

基于联盟链的 区块链短信平台研究

Research on Blockchain SMS Platform Based on Alliance Chain

王九九¹, 马永亮¹, 沈超² (1. 中国联合网络通信集团有限公司, 北京 100033; 2. 联通在线信息科技有限公司, 北京 100032)
Wang Jiujiu¹, Ma Yongliang¹, Shen Chao² (1. China United Network Communications Group Co., Ltd., Beijing 100033, China; 2. China Unicom Online infotech Co., Ltd., Beijing 100032, China)

摘要:

为保障用户安宁权, 解决现有的垃圾短信溯源效果不佳, 用户被大量垃圾信息骚扰的难题, 通过对区块链技术在行业短信领域的研究, 基于区块链技术公开透明、不可篡改、可追溯的特性, 探索用于行业短信应用场景的区块链短信技术。同时, 研发了一套基于联盟链技术的区块链短信平台, 实现了行业短信全流程上链以及行业短信全程可溯源。通过测试, 平台的性能和扩展性能够满足某运营商全行业短信业务需求, 取得了较好的效果。

Abstract:

In order to protect users' right without disturbing and solve the problems of poor traceability of existing spam messages and users are harassed by a large amount of spam information, it explores the application of blockchain technology in the field of industry SMS based on its characteristics of open, transparent, tamper proof and traceable through research on blockchain technology in the field of industry SMS. At the same time, a blockchain SMS platform based on consortium blockchain has been developed, which achieves full process on chain and full traceability of industry SMS. The test results show that the platform's performance and scalability can meet the full industry SMS business needs of a telecom operators and achieving good results.

Keywords:

Blockchain; SMS; Alliance chain; Hyperledger fabric

引用格式: 王九九, 马永亮, 沈超. 基于联盟链的区块链短信平台研究[J]. 邮电设计技术, 2024(6): 78-83.

1 概述

近年来随着互联网产业的兴起, 身份验证、通知消息、营销维系类短信在国民经济中发挥了重要作用。同时, 企业为满足商业需求, 利用行业短信的便捷和低成本特性, 向用户批量发送商业性短信, 引发了短信息服务管理、个人隐私保护方面的问题^[1]。根据我国垃圾短信举报平台公布的工作数据统计^[2], 2019年行业短信的短信举报量就已超过点对点类短信举报量, 其中商业性短信投诉占大多数。

2021年4月, 习近平总书记作出“坚持以人民为中心,

关键词:

区块链; 短信; 联盟链; 超级账本

doi: 10.12045/j.issn.1007-3043.2024.06.016

文章编号: 1007-3043(2024)06-0078-06

中图分类号: TN919

文献标识码: A

开放科学(资源服务)标识码(OSID):



心, 全面落实打防管控措施, 坚决遏制电信网络诈骗犯罪多发高发态势”重要指示, 要注重源头治理、综合治理, 坚持齐抓共管、群防群治, 全面落实打防管控各项措施和金融、通信、互联网等行业监管主体责任。

现有的垃圾短信管控, 无法做到精细化控制, 加之黑名单管控混乱, 使得现有的管控机制效果不佳, 用户被大量垃圾信息骚扰。对于合理的通知短信以及用户愿意接收的营销短信, 因为没有合适的手段区分该类短信与垃圾消息, 导致被误判误拦, 不利于行业的健康发展。

因此, 基于新技术成果并结合行业短信业务特征, 研究新行业短信业务形态和监管手段, 从根本上解决行业短信痛点, 已经成为业内迫切需要解决的难

收稿日期: 2024-04-25

题。

2 区块链电子存证技术

在区块链技术方面,丁勇等设计实现了一种结合 Fabric 技术的电子存证方案,将区块链的共识验证机制与星际文件系统结合,使电子证据安全可信以及责任可追溯^[3]。吕伟龙等针对过期或者无效交易数据需要被压缩或删除的问题,提出了一种适用于联盟链的多中心化的账本修改方案^[4]。郑颖慧从联盟链细粒度访问控制、属性更新、访问策略更新、密钥安全分发、数据高效安全分布式存储等方面,提出了新的联盟链存储和访问控制策略^[5]。

