区块链在电信运营商应用场景的探讨

Discussion on the Application Scenarios of Blockchain in Telecom Operator

薛　淼，刘千仞，符　刚，王光全（中国联通网络技术研究院，北京 100048）
Xue Miao，Liu Qianren，Fu Gang，Wang Guangquan（China Unicom Network Technology Research Institute，Beijing 100048，China）

摘　要：
区块链是一种由多方共同维护，以块-链结构存储数据，利用分布式节点共识算法同步和更新数据，利用加密技术实现传输及访问安全，利用可自动化执行代码组成的智能合约操作数据，能够实现数据一致存储、无法篡改、无法抵赖的技术体系。区块链的去中心化、可溯源及防篡改等特征催生了新的应用生态。介绍了区块链的基本原理及区块链标准进展情况，结合电信运营商场景进行分析，提出区块链在运营商场景的应用示例，并分析了区块链应用面临的挑战。

关键词：
区块链；运营商；分布式应用
doi：10.12045/j.issn.1007-3043.2019.04.017
中图分类号：TN915.08
文献标识码：A
文章编号：1007-3043（2019）04-0076-05

Abstract：
Blockchain is a technology system which is maintained by many parties and stores data in block-chain structure. It uses distributed node consensus algorithm to synchronize and update data，uses encryption technology to realize transmission and access security，and uses intelligent contract operation data composed of automated executable code to achieve data consistent storage，anti-tampering and non-repudiation. The features of decentralization，traceability and anti-tampering generate new application ecosystem. It briefly introduces the block chain principle and the state of the blockchain standards . Based on the analysis of the scenarios of telecom operators，the application use cases in telecom operator scenario are put forward. Finally the challenges faced by the application of block chains are summarized.

Keywords：
Blockchain；Distributed application；Telecom operator

引用格式：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.

0 前言

区块链是一种由多方共同维护，以块-链结构存储数据，利用分布式节点共识算法同步和更新数据，利用加密技术实现传输及访问安全，利用可自动化执行代码组成的智能合约操作数据，能够实现数据一致存储、无法篡改、无法抵赖的技术体系。区块链因其去中心/去中介、天然的可溯源/不可篡改及分布式应用特征吸引行业人员关注。

2017年加密货币的火爆使区块链为大众认知，2018年区块链技术在逐渐完善的同时，在应用落地方面呈现多元化发展，向实体经济延伸，强调与实体产业结合。落地应用由金融领域向其他垂直领域扩展，探索各垂直领域创新应用，形成“多点开花”局面。

区块链在电信运营商的应用场景仍处于探索阶段，国内外主流运营商均在区块链应用方面进行尝试。电信运营商一方面需要梳理区块链能够应用在运营商哪些场景，贴合区块链特性，另一方面也需考虑区块链的刚性需求及相对现存竞品的优势。本文主要介绍了区块链技术基本原理、标准进展、运营商场景应用分析以及面临的挑战。

收稿日期：2019-03-01

1 区块链技术简介

1.1 区块链原理

1.1.1 区块链账本

如图1所示，区块链以块-链方式存储记录或交易。区块包含区块头和区块体，区块头通常包含前一个区块的哈希散列值、Merkle根、时间戳等，区块体包含从网络广播中收集的记录或交易。在区块头中的Merkle根是对每一笔记录或交易的Hash值进行两两Hash得到的，对任何一个记录或交易的改变都会导致Merkle根的改变，从而保证了交易的不可篡改。区块头存储了前一个区块的Hash值，保证了每一个记录或交易的可追溯。

