基于区块链的供应链金融服务平台

马小峰[1]，杜明晓[1]，余文兵[2]，王意[1]
1. 同济大学控制科学与工程系，上海 201804；2. 上海欧冶金融信息服务股份有限公司，上海 201804

摘要
区块链具有去中心化、稳定安全和防篡改的特点，随着区块链技术的进一步完善与应用，区块链将与金融、医疗、物流等传统行业结合。这将会颠覆部分行业中现有的运作模式，重构一张价值传递的网络。在供应链金融领域进行了区块链应用的探索，构建了一个基于联盟型区块链的供应链金融服务平台。该平台将区块链技术与传统系统结合，为供应链上的各方提供了更加便捷的融资方式，提高了供应链的透明度、可追溯性和安全性。

关键词
区块链；供应链金融；大数据

中图分类号：TP393.02　　文献标识码：A　　doi: 10.11959/j.issn.2096-0271.2018002

Blockchain based supply-chain finance service platform

MA Xiaofeng[1], DU Mingxiao[1], YU Wenbing[2], WANG Yi[1]
1. Department of Control Science and Engineering, Tongji University, Shanghai 201804, China
2. Shanghai Ouyeel Financial Information Service Ltd., Co., Shanghai 201804, China

Abstract
Blockchain has the characteristics of decentralization, stability, security, and non-modifiability. With the further improvement and application of the blockchain technology, it will be connected with the traditional industries such as finance, medical treatment and logistics. This will radically change the existing operation modes in some industries and restructure a value network. An application of blockchain in the field of supply-chain finance was tried, and a supply-chain finance service platform based on the blockchain technology was constructed. The platform combines blockchain technology with other traditional systems, providing a more convenient way of financing for all parties in the supply-chain, improving the transparency, traceability and security of the supply-chain.

Key words
blockchain, supply-chain finance, big data

1 引言

2008年，中本聪首次提出区块链的概念[①]，他将区块链技术作为构建比特币基本数据结构以及将数据加密并且安全传输的基础技术，实现了记录比特币交易的去中心化数据库。区块链具有去中心化、集体维护、高度透明、去信任、匿名等特征，在比特币体系中得到了创新性应用，也受到了世界各国政府和企业的广泛关注，全球很多国家已将区块链技术提到战略高度。我国也在“十三五”国家信息化规划中多次提及区块链技术，凸显了国家对战略性前沿技术的关注和重视程度。桑坦德银行认为，到2020年如果全世界的银行都使用区块链技术，每年约省下200亿美元的成本。世界经济论坛（World Economic Forum）预测，到2027年世界GDP的10%将被存储在区块链网络上。

比特币也是区块链在金融领域的首个应用，区块链作为比特币等数字货币的底层技术，具有去中心化、稳定安全、不可篡改等特点，其在构筑可信任系统方面具有良好的应用前景。目前，区块链的应用已延伸到金融业、物联网、智能制造、数字资产交易、产权保护等多个领域。

在供应链金融领域，中国作为世界最主要的大宗商品生产国和消费国，在全球大宗商品领域具有举足轻重的地位。然而随着全球经济进入下调周期，违约、骗贷事件频出，大宗商品的信用危机也逐渐显现。因质押物信息不对称导致的重复质押、空单质押等风险事件的发生，严重挫伤了融资各方的相互信任，诚信经营难保障，仓储监管成难点；金融秩序被扰乱，银行贷款坏账数量上升，金融机构趋向于减少贷款、加速收贷；同时，大宗货物流通困难，贸易商资金链条紧张、贷款更难，经营发展陷入困境。

区块链技术能有效地解决货物在仓储、物流、监管环节的信息不对称问题。基于区块链数字资产进行融资，既为企业提供了便捷有效的融资途径，也为仓储企业拓展了业务范围。区块链供应链数字资产体系的构建能进一步促进大宗商品交易及融资信用体系的重塑，促进行业的规范性发展。

本文使用区块链技术构建了一个供应链金融服务平台，方便供应链中的核心企业和金融机构共同管理上下游企业的信息流和资金流，提高供应链金融的透明度、可追溯性和安全性，解决传统供应链金融中的信息不对称问题，降低金融风险等级，提升供应链金融的总体效率，降低供应链总体成本，为供应链相关各方提供更好的金融服务。

