一种基于区块链的物联网架构

陈诗鹏[1,2]，陈彬[1,2]，代明军[1,2]，王晖[1,2]
（1. 深圳大学区块链技术研究中心，广东 深圳 518060；2. 深圳大学电子与信息工程学院，广东 深圳 518060）

摘 要：基于传统互联网的物联网架构面临着数据隐私安全问题、中心服务器单点问题等，构建数据安全的生态系统是未来物联网发展面临的一个挑战，区块链技术所具备的去中心化自治、防篡改、安全性等特性为应对这一挑战提供了新的思路。提出了一种基于区块链技术的物联网架构作为去信任网络的基础平台，为物联网提供信息安全的网络服务。基于区块链技术的去中心化特性，该架构可以替换传统物联网的客户端—服务器（C-S, client-server）集中式通信模型，解决了传统物联网中的单点负载以及数据安全问题。

关键词：物联网；区块链；智能合约；信息安全
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.2096–3750.2020.00171

Blockchain-based IoT architecture

CHEN Shipeng[1,2], CHEN Bin[1,2], DAI Mingjun[1,2], WANG Hui[1,2]
1. Blockchain Technology Research Center, Shenzhen University, Shenzhen 518060, China
2. College of Electronics and Information Engineering, Shenzhen University, Shenzhen 518060, China

Abstract: The Internet of things (IoT) architecture based on the traditional Internet is facing data privacy security issues, central server single point issues, and etc. Building a data security ecosystem is a challenge for the future development of the IoT. The decentralized autonomy, tamper-resistance and security of the blockchain technology are proposing a new solution to this challenge. An IoT architecture was proposed based on the blockchain technology as the foundation of a trust-free network, which provided an information-secure network service for the current IoT. Based on the decentralized characteristics of the blockchain technology, the proposed architecture could replace the client-server (C-S) centralized communication model of the traditional IoT to solve the overload problem of the central server and the data security issues.

Key words: Internet of things, blockchain, smart contract, information security

1 引言

物联网（IoT, Internet of things）被认为是继互联网时代后信息产业革命发展掀起的第 3 次浪潮，IoT 技术依赖于互联网环境，将各种终端设备与互联网结合起来，形成一个物—物相连的巨大网络。随着信息技术的发展，IoT 技术已经逐步深入到人们生活的各个方面。

IoT 层次结构自底向上可分为 3 层：感知层、网络层和应用层[1-3]。感知层主要负责数据采集；网络层利用无线或有线的网络将来自感知层的各类数据信息进行组网传输汇聚；应用层作为结构模型

收稿日期：2020−03−20；修回日期：2020−05−02
通信作者：陈彬，bchen@szu.edu.cn
基金项目：教育部科技发展中心产学研创新基金—新一代信息技术创新项目（No.2019J02002）；深圳市基础研究项目（No.JCYJ20170818091801577）；广东省自然科学基金资助项目（No.2018A0303130131）
Foundation Items: The Industry-University-Research Innovation Fund of Science and Technology Development Center of Ministry of Education-New Generation Information Technology Innovation (No.2019J02002), The Fund of Shenzhen Basic Research (JCYJ20170818091801577), The Natural Science Foundation of Guangdong (No.2018A0303130131)

的顶层，通过云计算平台等对所获得的数据进行处理，为用户提供基于数据的应用。随着 IoT 应用的日益普及，IoT 环境下的信息安全问题也日益突出[4-5]，主要表现在以下 3 个方面。

1) 集中式结构造成的潜在单点故障以及可扩展性问题

传统的 IoT 架构采用客户端—服务器（C-S, client-server）集中式通信模型，IoT 设备之间通过中心服务器进行数据交互。一旦中心服务器发生故障，依托于中心服务器的 IoT 设备都将无法正常运转。同时随着 IoT 设备数量的日益增多，中心服务器所需要处理的数据量也将剧增，网络将面临可扩展性问题[6]。

2) IoT 设备数据隐私安全问题

当前的 IoT 架构采用集中式模型，所有 IoT 设备都依托中心服务器进行数据的汇聚处理，一旦中心服务器的安全得不到保障，节点数据就会存在被泄露的可能[7]。

3) IoT 设备资源有限，容易被黑客攻克用作分布式阻断服务（DDoS, distributed denial of service）攻击的工具

IoT 设备作为网络终端节点主要为物联网提供数据采集与数据传输等轻量级服务，其计算与存储能力有限，难以满足复杂的安全性要求，容易受到网络攻击，被黑客当作 DDoS 攻击的工具[8-9]。