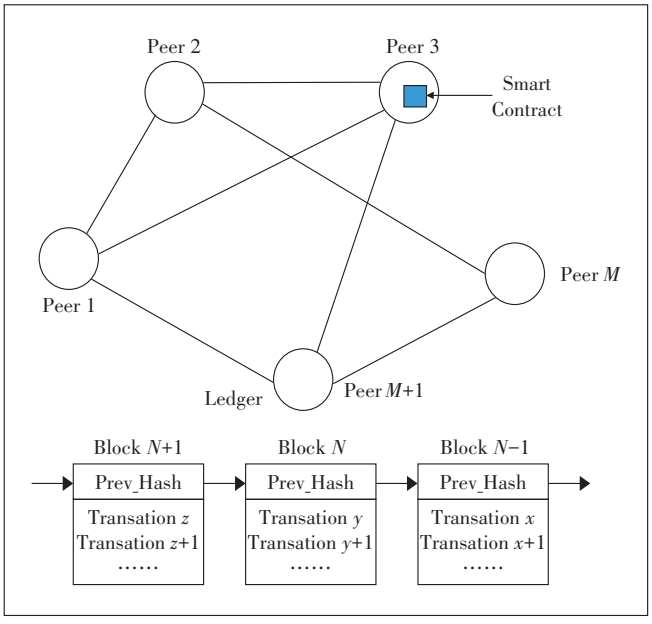

图1　区块链架构示意图

1.1.2 共识机制

每个区块被加到区块链尾部时，需要经过区块链节点的验证共识。区块链中达成共识的流程一般是先由一些节点进行记账，然后由其他节点进行验证，验证通过即达成共识。

传统分布式系统共识算法主要解决节点通信不可靠、宕机、时序等问题，通常假设不存在主观做恶的节点。而在区块链系统中，更加侧重存在恶意节点时，实现数据存储的一致性，即非可信网络环境下形成的可信数据存储。

比特币PoW共识机制流程如下。

a）节点收集广播中还没有被记录到账本的原始交易信息（交易信息主要是比特币网络参与者的转账/支付信息）。

b）检查每个交易信息中付款地址有没有足够的余额。

c）验证交易是否有正确的签名。

d）把验证通过的交易信息进行打包记录。

e）添加一个奖励交易：给自己的地址增加特定数量的比特币。

f）选择随机数，然后不断尝试计算nonce哈希，满足某一个难度标准（若干前导0开头的Hash值）。

g）如果计算成功，则挖矿成功，向全网广播挖矿所得，全网节点验证后，把这个区块连接到区块的尾端，并且在全网达成一致。

1.1.3 智能合约（SC）

智能合约是记录在区块链上的一段程序代码，其可以自动执行并对账本上的数据进行操作。智能合约可以用来将特定交易流程的规则代码化并保证严格执行预定义的规则。在特定的区块链实现中，智能合约也可以作为上层应用读写账本的接口。智能合约是区块链构建分布式应用的基础。

1.2 区块链分类

目前区块链已经存在很多变种以及各自针对的场景。如表1所示为区块链针对不同参与对象的一种分类：公有链、联盟链、私有链。

1.3 区块链认识误区

a）区块链就是比特币。区块链不等于比特币。虽然区块链源于比特币，但是比特币仅是区块链承载的一种应用。区块链经过多年的发展，无论是适用场景还是技术实现都已经有了很大改进。

表1　区块链分类

项目	Permissionless	Permissioned	
	公有链	联盟链	私有链
定义	链上的所有用户都可读取、发送交易且能参与确认共识的区块链	联盟链是指有若干个机构或分支共同参与管理的区块链，每个机构都运行着一个或多个节点，其中的数据只允许联盟内不同的机构进行读写和发送交易	写入权限仅在一个组织控制的区块链
参与者	所有人	预先设定或满足条件后允许加入（企业联盟或内部）	中心控制者决定参与成员（内部）
中心化程度	完全去中心	多中心	中心化
典型代表	比特币、以太坊	HyperLedger Fabric、R3、瑞波	Overstock

b）区块链耗能严重。目前大量基于公有链的加密货币项目采用PoW共识机制，PoW会消耗大量的资源。但是PoW仅是区块链的一种共识机制，区块链也可以采用PoS、PBFT等耗能低的共识机制。

c）区块链无法监管。企业场景下的联盟链采用多中心方式，能够进行集中监管。

2 区块链标准及开源

2.1 标准情况

目前国内外的标准组织及行业联盟均在开展区块链相关标准的制定。区块链标准主要按照4个维度开展（见图2），标准组织多数集中在制定区块链High-Level框架标准。当前阶段大多数标准仍在制定过程中，只有少数初稿发布审查。更多标准文档预计会在2019年发布。

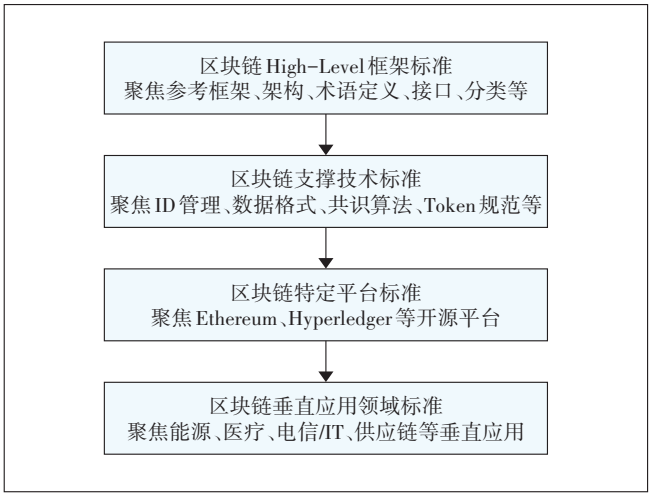

图2 区块链标准分类

区块链的标准化工作主要由如下几个组织制定。

a）ISO。ISO于2016年9月成立了ISO/TC307（区块链及电子化的分布式账本技术），负责区块链的标准研制，主要工作领域包括：架构和分类、用例、安全和隐私、身份、智能合约、区块链治理以及区块链之间的互操作性。