2 区块链技术

2.1 区块链与比特币

中本聪发表的论文阐述了他对电子货币的新构想，设计出基于区块链底层的比特币，解决了长期以来困扰电子货币发展的三大难点：重复支付、依赖第三方中心、发行量控制。比特币核心技术主要有以下几点：

- 采用对等网络技术进行交易；
- 交易无需金融机构参与；
- 采用非对称加密、可复用的工作证明（proof of work，POW）取代中心信任；
- 系统中大多数节点是忠实的，共同维护最长链；
- 节点可以离开或重新加入网络，接收最长链的变化并更新账本。

上述技术中，对等网络技术、非对称加密技术解决了分布式交易账本的建立问题；可复用的POW解决了“双重支付”的

① http://www.bitcoin.org/bitcoin.pdf

问题，杜绝了那些不怀好意的人通过攻击中央服务器进行比特币无限重复消费的现象。此外，比特币的数量被限定为2 100万个，保证了比特币的稀缺性。

比特币在交易时的表现形式是一串字符，这串字符包含了上一次交易的信息和下一个所有者的公开密钥（以下简称公钥）信息，并将其发送给收款方（下一个所有者）。收款方会对这串字符进行验证，并向全网络广播。被认可的交易信息将被确认形成区块，收款方可通过自己的私有密钥（以下简称私钥）接收比特币汇款，**图1**为比特币交易示意。

2.2 区块链技术

传统的交易需要一个中心化的信任机构，交易的确认、记录完全依靠该信任机构，在交易成本、效率以及安全性上面临许多问题。区块链技术改变了这一现状，区块链具有去中心化的特点，参与区块链的节点拥有平等的地位，节点间无需相互信任，通过事先约定的规则，按照多数占优的原则达成共识，共同完成数据的分布式存储、交易信息的确认等功能，高效、低成本地解决节点间的交易问题。区块链包含对等网络技术、非对称加密、共识机制、分布式账本等各类计算机技术，是一个全面的计算机技术的综合体系。

对等网络技术又称对等互联网技术或点对点技术，是区块链系统连接各对等节点的组网技术，是与中心化连接网络相对应的一种构建在互联网上的连接网络。在对等网络中，各节点的计算机地位相等，节点间通过特定协议进行信息或资源的交互，与中心化网络中心服务器服务全网的模式形成鲜明的对比。在比特币出现之前，对等网络技术主要用于文件共享和下载、网络视频播放等。对等网络技术是构成区块链技术架构的核心技术之一。

非对称加密算法是一种基于密钥的信息加解密方法，需要两个密钥：公开密钥和私有密钥。公钥和私钥是一对。如果使用公钥对数据进行加密，则只有用对应的私钥才能解密。由于加密和解密使用的是不同的密钥，所以这种加密算法被称为非对称加密算法。公钥可公开发布，用于发送方加密要发送的信息，私钥用于接收方解密接收到的加密内容。常用的非对称加密算法有RSA、ECC等。区块链使用非对称加密的公私钥对来构建节点间的保密通信，保证节点的可信及可验证性。随着对交易隐私的保护需求增加以及量子计算的发展，基于零知识证明[1,2]、同态加密[3]、环签名的隐私保护机制和基于格理论[4]等的各种抗量子攻击的加密