由上述分析可知，大规模 IoT 网络的安全和可扩展性等问题主要受制于传统互联网 C-S 集中式通信模型。

传统 IoT 的中心化 C-S 结构与基于区块链的分布式 IoT 结构如图 1 所示。传统 IoT 结构基于现有互联网环境，依赖于中心服务器进行设备之间的数据交互，而区块链技术有机地融合了分布式系统、哈希算法、默克尔树、数字签名、P2P 网络等一系列技术并结合奖励机制，在主机类型和数量不受限制的异步公共网络中实现分布式系统的共识，保证了分布式系统中数字信息的不可篡改性和唯一性，其去中心化的处理方式保证了网络的可扩展性与安全性。近年来，引入区块链技术来解决 IoT 的安全问题受到研究学者的关注[10-12]。

然而，在区块链技术引入 IoT 的过程中还需要解决两个问题：1) 由于 IoT 设备资源约束，大多数设备仅具备数据采集功能，不具备存储完整区块链账本的存储能力，无法作为区块链中的节点；2) 随着设备数量呈指数级增长，IoT 设备记录的数据信息量也将剧增[13-14]，将数据直接存储于区块链上的方式将会导致能够完整存储账本的节点数量减少，而这将削弱去中心化系统架构的安全性。为此，本文提出一种将区块链作为中间层的 IoT 架构，利用区块链的去中心化、去信任以及数据加密传输等特点为 IoT 提供可靠的网络环境，同时提供一种基于链上验证结合链下云存储服务的方案以解决数据存储的问题。

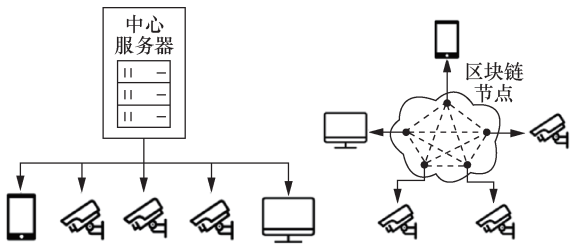

图 1　传统 IoT 的中心化 C-S 结构与基于区块链的分布式 IoT 结构

2　基于区块链的 IoT 架构

2.1　网络模型

本文针对传统 IoT 的 3 层架构进行改进，基于区块链的 IoT 层次结构如图 2 所示，在传统的网络层上增添一层区块链层，该层的作用是在基础网络上利用区块链中的加密技术为数据的隐私安全提供保障，利用区块链去信任的特点去除中心服务器，将 IoT 传统的 C-S 集中式通信模型转换为分布式 P2P 模型，为上层应用层提供可靠的网络环境。

