计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2019,28(7):65−71 [doi: 10.15888/j.cnki.csa.006968]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

区块链技术在电力行业物资合同管理中的应用①

郭欣沅, 董思晴, 黄文涛, 熊志敏

(国网辽宁省电力有限公司 物资分公司, 沈阳 110000)
通讯作者: 郭欣沅, E-mail: 296206234@qq.com

摘　要: 在现代化的电力行业中, 每年都需要采购大量的电力设备用于建设电网工程, 由于电网建设环节复杂、所需物资设备类型较多, 很难管理和众多供应商签订的物资合同. 为了提高合同签订效率、保障电网建设工程的进度和质量, 文章提出了把区块链技术应用在电力行业物资合同的管理中, 由电网企业和设备供应商之间建立的用于签订合同的联盟链, 并提出了一种基于改进的委托权益证明 (DPoS) 的实用拜占庭容错 (PBFT) 的共识机制, 该机制结合合同签订次数给节点动态授权, 优化了代理节点的选择策略. 以区块链技术实现的电子合同既有传统电子合同建立在密码学算法基础上的安全性, 又有多方协作、不可篡改和可追溯的透明性和真实性, 使物资合同的签订和后续的管理都更加便捷和安全.

关键词: 区块链技术; 物资合同; 联盟链; 电力行业

引用格式: 郭欣沅,董思晴,黄文涛,熊志敏.区块链技术在电力行业物资合同管理中的应用.计算机系统应用,2019,28(7):65–71. http://www.c-s-a.org.cn/1003-3254/6968.html

Application of Blockchain Technology in Material Contract Management of Power Industry

GUO Xin-Yuan, DONG Si-Qing, HUANG Wen-Tao, XIONG Zhi-Min

(Material Branch, State Grid Liaoning Electric Power Co. Ltd., Shenyang 110000, China)

Abstract: In the modern power industry, a large amount of power equipment needs to be purchased every year for the construction of power grid projects. Due to the complicated construction of the power grid and the large number of materials and equipment required, it is difficult to manage the material contracts signed by many suppliers. Signing the efficiency and ensuring the progress and quality of the power grid construction project, the article puts forward the application of the blockchain technology in the management of the power industry material contract, the alliance chain established between the grid enterprise and the equipment supplier for signing the contract, and A practical Byzantine Fault Tolerance (PBFT) consensus mechanism based on improved Debt Proof of Entitlement (DPoS) is proposed. This mechanism combines the number of contract awards to dynamically authorize nodes and optimizes the selection strategy of proxy nodes. The electronic contract realized by blockchain technology not only has the security of traditional electronic contracts based on cryptographic algorithms, but also has multi-party cooperation, non-tampering and traceability of transparency and authenticity, so that the signing and follow-up of material contracts Management is more convenient and safe.

Key words: blockchain technology; material contracts; alliance chains; power industry

① 收稿时间: 2018-12-10; 修改时间: 2019-01-18; 采用时间: 2019-01-31; csa 在线出版时间: 2019-07-01

随着我国经济建设的快速发展和居民用电量的增加, 电力行业又作为国民经济的“先行官”, 得到了充分的重视发展. 伴随着电力改革、新能源和储能装置等的快速发展, 未来电网投资的重点将向电网智能化和配电网的建设转变. 电网建设工程不同于一般的工程, 物资合同关系着电力设备的技术要求和专业生产, 由于电网工程的系统性和施工环节的严苛性, 在建设工程前, 项目所需的物资合同的签订和管理显得尤为重要.

电力行业使用的物资合同大部分为纸质合同, 少量合同的签署采用信息化平台提供的电子合同的形式. 传统纸质合同内容承载为纸质实体, 需要严格的审批流程, 签署形式分为当面签署、扫描件签署或快递签署, 当面签署的安全性高, 但其便捷性差, 并且效率低; 扫描件签署双方需要设备支持; 快递签署存在耗时长、需要额外的快递费用和签名可能被伪造等问题. 电子合同的内容和签名表现为数据报文, 签署渠道相比纸质合同更加多样, 在仓储成本、工作效率、安全性和环保价值等方便都优于传统的纸质合同.