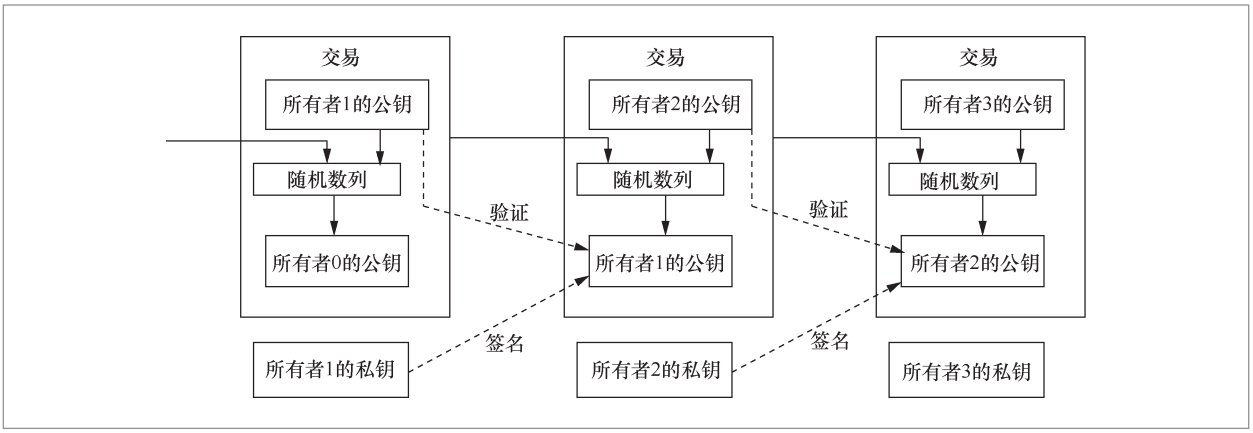

图1 比特币交易示意

方法也正在不断被融入区块链之中。

共识机制是区块链中多节点达成一致性的算法，区块链通过共识机制共同验证交易来解决双重花费问题。在区块链系统中，多个节点能够点对点地通信，但有的节点会受到恶意攻击，通信内容被篡改。正常节点需要分辨这些被篡改的信息，并与其他正常节点取得一致结果，根据节点所处的环境不同，需要设计相应的共识算法。当前，在公有链中常用的共识算法有POW和股权证明（proof of stake，POS），在联盟链中，则主要选用实用拜占庭容错（practical Byzantine fault tolerance，PBFT）算法或者类Paxos算法（如Raft算法）。

POW算法是节点间通过算力的竞争来分配记账权和奖励。不同节点根据前一个区块信息竞争计算一个数学问题的特定解，这个数学问题难于求解但易于计算，最先解决这个数学问题的节点可以创建下一个区块，并获得一定数量的比特币奖励。POS算法②则在POW的基础上增加了币龄的概念，通过将持币数量、持币时间与计算难度结合，一定程度上解决了POW的资源浪费问题。

在分布式系统中，拜占庭容错技术能够很好地解决节点和传输错误的问题，但早期拜占庭系统需要指数级的算法复杂度，直到1999年提出了PBFT系统[5]，将算法复杂度降为多项式级别，极大提高了效率。在拜占庭将军问题[6]提出后，Lamport在1990年提出了Paxos算法，用于解决特定前提下的一致性问题，但由于其论文内容难以被理解而未被接收。1998年Lamport重新发表论文，并于2001年对Paxos进行了简述[7,8]，随后Paxos在一致性算法领域占据统治地位，并在其基础上衍生出许多其他算法。但Paxos算法过于理论化，在理解和工程实现上都有着很大的难度。2013年，美国斯坦福大学的Ongaro D等人[9]发表论文提出Raft算法，实现了与Paxos同样的效果，并且更便于工程实现和理解。Raft算法无法解决拜占庭容错问题，但在只存在宕机错误、不存在恶意节点的情况下，能够更快地完成节点间同步，吞吐量也显著优于PBFT算法。

② https://www.peercoin.net/assets/paper/peercoin-paper.pdf

3 供应链金融领域区块链的应用

近年来，供应链大宗商品的融资市场水深火热。以钢铁大宗商品为例，钢铁市场需求疲软，钢材价格持续走低，钢铁贸易价格倒挂，在钢铁行业面临发展困境的大背景下，钢铁贸易企业严峻的资金压力越来越多地转化为现实的诚信危机。2012年，国内钢材仓储领域曾爆发上百起重复质押、空单质押等信贷案件，涉案金额超过千亿元。这也导致仓储物流业的信用环境遭到破坏，优质的仓库得不到认可，仓储管理走向恶化。困境之下急需行之有效的解决方案化解危机。

在供应链中，竞争力较强、规模较大的核心企业在协调供应链信息流、物流和资金流方面具有不可替代的作用，正是这一情况造成了供应链成员事实上的不平等以及信息的不对称。

基于以上背景，在传统供应链管理、融资平台的基础上，搭建了区块链和大数据分析相结合的供应链金融服务平台，平台围绕核心企业，由金融机构与核心企业共同搭建，能提供线下资产转换为电子资产、资产融资、资产交易、资产竞价的功能，对用户的行为进行记录，并进行大数据分析，给出合理的用户信用评级建议，督促相关参与方增强诚信意识。借助区块链技术建立点对点的信任机制，打造动态增信资产的综合融资模式。

该平台把区块链分布式账本与传统的中心化平台融合，形成有限分布式混合架

构，既能兼顾中心化平台的内控要求，满足现行监管要求，又可以充分发挥区块链分布式账本的典型特征，优势互补。采用自主设计的区块链——梧桐链作为底层区块链平台，并采用跨链技术，使业务记账与账户体系运行在不同的链上，共同完成业务流程，但业务记账链和数字资产流通链相互隔离。