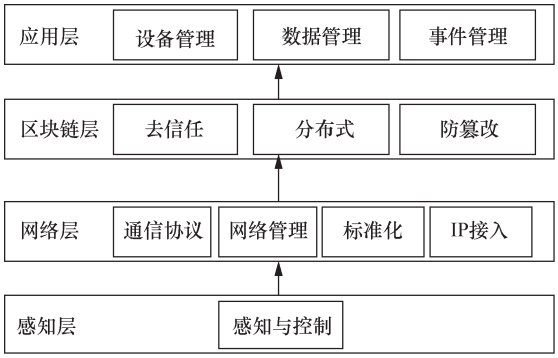

图 2　基于区块链的 IoT 层次结构

本文以智慧小区为研究场景，以智慧小区为模型的实体结构如图 3 所示，主要由 4 个部分组成。

1) IoT 设备：指传感器、监控设备以及家庭个人设备等，负责数据采集，与节点相连进行信息交互。

2) 家庭住户节点：家庭住户的个人计算机等智能设备作为区块链网络节点用以连接公共区块链网络，并充当家庭内部 IoT 设备与区块链网络的中介。

3) 公共网关节点：公共 IoT 设备所依托的网关节点，同时作为区块链网络节点，由小区物业管理运行，记录小区内部终端设备采集的数据信息。

4) 云存储服务节点：与区块链网络相连，提供链上权限验证和链下存储服务。

其中，家庭住户节点、公共网关节点与云存储服务节点都可以通过互联网与区块链网络连接，IoT 设备依托于网关节点进行链上的信息交互。

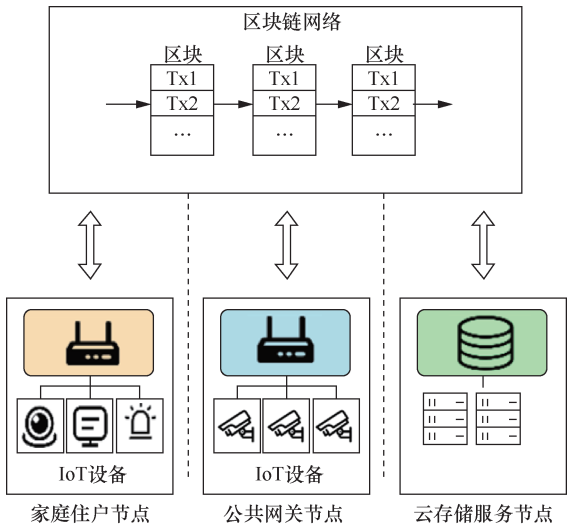

图 3　以智慧小区为模型的实体结构

2.2　公共区块链记录设备权限

IoT 设备不断地产生大量数据，将该数据直接存储于链上是不现实的。基于链上验证的链下云存储服务是一种可行方案，将于第 3 节进行详细分析。并且，公共区块链中的区块仅记录各种设备的权限 token 状态和智能合约，而不记录 IoT 设备产生的数据。

权限 token 作为设备在链上的可信凭证，标志着不同设备的权限以及权限持有人，将设备权限记录于链上能够保障权限记录的不可篡改性以及可验证性。节点之间通过验证权限 token 以及执行对应智能合约能对相应设备进行自定义控制，云存储服务通过链上验证节点存储服务的权限 token 进行链下数据的加密传输与存储。该区块链网络的功能包括权限 token 生成、权限 token 转移和权限 token 销毁。

1) 权限 token 生成

节点在将新的 IoT 设备加入区块链网络时，需要一笔权限 token 生成交易，当该交易在链上公布后，区块链中的所有节点都能通过该交易验证相应设备的权限以及权限持有人（家庭住户节点或公共网关节点），具备该设备权限的节点能对其进行控制。

以住户节点 A 将 IoT 设备 M 上链为例，权限 token 生成交易如图 4 所示。该笔 token 的交易输入设置为空，输出为节点 A 的公钥地址（address A），同时包含设备信息、权限、权限持有人等字段信息，最后以节点 A 的私钥进行数字签名（Signature A）。当该笔交易被打包进区块后，网络中的节点可以通过输出地址 address A 验证签名来确定该设备控制权属于 A。

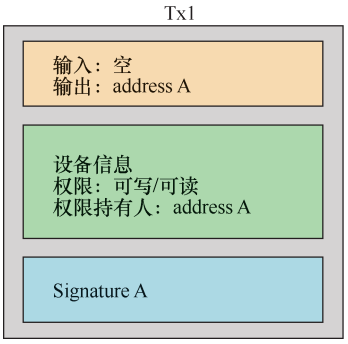

图 4　权限 token 生成交易

2) 权限 token 转移

在需要将设备的权限转移给其他节点时，如酒店将房间内部设备的控制权暂时交给房客，节点通过生成一笔 token 交易进行权限短时转移或持久转移。以节点 A 转移 IoT 设备 M 的权限转移给节点 B 为例，权限 token 转移交易如图 5 所示。权限转移的过程就是 token 交易的过程，在 token 交易中，输入指向包含 IoT 设备 M 地址的最后一笔 token 交易 Tx1，输出为新的控制节点 B 的公钥地址（address B），权限字段可以设置为转移赋予的读/写权限，通过设置失效时间字段来限制权限的使用时长，一般以区块高度作为时间基准。若需要更换 IoT 设备的网关节点，也可以将权限持有人进行永久转换。最后将该笔交易通过节点 A 的私钥进行签名，发布至链上。

3) 权限 token 销毁

如果某个 IoT 设备由于故障或者其他原因离开网络，则可以通过一笔输出地址为黑洞地址[15-17]的 token 转移交易来实现。

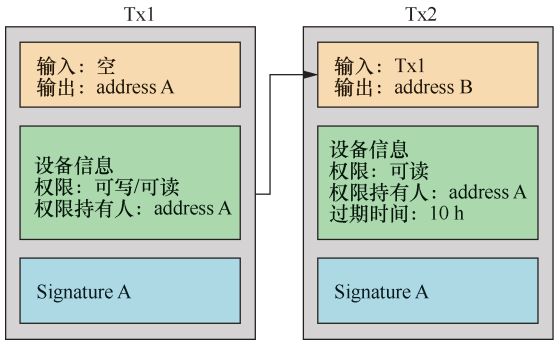

图 5　权限 token 转移交易

2.3　基于智能合约的设备控制方法

本文的设备控制主要以家庭内部智能设备的自主协调为例，IoT 设备通过无线或有线方式与家庭内部网关相连接，家庭内部网关作为公共区块链网络的节点，记录监听区块链上的状态变化。