在区块链与应用领域结合方面,任芳等描述了区块链技术在京东物流领域的应用,以及京东区块链防伪溯源平台的情况^[6]。曹颖提出了基于分布式信任的区块链分层抽象模型分析方法、一般征信智能合约模型实现方案以及两层区块链征信网络设计^[7]。刘小东等在药品追溯体系中提出了基于联盟链的药品信息化追溯系统设计方案^[8]。陆一鸣等基于司法电子证据易篡改遗失等问题,构建司法联盟链^[9]。Mittal 等设计实现了一种基于区块链的非接触交付系统,以保证供应链中的产品可追溯,并能安全记录货物及送货人员的健康情况^[10]。Long 等分析了将区块链应用于医药质量溯源领域的优势,提出基于区块链的中药药材溯源方案,以确保药材质量和安全^[11]。戚燕芳等利用区块链技术解决快递物流中涉及的用户隐私泄露问题,解决了快递物流数据的可溯源与责任人明确问题^[12]。杨艳梅等在 Conflux 测试网络中实现了基于区块链技术的公益活动平台,增加了活动透明度^[13]。王健等针对司法场景下的数据存储和共享需求,结合区块链技术设计了一种面向司法审判场景的电子数据安全存储链式结构,实现了司法存证的高效管理^[14]。易先颖等针对商业性短信通信记录信息(CDR)溯源困难问题,结合区块链技术和智能合约,实现了可信任自动化管理商业性短信 CDR 方案^[15]。

3 区块链短信技术方案

3.1 解决思路

为解决行业短信痛点,同时为监管机构提供快速的投诉查询、处理渠道,本文基于区块链技术“开放性”“去中心化”“防篡改性”“可溯源”等特性,通过行业短信所有参与方“上链”,共同推动行业短信业务的

良性发展。

基于区块链的可信数据共享系统,信用中心与各参与方互联,依靠区块链提供的分布式账本结构,使数据交易流通记录公开透明、不可篡改和可追溯,充分反映流通各环节状况,建立数据流通各链条之间的信任关系。

3.2 区块链短信平台整体架构

区块链短信平台底层基于超级账本智能合约的“联盟链”技术,通过区块链记录短信提交、发送、状态报告的全流程信息,实现了短信全流程“可溯源”。该平台采用多共识节点的“可信合作伙伴”机制,具备“防篡改”“稳定性高”等特点。

按照节点类型,区块链短信平台可划分为4种类型:网关节点、共识节点、区块数据节点和查询节点。

区块链短信平台由6个节点组成,其中2个为共识节点,共识节点记录了所有区块链上的操作,并产出区块数据,其他节点同步区块数据。

目前,在区块链短信平台架构中,区块数据节点与共识节点合设,网关节点与查询节点合设。后续根据业务需求,4种类型节点都可单独设置。

3.3 区块链短信实现方案

基于区块链短信平台架构,各业务方在区块链短信平台上实现短信全业务流程,并实现短信全业务流程上链。同时,通过区块链短信唯一标识,即 HashID,实现对区块链短信的全流程溯源。

由于短信全业务流程的所有参与方都在链上操作,且底层的可信联盟链记录了每个短信操作步骤及当时的短信数据,具有不可篡改性。当对垃圾短信进行溯源时,只需要根据短信内容、手机号等信息确定对应的区块链短信唯一标识,即可通过区块链短信全流程溯源,锁定垃圾短信的发送方,实现垃圾短信治理和监管。

3.3.1 区块链短信溯源原理

基于区块链短信平台实现短信参与方及短信全业务流程上链,其原理如下(见图1)。

a) 参与方上链。企业、代理商、运营商短信网关、监管部门等短信相关角色在可信联盟链上创建对应的区块链账号。

b) 短信全业务流程上链。企业客户在发送区块链短信前,先创建区块链短信唯一标识 HashID 并存储在可信联盟链上。各角色对短信的相关操作和短信信息,都被记录到可信联盟链,并与 HashID 关联。

