

基于区块链的5G物联网数据共享方案

乔康, 游伟, 王领伟, 汤红波

(信息工程大学, 河南 郑州 450001)

摘要: 海量的物联网数据拥有巨大价值, 而现有基于云的数据共享机制, 面临单点故障、内部泄露等问题, 无法确保用户数据的安全共享。为实现高效可信的数据共享, 利用区块链技术, 提出了基于区块链的5G物联网数据共享方案。该方案首先设计了数据共享框架和数据共享流程; 然后基于闪电网络方案, 提出了面向物联网数据共享的链下交易机制。实验分析表明, 基于区块链的5G物联网数据共享方案具有较强的抗攻击能力; 基于闪电网络的交易机制, 能够大幅提高交易吞吐量、降低交易时延。

关键词: 区块链; 5G; 物联网; 数据共享; 链下交易

中图分类号: TP399

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020041

Data sharing scheme for 5G IoT based on blockchain

QIAO Kang, YOU Wei, WANG Lingwei, TANG Hongbo

Information Engineering University, Zhengzhou 450001, China

Abstract: The massive amount of IoT data has great value, but the existing cloud-based data sharing mechanism faces problems such as single points of failure and internal leakage, which can not ensure the secure sharing of user data. In order to achieve efficient and reliable data sharing, the blockchain technology was used to propose a 5G IoT data sharing scheme based on blockchain. Firstly, the proposed scheme designed data sharing framework and data sharing process, based on the lightning network solution, an off-chain transaction mechanism for data sharing of the internet of things was proposed. Experimental analysis shows that the 5G IoT data sharing framework based on blockchain has strong anti-attack ability and the off-chain transaction mechanism based on lightning network can greatly increase transaction throughput and reduce transaction delay.

Key words: blockchain, 5G, internet of things, data sharing, off-chain transaction

收稿日期: 2020-01-07; 修回日期: 2020-02-03

通信作者: 乔康, 773441271@qq.com

基金项目: 国家重点研发计划网络空间专项 (2016YFB0801605); 国家自然科学基金创新群体项目 (61521003); 国家自然科学基金 (61801515)

Foundation Items: The National Key R&D Program Cyberspace Special (2016YFB0801605), The National Natural Science Foundation Innovation Group Project (61521003), The National Natural Science Foundation of China (61801515)

论文引用格式: 乔康, 游伟, 王领伟, 等. 基于区块链的5G物联网数据共享方案[J]. 网络与信息安全学报, 2020, 6(4): 45-55.

QIAO K, YOU W, WANG L W, et al. Data sharing scheme for 5G IoT based on blockchain [J]. Chinese Journal of Network and Information Security, 2020, 6(4): 45-55.

1 引言

目前,全球将5G的发展作为重要战略,积极推动5G商用。2019年11月,工业和信息化部与三大运营商正式宣布启动5G业务,标志着中国正式进入5G商用时代。5G支持超高速、大带宽、低时延、低功耗、泛在网、海量连接,并能够提供广泛的差异化服务^[1]。5G的到来,将开启一个“万物互联”的时代。华为预测,到2025年,通过5G NB-IoT连接的设备数量将超过1 000亿台,并且在这之后可能会呈指数型爆发式增长^[2]。

众多的5G物联网设备将产生海量数据,为实现对海量数据的存储,当前主要采用基于云的数据存储方式^[3]。海量的5G物联网数据拥有巨大价值,在云存储环境下,数据共享主要依赖云服务器的可靠性和可信度。然而,近年来,云服务器数据库泄露事件层出不穷^[4]。2019年1月,云存储服务商MEGA泄露87 GB数据,含7.7亿个邮箱;2019年4月,网络安全公司UpGuard的研究人员声称,在亚马逊云计算服务器上可公开访问的地方发现数亿Facebook用户的个人信息记录;2019年11月,谷歌云服务器上的数据库泄露了12亿用户的个人信息。因此,在不可信的云存储环境下,如何为5G物联网提供安全的数据共享,成为一项挑战。

近年来,新兴的区块链技术发展迅速,引起了学术界和产业界的广泛关注。区块链是一种分布式账本技术^[5],具有去中心化、匿名性、难篡改和可审计等关键特征,能够通过综合运用时间戳、加密哈希、数字签名、共识机制和智能合约等技术,在不完全可信的环境下,实现陌生节点之间点对点的价值传递。Esposito等^[6]强调利用区块链技术,可为基于云的医疗健康数据提供安全和隐私保障。Xia等^[7]通过区块链技术,在云服务提供商之间,实现了无信任的医疗数据共享。Liang等^[8]提出了一种基于区块链的数据保护架构,用于增强云环境下的数据隐私性和可用性。Rehman等^[9]利用区块链技术,为基于云的物联网应用提供安全服务。Shafagh等^[10]实现了一种基

于区块链的可审计物联网数据存储和共享方案。Wang等^[11]介绍了一种基于联盟链的安全和隐私保护的数据共享方案,用于云环境中的电子健康数据共享。综上所述,将区块链技术应用于云环境下的数据共享,已有理论基础和实际项目研发,然而,如何利用区块链技术实现5G物联网的数据共享仍处于探索阶段。

鉴于上述分析,本文面向5G物联网的应用场景,针对数据安全共享困难的问题,提出了基于区块链的5G物联网数据共享方案。该方案首先设计了数据共享框架和数据共享流程,目的是为云环境下的5G物联网数据共享提供解决思路。其中,数据共享框架包括数据提供节点、数据需求节点、区块链服务器和云服务器4个组成部分,数据共享流程包括节点状态更新、数据共享申请和数据访问等6个阶段。

此外,在基于区块链的5G物联网数据共享中,区块链的交易机制决定了交易处理性能。现有方案通常采用链上交易方式,受限于区块容量和验证速度,整体交易处理效率较低^[12]。例如,比特币每秒只能处理大约7笔交易,且交易需要等待6个区块(约1 h)后才能确认^[13]。和现有的支付系统相比,Visa的平均交易速度为每秒24 000笔,峰值速度为每秒50 000笔,比特币及其衍生区块链交易系统,在交易速度和扩展性上仍差距甚远^[14]。为此,研究人员提出了各种改进建议,包括采用侧链技术^[15]、分片技术^[16]和有向无环图^[17]等。多数解决方案存在效率和去中心化的矛盾问题。例如,EOS系统能够提供数百万笔的峰值交易速率,但存在中心化程度过高的安全问题。目前被认为安全有效的解决方案,是由Joseph等于2016年提出的闪电网络(lightning network)方案^[18]。