电子合同在合同的签署过程中使用密码学算法解决了传统纸质合同在签署过程中安全性不足的问题, 但因其采用电子化的形式存储合同, 在数据存证方面存在安全隐患, 首先在存储方式上, 大多采用中心化服务器集中存储, 存储设备的故障和黑客的攻击都容易造成合同数据的丢失和篡改; 其次在验证方式上, 一般不采用验证方式或由第三方权威机构验证, 安全性较差, 效率较低; 最后在溯源方式上, 证据单一难以溯源, 合同一旦出现问题, 说服力较弱.

1 物资合同管理现状

物资合同是由电力企业和供应商之间签署的供货协议和约定, 由于电网建设所需设备是按照所需场景和技术指标定量生产的, 工程前期需要管理物资采购合同以制定采购任务, 通过合同管理确定采购物资的型号、数量、成本、技术含量和交/验货方式[1,2], 所以合同的签订直接影响到了电力设备的供应, 对电网建设工程的进度影响非常大.

1.1 纸质和信息化方式管理的物资合同

在电力企业传统的物资合同管理模式中, 存在着物资供应商分布全国各地、合同的签字和盖章可以由他人仿冒, 在合同邮寄的过程中也可能发生篡改等问题, 为了加强合同的安全性, 由快递或者人工送达加上专人的审核、盖章等复杂的流程, 导致了合同从起草到签订整个流程上的繁琐特性. 随着信息化的提升, 利用电子签章技术可以实现合同的线上签订, 电子签名生成的电子合同既有和纸质合同同等的法律效力, 又可以通过线上的方式迅速锁定客户、降低成本和提升竞争力. 后期电力企业利用信息化平台可以对签订的电子合同分类管理进行优化, 使合同管理的效率得到了一定的提升, 有效的节省了人力和物力成本.

1.2 信息化方式管理物资合同的不足

利用信息化平台实现的电子合同在一定程度上提高了电力企业和供应商之间签订和管理合同的效率, 但是由于依赖信息化平台的智能管理系统, 主要将合同以电子档案的形式存放在数据库中, 存储方式高度依赖中心服务器, 而且加密方式通常是明码保存或加密方式单一, 存在容易被黑客攻击、数据易发生篡改等问题.

2 引入区块链技术的可行性

近年来随着区块链技术的成熟, 于原理上的契合, 以区块链技术[3−7]实现的电子合同可以真正把信任和安全建立在数据和算法之上. 具体而言就是在物资合同的签订、归档和存储环节引入区块链技术, 考虑到电力行业签订物资合同的当事人和环境, 本文采用以区块链技术实现的联盟链[8]对物资合同进行签订和管理, 联盟链不同于“广义”上的区块链追求去中心化、所有交易对外公开透明, 而是采用部分去中心化或多中心化, 联盟链的准入机制限定链中的节点由电网企业和供应商共同维护, 并利用同态加密算法保证合同的内容只对签署合同的双方可见, 保障合同内容不会泄露给第三方.

2.1 带有权限的开放性

区块链技术本质上是一种公共记账的技术方案, 账簿对所有人公开, 实现数据共享. 在合同管理领域, 由于合同的签订信息不能对所有人完全透明开放, 需要解决合同管理的隐私性和权限管理, 本文提出的联盟链不对外公开, 链中的节点由电力企业和物资供应商共同维护, 通过加入身份管理、权限管理和监管模块, 既能够低成本的运行和维护, 又可以实现较高的交易速度等良好的扩展性.

2.2 合同信息不可篡改

应用区块链存证技术, 合同信息一旦存储, 任何一方都无法篡改, 保证了合同的真实客观性. 合同信息的

不可篡改分布在存储前期和后期两个阶段, 存储前期依赖密码学和共识机制, 主节点验证合同的有效性后把加密过的合同信息广播到其他节点, 每一个节点都把合同信息维护到自己的链上, 后期依赖链中的每个节点都保存了电力企业同设备供应商之间签署的合同, 导致合同信息在链中处于“共享”状态, 保证任意一个节点都无法修改数据, 因此可以保证合同的安全性和透明性.

