



专栏：5G 商用和演进

基于区块链技术的 BaaS 平台架构及应用

齐磊, 祝好, 顾慧琼, 陈旭, 胡泊

(中国移动通信集团设计院有限公司, 北京 100080)

摘要: 为消除传统电信行业复杂和长链的相互关联操作, 解决对账、清算等一致性保证问题, 设计了基于区块链的 BaaS 平台, 利用区块链技术将用户和交易等信息上链, 共建透明互信的区块链账本, 实现电信行业所需的信任、安全和公平机制。

关键词: 区块链; 许可链; BaaS; 智能合约

中图分类号: TP319

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2020267

Application and farmework of BaaS platform based on blockchain

QI Lei, ZHU Hao, GU Huiqiong, CHEN Xu, HU Bo

China Mobile Group Design Institute Co., Ltd., Beijing 100080, China

Abstract: To eliminate the interrelated operational effects of complex and long chains in the telecom industry, and to solve the problem of data consistency guarantee such as reconciliation and liquidation. A blockchain-based BaaS platform was designed, a permissioned blockchain with user information was deployed, and a trusted blockchain ledger was built. It realizes the trust, security and fairness mechanism in telecommunication industry.

Key words: blockchain, permissioned blockchain, BaaS, smart contract

1 引言

在传统的电信交易模式中, 记账过程是交易双方分别进行的, 不仅要耗费大量人力物力, 而且容易出现对账不一致的情况, 影响结算效率。同时, 传统清算业务环节太多, 清算链条太长, 导致清算流程耗时过长, 对账成本居高不下。

区块链, 作为以分布式数据存储、点对点传输、共识机制、加密算法、智能合约等计算机技术创新而产生的分布式账本技术, 通过新的信任

机制改变了连接方式, 带来生产关系的改变。通过区块链系统, 交易双方或多方可以共享一套可信、互认的账本, 所有的交易及清结算记录全部在链可查, 安全透明、不可篡改、可追溯, 可极大优化现有交易流程, 高效提升对账准确度和效率。

2 区块链技术

区块链架构主要分为公有链 (permissionless blockchain) 和许可链 (permissioned blockchain)

两种。目前除虚拟货币采用公有链外,考虑监管要求及灵活调整机制,绝大部分的企业级信息化应用均采用许可链架构。本文如没有特殊说明,后续所有技术介绍均特指许可链。

区块链技术核心的四大特点如下。

- 共享账本机制:区块链以块-链方式记录商业网络中的所有交易,并在参与者之间共享记录,参与者通过同步可获取自己的备份。
- 智能合约:合约中的商业规则内嵌在区块链系统中,可验证的、被签署的合约由编程语言实现,并可在交易时被执行。
- 安全机制:账本是共享的,基于密码学技术,实现参与者具有各自的隐私保护,做到交易信息保密;交易是真实的,但无须与身份绑定。
- 共识算法:共识是交易验证与确认的过程,当参与者都是已知且可信时交易确认成本降低,存在恶意节点时通过权益证明、签名方案等技术实现数据存储一致性。

区块链技术,作为一种新的协作模式,初期广泛应用于金融行业,目前在应用落地方面呈现多元化趋势,逐步向其他垂直领域扩展。考虑其在信用、价值流通和风控等方面的金融业务本质,也适用于优化电信行业订购、交易、结算等业务流程,尤其适用于去中心系统架构变革、涉及多方协作、涉及开放性但需风险可控的业务场景。

3 区块链服务平台技术架构

结合区块链技术发展及其在电信运营商的应用场景需求,借助于中国移动已建的全网资源池网络,本文构建 BaaS (blockchain as a service, 区块链服务) 平台架构,旨在为用户提供可信、可靠、高效的区块链服务,推动区块链在电信应用场景的真实落地。

BaaS 平台,分为基础设施层、虚拟业务网络

层和业务层 3 层。其中基础设施层可基于每个城市区块链节点现有云资源池分配资源,或可复用业务支撑系统现有资源,搭建多节点的区块链网络,共同存储各智能合约的交易区块数据;虚拟业务网络层,通过共识算法,保障节点安全,实现共识网络;业务层,通过搭建智能合约扩展业务。

BaaS 平台提供基础设施服务,每个虚拟业务网络可运行多个智能合约。不同的用户可在 BaaS 平台上开发不同的智能合约,满足其不同的业务需求,形成“一个基础平台,多条业务链”的协同运营。BaaS 平台技术架构如图 1 所示。