闪电网络是一个去中心化的,无须信任对方以及第三方即可实现实时、海量的交易网络,其特点是交易速度快、手续费低和扩展性高,已经被证明对于高频且小额的支付具有适应性^[19]。而在基于区块链的5G物联网数据共享场景中,执行点对点的数据共享,大量的交易是小额的,且用户不需要实时提现,所以闪电网络方案适用于该场景。为提高交易处理速度和扩展性,

本文基于闪电网络方案,利用微支付通道和智能合约技术,提出了安全的链下交易机制。

2 区块链简介

2.1 区块链的数据结构

区块链是由区块按时间顺序串联起来的链式结构,区块由区块头和区块体构成,如图1所示。区块头包含版本号、区块高度、前一个区块的哈希值(父哈希)、当前区块的哈希值(目标哈希)、时间戳、Merkle(默克尔)根和随机数。其中,随机数是用于工作量证明(PoW)算法的计数器,其是选填项,由采用的共识算法而定。区块体包含具体的交易信息。为确保数据的完整性,并实现对某笔交易快速验证,区块链中采用Merkle树证明机制^[20]。

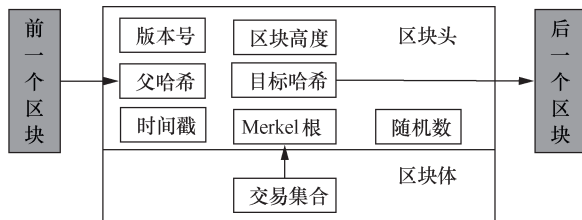


图1 区块链的数据结构
Figure 1 Data structure of the blockchain

2.2 Merkle树

Merkle树由Ralph Merkle提出,其是一个

哈希二叉树结构,相邻的两个哈希作为子哈希计算得出父哈希,最终得到一个根哈希,被称作Merkle Root。利用Merkle树,可以单独下载一个分支对部分数据进行校验,实现高效的交易验证。如图2所示,为校验交易Tx6的完整性,只需获取Hash5、H78和H1234,按照图中路径依次向上运算,即可实现完整性验证。

2.3 区块链分类

根据参与者的不同,区块链可以划分为公有链(public blockchain)、私有链(private blockchain)和联盟链(consortium blockchain)^[21],如表1所示。其中,联盟链指由若干个机构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,其中的数据只允许系统内不同的机构进行读写和发送交易,并且共同来记录交易数据。

公有链:没有权限设定和节点数量限制,任何人都可以随时参与,信息完全公开,通常被认为是完全去中心化的,如比特币区块链和以太坊区块链。如果进一步引入许可机制,可以实现私有链和联盟链两种类型。

私有链:有权限设定,节点数量和状态可控,仅对单个组织内部的成员开放,信息不公开,一般应用于企业内部,如企业内部账务审计、票据管理等。

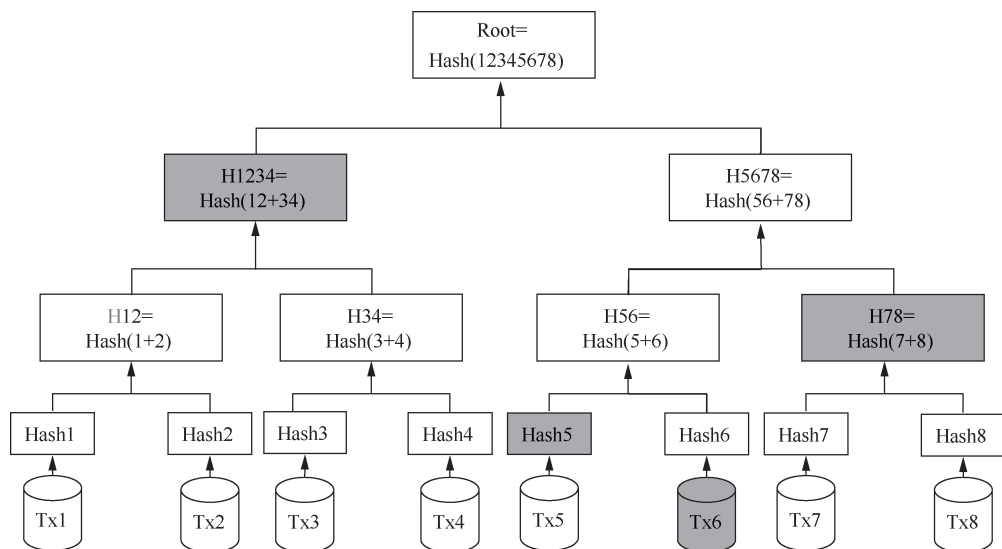


图2 Merkle树
Figure 2 Merkle tree

表 1 区块链分类
Table 1 Classification of blockchain

区块链分类	参与者	记账人	激励机制	共识机制	典型场景	承载能力
公有链	任何人自由进出	所有参与者	需要	PoW/PoS/DPoS	“数字货币”	3~20 笔/秒
私有链	个体或公司内部	自定义	不需要	分布式一致性算法 (PBFT/Paxo)	审计、发行	1 000~100 000 笔/秒
联盟链	联盟成员	联盟成员协商确定	可选	分布式一致性算法 (PBFT/Paxo)	支付、结算	1 000~10 000 笔/秒

联盟链：有权限设定，节点数量和状态可控，对多个组织构成的联盟成员开放，信息不公开，通常应用于企业间合作，如银行间的结算、企业间物流管理等。

本文面向的 5G 物联网数据共享场景，具有两方面特点：一是参与者类型多样，由来自不同地理位置、不同机构的各类物联网设备构成；二是对安全和效率要求高，需要建立权限准入机制和具备较高的交易处理能力。基于上述特点，本文采用联盟链作为底层区块链。

3 基于区块链的数据共享方案

3.1 数据共享框架

基于区块链的 5G 物联网数据方案设计了数据共享框架和数据共享流程，其中数据共享框架主要由 4 个部分组成，包括数据提供节点 (supply node)、数据需求节点 (demand node)、区块链服务器 (blockchain server) 和云服务器 (cloud server)，如图 3 所示。

