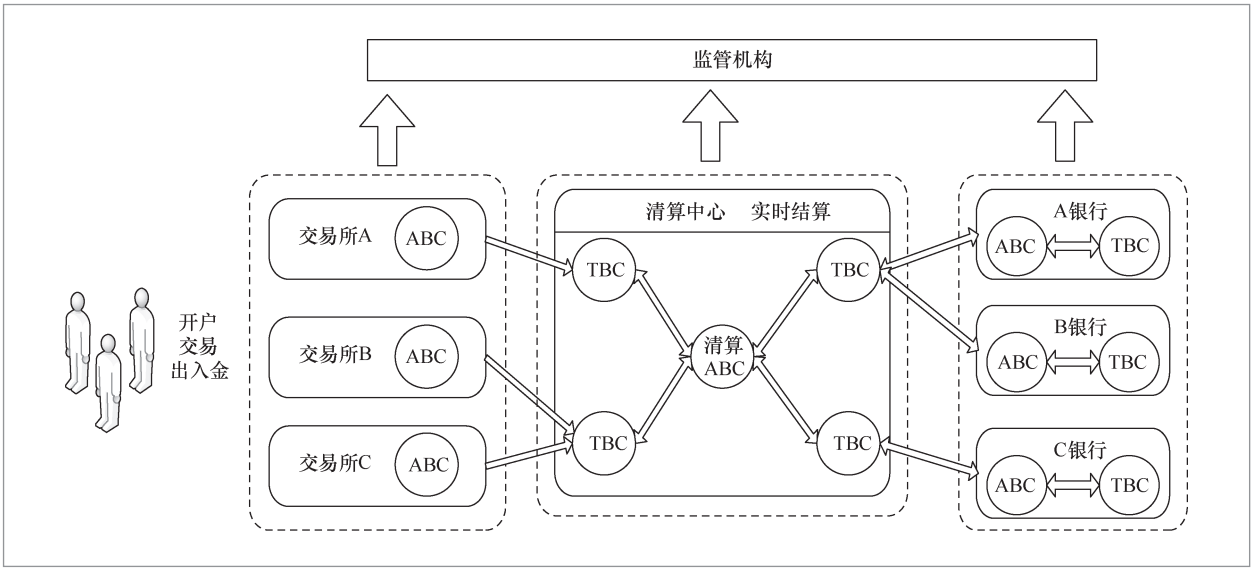

图 2 清算系统技术架构

包含交易ID、原始交易、原子交易、签名字符串，具体流程如**图3**所示。

下面将举例说明如何将1笔原始交易拆解为多笔原子交易集合。

（1）拆解原始交易

交易双方为A和B，A花费10 000元从B处购买了10吨铜，从资金、资产和手续费（默认双方付费5%）3方面来看，将产生6笔原子交易，见**表1**。

（2）原始交易存储

由区块链将共识后的原始交易信息以区块为单位写入交易二级索引表（ITX表）和TBC表，其中TBC表是将区块的ID进行散列后作为行的关键值Rowkey，以该区块内发生的所有交易ID作为列名，这样可以将区块数据均匀地分布在多个RegionServer上，解决数据的局部热点问题，防止数据倾斜。

（3）交易记账/分账

由ABC表对原子交易执行分账记账功能，该表提取出账户的量化信息和非量化信息，量化信息中如果有同账户操作，首先进行累加合并，然后对同账户、同名称的操作和原始值进行数值计算，最后以账户为单位写入账户二级索引表（IACT表）和ABC表。该表同样将区块的ID进行散列后作为行的关键值Rowkey，以区块内发生交易的所有账户以及平台账户为列，对同一区块内发生的所有交易，按账户进行分组归并后进行持久化存储[4]。