b）IEEE。IEEE启动P2418系列，研究区块链通用框架与架构、互操作、数据格式及在物联网、农业、能源、供应链金融等垂直领域的标准要求。

c）ITU-T。ITU-T的多个FG和SG都有区块链相关的研究项目（见表2）。

d）GSMA。GSMA重点关注区块链技术在电信领域的应用。

（a）在IG（Internet Group）中启动了Blockchain：Opportunities for enhancedoperators propositions项目，分析区块链技术特点、在运营商的应用场景、商业机会、投资分析和建议，并发布白皮书。

（b）FASG（Fraud and Security Group）在探讨使用区块链技术防诈骗、增强网络安全、用户身份认证及通信安全。

（c）IDS（Interoperability Data specifications and Settlement Group）BCE子组探讨使用区块链作为漫游计费结算方案的可行性。

e）W3C。Blockchain Community Group致力于Web账本协议，用于根据ISO 20022生成区块链的消息格式标准，并制定存储使用指南，包括公有链、私有链和侧链。该小组将研究和评估与区块链相关的新技术以及区块链用例，如银行间通信。

f）ETSI ISG PDL。2018年12月，ETSI成立ISG PDL（Permissioned Distributed Ledgers），致力于研究PDL运营、业务用例、功能架构及运营解决方案，以及关于接口/API、协议及数据格式的定义。2019年1月24日ISG PDL召开首次kick-off会议。

g）EEA。EEA通过制定标准化架构和规范以加速企业以太坊的行业采用，聚焦企业区块链的技术规

表2 ITU-T区块链标准情况

FG-DLT	2017年5月成立，整合ITU-T内部及全球各个国家的政产学力量，对分布式账本技术的发展给出指导和工作组标准化建议，制定标准路线图，下设5个组，分别围绕术语定义、技术架构、监管策略等方面开展
FG-DPM	2017年3月成立，研究支持IoT和SC/C的数据处理和数据管理方法，下设5个组。其中WG3涉及应用区块链实现IoT的数据共享和管理
FG-DFC	2017年5月成立，研究具备安全性、互操作性、防止伪造的数字货币网络架构
SG13	Y.NGNe-BC-reqts，研究NGNe中区块链应用的场景和用例并给出通用框架；Y.BaaS-reqts，研究区块链作为云服务的应用场景，并提出相关功能需求
SG16	Q22研究DLT的要求及框架，聚焦基于DLT的电子服务及多媒体应用
SG17	Q14研究DLT安全，目前在研10个项目，研究基于区块链的应用和服务，识别安全问题和威胁，研究安全机制、协议和技术，研究个人信息保护、安全管理和互联互通安全，制定安全方案建议等
SG20	Y.IoT-BoT-fw，制定应用于物联网的区块链平台框架标准及用例；Y.SSC-BKDMS-ARC，研究基于区块链的统一PKI数据管理参考架构

范制定和认证。

h）CCSA。CCSA在TC1 WG6和TC10 WG1区块链子组承担区块链相关工作。TC1 WG6承担区块链总体技术要求、通用评测指标和测试方法标准工作；TC10 WG1承担区块链在物联网的相关项目研究。

2.2 开源社区及平台

超级账本（Hyperledger）是Linux基金会于2015年发起的推进区块链数字技术和交易验证的开源项目，有超过200家企业加入，中国企业约30家；目前包括8个开源项目。

a）Fabric：面向企业应用的联盟链开源项目，已有多个商用案例。

b）Iroha：基于fabric的移动应用。

c）Burrow：基于以太坊VM的客户端。

d）Sawtooth：基于PoET共识的区块链项目。

e）另外4个项目为开发者工具：Cello、Composer、Explorer、Indy。

Ethereum以太坊是一款能够在区块链上实现智能合约、开源的底层系统；以太坊在比特币的基础上进行优化，提供了图灵完备的智能合约语言，并创新性地提供了基于以太坊虚拟机的智能合约运行环境。2015年7月，以太坊客户端第1版上线。以太坊是比特币后最成功的一条区块链。目前基于以太坊生态环境，存在大约1 000个Dapp，包括版权管理、数字签名、Token发行、在线博彩、游戏等。