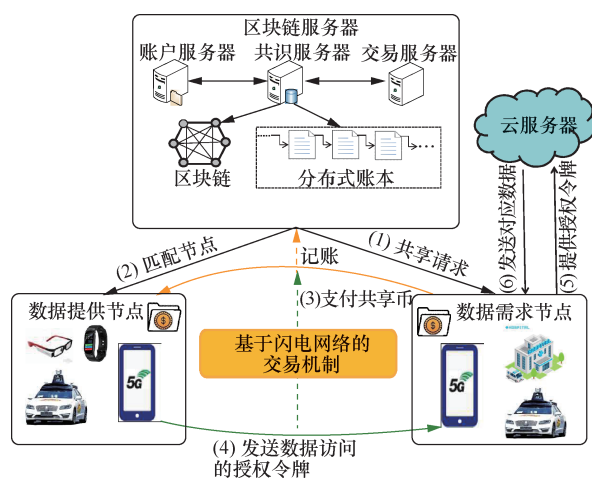


图 3 基于区块链的 5G 物联网数据共享框架
Figure 3 Data sharing framework for 5G IoT based on blockchain

数据提供节点：主要由各种提供数据的物联网设备组成，包括可穿戴设备、远程传感器、自动驾驶车辆和智能电表等。数据提供节点可将共享数据的简要情况（摘要）、销售价格和节点的地理位置上报给区块链服务器，以供区块链服务器根据实际情况，为其匹配合适的数据需求节点。

数据需求节点：主要由各种需要数据的物联网设备和机构组成，包括自动驾驶车辆、医疗机构、数据机构和互联网咨询公司等。数据需求节点可向区块链服务器申请数据共享，并兑换一定数量的共享币，用于支付数据共享费用。为减少节点的存储压力，本文采用轻量级钱包设计，普通的物联网节点仅保存区块头信息，完整的区块链账本存储在共识服务节点中，依靠 Merkle Root 实现简化支付验证 (SPV, simplified payment verification)。

区块链服务器：由 3 个主要实体构成，包括账户服务器、交易服务器和共识服务器。账户服务器负责发行共享币，并记录物联网节点的账户余额（采用类似比特币的 UTXO 模型^[22]），其角色类似于银行。为实现可控的目的，账户服务器可由国家机构监管和维护。交易服务器处理物联网节点的数据共享申请，并为申请者（数据需求节点）匹配对应的数据提供节点，数据提供节点可能是一个或多个，根据申请者的数据需求而定。共识服务器由多个共识节点组成，负责区块的打包、验证和记录，维护区块链账本的一致性。为激励节点参与维护区块链，本文设计了经济激励措施来回馈共识节点的工作。每笔交易会按照比例收取一定的服务费，所有共识节点均分 50% 的服务费，负责成块的主节点额外获得剩余 50% 的服务费。

云服务器：存储数据的云端，存储着数据提供节点的加密数据 data_k 。 data_k 是由数据提供节点使用对称密钥 D_k 对明文数据进行加密得到的。当数据需求节点请求数据访问时，云服务器首先验证授权令牌，验证通过后，再将对应的加密数据 data_k 发送至数据需求节点。

本文将基于区块链的5G物联网数据共享框架分为7层，包括物理层、数据层、网络层、共识层、激励层、智能合约层和应用层，如表2所示。物理层为数据共享的传输和存储提供物理媒体支持，主要由物联网设备和云服务基础设施构成。数据层封装了区块链底层区块数据、链式结构、数字签名、Merkle树和相关数据加密技术。网络层包含P2P网络、区块传播机制、区块验证机制和云服务网络等。共识层由本文提出的基于可信列表的拜占庭容错算法（CPBFT）构成。激励层包含用于数据交易的“数字货币”的发行和分配机制。智能合约层包含利用智能合约部署自动化执行的规则条款。应用层为基于区块链的5G物联网数据共享的应用场景。

表2 数据共享框架结构
Table 2 Data sharing framework structure

层次	组成
应用层	基于区块链的5G物联网数据共享的应用场景
智能合约层	利用智能合约部署自动化执行的规则条款
激励层	发行、分配机制
共识层	基于可信列表的改进拜占庭容错算法
网络层	P2P网络、区块传播机制、区块验证机制、云服务网络
数据层	区块数据、链式结构、数字签名、Merkle树、非对称加密等
物理层	物联网设备（数据提供节点、数据需求节点）、云服务基础设施等

3.2 数据共享流程

本文将5G物联网数据共享划分为6个流程（Step），如图4所示。流程中涵盖了图3中的6个步骤，具体描述如下。

Step1 系统初始化阶段。底层区块链采用联盟链，希望参与数据共享的物联网节点需要提前注册，经注册中心许可后成为合法节点，注册中心可由国家监管机构担任。每一个物联网节点 i 以