依赖于链上的设备权限 token 记录，家庭内部的智能化操作通过执行发布于区块链上的智能合约来完成。网关节点监听智能合约的状态变化，根据状态变化执行智能合约指定 IoT 设备的控制指令，以实现对设备的远程控制。

以节点 A 控制家庭内部的电视机设备 Q 的开关为例。

步骤 1　智能合约发布

节点 A 首先发布一个电视开关的智能合约，将对应的权限验证策略（access strategy）写入合约内部，权限验证策略作为合约内部的函数用以验证合约调用者是否满足权限条件，智能合约如图 6 所示。在该例中将权限持有人（owner）赋值为电视机 Q 权限 token 的生成交易（Txgenerate Q）并记录于合约内部，权限验证策略则需要判断合约调用者的地址是否为 owner。发布成功后，该合约作为一笔交易被记录在区块链网络上，获得返回的合约地址 address C，家庭网关节点持续监听开关状态（state）的变化。

步骤 2　智能合约执行

当节点 A 在任意地方、任意时候进行控制电视机 Q 的开关操作时，节点 A 连接到该区块链，发起一笔合约调用。合约执行如图 7 所示，请求节点调用合约地址 address C 的 open 函数，合约内部通过 access strategy 验证请求节点是否具备该合约函数的执行权限。验证成功后执行 open 函数，改变开关 state。家庭内部网关节点监听到开关 state 变化的事件，便会控制电视机设备 Q 开机。

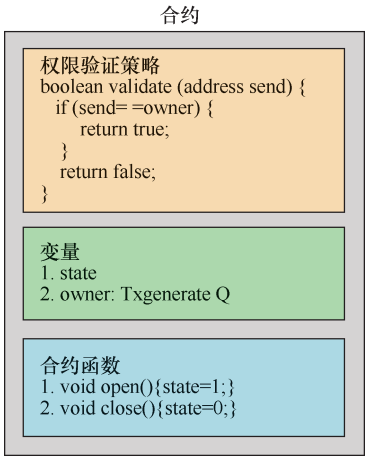

图 6　智能合约

本文基于以太坊平台对智慧小区进行模拟，利用 Geth 搭建私有链环境，基于以太坊 ERC20 协议开发权限 token，利用多个树莓派以及计算机主机模拟小区网关节点，以树莓派所连接的小灯泡模拟 IoT 设备，通过部署以太坊智能合约进行控制。

3　链下云存储服务

区块链技术是一种分布式存储技术，由多个节点来备份链上数据，不适合 IoT 设备大数据量的存储。因此，本文为基于区块链的 IoT 提供安全的链下云存储服务，以降低区块链的存储成本，通过链上提供的防篡改权限验证机制为链下的数据读/写操作提供访问控制。

3.1　云存储服务智能合约生成

云存储服务运营商发布的云存储订阅合约如

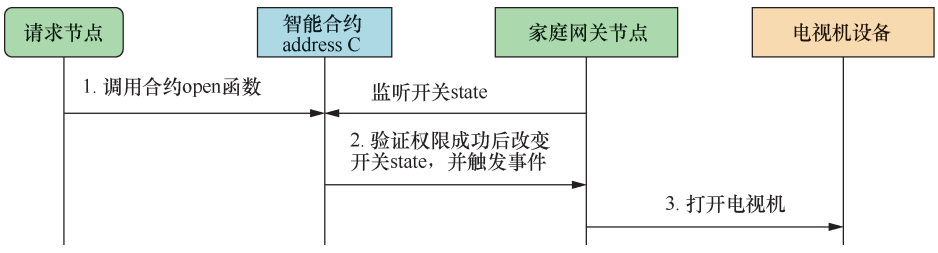

图 7　合约执行

图 8 所示，该合约具备以下 3 个主要功能：申请存储空间、读请求和写请求。合约内部写入权限验证策略以避免恶意读/写请求，在本例中为判断请求节点是否存在于节点列表（List）中。