3.1 公有链与联盟链

区块链根据开放程度可分为公有链和联盟链。公有链是指某一公开区域的所有人都可访问的区块链。每个人都可以成为其中的节点，并按照相应规则做出贡献、取得奖励，节点间不具有信任关系。公有链是完全开放和去中心化的，适用于完全开放的场景，目前也已经有了比较成熟的应用。POW和POS是公有链中最常使用的共识算法。

联盟链则是指多方参与且共识节点为参与方预先指定的节点的区块链。联盟链的参与方之间不完全信任，每方按照联盟规则选定己方的共识节点，交易需要大多数共识节点确认。联盟链的节点加入需要符合联盟链预先设定的规则，且只有参与方的节点拥有读取权限，对外界开放部分权限。联盟链的开放程度和去中心化程度弱于公有链，但交易处理的速度和等待时间都优于公有链。联盟链应用于半封闭的网络，如由不同企业共同搭建的网络。在这种网络里，同企业间可能存在利益冲突，可能存在恶意篡改数据的节点。

该平台将供应链中的核心企业作为相对可信任的机构，核心节点的数据交互共识在可信度较高的几个验证企业之间进行，因此平台采用联盟链作为区块链的底层组网形式。平台共识节点的初始加入由核心企业筛选，后续共识节点的加入需要由现有共识节点共同投票决定。

3.2 平台架构设计

平台初始参与区块链验证的节点设定为核心企业、物流企业、仓库和银行，这些企业是供应链中的核心，且维护系统的稳定更符合参与节点的利益，在不发生外部攻击的情况下，单节点对数据的篡改不影响整个系统的稳定性与数据的准确性。其他的个体或参与企业则作为系统的用户，只参与区块链上的业务，不参与共识。

考虑到目前区块链系统并不适合用来存储较大的文件，对平台区块链部分的数据进行了设计，不同的业务封装为功能模块，各模块通过接口进行交互，并与外部通信，各交易模块按照业务和隐私保护的需求，选择必需的关键数据，采用不同的加密方式对数据加密后，记录在区块链上。如**图2**所示，基于区块链的供应链金融服务平台由区块链底层平台和对外服务应用层组成，应用模块包括权限管理模块、数字资产管理模块、数字资产交易模块和信用管理模块。

权限管理模块负责平台用户权限的管理，用户在平台注册时，权限管理对用户的信息进行后台审核，然后给予系统不同的权限，例如管理员用户可完成数字资产申请的审核。同时，权限管理模块会与信用评分模块相结合，降低高风险、低评分的用户的操作权限（如不能申请数字资产、不能交易数字资产等），并在平台上进行警示。

数字资产管理模块负责用户申请线下资产登记为线上资产的审核与审核通过后的线上数字资产的管理。**图3**为典型的数字资产发行流程，用户将线下的实物资产申请确认为线上资产，数字资产管理模块通过对实物资产进行审核，例如大宗物品仓单的审核需要对接仓库系统，由仓库系统对仓单物品的数量、质量等信息进行审核。审核通过的线下资产被冻结，并由具