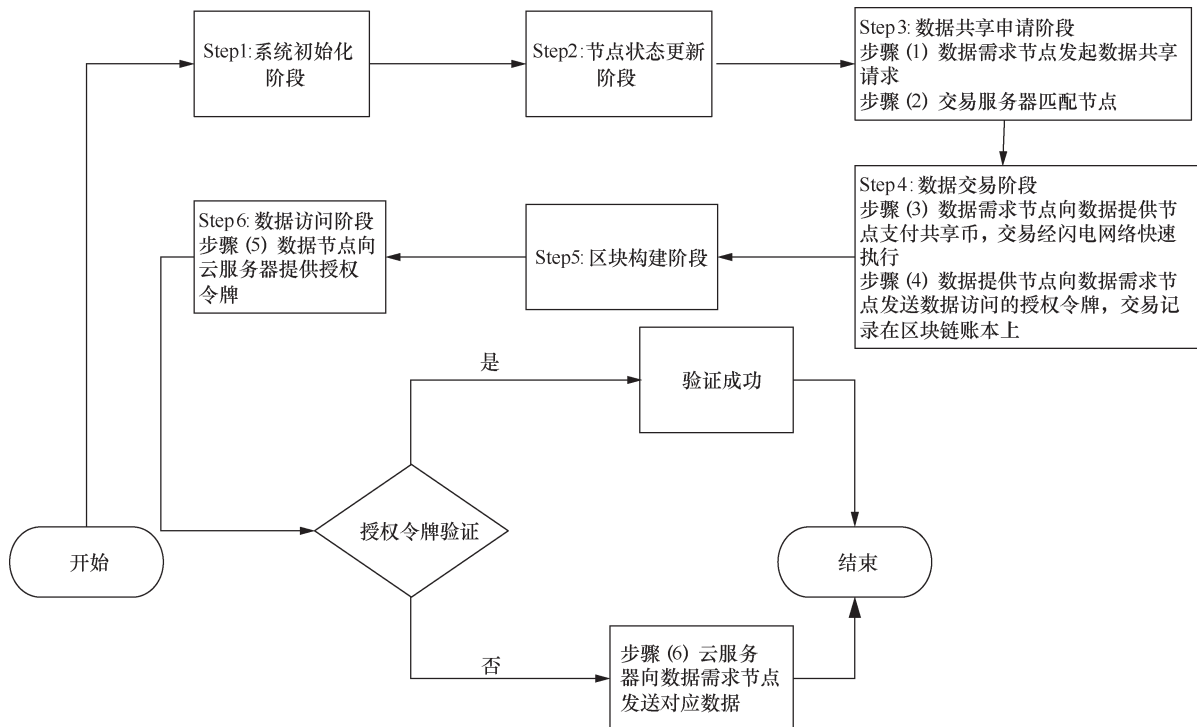


图4 基于区块链的5G物联网数据共享流程
Figure 4 Data sharing flow for 5G IoT based on blockchain

真实身份 ID_i 注册, 经许可后获取证书、公钥对 (PK_i, SK_i) 和一组钱包地址 $\{WAD_{i,k}\}_{k=1}^w$ 。注册中心生成映射列表 $\{ID_i, Cert_i, PK_i, SK_i, \{WAD_{i,k}\}_{k=1}^w\}$, 并存储在账户服务器中。当节点 i 执行初始化时, 节点 i 将其钱包地址上传到最近的账户服务器, 当需要检查其钱包的完整性时, 节点可从最近的共识服务节点下载区块链, 区块链上记录着所有的交易信息。

Step2 节点状态更新阶段。为更高效地提供数据共享服务, 在数据交易前, 区块链服务者预先获取节点现有的状态信息。基于区块链的 5G 物联网数据共享中包含 3 种类型的节点, 分别是数据提供节点、数据需求节点和共识节点。物联网节点根据自身的数据使用需求, 决定担任数据提供节点或数据需求节点, 这两类节点可相互转换。需要出售数据的提供节点向交易服务器上报告共享数据的摘要、数据价格 (price) 和地理位置 (Location), 以供交易服务器匹配合适的数据需求节点。共识节点负责维护区块链的一致性, 其将在共识算法执行前确定下来。

Step3 数据共享申请阶段。有数据需求的物联网节点向交易服务器发送申请 $\{Cert_i, PK_i, WAD_i, Dbuy_i, Location_i\}$, 申请消息中包含节点的证书 $Cert_i$ 、公钥 PK_i 、钱包地址 WAD_i 、数据需求 $Dbuy_i$ 和地理位置 $Location_i$ 。交易服务器收到申请后, 搜寻本地的数据提供节点, 并根据数据需求进行节点匹配, 可以是 1 对 1, 也可以是 1 对 N 或 N 对 1。如图 5 所示, 数据需求节点 1 的数据来源于数据提供节点 $Dsell_1$ 、 $Dsell_2$ 和 $Dsell_3$, 匹配关系为 $Dbuy_1 = Dsell_1 + Dsell_2 + Dsell_3$; 数据提供节点 $Dsell_3$ 分别为数据需求节点 1、节点 2 和节点 3 提供数据, 匹配关系为 $Dsell_3 = Dbuy_1 + Dbuy_2 + Dbuy_3$ 。

Step4 数据交易阶段。首先, 节点匹配完成后, 需求节点根据数据价格和数量, 向提供节点支付共享币 Coin, 共享币从需求节点的钱包地址 WAD_i 转移到提供节点的钱包地址 WAD_j 。这笔交易采用闪电网络交易机制, 通过微支付通道进行。然后, 提供节点将数据访问的授权通证 Token 发送至需求节点。Token 是一笔记录在区块链上的

交易, 包含由提供节点使用私钥 SK_i^S 签署的数字签名 $\{D_k^S, hash_{data}, ID_i\}_{sig}$, 其中 D_k^S 为隐蔽密钥, $hash_{data}$ 是明文数据 $data$ 的哈希值, ID_i 是需求节点的身份证明。隐蔽密钥 D_k^S 是由数据提供节点使用需求节点的公钥 PK_i^d 对 D_k 进行加密得到的。

数据提供节点获得的金额为 $V_{sell_i} = price(1 - fee)$, 其中 $price$ 代表数据价格, fee 代表服务费率。如图 5 所示, 假设服务费率为 $fee = 1\%$, 数据提供节点 1 提供了价值 50 Coin 的数据, 节点 2 提供了价值 30 Coin 的数据, 节点 3 提供了价值 20 Coin 的数据。那么, 数据需求节点 1 需支付 100 Coin, 而数据提供节点 1 获得 49.5 Coin, 节点 2 获得 29.7 Coin, 节点 3 获得 19.8 Coin, 共识节点获得 1 Coin。

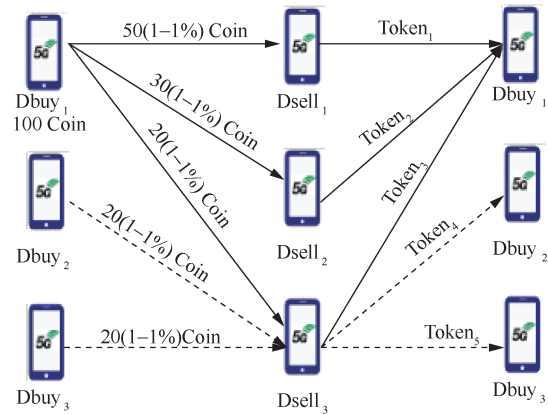


图 5 节点匹配
Figure 5 Node matching

Step5 区块构建阶段。待确认的交易首先存储在交易池中, 等待打包成块上链。当交易成功上链以后, 交易才算验证成功, 数据提供节点才真正获得共享币。账户服务器则根据区块链账本更新用户钱包信息。共识服务器收集交易池中的待确认交易, 共识主节点验证交易后, 将交易添加到区块中, 然后向其他共识节点广播区块信息。当主节点收到不少于 $2f + 1$ 条确认回复信息后, 则完成此次共识, 区块成功上链。在绝大多数区块链应用中, 每一个区块的存储容量约为 1 MB, 每次共识只能验证一部分交易, 因此交易的吞吐量取决于共识速率。