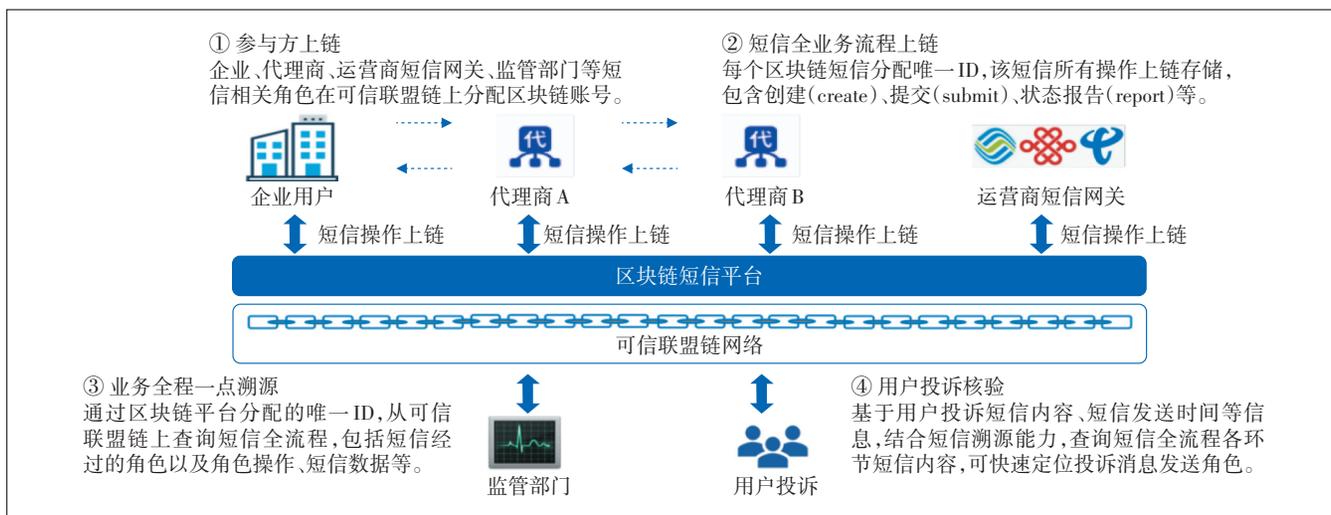


图1 区块链短信溯源原理

c) 业务全流程一点溯源。监管部门、用户可通过区块链短信唯一标识,从可信联盟链上查询短信全流程,包括短信经过的角色以及角色操作、短信数据等。

d) 用户投诉核验。基于用户投诉短信内容、发送时间等信息,结合平台短信溯源能力,快速定位投诉消息发送角色。

3.3.2 区块链短信数据存储结构

为实现区块链短信全业务上链,在底层可信联盟链上创建短信数据存储表。底层可信联盟链采用超级账本技术实现,在超级账本上创建短信数据存储表,短信数据存储表包括短信记录表(cucc_sms_record)和短信操作表(cucc_sms_operation)。

3.3.2.1 短信记录表(cucc_sms_record)

cucc_sms_record用于记录单条短信在不同下发阶段的状态,每条短信只有一条cucc_sms记录,且有唯一的HashID,cucc_sms_record表结构如表1所示。其中,user_list字段标识了该短信经过的不同角色(企业、代理商、短信网关等)。

3.3.2.2 短信操作表(cucc_sms_operation)

cucc_sms_operation记录了不同角色用户对区块链短信的操作记录,其结构如表2所示。其中,content字段为该用户的短信内容。后续用户投诉核验时,可通过对比该字段,确定垃圾短信的具体发送账号。