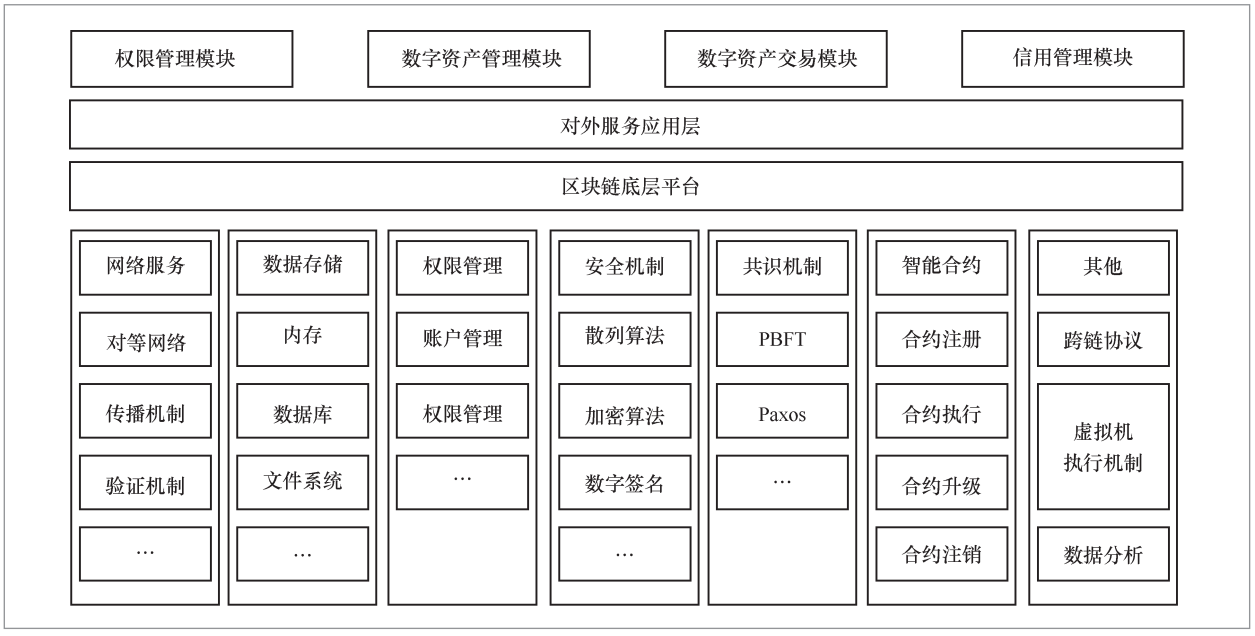

图 2 基于区块链的供应链金融服务平台架构

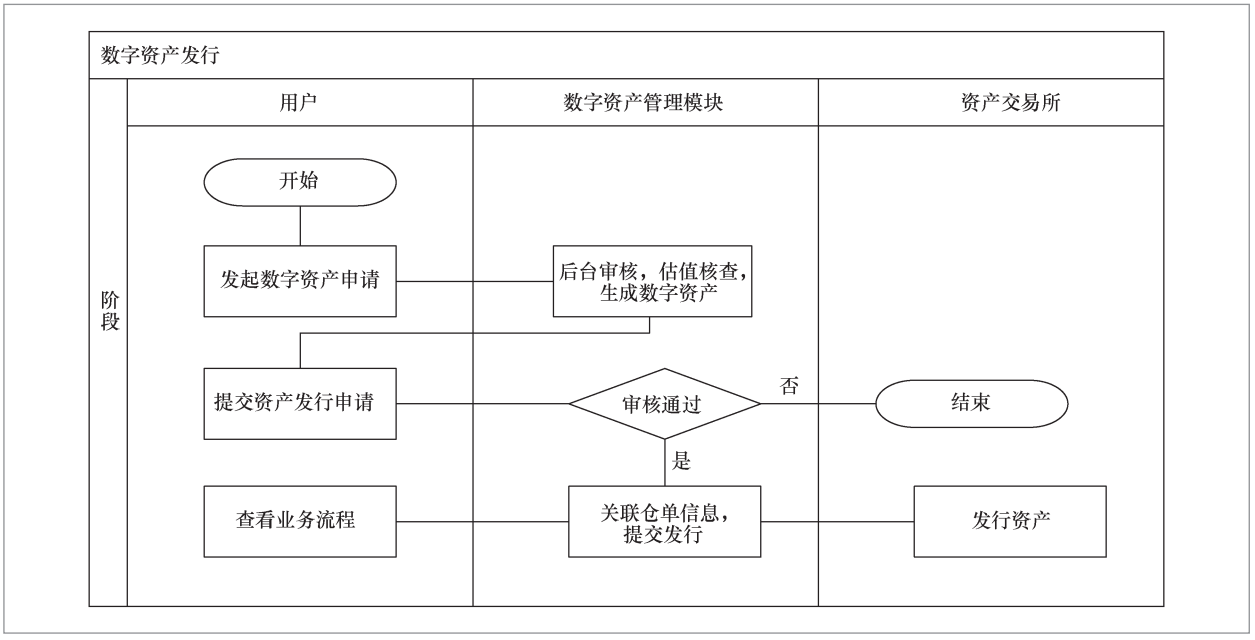

图 3 数字资产发行流程

有资质的第三方机构对物品进行估值，生成带有线下资产详情和估值的数字资产。被冻结的物流信息会由仓库负责监控，对物流的变动和交接在系统内实时记录在区块链上，如果物品脱离监管，系统会冻结数字资产。数字资产申请的流程及生成的数字资产记录到区块链上。数字资产的退出与申请的流程相似，在数字资产管理模块审核通过后，通过智能合约自动完成管理费用的支付，解冻线下资产。