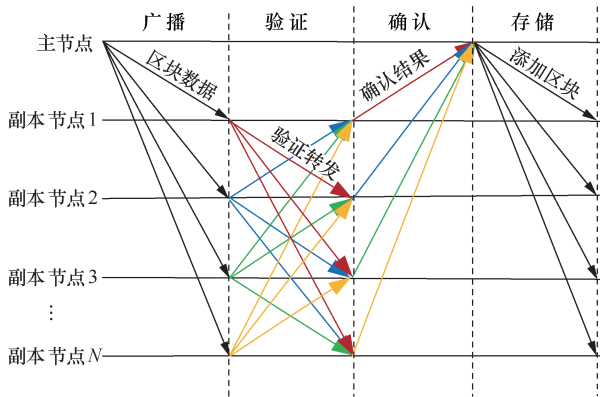


图6 区块构建过程
Figure 6 Block construction process

Step6 数据访问阶段。首先，需求节点向云服务器提供授权令牌，云服务器验证令牌的签名后，向需求节点发送存储在云端的对应加密数据 $data_k$ ， $data_k$ 是由数据提供节点使用对称密钥 D_k 对明文数据进行加密得到的。获取加密数据 $data_k$ 后，需求节点使用自己的私钥 SK_i^d 解密 D_k^s 得到 D_k ，再由 D_k 解密 $data_k$ 得到明文数据 $data$ 。之后，需求节点计算明文数据 $data_k$ 的哈希值，与 $hash_{data}$ 比对，验证数据的完整性。

3.3 基于闪电网络的链下交易机制

在基于区块链的5G物联网数据共享场景中，执行点对点的数据共享，大量的交易是小额的，且用户不需要实时提现，因此比特币闪电网络方案适用于此。同时，可以通过序列到期可撤销合约（RSMC, revocable sequence maturity contract）和哈希时间锁定合约（HTLC, hashed timelock contract）机制，来实现交易性能的提高。

具体来说，RSMC 是在数据共享节点之间建立一个微支付通道，类似于资金池的原理。在交易前，交易双方预存一定的资金在微支付通道中。每次交易时，交易双方对交易后的资金分配方案进行确认签名，并废除旧的资金分配方案。当共享节点需要提现资金时，将经交易双方签署好的分配方案写入区块链，通过区块链进行确认。通过这种方式，交易时不需要上链，只在提现时才通过区块链，减少了区块链的请求次数。其中，交易双方签署的资金分配方案是一个智能合约，即 HTLC。通过该智能合约，转账方先冻结一部分资金，并提供一个已知哈希值，在一定时间内，

若接收方能给出匹配的哈希值，则可以将冻结资金转入。

如图7所示，在基于区块链的5G物联网数据共享中应用闪电网络方案，数据需求节点预存购买数据的资金，和匹配的一个或多个数据提供节点签署资金分配方案，并设置限定时间。当数据提供节点需要提现资金时，将签署好的分配方案写入区块链，经区块链确认后，数据提供节点即可获得相应资金。

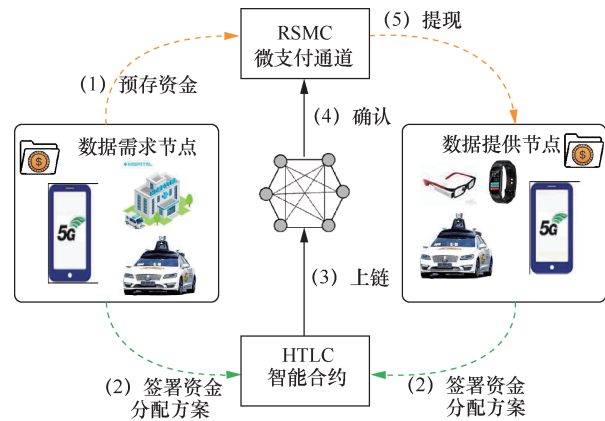


图7 基于闪电网络的链下交易模型
Figure 7 Off-chain transaction model based on lightning network

基于闪电网络的链下交易流程如下。

Step1 获取节点信息。分别获取数据需求节点和数据提供节点的相关信息，包括节点 IP 地址、ID 信息、端口号 port、网络名称、版本号 version 和区块高度 blockheight。

Step2 创建支付通道。闪电网络的 RSMC 微支付通道是实现链下交易的开始，通道建立以后，就可以在区块链下实现交易，无须再广播到链上。创建过程是一个预存数据购买资金的过程，如图7步骤(1)所示。首先数据需求节点向管理的钱包地址存入用于建立通道的资金，然后将这笔资金添加到资金池，之后使用资金池金额的一部分创建微支付通道。

Step3 在闪电网络内进行支付。闪电网络通道中的支付过程是由接收侧发起的，如图7步骤(2)所示。首先数据提供节点生成一个接收单据，然后数据需求节点按照支付的资金大小获得一个从需求节点到提供节点的支付路由，最后根据该路由信息发送资金，并设置限定时间。

Step4 提现资金。如图7步骤(3)~步骤(5)所示。数据提供节点查询通道的最新资金分配方案，并将分配方案写入区块链，经节点确认后，区块生效，数据提供节点获得相应资金。

基于闪电网络的链下交易过程如下。

开始

//准备一笔资金

1) cli/lightning-cli newaddr//数据需求节点生成一个新的地址

2) qtum-cli sendtoaddress//将预存资金发送到数据需求节点的管理钱包地址

3) qtum-cli getrawtransaction//获取交易记录

4) cli/lightning-cli addfunds//增加到资金池
//创建闪电网络通道

5) cli/lightning-cli connect //需求节点与提供节点建立连接

6) cli/lightning-cli fundchannel //需求节点向通道存入资金

//通道内进行支付

7) cli/lightning-cli fundchannel invoice//提供节点生成接收单据

8) cli/lightning-cli fundchannel getroute//需求节点获得支付路由

9) cli/lightning-cli sendpay//需求节点发送资金到提供节点

//查看支付后结果

10) cli/lightning-cli fundchannel getpeers//节点查询资金分配情况

结束

4 实验分析

为评估本文提出的基于区块链的5G物联网数据共享方案的安全性，参照文献[23]的安全性分析方法，对本文方案进行抗攻击能力分析；同时，为衡量基于闪电网络的链下交易机制的性能，以交易吞吐量和时延为指标，进行仿真测试。