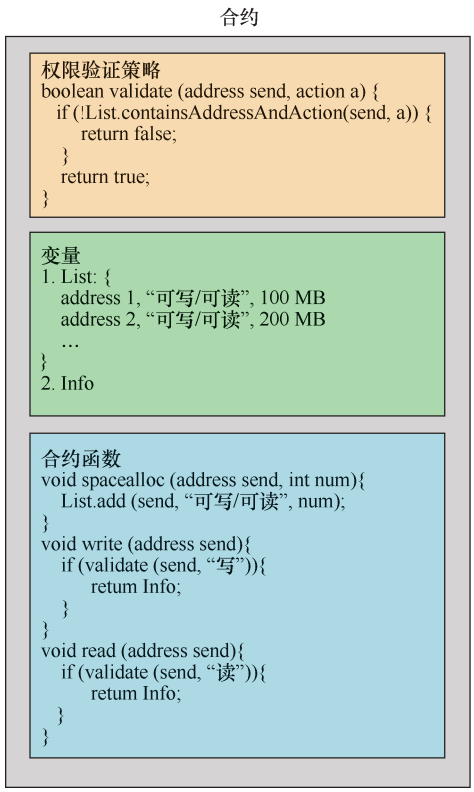

图 8　云存储订阅合约

3.2　云存储空间申请

节点申请云存储空间的操作如下。

1) 请求节点通过云存储服务的智能合约地址，根据申请空间的大小（num）支付一定数量的金额给该合约账户，来调用该合约申请的存储空间。

2) 在智能合约接收到请求以及确认金额数量满足后，合约内部执行 space_alloc 函数将请求节点地址添加至 List，并赋予对应节点存储空间以及读/写权限。

3.3　请求云存储服务读/写操作

节点请求云存储服务的读/写操作由以下环节组成。

1) 请求节点通过云存储服务的智能合约地址调用合约读/写操作，合约内部通过 List 检测是否包含请求节点，并检测是否具备请求操作的对应权限，若具备则执行返回云存储服务链下连接信息（Info）。

2) 请求节点接收到返回的 Info 后，在链下与云存储服务进行连接，提交新的读/写请求，利用私钥进行签名并发送。

3) 云存储服务接收到读/写请求后，先通过请求节点公钥进行签名验证，并检测合约内部是否具备请求节点公钥以及是否具备相应请求操作，若验证成功则生成对称密钥 s，同时，利用请求节点公钥进行加密并返回。

4) 请求节点解出对称密钥 s，然后在链下通过对称密钥 s 与云存储服务进行信息交互和数据读取。

云存储服务读/写操作流程如图 9 所示，给出了将链上权限转移控制为链下的云存储服务功能，同时可选择加密技术以保证链下数据传输的安全性。

4　结束语

区块链具备的分散、自治和去信任的特点使其成为 IoT 解决方案的一个理想组件。本文针对区块链在智慧小区 IoT 中的应用模型，给出了区块链的设计方法，使得 IoT 能够利用区块链的分布式特性来提高 IoT 的可拓展性和安全性。同时，也为该应用设计了数据的链上赋权、链下存储方法，从而保证了该方法的实用性。

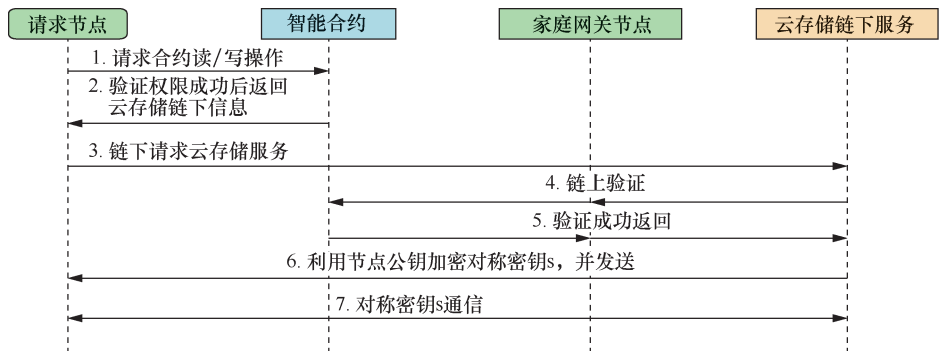

图 9　云存储服务读/写操作流程

参考文献：

[1] 沈苏彬, 范曲立, 宗平, 等. 物联网的体系结构与相关技术研究[J]. 南京邮电大学学报(自然科学版), 2009, 29(6): 1-11.
SHEN S B, FAN Q L, ZONG P, et al. Study on the architecture and associated technologies for Internet of things[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science), 2009, 29(6): 1-11.