区块链技术采用单向哈希算法, 每个新产生的区块严格按照时间线顺序推进, 每个区块的头部信息都有其前一个区块的 Hash 值, 该 Hash 值是由前一个区块的头部信息经过 Hash 算法生成的固定长度的字符串, 由区块头部的 Hash 值和“时间戳”形成区块之间的链条, 时间的不可逆、不可撤销导致任何形式试图入侵篡改区块链内部的合同信息的行为易被追溯, 还会导致其他节点的排斥, 造假成本极高. 这便于对合同历史信息进行追踪, 可以有效解决合同后期存在纠纷等问题.

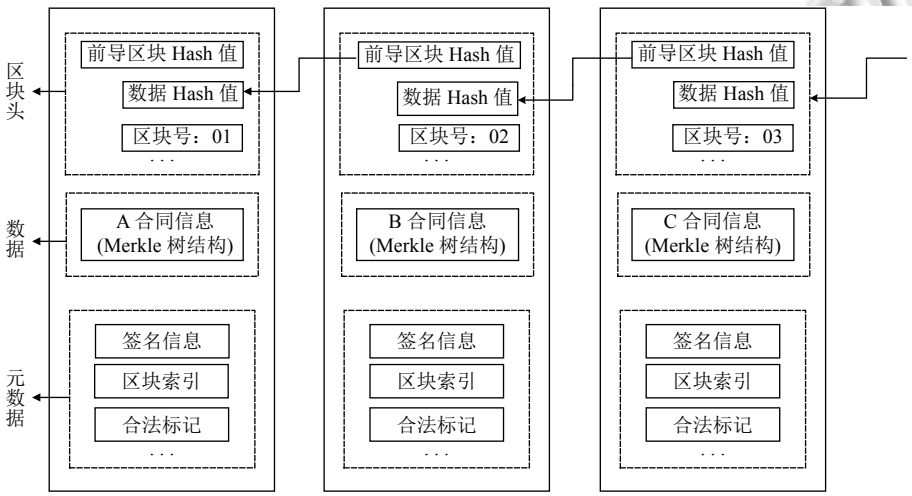

图 1 区块结构图

3 区块链技术应用于物资合同管理

经过第 2 节的可行性分析, 不难发现把区块链技术应用于物资合同管理可以弥补传统电子合同的存储安全缺陷, 以区块链技术实现的电子合同在合同的签署前都无异于传统的电子合同, 合同的安全性都建立在密码学的基础之上, 在合同的存证阶段, 区块链技术实现的电子合同的安全性和透明性等优势才真正展现出来, 利用本文提出的共识机制验证合同的有效性和分布式“记账”存储是区块链技术应用于物资合同管理的核心优势.

针对电力行业物资合同签署麻烦和后期管理困难的现状, 本节介绍利用区块链技术实现电力企业和物资供应商组成的联盟链, 用于电力企业和物资供应商之间签署合同. 联盟链的底层由物资合同履约平台提供数据和 Web 交互界面, 联盟链的设计由基础层、逻辑层、安全层和业务层组成.

3.1 底层的物资合同履约系统

本文阐释的以区块链技术实现的电子合同依托于国网辽宁电力有限公司物资分公司的物资合同履约平台, 在系统的业务应用层中的合同管理模块加入区块链技术, 令合同的签订成本更低, 线上签署合同更加便捷, 以此形成真实有效的物资管理合同大数据, 用于驱动交易, 简化管理, 图 2 展示的是物资合同履约平台的架构图.

3.2 合同管理联盟链架构

结合物资合同履约平台的数据通信层和业务应用层, 由数据通信层提供电力行业供应商的相关信息, 业务应用层接收数据并构建“物资业务大数据中心”, 通过“合同管理应用”对物资合同进行线上的签署和管理. 合同管理应用是一个分布式的应用系统, 整个系统架构设计如图 3.

底层是 P2P 的分布式网络, 第二层是逻辑层, 主要应用共识机制来保证了分布式系统的一致性问题, 安全层主要设计了身份管理、权限管理和监管模块等功能, 应用层借助于物资业务管理系统的数据接口中的 Web 服务, 提供友好的 Web 交互界面方便线上操作.