4.1 抗攻击能力分析

为了应对5G时代大规模物联网场景，国内外标准制定机构的安全研究早已展开^[24]。2019年2月，欧洲电信标准协会(ETSI)推出了新的物

联网通用标准。2018年10月，中国信息通信研究院与中国通信标准化协会共同研究编制《区块链安全白皮书—技术应用篇(2018版)》^[25]。参考国内外的安全研究成果，本文梳理了7种区块链/物联网常见攻击类别，并分析了基于区块链的5G物联网数据共享框架的抗攻击能力，结果如表3所示。从表3可以看出，对于常见的攻击，本文方案具有较强的抵抗能力。

4.2 基于闪电网络的链下交易机制的性能分析

吞吐量指每秒完成的交易数，基于闪电网络的交易机制是一种安全的链下交易机制，交易时不需要上链，只在提现时才通过区块链，而链下的交易是即时的，不需等待验证。基于闪电网络的交易机制的吞吐量计算公式为

$$\text{TPS}_{\text{LN}} = \begin{cases} \frac{\text{Tx}}{T_{\text{block}} + \text{Tx} \cdot T_{\text{offchain}}}, \\ \text{Tx} \cdot r \leq \frac{\text{SizeBlock}}{\text{SizeTx}} \\ \frac{\text{Tx}}{\left\lfloor \frac{\text{Tx} \cdot r \cdot \text{SizeTx}}{\text{SizeBlock}} \right\rfloor \cdot T_{\text{block}} + \text{Tx} \cdot T_{\text{offchain}}}, \\ \text{Tx} \cdot r > \frac{\text{SizeBlock}}{\text{SizeTx}} \text{ 且 } \frac{\text{Tx} \cdot r \cdot \text{SizeTx}}{\text{SizeBlock}} \in N^* \\ \frac{\text{Tx}}{\left\lfloor \frac{\text{Tx} \cdot r \cdot \text{SizeTx}}{\text{SizeBlock}} + 1 \right\rfloor \cdot T_{\text{block}} + \text{Tx} \cdot T_{\text{offchain}}}, \\ \text{Tx} \cdot r > \frac{\text{SizeBlock}}{\text{SizeTx}} \end{cases} \quad (1)$$

其中，TPS表示吞吐量，Tx表示交易数，SizeBlock表示区块的存储容量，SizeTx表示交易的大小， T_{block} 表示成块的时间， T_{offchain} 表示链下单个交易时间， r 表示提现率(即需要上链的交易比例)， $\lfloor \cdot \rfloor$ 表示向下取整。取 $r=100\%$ ， $T_{\text{offchain}}=0$ ，得到比特币网络的吞吐量计算公式为

$$\text{TPS}_{\text{bitcoin}} = \begin{cases} \frac{\text{Tx}}{T_{\text{block}}}, \text{Tx} \leq \frac{\text{SizeBlock}}{\text{SizeTx}} \\ \frac{\text{Tx}}{\left\lfloor \frac{\text{Tx} \cdot \text{SizeTx}}{\text{SizeBlock}} \right\rfloor \cdot T_{\text{block}}}, \text{Tx} > \frac{\text{SizeBlock}}{\text{SizeTx}} \text{ 且 } \frac{\text{Tx} \cdot \text{SizeTx}}{\text{SizeBlock}} \in N^* \\ \frac{\text{Tx}}{\left\lfloor \frac{\text{Tx} \cdot \text{SizeTx}}{\text{SizeBlock}} + 1 \right\rfloor \cdot T_{\text{block}}}, \text{Tx} > \frac{\text{SizeBlock}}{\text{SizeTx}} \end{cases} \quad (2)$$

表3 7种区块链/物联网常见攻击类别及防御方式分析
Table 3 Seven common attack categories and anti-attack ways of blockchain or IoT

攻击类别	攻击描述	防御方式
追踪攻击	攻击者通过分析区块链公开账本,得出各个交易输入地址和输出地址的连接关系,进而追踪特定地址的交易	本文使用闪电网络,大部分交易发生在主区块链外,通过闪电网络通道进行的所有微支付无法被追踪
链接攻击	攻击者通过分析区块链公开账本,配合IP地址、ID信息等可以链接到真实用户和交易的关联性	节点经注册中心许可后成为合法节点,注册中心由国家监管机构担任,攻击者无法得知实际地理位置、IP地址和ID信息
区块篡改攻击	攻击者首先争得记账权并篡改区块数据,然后将篡改后的区块广播到全网	一方面,通过注册中心监管节点,增大攻击者进入门槛的难度;另一方面,利用共识算法和激励机制,增大攻击者获得记账权的难度
存储篡改攻击	攻击者篡改或删除云数据库中存储的5G物联网数据	云数据库中存储的是加密后的数据,加密数据是由数据提供节点使用对称密钥对明文数据进行加密得到的,攻击者没有密钥则无法篡改数据
越权访问攻击	现有方案大多缺乏权限准入和数据访问机制,难以防止恶意节点的加入	本文采用联盟链技术设置准入权限和数据访问权限增强节点可控性。节点需经注册中心许可才能参与
拒绝服务(DoS)攻击	攻击者作为单个节点向区块链服务器申请大量的数据共享请求,耗尽区块链服务器的网络资源,导致合法用户请求无法通过	物联网节点申请数据共享需要支付一定数额的共享币,攻击者发动拒绝服务攻击将付出巨大经济代价,往往得不偿失,这是一种通过经济博弈来预防攻击的手段
分布式拒绝服务(DDoS)攻击	攻击者通过感染大量物联网节点,向区块链服务器申请大量的数据共享请求	物联网节点间的数据共享采用点对点通信,使用非对称加密机制,攻击者极难获取节点私钥

对于单笔交易,时延是指请求时间(t_1)和上链完成时间(t_2)的差值 $t_2 - t_1$ 。对于一组交易,时延是指一组交易中第一笔交易的请求时间和最后一笔交易上链时间的差值。本文针对一组交易的时延,定义基于闪电网络的交易机制的时延计算公式为

$$\text{Delay}_{LN} = \begin{cases} T_{\text{block}} + T_x \cdot T_{\text{offchain}}, & T_x \cdot r \leq \frac{\text{SizeBlock}}{\text{SizeTx}} \\ \left\lceil \frac{T_x \cdot r \cdot \text{SizeTx}}{\text{SizeBlock}} \right\rceil \cdot T_{\text{block}} + T_x \cdot T_{\text{offchain}}, & T_x \cdot r > \frac{\text{SizeBlock}}{\text{SizeTx}} \text{ 且 } \frac{T_x \cdot r \cdot \text{SizeTx}}{\text{SizeBlock}} \in N^* \\ \left\lceil \frac{T_x \cdot r \cdot \text{SizeTx}}{\text{SizeBlock}} + 1 \right\rceil \cdot T_{\text{block}} + T_x \cdot T_{\text{offchain}}, & T_x \cdot r > \frac{\text{SizeBlock}}{\text{SizeTx}} \end{cases} \quad (3)$$