（3）信息查询检索

通过构建二级索引加快HBase数据检索速度。主要针对以下2个业务场景。

- 场景1：用户提出账户的余额有问题，要查看交易的完整记录（需要建立用户账户和交易的索引表）。

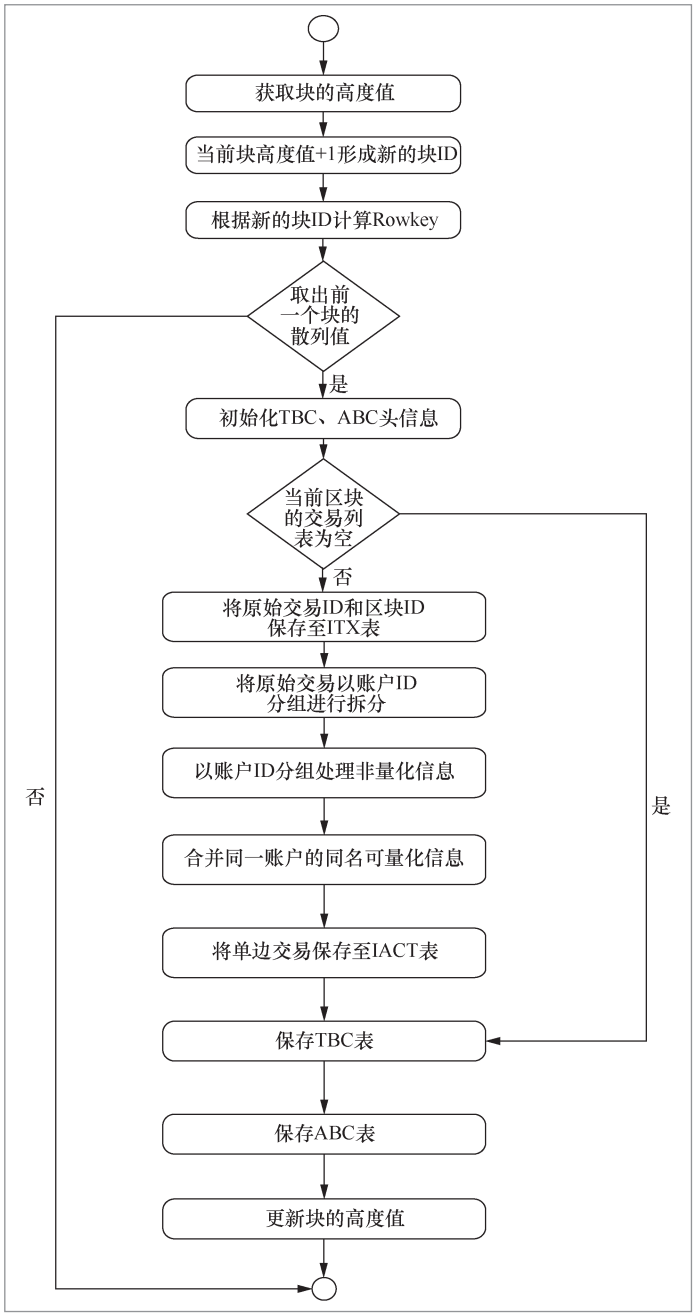

图 3 双链式清算系统的账务处理流程

表 1 拆解原始交易

资金	资产	手续费
A资金减少10 000元	A资产增加10吨铜	平台账户增加A交易费用的5%
B资金增加10 000元	B资产减少10吨铜	平台账户增加B交易费用的5%

● 场景2：某交易有问题，要查看原始的区块信息（需要建立交易和区块的索引表）。

针对场景1，引入IACT表，建立账户的二级索引表，该表将账户ID散列后以Rowkey存储，列信息主要包括3个部分：非量化信息、可量化信息和区块标志位信息。其中，非量化信息主要包括地址、联系方式等不可进行数值计算的信息；量化信息主要包括可进行数值计算的信息，比如资产账户以及人民币、美元等资金账户等；区块标志位存储的是和账户发生交易关联的区块，以“1”作为标志位[5]。