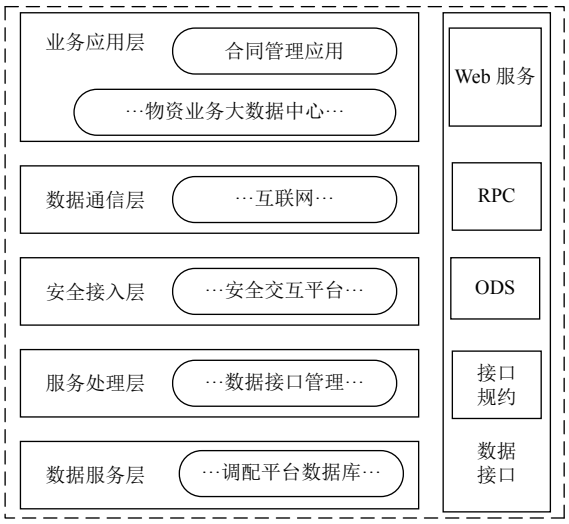

图 2 物资合同履约平台架构

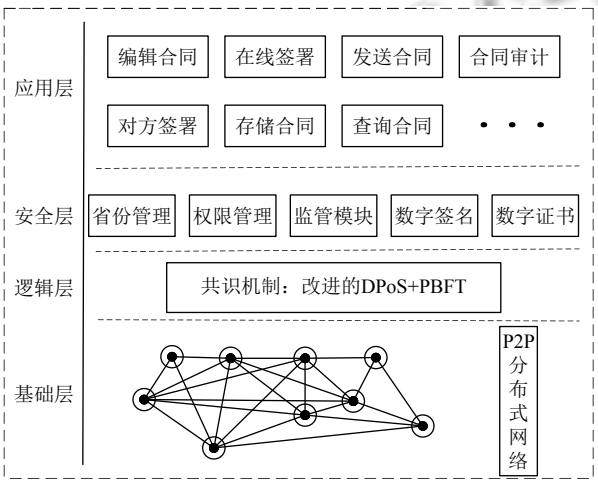

图 3 合同管理联盟链架构

3.2.1 基础层的设计

基础层分布着以 P2P 方式交互的节点服务器[9–12], 节点由电力企业和物资供货商等机构维护, 所有节点存储着合同的第三方存证. 基础层定义了数据的区块结构, 为了加强合同信息的安全性, 使电力企业和供应商之间签订的合同内容不被其他供应商节点获取, 区块中合同交易信息的加密存储采用同态加密.

同态加密是一种不需要对加密数据进行提前解密就可以进行其他计算的加密方法, 可以实现对多个密文进行计算之后再解密[13,14]. 同态加密是一种加密函数, 定义一个运算符 Δ, 对加密算法 E, 如果满足:

$$E(X\Delta Y)=E(X)\Delta E(Y) \tag{1}$$

链中的验证节点就不需要对区块数据解密而进行运算.

新签署一个合同要广播到联盟链中等待其他节点验证, 验证节点需要对区块进行一些计算操作, 而不需要知道区块的具体内容, 利用同态加密可以放心的让验证节点对待验证区块进行处理而无法访问区块中合同数据.

3.2.2 逻辑层的设计

为了保证联盟链底层节点维护区块的一致性问题, 本文提出了一种适用于电力行业物资合同管理中的共识机制——基于改进的委托权益证明 (Delegated Proof of Stake, DPoS) 的实用拜占庭容错算法 (Practical Byzantine Fault Tolerance, PBFT)[15,16], 委托权益证明的关键点是选出代理节点进行记账, 而实用拜占庭算法需要一个主节点接收客户端发送的请求并广播给其它节点, 故采用 DPoS 共识机制选出的代理节点作为 PBFT 算法的主节点. DPoS 算法通常按照节点持有的代币 (Token) 来衡量其在选举代理节点时的影响力, 考虑到本文联盟链中的节点类型, 本文采用和电力企业签署合同的次数作为供应商节点拥有权益的参照, 权益证明公式为:

$$S_i=\ln(N_i) \tag{2}$$

其中, S_i 代表网络中第 i 个供应商节点的权益, N_i 为电力企业和供应商 i 进行合同交易的次数. 之所以对 N_i 取对数, 基于以下三点考虑:

(1) 和作为甲方的电力企业合作交易的次数越多的供应商越值得信赖, 进而获得更多的权益, 由于对数函数是一个递增的函数, 故满足这一要求.