取 $r=100\%$, $T_{\text{offchain}}=0$, 得到比特币网络的时延计算公式为

$$\text{Delay}_{\text{bitcoin}} = \begin{cases} T_{\text{block}}, & T_x \leq \frac{\text{SizeBlock}}{\text{SizeTx}} \\ \left\lceil \frac{T_x \cdot r \cdot \text{SizeTx}}{\text{SizeBlock}} \right\rceil \cdot T_{\text{block}}, & T_x > \frac{\text{SizeBlock}}{\text{SizeTx}} \text{ 且 } \frac{T_x \cdot \text{SizeTx}}{\text{SizeBlock}} \in N^* \\ \left\lceil \frac{T_x \cdot r \cdot \text{SizeTx}}{\text{SizeBlock}} + 1 \right\rceil \cdot T_{\text{block}}, & T_x > \frac{\text{SizeBlock}}{\text{SizeTx}} \end{cases} \quad (4)$$

本文在配置为Intel Core i7-6700M @3.40GH处理器和16 GB内存,安装了Ubuntu 16.04系统的两台计算机上,通过Qtum闪电网络客户端进行闪电网络测试。在两台计算机上分别安装qtum-core和qtum-lightning,其中qtum-core用于连接主干网络,qtum-lightning使节点实现闪电网络功能。

为衡量基于闪电网络的交易机制的性能,以比特币网络为对比方案,共识机制均采用PoW。取成块时间 T_{block} 为10 min,区块的存储容量为1 MB,交易的大小为20 bit,提现率分别为1%、2%、5%、10%,参数设置如表4所示。本文分别取交易数为 10^3 ,

10^4 , 10^5 , 10^6 , 10^7 , 10^8 笔进行测试, 每组实验独立运行 10 次并求平均值作为测试结果。

表 4 吞吐量和时延实验参数

Table 4 Throughput and delay experimental parameters

参数	取值
T_{block}	10 min
SizeBlock	1 MB
SizeTx	250 bit
r	1%、2%、5%、10%

图 8 展示了比特币 (bitcoin) 网络和闪电网络 (LN) 的交易吞吐量和交易数目关系。随着交易数量的增加, 两个方案的吞吐量均先增加后趋于稳定, 且闪电网络的增速和最终吞吐量均高于比特币网络。当提现率 $r=1\%$ 时, 闪电网络的吞吐量 TPS_{LN} 最终稳定在 666.7 笔/秒, 约为比特币网络吞吐量 $\text{TPS}_{\text{bitcoin}}$ 的 100 倍。当交易数量固定时, 随着提现率 r 增加, 闪电网络的吞吐量逐渐降低, 且增速逐渐放缓。

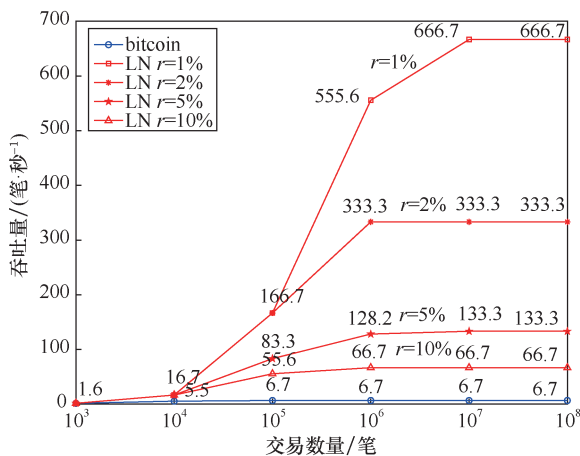


图 8 比特币网络和闪电网络的吞吐量与交易数量关系

Figure 8 The relationship between the throughput and the number of transactions in the bitcoin network and the lightning network

图 9 展示了比特币网络和闪电网络的交易时延和交易数目关系。随着交易数量的增加, 两个方案的时延均逐渐增加, 且比特币网络的时延增加幅度更大。在本文的参数条件下, 可以计算出单个区块能够容纳的最大交易数为 4 000 笔, 当提现的交易数量小于 4 000 笔时, 闪电网络的交易时延恒为 600 s, 如图 9 中的小图所示, 这是由于区块链中的交易是以区块为单位上链, 而单个

区块的成块时间为 600 s, 且此时闪电网络的链下交易耗时极少, 可忽略不计。当交易数量固定时, 随着提现率的增加, 闪电网络的时延逐渐增大, 且增速逐渐上升。当交易数量为 10^5 笔, 提现率 $r=1\%$ 时, 比特币网络的时延为 15 000 s, 闪电网络的时延为 600 s, 此时, 比特币网络的时延约为闪电网络的 25 倍。

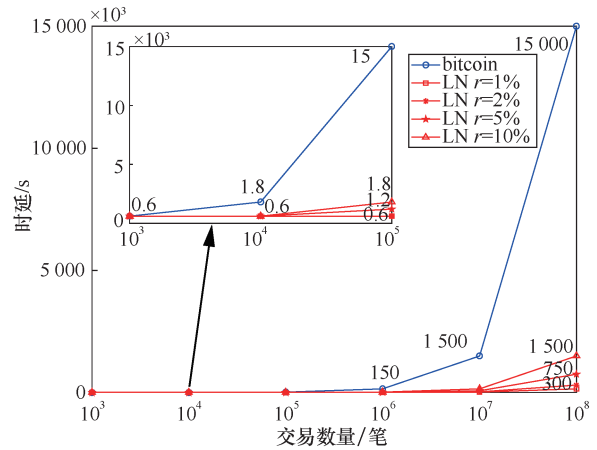


图 9 比特币网络和闪电网络的时延与交易数量关系

Figure 9 The relationship between the delay and the number of transactions in the bitcoin network and the lightning network