3.3.3 区块链短信业务流程

根据短信业务流程,区块链短信业务流程包括2种场景。场景1:区块链短信提交至短信网关,短信网关直接返回失败,无后续状态报告;场景2:区块链短信提交至短信网关成功,后续有状态报告。

表1 cucc_sms_record表结构

表字段	类型	说明
id	uint_64_t	主键ID
sms_id_hash	uint_64_t	短信唯一 HashID 值
pull_status	unt_64_t	短信拉取状态
pull_status_hash	unt_64_t	短信拉取状态哈希值
step	std:string	短信当前阶段(create、transfer、submit等)
result	int32_t	短信当前阶段的状态值
previous	name	短信上一级区块链账号
now	name	短信当前所属区块链账号
process	std:string	短信到目前为止经过的所有阶段的列表
user_list	std:string	短信到目前为止经过的所有区块链账号的列表
last_user	std:string	最终接收区块链短信用户,手机号
type	int8_t	短信类型
content	std:string	短信内容
ecnum	std:string	接入号
priority	int8_t	优先级
msgid	std:string	短信网关数据:短信在短信网关的唯一ID
submit_time	std:string	短信网关数据:短信提交响应时间
submit_result	std:string	短信网关数据:短信提交响应结果
dmsgid	std:string	短信网关数据:短信在短信中心的唯一ID
report_time	std:string	短信网关数据:短信状态报告时间
report_status_code	std:string	短信网关数据:短信状态报告状态码
report_err_code	std:string	短信网关数据:短信状态报告错误码

3.3.3.1 业务流程1:提交失败,无状态报告

向短信网关提交区块链短信,短信网关直接返回失败,后续无状态报告,其业务流程如图2所示。

表2 cucc_sms_operation表结构

表字段	类型	说明
id	uint_64_t	主键ID
trans_id	uint_64_t	区块链交易记录ID
sms_id	uint_64_t	cucc_sms_record中ID字段
sms_id_hash	uint_64_t	短信唯一HashID值
previous	name	短信上一级区块链账号
user	name	短信当前所属区块链账号
step	std:string	短信当前阶段(create、transfer、submit等)
ecnum	std:string	接入号
content	std:string	短信内容
memo	std:string	备注
result	int32_t	短信当前阶段的状态值
time	std:string	记录创建时间
report_status_code	std:string	短信网关数据:短信状态报告状态代码
report_err_code	std:string	短信网关数据:短信状态报告错误码

a) 链上操作。企业客户创建区块链短信,生成唯一的短信 HashID,并将携带该 HashID 的短信下发请求提交至 SP 账号,此后该短信在链上的所有发送请求均携带此 HashID。接口动作: create、transfer。