数字资产交易模块提供用户之间数字资产交易的功能。用户可将已生成的数字资

产在数字资产交易模块进行挂牌交易，其他用户如果符合卖方设置的限定条件（如信用等级、用户类型等），即可在交易模块中购买数字资产，数字资产的交易通过智能合约自动执行，并将交易信息记录在区块链上。

部分企业可将产能转换为数字资产，并在平台上进行预售，产能的预售与交易所的形式类似，交易模块可对交易的产品进行拆分，并自动匹配交易。企业也可将数字资产进行融资，通过平台预先设置的智能合约模板，将数字资产发布融资，并按照约定的期限赎回资产。如果无法按时完成还款，智能合约完成资产所有者的变更。

信用管理模块根据用户在平台上的行为以及用户的社会信用，综合产生用户在平台上的信用记录。该记录由分析模型自动生成，并记录在区块链上，交易时平台向交易双方展示信用情况，并根据用户的信用情况提供不同的操作权限。

3.3 区块链与大数据

从数据角度而言，区块链是一种不可篡改、全历史的数据库存储技术，巨大的区块数据集合包含着过往的每一笔交易。随着区块链的应用迅速发展，数据规模会越来越大，不同业务场景区块链的数据融合也进一步扩大了数据规模，提高了数据的丰富性。大数据技术的日趋成熟也为供应链的金融风控提供了可能。平台会将用户的行为记录在区块链上，通过对这些数据进行建模分析，利用非金融领域的数据（交易、支付）为金融机构提供企业征信评估的依据，给出合理的用户信用评级建议，督促相关参与方增强诚信意识，构建一个诚信的平台。

图4为平台信用服务技术路线。该平台的大数据信用分析模块收集大量的企业业务信息，以此作为企业征信的核心数据系统，并补充各类政府、工商、银行、个人等公共信息，通过模型化处理，建立企业征信体系。随着真实业务数据的积累和变化，平台能做到对企业信用的动态化跟踪，发布企业最新的信用情况，使供应链金融服务中嵌入企业征信数据。

4 结束语

本文构建的供应链金融服务平台是区块链技术在大宗商品供应链领域的一次尝试，该平台融合了区块链技术和大数据分析，使得原先单纯基于担保资产的融资模式转化为综合融资模式，建立点对点的信任机制，使得供应链各企业能更为平等地参与其中。但是目前平台仍然存在不足，如采用的共识方式的吞吐量有限、无法满足高频交易的需求、未充分考虑隐私保护的问题等。后续笔者将根据实际运行环境对共识算法进行改进，提高平台交易的吞吐量和确认延迟；尝试采用零知识证明和同态加密等方法，加强对参与用户的隐私保护。

参考文献:

[1] GOLDWASSER S, MICALI S, RACKOFF C. The knowledge complexity of interactive proof systems[J]. Siam Journal on Computing, 1989, 18(1): 186-208.

[2] MICALI S, PASS R. Local zero knowledge[C]//The 38th ACM Symposium on Theory of Computing, May 21-23, 2006, Seattle, USA. New York: ACM Press, 2006: 306-315.

[3] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978: 169-179.

[4] NGUYEN P Q, VALLE B. The LLL algorithm: survey and applications[M].