综上所述表明, 在本文仿真条件下, 和比特币网络相比, 闪电网络能够大幅提高交易吞吐量、降低交易时延, 提高区块链的扩展性, 支持大规模的交易场景。

5 结束语

本文面向 5G 物联网的应用场景, 针对数据安全共享困难的问题, 提出了一种基于区块链的 5G 物联网数据共享方案。该方案首先利用联盟链技术, 为物联网数据共享场景, 设计了可信安全的点对点数据共享框架; 其次, 基于闪电网络方案, 提出安全的链下交易机制, 实现了交易和验证的分离, 减少了链上操作次数, 提高了交易处理速度。本文重点介绍了链下的实时交易, 针对链上的提现交易, 本文未具体讨论。共识算法是决定链上交易处理速度的关键因素, 下一步将对共识算法的效率问题开展研究。

参考文献:

- [1] HOLMA H, TOSKALA A, NAKAMURA T. 5G technology: 3GPP

- new radio[R]. 2020.
- [2] AGIWAL M, SAXENA N, ROY A. Towards connected living: 5G enabled internet of things (IoT)[J]. IETE Technical Review, 2019, 36(2): 190-202.
 - [3] MOHAMED K S. IoT cloud computing, storage, and data analytics[M]//The Era of Internet of Things. 2019: 71-91.
 - [4] WU Y, LYU Y, SHI Y. Cloud storage security assessment through equilibrium analysis[J]. Tsinghua Science and Technology, 2019, 24(6): 738-749.
 - [5] VALDEOLMILLOS D, MEZQUITA Y, GONZÁLEZ-BRIONES A, et al. Blockchain technology: a review of the current challenges of cryptocurrency[C]//International Congress on Blockchain and Applications. 2019: 153-160.
 - [6] ESPOSITO C, DE SANTIS A, TORTORA G, et al. Blockchain: a panacea for healthcare cloud-based data security and privacy[J]. IEEE Cloud Computing, 2018, 5(1): 31-37.
 - [7] XIA Q I, SIFAH E B, ASAMOAH K O, et al. MeDShare: trust-less medical data sharing among cloud service providers via blockchain[J]. IEEE Access, 2017, 5: 14757-14767.
 - [8] LIANG X, SHETTY S, TOSH D, et al. Provchain: a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability[C]//Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. 2017: 468-477.
 - [9] REHMAN M, JAVAID N, AWAIS M, et al. Cloud based secure service providing for IoTs using blockchain[C]//IEEE Global Communications Conference (GLOBECOM 2019). 2019.
 - [10] SHAFAGH H, BURKHALTER L, HITHNAWI A, et al. Towards blockchain-based auditable storage and sharing of IoT data[C]//Proceedings of the 2017 on Cloud Computing Security Workshop. 2017: 45-50.
 - [11] WANG Y, ZHANG A, ZHANG P, et al. Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain[J]. IEEE Access, 2019, 7: 136704-136719.
 - [12] NOFER M, GOMBER P, HINZ O, et al. Blockchain[J]. Business & Information Systems Engineering, 2017, 59(3): 183-187.
 - [13] CROSBY M, PATTANAYAK P, VERMA S, et al. Blockchain technology: beyond bitcoin[J]. Applied Innovation, 2016, 2(6-10): 71.
 - [14] HAZARI S S, MAHMOUD Q H. A parallel proof of work to improve transaction speed and scalability in blockchain systems[C]//2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). 2019: 0916-0921.
 - [15] SINGH A, CLICK K, PARIZI R M, et al. Sidechain technologies in blockchain networks: an examination and state-of-the-art review[J]. Journal of Network and Computer Applications, 2019: 102471.
 - [16] ZAMANI M, MOVAHEDI M, RAYKOVA M. RapidChain: a fast blockchain protocol via full sharding[J]. IACR Cryptology ePrint Archive, 2018(10): 931-948.
 - [17] KOTILEVETS I D, IVANOVA I A, ROMANOV I O, et al. Implementation of directed acyclic graph in blockchain network to improve security and speed of transactions[J]. IFAC-PapersOnLine, 2018, 51(30): 693-696.
 - [18] POON J, DRYJA T. The bitcoin lightning network: scalable off-chain instant payments[R]. 2016.
 - [19] BARTOLUCCI S, CACCIOLI F, VIVO P. A percolation model for the emergence of the bitcoin lightning network[J]. arXiv preprint arXiv: 1912.03556, 2019.
 - [20] WANG Y, ZENG H, YANG B, et al. Detection of entity-description conflict on duplicated data based on Merkle-tree for IIoT[C]//International Conference on Web Information Systems and Applications. 2019: 163-168.
 - [21] BENJI M, SINDHU M. A study on the Corda and Ripple blockchain platforms[C]//Advances in Intelligent Systems and Computing, 2019: 179-187.
 - [22] DELGADOSEGURA S, PEREZSOLA C, NAVARROARRIBAS G, et al. Analysis of the bitcoin UTXO set[C]//Financial Cryptography. 2018: 78-91.
 - [23] 葛琳, 季新生, 江涛, 等. 基于区块链技术的物联网信息共享安全机制[J]. 计算机应用, 39(2): 154-159.
 - GE L, JI X S, JIANG T, et al. Security mechanism for internet of things information sharing based on blockchain technology[J]. Computer Applications, 39 (2): 154-159.
 - [24] 陈强, 刘彩霞, 李凌书. 基于粒子群优化算法的5G网络切片功能迁移机制[J]. 网络与信息安全学报, 2018, 4(8): 47-55.
 - CHEN Q, LIU C X, LI L S. 5G network slicing function migration mechanism based on particle swarm optimization algorithm[J]. Chinese Journal of Network and Information Security, 2018, 4(8): 47-55.
 - [25] 中国信息通信研究院. 区块链安全白皮书—技术应用篇[R]. 2018.
 - China Institute of Information and Communications. Blockchain security white paper-technology application[R]. 2018.

[作者简介]



乔康(1994—), 男, 四川邛崃人, 信息工程大学硕士生, 主要研究方向为移动通信网络安全和区块链技术。

游伟(1984—), 男, 江西丰城人, 博士, 信息工程大学讲师, 主要研究方向为密码学和移动通信网络。

王领伟(1983—), 男, 河南三门峡人, 信息工程大学讲师, 主要研究方向为移动通信网络安全。

汤红波(1968—), 男, 湖北孝感人, 信息工程大学教授、博士生导师, 主要研究方向为移动通信网络、新型网络体系结构。