针对场景2，引入ITX表，该表将交易ID进行散列后存储，列为TBC、ABC的Rowkey，在需要查询原始交易时，通过二级索引可以很快检索出需要的交易信息。

在双链式清算系统中，TBC链负责存储原始交易信息；ABC链负责存储实时记账/分账信息；IACT表负责存储账户的可量化信息、非可量化信息以及关联区块的标识位；ITX表负责存储交易和区块的相关信息[6]。

区块链应用层通过双写数据解决交易二级索引表和账户二级索引表的数据一致性的问题。在写入交易数据和账户数据的同时，将索引字段和Rowkey的对应关系作为索引数据写入另一张表，也就是将应用数据和索引数据同时写入，这种双写数据的方式可以做到非常好的索引实时性。未来改进的方法是采用HBase协处理器，以对应用透明的方式实现交易二级索引表和账户二级索引表的数据更新操作。

在本文清算系统的账务处理流程设计中，一项非常重要的工作就是对原始交易进行分解。一笔商业交易可能会涉及6个及以上的账户变动，如果放在一起处理，区块链分片无效。如果分开处理，原子交易就可以在一个分片上单独处理，这样就解决了以太坊无法解决的问题。

5 清算交易数据安全传输设计

在清算系统工作的整个过程中，需要保证所有进出的数据在传输和存储过程中的安全性[7]，因此针对清算系统数据流动的整个过程，结合区块链加密解密的特性进行了如**图4**所示的设计。

（1）JBCC客户端

● JBCC客户端对交易信息进行散列；

● 使用JBCC服务端的私钥对交易信息签名，形成签名字符串；

● 产生对称密钥；

● 使用对称密钥对交易明文加密，形成交易密文；

● 使用JBCC服务端的公钥对对称密钥加密，形成密钥密文；

● 将签名、密钥密文和交易密文一起发送给JBCC服务端。

（2）TDBC

● TDBC使用自己的私钥对密钥密文进行解密，得到对称密钥；

● 使用对称密钥解密交易密文，得到交易明文；

● 使用TDBC公钥对对称密钥加密，得到密钥密文；

● 使用JBCC客户端的公钥对交易明文的散列和签名进行验签。

需要重点说明的是，JBCC客户端是区块链客户端的代理，是区块链核心程序提供给客户端的封装包，提供区块链写入和查询接口；JBCC服务端是区块链服务端的代理，主要在JBCC客户端和区块链核心程序之间进行数据转接，是区块链对外提供分布式存储和交易数据、区块链数据校验等服务的窗口；TDBC端负责交易数据的解密验签、共识、存储等工作[8]。