4 区块链服务平台功能架构

区块链服务平台主要包含实时交易链 EOS (enterprise operation system, 基于商用分布式应用设计的区块链操作系统)、智能合约开发和业务上链(包括生命周期管理、咪咕应用链、能开应用链和结算应用链等)等核心功能。

4.1 EOS 实时交易链支撑

区块链服务平台,既支持第三代基于 EOS 技术对并发、实时性要求的业务场景,同时支持第二代基于 Fabric 技术的对实时性要求一般的业务场景。Hyperledger Fabric 是企业构建的领先的开源、通用区块链结构,旨在作为开发模块化体系结构的区块链应用程序的基础,以便诸如共识和会员服务等组件可以即插即用。

区块链服务平台较传统基于 Fabric 技术的基础能力,引入 EOS 链支撑,主要实现 EOS 钱包管理、共识算法管理、账户管理、应用并行管理、资源配额管理以及 API 开发等功能,如图 2 所示。

- EOS 链支撑管理功能:实现对 EOS 链节点配置、测试、上线、升级、告警等方面的统一管理和状态监控;管理 EOS 智能合约的注册和激活;提供对 EOS 链交易状态的存储和查询。

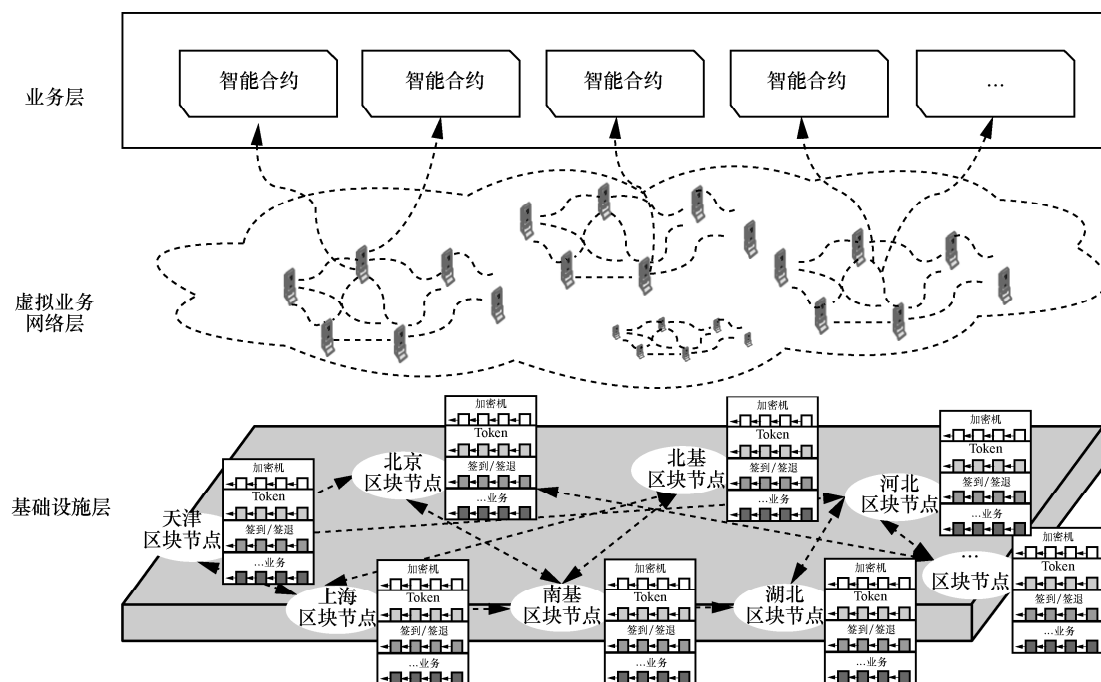


图1 BaaS平台技术架构

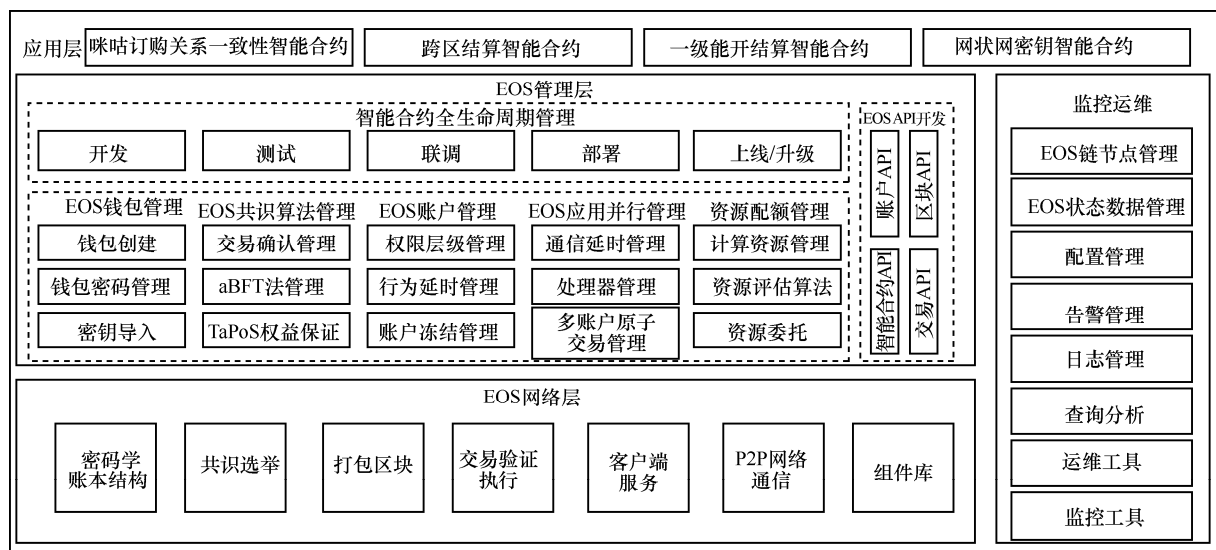


图2 EOS功能架构

- EOS 钱包管理：实现所有集群应用的统一部署和应用版本升级。
- EOS 共识算法管理：建立 EOS 共识算法模型，对业务交易进行安全管理。
- EOS 账户管理：对 EOS 账户行为和权限等进行管理，保证账户安全交易。
- EOS 应用并行管理：基于集群性能数据采

集，采用 cad-only 处理机制和多账户原子交易提升 EOS 应用管理质量。

- 资源配额管理：使用 EOS 可对带宽、存储、CPU、内存等资源进行配额管理，防止资源占用，并提供资源评估、资源委托、成本管理等功能。

引入 EOS 链支撑，通过并行链和 DPoS

(delegated proof of stake, 授权股权证明) 的方式解决了区块链时延和吞吐量限制, 且其提供分布式应用的性能扩展和更高的安全性。经业务测试, EOS 区块生成间隔仅为 0.5 s, 且处理性能最高可以达到百万 TPS (transaction per second, 每秒事务处理量), 在业务应用场景上, 可以良好支撑订购关系同步、跨区实时结算和大并发通知类交易等业务场景。