b) 链上操作。SP 账号通过区块链短信接口向短信网关提交短信下发请求。接口动作: transfer。

c) 链上操作。短信网关账号校验 SP 的下发权

限、接入号等信息,校验通过后,向链下短信网关提交短信。接口动作: submit。

d) 链下操作。短信网关通过短信中心等底层设备,提交短信至终端用户(手机号)。

e) 链下操作。终端用户(手机号)返回短信提交失败响应。

f) 链下操作。短信网关返回短信提交响应,并通过内部接口上传至区块链短信平台。

g) 链上操作。利用终端用户(手机号)托管账号,由终端用户(手机号)返回短信提交响应至短信网关账号。接口动作: back。

h) 链上操作。短信网关账号返回提交响应至 SP 账号。接口动作: back。

i) 链上操作。SP 账号返回提交响应至企业客户账号。接口动作: back。

j) 链上操作。监管部门通过区块链短信查询接口,查询短信全流程状态,可进行多维度查询,如通过手机号查询。

3.3.3.2 业务流程2:提交成功,有状态报告

向短信网关提交区块链短信成功,后续有状态报告,其业务流程如图3所示。

a) 链上操作。企业客户创建区块链短信,生成唯

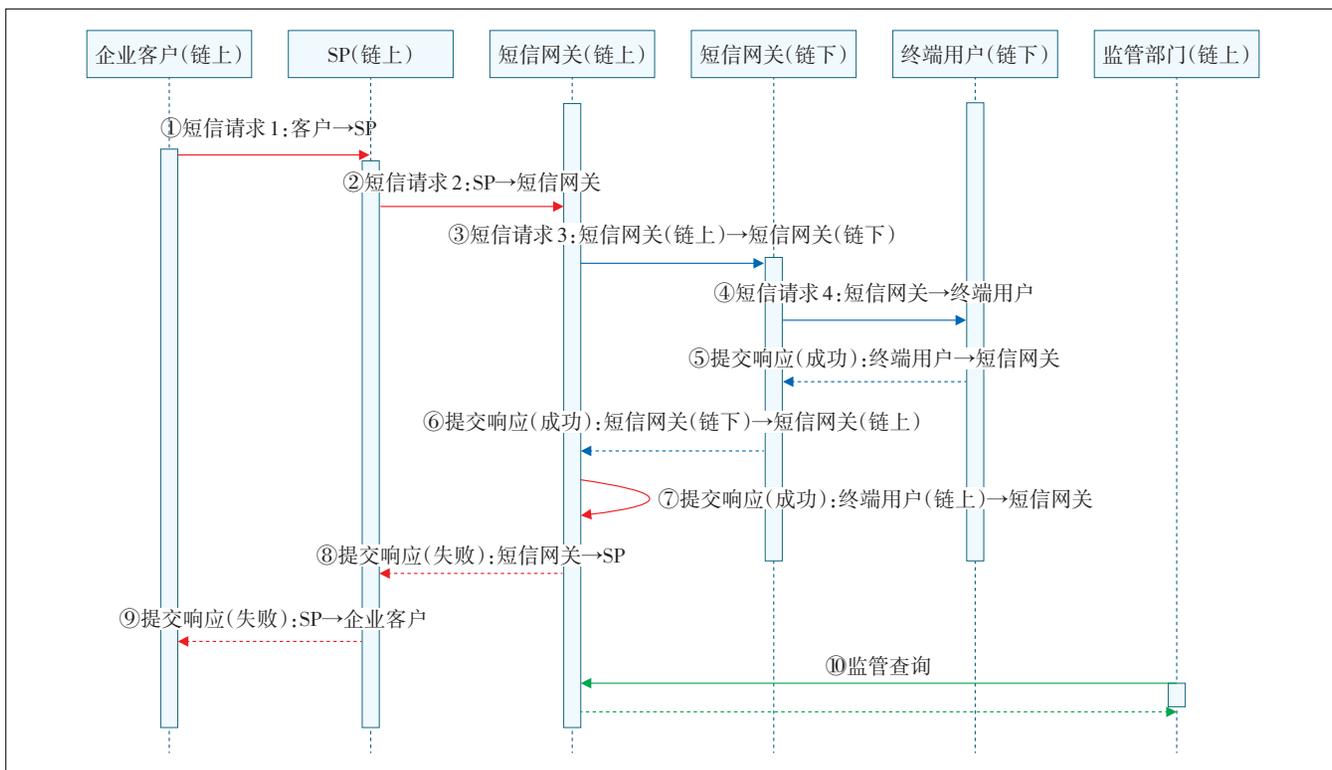


图2 业务流程1:提交失败,无状态报告

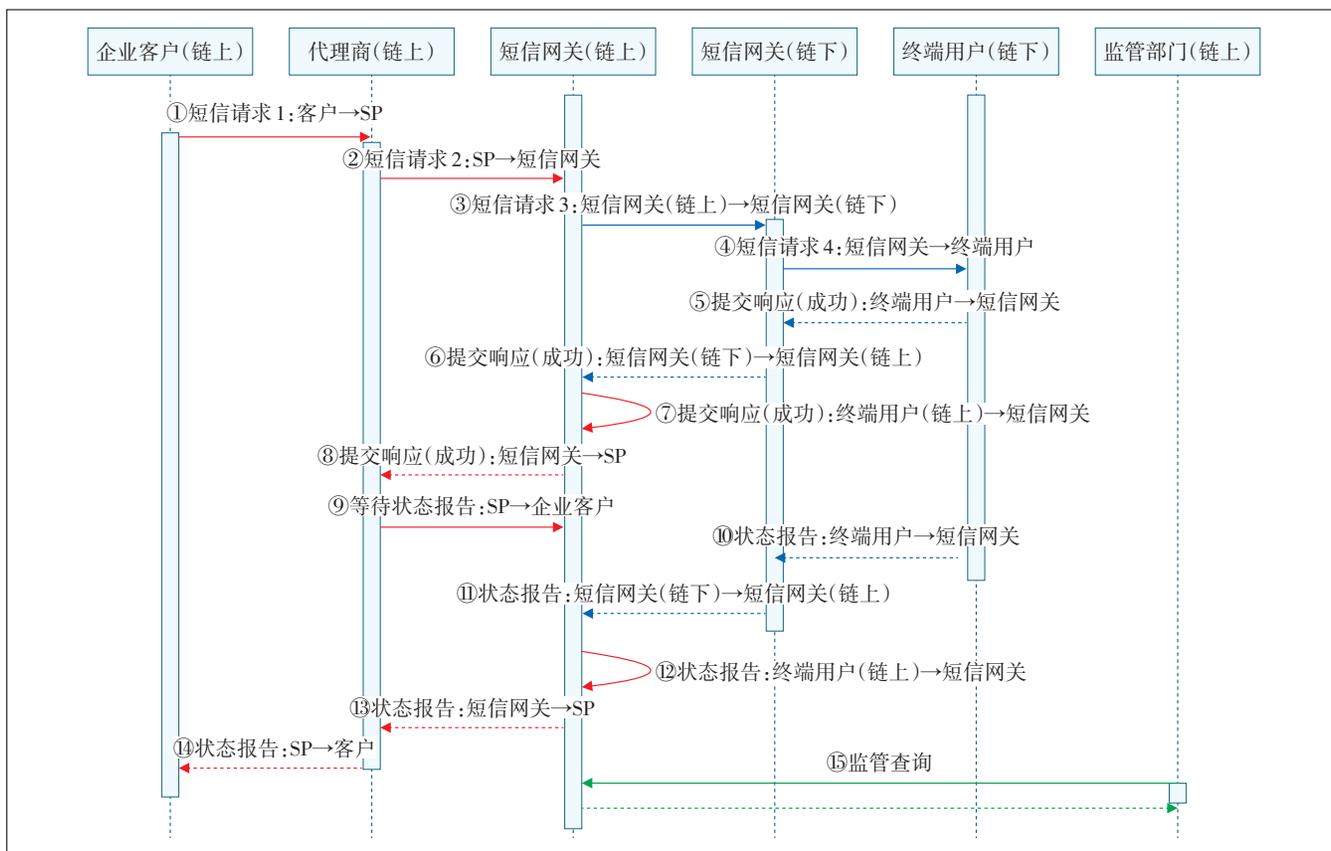


图3 业务流程2:提交成功,有状态报告

一的短信 HashID,并将携带该 HashID 的短信下发请求提交至 SP 账号,此后该短信在链上的所有发送请求均携带此 HashID。接口动作: create、transfer。