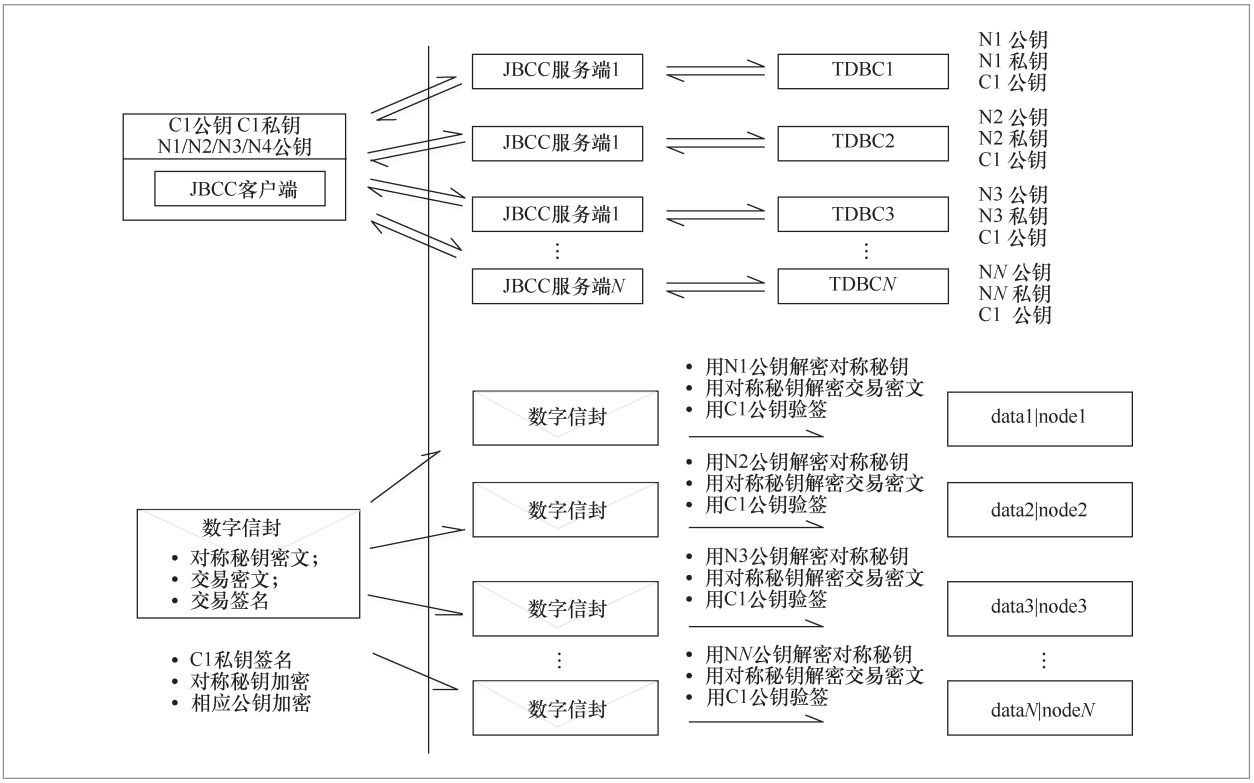

图 4　天德链应用数据安全访问流程

6 清算系统核心数据结构设计

数据结构的设计在整个清算系统中是重中之重，以下将列举在该系统中使用的2种通用三方交易的数据结构的格式。

6.1 原始交易的数据结构

原始交易的数据结构包含交易ID、资产交易数额、资金交易金额、交易单位、交易单价、发起方账户ID、接收方账户ID、交易平台手续费账户ID、交易平台手续费率、正方交易平台手续费金额、对手方交易平台手续费金额、交易时间戳、交易描述及原始交易中需要保持的非量化信息[9]。原始交易的数据结构见**表2**。

6.2 原子交易的数据结构

原子交易的数据结构包含1笔非量化信息和n笔量化信息。原子交易的数据结构见**表3**。

6.2.1 非量化原子交易的数据结构

原子交易中的非量化信息用于对账户的基础信息进行记录与更新。非量化原子交易数据结构见**表4**。

6.2.2 量化原子交易的数据结构

量化原子交易的数据结构用于对账户的量化信息进行累计，原子交易中的量化信息描述了原子交易里的涉及数值计算的相

表 2 原始交易的数据结构

序号	名称	字段	类型	描述
1	交易ID	txID	String	唯一ID
2	资产交易数额	txAssetAmount	BigDecimal	例如1 000吨
3	资金交易金额	txFundAmount	BigDecimal	100 000元
4	交易单位	txUnit	String	吨、千克、克拉、桶、吨、加仑、升、立方米等
5	交易单价	txUnitPrice	BigDecimal	100元/吨
6	发起方账户ID	txSelfID	String	account1001
7	接收方账户ID	txPeerID	String	account1002
8	交易平台手续费账户ID	txFeePlatformAccountID	String	Fee_0
9	交易平台手续费率	txFeeRate	BigDecimal	0.005
10	正方交易平台手续费金额	txFeeFromSelf	BigDecimal	
11	对手方交易平台手续费金额	txFeeFromPeer	BigDecimal	
12	交易时间戳	txTimestamp	String	
13	交易描述	txDescription	String	如购买大宗商品铜
14	原始交易中需要保持的非量化信息	nonquantifiableInfo	HashMap <String, String>	比如地址的更新、手机号的更新等