[2] 孙其博, 刘杰, 黎羴, 等. 物联网: 概念, 架构与关键技术研究综述[J]. 北京邮电大学学报, 2010, 33(3): 1-9.
SUN Q B, LIU J, LI S, et al. Internet of things: summarize on concepts, architecture and key technology problem[J]. Journal of Beijing University of Posts and Telecommunications, 2010, 33(3): 1-9.

[3] WU M, LU T J, LING F Y, et al. Research on the architecture of Internet of things[C]//2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). IEEE, 2010, 5: V5-484-V5-487.

[4] SINGH S, SINGH N. Internet of things (IoT): security challenges, business opportunities & reference architecture for e-commerce[C]// 2015 International Conference on Green Computing and Internet of Things (ICGCIoT). IEEE, 2015: 1577-1581.

[5] 王宗慧, 张胜利, 金石, 等. 区块链数据隐私保护研究[J]. 物联网学报, 2018, 2(3): 71-81.
WANG Z H, ZHANG S L, JIN S, et al. Survey on privacy preserving techniques for blockchain[J]. Chinese Journal on Internet of Things, 2018, 2(3): 71-81.

[6] GOMES M, DA ROSA RIGHI R, DA COSTA C A. Internet of things scalability: analyzing the bottlenecks and proposing alternatives[C]// 2014 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). IEEE, 2014: 269-276.

[7] ZHANG Z K, CHO M C Y, WANG C W, et al. IoT security: ongoing challenges and research opportunities[C]//2014 IEEE 7th International Conference on Service-Oriented Computing and Applications. IEEE, 2014: 230-234.

[8] KOLIAS C, KAMBOURAKIS G, STAVROU A, et al. DDoS in the IoT: Mirai and other botnets[J]. Computer, 2017, 50(7): 80-84.

[9] LALLY G, SGANDURRA D. Towards a framework for testing the security of IoT devices consistently[C]//International Workshop on Emerging Technologies for Authorization and Authentication. Springer, 2018: 88-102.

[10] FERNÁNDEZ-CARAMÉS T M, FRAGA-LAMAS P. A review on the use of blockchain for the Internet of things[J]. IEEE Access, 2018, 6: 32979-33001.

[11] BANERJEE M, LEE J, CHOO K K R. A blockchain future for Internet of things security: a position paper[J]. Digital Communications and Networks, 2018, 4(3): 149-160.

[12] 查选, 王旭, 倪巍, 等. 区块链技术的一致性和容量的研究与发展及在物联网中的应用[J]. 物联网学报, 2017, 1(1): 21-33.
ZHA X, WANG X, NI W, et al. Blockchain for IoT: the tradeoff between consistency and capacity[J]. Chinese Journal on Internet of Things, 2017, 1(1): 21-33.

[13] International Data Corporation (IDC). Worldwide and regional Internet of things (IoT) 2014-2020 forecast: a virtuous circle of proven value and demand: IDC #248451[R]. 2014.

[14] 钱卫宁, 邵奇峰, 朱燕超, 等. 区块链与可信数据管理: 问题与方法[J]. 软件学报, 2018, 29(1): 150-159.
QIAN W N, SHAO Q F, ZHU Y C, et al. Research problems and methods in blockchain and trusted data management[J]. Journal of Software, 2018, 29(1): 150-159.

[15] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. 2019.

[16] WOOD G. Ethereum: a secure decentralized generalized transaction ledger[J]. Ethereum Project Yellow Paper, 2014, 151: 1-32.

[17] 张胜利, 王滔滔, 杨晴, 等. 高性能许可公链[J]. 深圳大学学报理工版, 2020, 37(3): 227-233.
ZHANG S L, WANG T T, YANG Q, et al. Permissioned public blockchain with high performance[J]. Journal of Shenzhen University Science and Engineering, 2020, 37(3): 227-233.

[作者简介]

陈诗鹏（1996– ），男，深圳大学硕士生，主要研究方向为区块链共识技术以及智能合约。

陈彬（1975– ），男，博士，深圳大学副教授、硕士生导师，主要研究方向为区块链共识机制以及智能合约安全机制、深度强化学习在云计算网络优化中的应用等。

代明军（1982– ），男，博士，深圳大学副教授，主要研究方向为网络编码、协作通信、软件定义网络等。

王晖（1969– ），男，博士，深圳大学教授、博士生导师，主要研究方向为区块链、无线网络等。