(2) 根据电力企业作为甲方和供应商和乙方签订合同的历史数据分析, 签订合同的次数越多, 出现签订失败或者合同违约的次数就越多. 当合同交易失败或者出现违约情况, 权益的增速就会递减.

(3) 由于 DPoS 自身的局限性, 随着时间的增加, 权益越大的节点获得记账的权利就越大, 越容易产生马太效应, 即权益越大的节点会获得更多的权益, 从而形成两极分化的现象, 最终产生超过 50% 的中心化节点, 被动的演化为“假的”去中心化的结果. 对交易合同的次数取对数后, 可以有效的限制和电力企业有频繁交易的供应商节点获得更多的权益.

本文使用的共识机制紧密结合实际使用场景, 对比其它联盟链中常用的共识机制, 因采用合同签订次

数作为权益, 避免了使用代币而产生的维护成本, 结合 DPoS 和 PBFT, 动态给节点授权让代理节点的选择更加可靠, 节点作恶篡改合同的可能性变小, 进一步加强了合同存证的安全性.

表 1 联盟链中常用共识机制对比

	模型类型	容忍出错节点数 (*N* 为总节点数)	是否需要 token	缺陷
Raft	算法	(*N*–1)/2	否	不支持容错作恶节点
DPoS	经济	(*N*–1)/2	是	依赖 token, 记账节点相对固定
PBFT	算法	(*N*–1)/3	否	超过 1/3 以上节点停止工作, 系统将无法提供务
本文共识机制	经济+算法	(*N*–1)/3	否	弱中心化

3.2.3 安全层的设计

安全层包括了身份管理、权限管理和监管模块等. 由于本文的联盟链节点是电力企业和供应商企业共同维护, 为了节点的正常工作, 需要赋予电力企业节点和供应商节点不同的权限[14], 身份管理主要是身份认证、授权. 身份认证分为企业身份认证和个人身份认证, 企业身份认证主要通过企业公商注册信息、法人身份认证和 IP 地址进行确定; 个人身份认证通过物资合同履约平台中数据接入层提供的接口获得数据验证个人姓名、身份证号和手机号是否匹配, 最终确认个体身份. 监管模块主要有成员管理、监控和审计功能, 成员管理主要的功能是增加和删除供应商节点, 监控供应商节点的权益, 配合本地 CA 系统审核合同的电子签章和统计节点的记账权.