4.2 智能合约生命周期管理

区块链基础平台提供智能合约的开发、测试、联调环境, 31 省 BOSS (business operation support system, 业务运营支撑系统) 和业务平台可快速开发自己的智能合约。精简的智能合约开发上线管理流程, 从需求提出及评审, 仅需经过智能合约服务目录匹配、合约开发、沙箱测试及加入等简单的几个步骤, 即可实现服务的快速构建到部署的敏捷交付流程。智能合约采用组件化的插件方式, 使应用的结构更加清晰, 简化开发和部署的难度。统一规划, 集中管理, 逐步丰富智能合约服务目录, 在开发方面减少对省端的强依赖。

提供区块链全网运营监控平台, 通过监控节点物理分布、数量、节点健康状态、区块数量、区块产生速度、交易量、合约数量、节点综合性能等, 为运营管理者提供实时、全面、准确的区块链业务运营综合概况, 便于辅助业务决策。

4.3 BaaS 平台业务开发及协作模式

BaaS 平台作为基础设施平台, 提供开发 EOS API, 包括账户 API、区块 API、智能合约 API、交易管理 API, 方便更多用户自助接入上链。并引入 3 种业务支撑开发模式。

(1) 合作方没有区块链平台, 有智能合约开发能力, BaaS 平台提供开发环境, 合作方开发智能合约, 实现业务上链。

(2) 合作方没有区块链平台, 且无智能合约开发能力, 提出业务需求, BaaS 平台提供开发环境, 并帮助其开发智能合约, 实现业务上链。

(3) 合作方如有区块链平台, 则双方各自开发智能合约, 采用联盟链的方式对接, 实现链之间的业务协作和互通。

以常用的第 (3) 种场景为例: A 部门区块链支持特定的业务场景, BaaS 平台可以采用联盟链的方式实现与不同区块链的对接。联盟链是一个业务支撑体系, 支撑着联盟多主体成员之间灵活有效地开展分布式协作业务。该方式不同于传统的中心化的强依赖应用, 成员之间在链上是对等的 (行为对等、账户对等、数据对等), 从支撑手段技术上保证任何一家成员不能干预其他成员, 极大提高协作效率, 保障数据安全, 保证业务流程一致, 实现多合作方的链上共享数据。