表 3 原子交易的数据结构

序号	名称	字段	类型	描述
1	非量化信息	nonQuantifiableInfo	HashMap <String, String>	非量化用户基础信息，原子交易里的非量化Bean，用于对账户的基础信息进行记录和更新
2	量化信息	quantifyInfo	ArrayList<ABCAtomicQuantifyBean>	量化单方交易信息，原子交易里的量化Bean的列表，用于对账户的量化信息进行累计

表 4 非量化原子交易数据结构

名称	字段	类型	描述
非量化信息	nonQuantifiableInfo	HashMap<String,String>	非量化用户基础信息，原子交易里的非量化Bean，用于对账户的基础信息进行记录和更新

关操作。

清算系统需要使用量化原子交易数据结构表述交易用户对其账户的资金或资产进行操作的过程。通常情况下，原子交易中的量化信息应该是一个列表数据结构：List<ABCAtomicQuantifyBean>，列表中每一项由账户ID、原始交易ID、量化名称、量化类型、量化数额、交易描述及业务时间戳组成，见**表5**。

7 清算系统界面及功能设计

该清算平台的设计目标是定期将清算所的用户注册、银行出入金以及盘中持仓买卖交易记录到区块链系统中，并能进行多个维度的查询，从功能上可以划分为基本的用户注册、商品交易和数据查询以及

表 5 量化原子交易数据结构

序号	名称	字段	类型
1	账户ID	accountID	String
2	原始交易ID	origialTxID	String
3	量化名称	quantifyName	String
4	量化类型	quantifyType	String
5	量化数额	amount	BigDecimal
6	交易描述	description	String
7	业务时间戳	businessTimestamp	String

批量数据导入等模块[6]。

（1）批量数据导入

为方便用户操作，本模块支持手动或自动方式，批量导入交易所的日终交易文件。其中，手动方式可以通过浏览器http方式访问，也可以在shell终端下用wget执行；自动方式可以通过设置Linux环境下的定时任务进行定期导入。

（2）会员信息查询

查询会员的基本信息和交易账户信息。本模块可以根据会员编码、交易账号查询会员的详细信息列表，包括会员编号、会员全称、会员简称、会员类型、会员状态、会员主体类型、会员编号（交易所）、经济会员编号、注册日期时间等。

（3）资金数据查询

查询会员的资金账号和账户余额信息。本模块可以根据会员编码、交易账号查询资金账号的详细信息列表，包括资金账号、会员编码、会员名称、交易所、创建时间等信息。

（4）交易数据查询

查询交易成交记录和银商流水等信息。本模块可以根据会员编码、交易账号查询交易账号的详细信息列表，包括交易账号、会员编码、会员名称、原交易账号、原会员编号、创建时间等信息。

（5）资产数据查询

查询持仓总汇和持仓明细等信息。本模块可以根据会员编码、产品代码查询持仓总汇的详细信息列表，包括会员编号、资金账号、产品代码、总持仓数量、持仓成本等信息。

（6）区块链信息查询

查询区块的高度、时间戳、块内交易大小和块散列等信息。本模块可以查询最近区块的详细信息列表，包括块高度、时间戳、链长度、块散列值等信息。

8 清算系统测试与分析

此测试场景的区块链节点部署模式采用4×4矩阵式部署，即约定4个区块链节点，每个节点需配置4台服务器作为区块链应用的宿主机及大数据平台的支撑环境，另外增加2台x3850作为加解密服务器，具体配置见**表6**。