3 区块链在电信运营商场景应用

3.1 区块链在运营商场景应用分析

虽然区块链底层实现使用P2P网络进行同步，可以认为是网络技术，但是整体上看，区块链的功能主要面向IT应用。从业务场景来看，存在不可信的多方参与且多方需要协作是采用区块链技术的必要前提，而且项目实现中需要使用数据库且存在多方写入数据的需求。判断应用是否需要使用区块链的分析如图3所示。

根据与运营商的关系，涉及电信场景应用存在如下几种（不信任）多方的场景，这些场景具有使用区块链的潜在需求。

a）国内运营商间，如号码携带、数字身份等场景。

b）国内运营商与国际运营商，如国际漫游结算场景。

c）运营商与合作伙伴，如供应链、PKI发布场景。

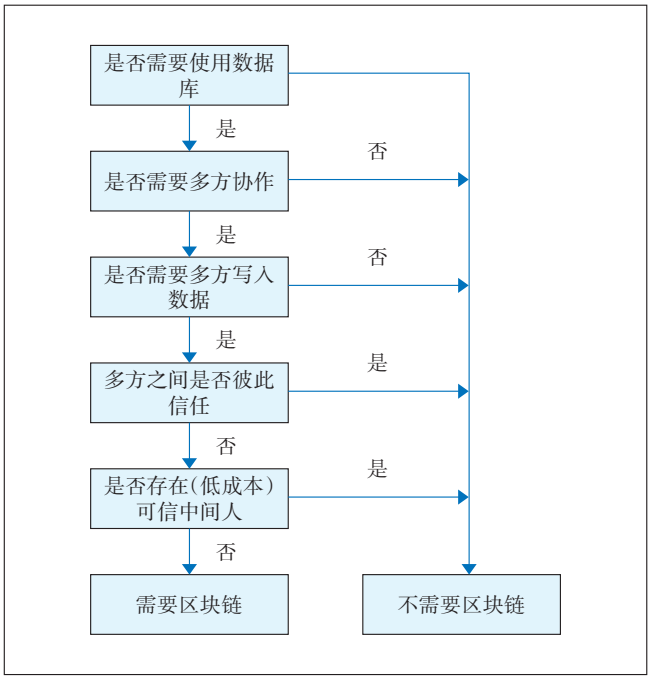

图3　区块链使用分析

d）运营商与监管部门，如数据审计、监管及合法监听记录等场景。

e）运营商与个人/企业用户，如积分管理、用户管理、合同管理场景。

f）运营商内部责任个体间（管理维度），如数字资产管理、数据管理、办公流程管理等场景。

g）运营商内部责任个体间（网络维度），如网络资源共享、资产共享、记录存证等场景。

3.2 区块链在运营商场景的应用

结合上节分析，区块链在电信运营商的网络域、O域/B域、D域、M域均有应用场景示例。

表3示出的是区块链在电信运营商场景的应用。

4 面临挑战

a）业务模式创新。区块链业务具有原生的分布式应用特征，与传统集中化的业务模式有着明显差别；电信网场景下基于区块链的2C/2B分布式应用孵化与开发需探索创新业务模式，同时也需要综合考虑成本、竞品的因素。

b）技术积累。区块链技术方案多样，包括隐私保护、可扩展性（规模/性能）、智能合约方案等存在差异，为产品选型带来挑战；同时分布式应用的日常运营维护及Troubleshooting需要积累经验；区块链应用的开发、选型、维护都需要技术积累。