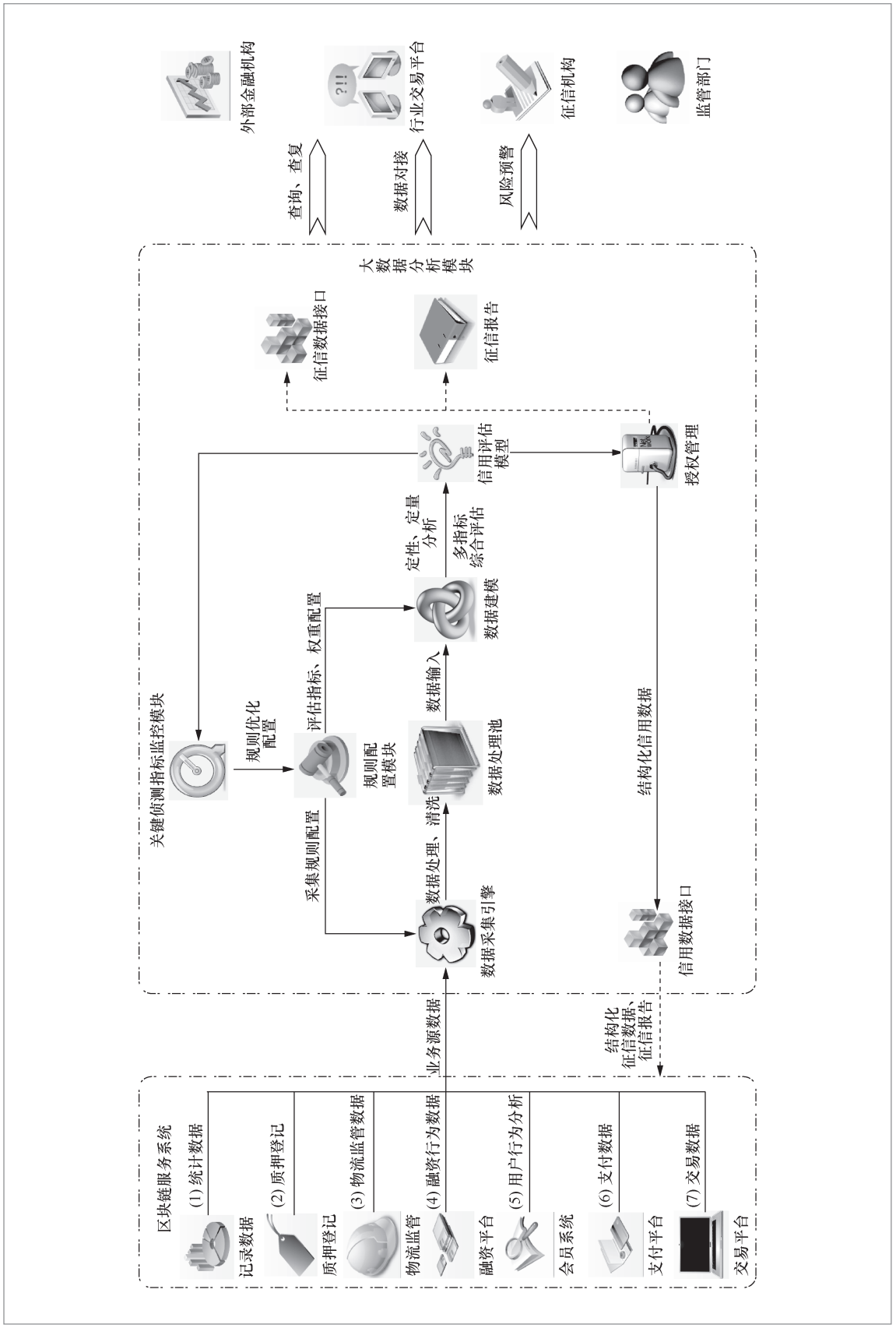

图 4 平台信用服务技术路线

Berlin: Springer Publishing Company, Incorporated, 2010.
[5] CASTRO M, LISKOV B. Practical byzantine fault tolerance[C]//The 3rd Symposium on Operating Systems Design and Implementation, February 22-25, 1999, New Orleans, USA. Berkeley: USENIX Association, 1999: 173-186.
[6] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine generals problem[J]. ACM Transactions on Programming Languages & Systems, 1982, 4(3): 382-401.
[7] LAMPORT L. Paxos made simple[J]. Sigact News, 2001, 32(4): 51-58.
[8] LAMPORT L. The part-time parliament[J]. ACM Transactions on Computer Systems, 1998, 16(2): 133-169.
[9] ONGARO D, OUSTERHOUT J. In search of an understandable consensus algorithm[C]//The 2014 USENIX Conference on USENIX Anmual Technical Conference, June 19-20, 2014, Philadelphia, USA. Berkeley: USENIX Association, 2014: 305-320.

作者简介

马小峰(1975-),男,博士,同济大学控制科学与工程系副教授,苏州同济金融科技研究院院长,主要研究方向为区块链与大数据。

杜明晓(1992-),男,同济大学控制科学与工程系博士生,主要研究方向为区块链。

余文兵(1978-),男,上海欧冶金融信息服务股份有限公司动产经营部工程师、副总经理,主要研究方向为B2B电子商务、供应链金融。

王意(1993-),男,同济大学控制科学与工程系硕士生,主要研究方向为区块链。

收稿日期: 2017-12-11