为了充分验证本架构的可行性，分别测试了33.34亿笔历史交易以及6 201 762笔线上实时交易。批量历史交易数据显示系统每秒处理约5 000笔交易数据；线上实时交易数据稳定测试一个月左右。通过与现有清算系统对比，这套大数据版的区块链清算系统的实测正确率达到100%。见**表7**，主要从原始交易笔数、原子交易笔数、交易数据量、每秒执行的交易数量、最大块容量、节点数6个维度进行了对比分析。

通过分析上述实验结果，33.34亿笔历史交易量相当于比特币自2008年到2017年

表 6 测试环境软硬件配置

需求名称	详细要求
硬件要求	区块链节点：16台IBM x3650 E5-2670*2，64 GB内存，2 TB SSD硬盘，万兆网络 加解密服务节点：2台IBM x3850，4颗4850V3，14核、2.2 GB CPU，128 GB内存，6块480 GB SSD，万兆网络
软件要求	CentOS7.0,JavaSDK1.8,Redis3.2.4, Hadoop2.7,Hbase 1.2.4,TDBC_SLL1.01

表 7 测试结果

类别	批量历史交易数据	线上实时交易数据
原始交易笔数/笔	33.34亿	1 033 627
原子交易笔数/笔	200亿	6 201 762
交易数据量	3.45 TB	1.4 GB
TPS	5 000，5000×6(Atomic Tx)	150，150×6(Atomic Tx)
MaxBlockSize	35 000	10 000
节点数	4×4	4×1

所有历史交易数量的15.5倍（按比特币现在的交易速度，仍需22年才能达到33.34亿笔交易总量）、美国纳斯达克股票交易所16个月的交易数量、英国伦敦股票交易所14年的交易数量、Visa信用卡全球231 h的交易数量。

由于大数据版的区块链系统复杂、组件众多，单点资源耗费相对较大。在启动大数据版区块链后，通过VisualVM查看线程状态可知，系统启动时区块链节点的线程实时峰值为316左右，运行一段时间后达到稳定期，线程数降到200左右。在此处笔者做了大量优化HBase的连接池、优化SpringBoot核心线程数、调整最大连接数、核心连接数和过期时间，以期达到平衡线程数与区块链最大系统吞吐率的目的。区块链测试节点线程状态如**图5**所示。

天德大数据版的清算链系统与其他区块链系统的性能对比，见**表8**。

显然天德清算链在实际处理速度上远超其他区块链，并行拜占庭共识协议（CBFT）的交易与投票并行执行，高度在投票完成时决定，以此来支持高频交易，提高扩展性。

9 清算系统风险决策与风险评估模型展望

清算系统每天处理种类繁多、数量庞大的交易数据，而且涉及金额巨大，所以清算系统的风险决策与风险评估模型的重要性不言而喻。在高速、自动化的交易清算业务过程中，更需要自动化的风险决策机制，这就是把大数据平台融合在区块链系统中的重大优势，也是天德区块链非常大的创新与尝试。

大数据版区块链和“区块链+大数据”最大的不同在于数据可以直接在区块链平台上进行大数据分析，而不用从链中分离。例如要对3年的区块链链上数据进行分析，如果把区块链历史数据迁移到大数据平台上进行分析，那么数据在做数据抽取、转换、加载（extract-transform-load，ETL）的过程中可能会被篡改，而把大数据平台融合在区块链里面，就可以直接在区块链中进行数据分析操作。

由于区块链与大数据平台的高度融合，所有区块链上的数据都存储在大数据平台中，这样可以充分利用目前已有的大数据分析工具，如R、MLlib、统计产品与服务解决方案（statistical product and service solutions，SPSS）、统计分析系统（statistical analysis system，SAS）等，在区块链链上进行大数据分析。例如在清算系统中，可以通过分析交易信用识别和降低虚假交易，提高交易清算效率，防范欺诈风险，同时也为建立、健全清算系统的风险决策与信用风险评估模型提供了一条新的路径[10]。