表3　区块链在电信运营商场景应用

应用域	应用场景	应用点
网络域	数字身份	基于移动码号的数字身份：基于移动运营商码号/SIM建立移动应用认证平台，为互联网应用提供具有电信属性的身份认证服务
	PKI分发	设备接入认证：设备商、运营商作为区块链的节点，使用联盟链实现证书的分布式发布和管理
	电信业务	① 国际漫游结算：当用户在漫游地产生通信行为时，将漫游通信话单、账单数据存储到区块链上，运营商可直接结算，降低结算成本 ② 号码携带：构建运营商间的联盟链，各运营商将签约转网号码上链，减少业务开通时间，降低集中建设携号数据库及运维成本 ③ 边缘CDN：基于区块链的边缘CDN服务，共享用户侧或者边缘云闲置带宽和存储，通过区块链记录用户资源贡献，实现用户激励、增加用户黏性及南北流量的降低 ④ 云服务（BaaS）：运用运营商网络优势、算力优势、信用优势等，帮助企业或用户以低成本、低门槛构建区块链应用
	物联网	数据记录/协作/权限控制：为物联网提供数据记录、数据协作、权限控制、跨网统一身份、数字支付等服务，保证物联网数据高可信
	电信网络优化	网络基础设施共享：多家运营商对同一地区重复覆盖，造成社会资源的浪费，通过区块链实现跨运营商的网络共享
O/B域	电信资产管理	① 电信设备管理：电信设备管理系统，促进更透明、更高效的穿透式设备管理 ② 用户丢失移动终端IMEI管理：运营商共享用户丢失移动终端IMEI，禁止盗窃/丢失设备入网，降低设备盗窃，保护用户隐私 ③ 数据资产管理：进行数据资产的全生命周期管控，包括数据开放审批、安全审计等；数据确权、数据使用授权；数据采集、数据加工、数据共享的质量和效率监管 ④ 数字资产管理：数字资产的追踪管理与多方信息共享，如IP地址、DNS数据、SIM数据、用户积分等
D域	数据流通	① 运营商价值数据共享：通过联盟链的形式，将符合监管要求的数据（如黑名单信息、恶意网站、用户标签库、位置信息等）上传到区块链中，建立全面、完备的运营商共享数据库 ② 征信数据流通：引入各个征信数据拥有方（各商业银行、电信公司、互联网金融公司等），通过区块链实现征信数据的共享和交易
M域	资产与支付管理	① 合同管理：实现电子合同多方共享，可追溯合同变更记录、支付进度，便于存证验真、审计核查 ② 供应链管理：企业内部资产如易耗品的采购及付款、物品发放等

5 结束语

本文介绍了区块链的基本原理及区块链标准进展情况，结合电信运营商场景进行分析提出区块链在运营商场景应用示例，并分析区块链应用面临的挑战。

区块链在电信运营商场景的应用仍处于探索阶段，一些典型应用如PKI发布、数字身份、数据管理等应用已经在行业内进行试验，但是区块链的分布式特征与电信运营商的集中化管理的适配仍需进一步检验。

参考文献：

[1] LIMA C. Developing Open and Interoperable DLT/Blockchain Standards[EB/OL].[2018-12-05]. https://www.computer.org/csdl/mags/co/2018/11/08625908.pdf.

[2] 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)：3-22.

[3] 中国信息通信研究院. 可信区块链推进计划[EB/OL].[2018-12-05]. http://www.trustedblockchain.cn/.

[4] GSMA. Blockchain-Operator Opportunities [EB/OL].[2018-12-05]. https://www.gsma.com/newsroom/all-documents/ig-03-blockchain-operator-opportunities-v1-0/.

[5] DYLAN Y，PETER M，NIK R. Blockchain Technology Overview[EB/OL].[2018-12-05]. http://3ms.epipe.cn/industry-research/details/779.html.

[6] IEEE. IEEE blockchain standards[EB/OL].[2018-12-05]. https://blockchain.ieee.org/standards.

[7] Blockchain and Distributed Ledger Technologies[EB/OL].[2018-12-05]. https://www.iso.org/committee/6266604.html.

[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.

[9] 朱建明，付永贵. 区块链应用研究进展[J]. 科技导报，2017，35(13)：70-76.

[10] 彭劲杰，龙若兰. 区块链应用环境下安全保护关键技术研究[J]. 网络安全技术与应用，2018，210(6)：29，36.

[11] 杨浩. 区块链应用在网络安全的案例[J]. 计算机与网络，2018，44(9)：57-58.

[12] 佚名. 区块链应用现状及安全风险研究[J]. 科技创新与应用，2018，250(30)：29-30.

[13] 彭永勇，张晓韬. 基于区块链应用模式的可信身份认证关键技术研究[J]. 网络安全技术与应用，2018(2).

[14] 何蒲，于戈，张岩峰，等. 区块链技术与应用前瞻综述[J]. 计算机科学，2016，44(4)：1-7.

[15] 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.

作者简介：
薛淼，高级工程师，博士，主要从事区块链标准及应用研究工作；刘千仞，工程师，硕士，主要从事区块链技术及应用研究工作；符刚，高级工程师，硕士，主要从事移动通信核心网络新技术跟踪研究工作；王光全，教授级高级工程师，学士，主要从事高速光纤通信技术及应用研究工作。