BaaS 平台与 A 部门 BaaS 平台通过构建联盟链实现对接, 共同协作实现业务的流转和数据的互通。

5 区块链服务平台应用场景

区块链的功能主要面向 IT 应用, 以中国移动现网总部及 31 省业务支撑系统 (BOSS) 为例, 随着接入系统和业务逐渐增多, 数据的一致性、安全性、高可用性和可追溯性已经成为质量的重点。尤其是在长业务流程、多系统间数据交互过程中, 存在较多订购关系不一致、非实时结算准确率低、结算对账不一致、数据一致性差、交易记录追踪困难的问题。贴合区块链技术特性, 梳理区块链服务平台能够应用的业务场景, 挖掘区块链技术优势, 方能打造持续良性运转的 IT 生态链。

5.1 订购关系一致性保证

现有支撑系统当用户订购关系发生变更时, 如涉及变更 N 个平台, 则省 BOSS 会向总部平台发送 $(N+1)$ 条订购关系同步数据, 信息大量重复, 效率低, 容易导致订购关系不一致问题产生。

通过区块链服务平台存储订购关系数据, 当订购关系发生变化时, 省 BOSS 只需要向区块链

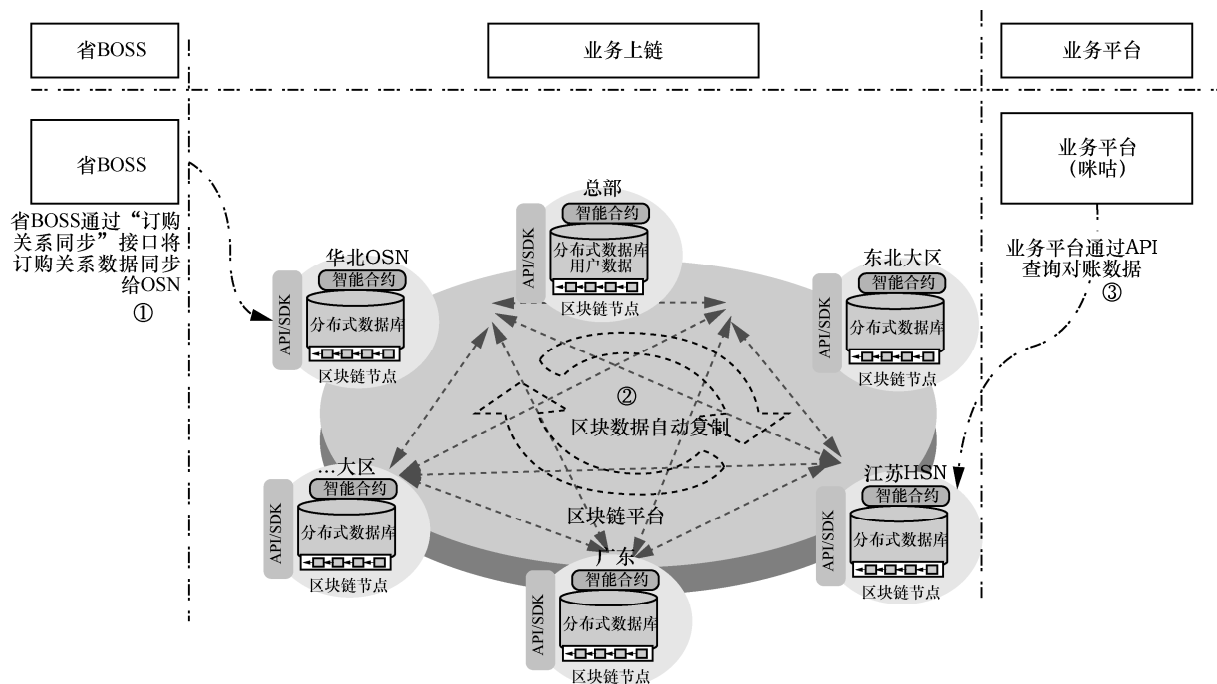


图3 区块链订购关系一致性保障示意图

平台发送一条订购关系变更数据，由区块链机制实现自动同步，保证数据强一致性。BaaS平台基于智能合约技术保障每个节点的业务处理程序相同，实现业务流程的标准化，避免因业务处理程序不同而造成的数据不一致问题。