10 基于区块链的清结算方案的现状

2017年1月，美国存管信托和结算公司（DTCC）联手IBM、Axoni和R3开发基于区块链的清结算系统，DTCC声称这是一个庞大而现实的项目，并计划该系统在2018年上线。Clearstream和Eurex与德国中央银行以及其他欧洲国家中央银行一起宣布，他们将共同合作开发一个区块链原型，通过银货对付（delivery versus payment，DVP）流程进行跨境安全结算。

DTCC的Mark Wetjen最近对分布式账本技术（distributed ledger technology，DLT）的解决方案发表了评论⑤："由于DLT进一步降低风险，降低金融交易处理成本以及在衍生品数据处理中的潜在应用潜力，DLT已经引起了极大关注。但是，使用DLT不一定能保证所有交易后处理的效率和节约成本。例如，DTCC没有看到使用DLT在美国股市和大部分固定收益市场做清结算的近期好处。"

2017年4月，Mark Wetjen在美国麻省理工学院（MIT）金融科技会议上发表了关于防止区块链用于交易结算的常见区块链设计："有没有什么方法可以使净额（余额）不再那么重要？在这种情况下，像区块链这样的技术是否可以起作用？若不能，系统必须整体结算，每天要结算一天中发生的每一笔交易。这样工作量是巨大的，并且引入了更多风险，所以大多数公司不想这样做。"

这表明Mark Wetjen对不能支持余额计算和不能处理大数据的区块链有意见。除非区块链能够处理大数据（工作量巨大）和余额计算，否则，使用区块链在清结算上反而会增加风险。

然而这些问题并没有出现在中国版的区块链清结算方案上，中国使用的区块链清结算是基于大数据平台拥有多层次账户结构的全额结算与净额结算相配合的模式，从而避开了DTCC碰到的困难。

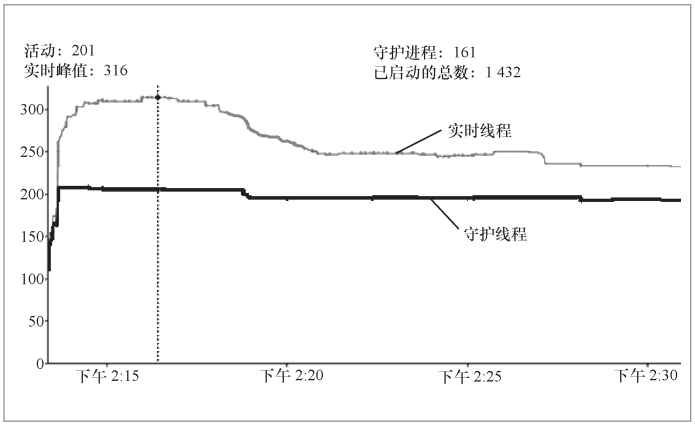

图 5 区块链测试节点线程状态

表 8 区块链性能对比

类别	共识算法	TPS
比特币	PoW	最多7笔交易
以太坊	PoW+PoS	最多25笔交易
超级账本	PBFT	最多1 000笔交易
天德清算链	CBFT	>5 000笔交易

⑤ http://www.dtcc.com/news/2017/may/31/dtccs-wetjen-discusses-impact-of-distributed-ledger-technology-at-fia-law-and-compliance-event

2017年4月，天德大数据版区块链在一个清算系统上成功运行一个月，处理了33.34亿笔清算交易，在区块链系统中完成这么大量的交易量，是区块链历史上的一个记录。天德大数据版区块链吸引了100多个来自中国、美国、英国、日本等地的团队进行共同探讨，其中包括地方政府、银行、世界著名IT和金融科技公司[11]。

11 结束语

本文介绍了天德大数据版区块链技术在清算系统中的应用，通过使用大数据平台存储和分析区块链上数据，打通了大数据、区块链和清算系统之间的信息壁垒，同时提出应该对有意义的区块数据进行深度加工和挖掘，为清算系统风险决策、风险评估及审计方面提供信息支撑。

参考文献:

[1] TSAI W T, BLOWER R, ZHU Y, et al. A system view of financial blockchains[C]//2016 IEEE Symposium on Service-Oriented System Engineering (SOSE),June 12-16, Kongsberg, Norway. New Jersey: IEEE Press, 2016: 450-457.