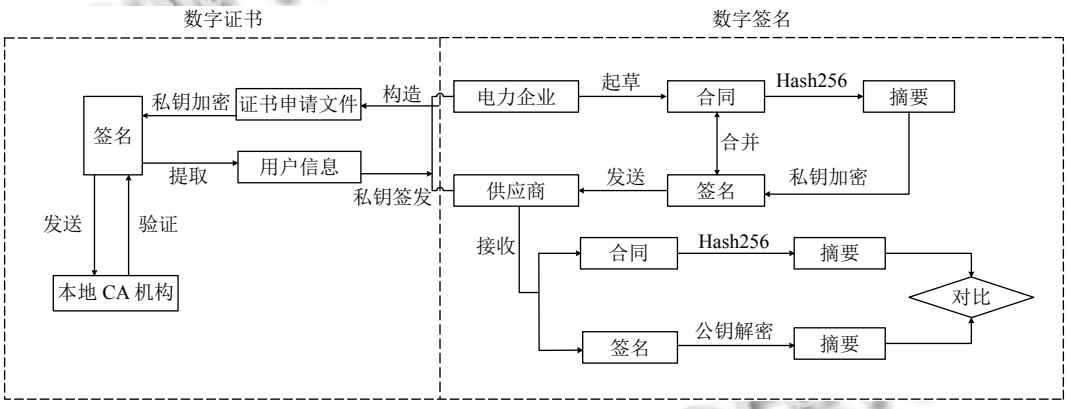

图 4 数字签名和数字证书流程图

本文使用区块链技术实现合同的第三方存证, 保证了合同在存储方面的安全, 线上签署合同的安全依赖数字签名和数字证书, 利用数字签名技术[17–19]即可以保证合同内容的完整性, 同时又可以确认合同来源, 具有不可抵赖性. 由于数字签名是一种非对称加密技术, 通过本地 CA 系统分发公钥和私钥, 保证公钥和私钥自身的安全性. 安全层通过搭建本地的 CA(Certificate Authority) 系统, 用于负责验证电力企业和供应商提交的证书申请文件, 验证通过之后用 CA 的私钥对提取到的用户信息并加上颁发信息进行签发, 最终将数字证书发送给电力企业和供应商.

3.2.4 应用层是设计

应用层实现了签署合同相关的业务交互逻辑, 电力企业和供应商通过 Web 客户端起草合同、在线签署、发送合同、对方签署、存储合同、修改合同和查询合同. 在合同的签署阶段和传统的电子合同没有区别, 使用加密算法签署的合同和纸质版的合同同样具有法律效力. 引入区块链技术在于通过第三方存证来存储合同, 合同一旦签署成功, 客户端向网络中的代理节点发送请求, 代理节点接收到客户端请求后, 代理节点广播消息给其它节点并等待其它节点确认, 一旦超过[(*N*–1)/3]+1 个节点确认, 表示大部分节点已经完成共识, 所有节点把带有合同信息的区块维护到自己的链上, 保证了合同信息不被篡改并且易于追溯.

4 仿真实验结果分析

本文设计的使用区块链技术实现的合同管理应用通过和 34 家电力设备供应商试运行 3 个月的时间, 证

实了区块链技术适用于国网公司同物资供应商之间签署合同管理的场景, 并且通过系统稳定运行以及和其它共识机制的横向对比, 验证了本文提出的共识机制的可用性和先进性.

4.1 实验过程设计

为了保证国网公司物资采购业务的正常运转, 区块链系统试运行的 3 个月内, 既在物资合同履约平台上的合同管理应用中签署合同, 又同时签署纸质合同, 试运行阶段, 验证可用性的环节有增加新的供应商节点、对供应商节点的权限管理、合同签署之后是否被区块链所“认可”.

在共识机制对比环节中, 因 Raft 算法不支持容错作恶节点, DPoS 权益机制依赖代币, 权益越大的节点获得的记账权利越大, 会形成强者愈强、弱者愈弱的马太效应, 故不考虑对比上述两个共识机制, 主要和 PBFT 共识机制进行对比, 对比方法为同时运行基于 PBFT 共识机制和本文共识机制的两个联盟链, 通过观察记账节点的变动, 人为干预一定数量的节点作恶, 通过观察合同信息是否被篡改, 验证共识机制的先进性.

4.2 结果分析

系统试运行阶段, 在保证节点通信正常的情况下, 合同从起草到修订再到最后的签名确认, 最终签署 75 份合同, 比纸质合同签署平均节省 11 天, 在人力资源、工作效率和管理体验等方面都优于纸质合同.

在对比共识机制的过程中, PBFT 算法的记账节点选择、变更的较随意, 而本文的共识机制根据合同签订次数作为权益, 在选举记账节点时, 和国网公司合作更密切的供应商 A、B 和 C 作为记账节点的次数更多, 在不考虑节点故障等不可避免的问题后, 经过 15 次人工干预 20 个节点作恶, 使用 PBFT 共识机制的系统出错 9 次, 使用本文共识机制的系统出错 4 次. 验证了本文提出的共识机制在应对作恶节点数大于 $(N–1)/3$ 时, 比 PBFT 共识机制有较强的容错性.