以咪咕业务订购关系一致性保障服务为例，考虑咪咕业务受理、订购、退订流程复杂，且涉及省BOSS、咪咕平台、总部业支等多个系统，其技术支撑方案如下。

(1) 区块链平台城市节点 OSN (origination switch node, 发起交换节点) 和 HSN (home switch node, 终结交换节点) 上链，先保证区块链平台 OSN 和 HSN 数据强一致性，对咪咕业务平台提供数据查询智能合约 API，业务平台携带自己的私钥+证书，从就近区块查询本平台的对账数据。

(2) 业务平台和省 BOSS 上链，在咪咕业务和省 BOSS 的生产流程中建立区块链节点，区块链自动复制数据给咪咕节点和省 BOSS。通过区块链数据强一致性保证从源端到目标端的各方订购关系数据强一致性。使用区块链平台后，咪咕数

据一致率由 99.87%提升为 100%；针对用户订购产生的异常交易，一个月内处理并解决 3 万笔异常交易数据，有效降低由于数据不一致可能导致的潜在用户投诉。

5.2 实现实时无差错结算

传统结算模式，一般事后按月结算，常发生数据采集不全、传输中断、交易异常、冲正机制等导致的结算不准确、账单下发失败等问题。

区块链实时无差错结算示意图如图 4 所示，引入区块链服务平台，可采用区块链分布式账本，实现跨区实时结算，结算透明准确无差错，且可多方互信，准确率和效率带来极大的提升，减少了数据稽核工作量。

基于 EOS 实时交易链，支持跨多个参与方的复杂数据集，且实时具有高度的信任 and 安全性。区块生成间隔优化到 0.5 s，远远小于传统区块链 10~30 s 的生成间隔。区块链可在实时结算、大并发量通知类交易流程中得到较好应用，现网测试数据显示，区块链服务平台可将运营商间语音结算时间从几十小时减少到数分钟级别。

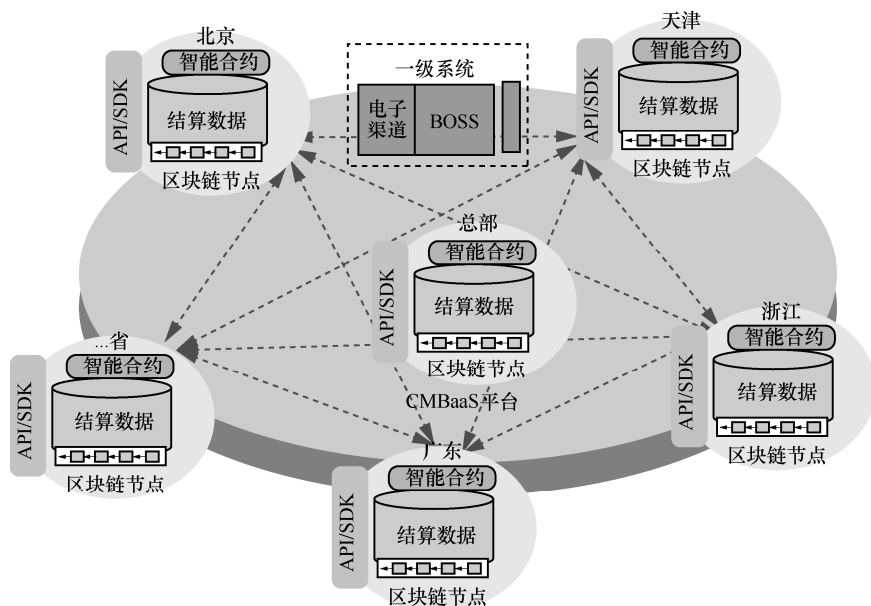


图4 区块链实时无差错结算示意图

5.3 全网数据分发和监管

(1) 全网配置数据分发

现有两级业务支撑架构下，总部获取配置数据后，先更新总部数据库，再同步更新至31省，现网数千台服务器刷新周期长、同步不完整、效率低，密钥和配置数据更新易出错，同步不完整，出现异常需要投入较多运维人力排查的问题。

采用区块链技术，基于区块链密钥等安全内容全网同步功能、签到签退全网同步功能、数据库配置全网同步、规则全网同步、局数据全网同步等功能，有效解决传统架构下全网同步安全、同步失败率高、故障难排查等问题，大幅提升分发效率及数据强一致性。