[2] MCCONAGHY T, MARQUES R, MÜLLER A, et al. BigchainDB: a scalable blockchain database[R]. 2016.

[3] 蔡维德, 赵梓皓, 张弛, 等. 英国央行数字货币RSCoin探讨[J]. 金融电子化, 2016(10): 78-81.
TSAI W T, ZHAO Z H, ZHANG C, et al. Digital currency of centre bank of England[J]. Financial Computerizing, 2016(10): 78-81.

[4] PINNA A, RUTTENBERG W. Distributed ledger technologies in securities post-trading revolution or evolution[J]. Social Science Electronic Publishing, 2016.

[5] TSAI W T, BAI X, YU L. Design issues in permissioned blockchains for trusted computing[C]//2017 IEEE Symposium on Service-Oriented System Engineering (SOSE),April 6-9, 2017, San Francisco, USA. New Jersey: IEEE Press, 2017: 153-159.

[6] TSAI W T, FENG L, ZHANG H, et al. Intellectual-property blockchain-based protection model for microfilms[C]//2017 IEEE Symposium on Service-Oriented System Engineering(SOSE), April 6-9, 2017, San Francisco, USA. New Jersey: IEEE Press, 2017: 174-178.

[7] ZHU Y, GUO R, GAN G, et al. Interactive incontestable signature for transactions confirmation in bitcoin blockchain[C]//2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), June 10-14, 2016, Atlanta,USA. New Jersey: IEEE Press, 2016: 443-448.

[8] 蔡维德, 郁莲, 王荣, 等. 基于区块链的应用系统开发方法研究[J]. 软件学报, 2017, 28(6): 1474-1487.
TSAI W T, YU L, WANG R, et al. Blockchain application development techniques[J].Journal of Software, 2017, 28(6): 1474-1487.

[9] 蔡维德, 郁莲. 区块链技术在金融领域的应用解析[J]. 金融电子化, 2016(5): 57-60.
TSAI W T, YU L. Analysis on applying blockchains to bank &finance[J]. Financial Computerizing, 2016(5): 57-60.

[10] YU L, TSAI W T, LI G, et al. Smart-contract execution with concurrent block building[C]//2017 IEEE Symposium on Service-Oriented System Engineering (SOSE),April 6-9, 2017, San Francisco, USA. New Jersey: IEEE Press, 2017: 160-167.

[11] 郁莲, 邓恩艳. 区块链技术[J]. 中国计算机学会通讯, 2017, 13(5): 10-15.
YU L, DENG E Y. Blockchain technologies[J]. Communications of the CCF, 2017, 13(5): 10-15.

作者简介

蔡维德(1958-),男,博士,北京航空航天大学教授、博士生导师,国家“千人计划”特聘专家,主要研究方向为区块链技术、软件工程、分布式系统、云计算与大数据。

郁莲(1963-),女,博士,北京大学软件与微电子学院教授,主要研究方向为分布式计算、形式化方法、区块链技术、软件分析与验证。

袁波(1985-),男,北京天德科技有限公司高级工程师,主要研究方向为云计算、大数据、区块链相关技术。

邓佑权(1979-),男,北京天德科技有限公司工程师,主要研究方向为区块链技术、大数据、分布式系统。

李琪(1996-),女,北京航空航天大学本科生,主要研究方向为区块链、信息安全。

郭斌(1991-),男,北京航空航天大学硕士生,主要研究方向为区块链、分布式系统。

收稿日期: 2017-12-05

基金项目: 国家自然科学基金资助项目(No.61672075, No.61690202)

Foundation Items: The National Natural Science of China(No.61672075, No.61690202)