表 2 合同签订次数统计

	供应商 A	供应商 B	供应商 C	供应商 D	供应商 E	…	供应商 E
次数	17	15	9	4	1	…	1

5 结论

电力企业中合同管理是建设电网工程项目管理的核心, 做好合同管理这一环节在很大程度上能降低合同的风险, 使电网建设工程的进度和质量得到保障, 传统的电子合同在很大程度上解决了纸质合同签订流程繁琐、需要专人送达和后期管理不便等问题. 但由于电子合同是存储在计算机中, 很容易由于不可抗力因素或者黑客攻击造成合同信息的泄露或丢失. 把区块链技术引入电子合同可以解决传统电子合同的一系列安全隐患, 电力企业和供应商建立联盟链, 通过以合同签订次数作为权益的共识机制可以提供更加安全可靠的通信节点, 区块链技术的加入可以实现低信任的成本换来更开放、高效和不可抵赖的物资合同签署.

参考文献

1 张和平, 王正蓉, 赵蓉. 解析电网企业物资合同管理. 科技与创新, 2015, (15): 56, 58.

2 徐涓涓. 电网工程类合同中常见风险与防范措施. 经济研究导刊, 2014, (14): 276–277. [doi: 10.3969/j.issn.1673-291X.2014.14.116]

3 蔡维德, 郁莲, 王荣, 等. 基于区块链的应用系统开发方法研究. 软件学报, 2017, 28(6): 1474–1487.

4 朱岩, 甘国华, 邓迪, 等. 区块链关键技术中的安全性研究. 信息安全研究, 2016, 2(12): 1090–1097.

5 沈鑫, 裴庆祺, 刘雪峰. 区块链技术综述. 网络与信息安全学报, 2016, 2(11): 11–20. [doi: 10.11959/j.issn.2096-109x.2016.00107]

6 谢辉, 王健. 区块链技术及其应用研究. 信息网络安全, 2016, (9): 192–195. [doi: 10.3969/j.issn.1671-1122.2016.09.038]

7 黄锐. 金融区块链技术的监管研究. 学术论坛, 2016, 39(10): 53–59. [doi: 10.3969/j.issn.1004-4434.2016.10.012]

8 高志豪. 公有链和联盟链的道法术器. 金卡工程, 2017, (3): 35–39. [doi: 10.3969/j.issn.1671-2498.2017.03.014]

9 Androutsellis-Theotokis S, Spinellis D. A survey of peer-to-peer content distribution technologies. ACM Computing Surveys (CSUR), 2004, 36(4): 335–371. [doi: 10.1145/1041680]

10 袁巍, 李津生, 洪佩琳. 一种 P2P 网络分布式信任模型及仿真. 系统仿真学报, 2006, 18(4): 938–942. [doi: 10.3969/j.issn.1004-731X.2006.04.032]

11 史艳芬, 葛燧和. 一种 P2P 网络安全信任模型的设计与实

现. 计算机应用, 2005, 25(3): 554–556.
12 Jayapandian N, Zubair Rahman AMJ. Secure and efficient online data storage and sharing over cloud environment using probabilistic with homomorphic encryption. Cluster Computing, 2017, 20(2): 1561–1573. [doi: 10.1007/s10586-017-0809-4]
13 张永, 李晓辉. 一种改进的区块链共识机制的研究与实现. 电子设计工程, 2018, 26(1): 38–42, 47. [doi: 10.3969/j.issn.1674-6236.2018.01.008]
14 黄方蕾. 联盟区块链中成员动态权限管理方法的设计与实现[硕士学位论文]. 杭州: 浙江大学, 2018.
15 韩璇, 刘亚敏. 区块链技术中的共识机制研究. 信息网络安全, 2017, (9): 147–152. [doi: 10.3969/j.issn.1671-1122.2017.09.034]
16 王海勇, 郭凯璇, 潘启青. 基于投票机制的拜占庭容错共识算法. 计算机应用. http://kns.cnki.net/kcms/detail/51.1307.TP.20190129.1009.002.html, [2019-01-29/2019-02-22].
17 关振胜. 《电子签名法》与数字签名的技术实现. 电子商务, 2006, (1): 36–43. [doi: 10.3969/j.issn.1009-6108.2006.01.005]
18 Moldovyan NA, Moldovyanu PA. New primitives for digital signature algorithms. Quasigroups and Related Systems, 2009, 17(2): 271–282.
19 Seberry J, To V, Tonien D. A new generic digital signature algorithm. Groups–Complexity–Cryptology, 2011, 3(2): 221–237.