(2) 核心数据集中管理

目前客户数据、订购关系等数据分散在31个归属省管理，缺乏全网统一的核心数据管理视图。多头数据管理，全网业务数据质量不高，影响整体运营协同能力。

区块链去中心化的共识机制，每个参与交易的区块节点，都完整记录所有用户数据和交易数据，并实现业务规则在多个参与方的统一，符合

IT系统管理集中、分布式构架、安全高可用的长远规划思路。

(3) 数据的安全和追溯监管

目前数据安全是电信行业交易中的头等大事，数据分散存储及长流程的数据传输环节中，很多关键环节和数据都存在泄露风险。必须有更好的数据传输、加密和认证机制解决交易过程中的安全问题。

区块链数据存储采用分布式安全存储、时间戳、非对称加密等技术，保障数据安全可靠性；每一区块都会记录前一区块的信息，并实现验证，确保无法篡改，不可伪造。一方数据丢失，完整数据可快速恢复。

区块链服务平台搭建跨网络共享、不可更改的分布式交易记录系统，完整记录交易信息，并保证共享账本适当的可见性及交易的真实性，实现交易过程可追溯，满足关键交易的审计和历史查询。

6 结束语

区块链服务平台，为不同参与主体间，甚至不同行业间共建透明互信的区块链账本，可实现



交易、结算、对账等数据的快速准确交互，在提高运营效率、降低运营成本、增强对账透明度与提升信任度等方面取得了一定效果。区块链，作为一种新的业务协作模式，将在传统技术难以解决的诸多领域发挥重要作用，推动商业模式变革，助力运营商实现从“信息互联网”向“价值互联网”的转变。

参考文献：

- [1] 李董, 魏进武. 区块链技术原理、应用领域及挑战[J]. 电信科学, 2016, 32(12): 20-25.
LI D, WEI J W. Theory, application fields and challenge of the blockchain technology[J]. Telecommunications Science, 2016, 32(12): 20-25.
- [2] 李梦炜. 基于联盟区块链的中国福利彩票系统设计[J]. 信息技术与网络安全, 2020, 39(8): 9-14.
LI M W. China welfare lottery system based on the consortium blockchain[J]. Information Technology and Network Security, 2020, 39(8): 9-14.
- [3] 薛淼, 刘千仞, 符刚, 等. 区块链在电信运营商应用场景的探讨[J]. 邮电设计技术, 2019(4): 76-80.
XUE M, LIU Q R, FU G, et al. Discussion on the application scenarios of blockchain in telecom operator[J]. Designing Techniques of Posts and Telecommunications, 2019(4): 76-80.
- [4] 邵奇峰, 金澈清, 张召, 等. 区块链技术: 架构及进展[J]. 计算机学报, 2018, 41(5): 969-988.
SHAO Q F, JIN Z Q, ZHANG Z, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988.
- [5] 许丹丹, 张云勇, 张道琳, 等. 5G 时代区块链发展趋势及应用分析[J]. 电信科学, 2020, 36(3): 117-124.
XU D D, ZHANG Y Y, ZHANG D L, et al. Development trend and application analysis of blockchain with 5G[J]. Telecommunications Science, 2020, 36(3): 117-124.
- [6] 李聪, 雷波, 解冲锋, 等. 基于区块链技术的可信网络[J]. 电信科学, 2019, 35(10): 60-68.
LI C, LEI B, XIE C F, et al. Trustworthy network based on blockchain technology[J]. Telecommunications Science, 2019, 35(10): 60-68.

[作者简介]



齐磊（1982- ），男，中国移动通信集团设计院有限公司高级工程师，主要研究方向为 IT 支撑系统技术及组网、大数据和云计算技术及应用。



祝好（1985- ），女，中国移动通信集团设计院有限公司高级工程师，主要研究方向为 IT 支撑系统技术及组网、运营管理系统方案及设计。

顾慧琼（1982- ），女，中国移动通信集团设计院有限公司高级工程师，主要研究方向为 IT 支撑系统技术及组网、业务支撑系统方案及设计。

陈旭（1987- ），女，中国移动通信集团设计院有限公司工程师，主要研究方向为 IT 支撑系统技术及组网、业务支撑系统方案及设计。

胡泊（1988- ），男，中国移动通信集团设计院有限公司工程师，主要研究方向为 IT 支撑系统技术及组网、安全管理系统方案及设计。