b) 链上操作。SP 账号通过区块链短信接口向短信网关提交短信下发请求。接口动作: transfer。

c) 链上操作。短信网关账号校验 SP 的下发权限、接入号等信息,校验通过后,向链下短信网关提交短信。接口动作: submit。

d) 链下操作。短信网关通过短信中心等底层设备,提交短信至终端用户(手机号)。

e) 链下操作。终端用户(手机号)通过短信中心返回短信提交成功响应。

f) 链下操作。短信网关返回短信提交响应,并通过内部接口上传至区块链短信平台。

g) 链上操作。利用终端用户(手机号)托管账号,由终端用户(手机号)返回短信提交响应至短信网关账号。接口动作: back。

h) 链上操作。短信网关账号返回提交响应至 SP 账号。接口动作: back。

i) 链上操作。SP 账号将短信重新提交给短信网

关账号,此时该短信的状态为“等待状态报告”。接口动作: transfer。

j) 链下操作。当终端用户(手机号)成功收到短信或者明确接收短信失败之后,返回包含最终下发结果的状态报告至链下短信网关。

k) 链下操作。短信网关通过区块链短信内部接口,提交短信状态报告至区块链短信平台。

l) 链上操作。利用终端用户(手机号)托管账号,由终端用户(手机号)返回状态报告至短信网关账号。接口动作: back。

m) 链上操作。短信网关账号返回区块链短信状态报告至 SP 账号。接口动作: back。

n) 链上操作。SP 账号返回区块链短信状态报告至企业客户账号。接口动作: back。

o) 链上操作。监管部门通过区块链短信查询接口,查询短信全流程状态,可进行多维度查询,如通过手机号查询。

3.4 测试及结论

3.4.1 测试环境

测试环境为局域互联网,网络带宽为 100 Mbit/s,

共设置2台测试服务器,以局域网方式互联。其中6台服务器配置为:32核CPU,256G内存,32T硬盘。

3.4.2 测试方案

测试阶段1:部署区块链短信平台及底层Fabric服务,使用1台测试服务器,部署单节点区块链共识。使用Jmeter客户端进行压力测试,测试平台整体最大处理能力以及单节点最大处理能力。

测试阶段2:部署区块链短信平台及底层Fabric服务,使用2台测试服务器,部署2节点区块链共识。使用Jmeter客户端进行压力测试,测试平台整体最大处理能力以及单节点最大处理能力。

测试阶段3:部署区块链短信平台及底层Fabric服务,使用2台测试服务器,部署6节点区块链共识。使用Jmeter客户端进行压力测试,测试平台整体最大处理能力以及单节点最大处理能力。

3.4.3 测试结果

区块链短信平台压力测试结果如表3所示。从表3可以看出,单节点处理能力与多节点处理能力基本持平,且随着测试阶段数量的增加,单节点平均交易能力大于等于第1阶段单节点交易能力,整体基本呈线性增长。从CPU负载可以看出,单服务器部署3个区块链共识节点时,CPU负载为50%。理论上,单物理节点最多可部署6个区块链共识节点。

表3 区块链短信平台压力测试结果

测试阶段	节点数量	服务器	CPU负载/%	并发连接数	整体性能/(次/s)	单节点性能/(次/s)
1阶段	1	1	16	300	2 388	2 388
2阶段	2	2	25	600	6 470	3 235
3阶段	6	2	50	1 000	14 310	2 385

一条短信全流程对应最大区块链交易次数为8次(图3中红色流程)。现某运营商行业短信业务峰值为8万条/s,折合区块链交易峰值为64万条/s,按照单物理服务器可部署5个共识节点(理论值为6个共识节点)计算,若要满足峰值行业短信实时交易需求,需要的服务器数量为 $640\,000/5/2\,385\approx 54$ 台,即需要54台物理服务器来满足该运营商峰值区块链短信交易需求。

3.4.4 结论

区块链短信为解决垃圾短信治理以及基于用户意愿的短信发送提供了重要的技术方向。区块链短信平台作为某运营商区块链短信的应用试点,实现了全链路全量行业短信上链以及垃圾短信的有效溯源

和监管。后续配合用户意愿采集、短信分类标识等功能,可真正实现基于用户意愿的短信发送,促进行业短信的良性发展,对于其他运营商也具有一定的借鉴价值。

参考文献:

- [1] 段亦乐. 自我监督的限度——以中国电信自我监管短信群发业务为例[J]. 理论界, 2013(6): 179-181.
- [2] 12321网络不良与垃圾信息举报受理中心. 网络不良与垃圾信息举报受理中心[DB/OL]. [2024-01-25]. <https://www.12321.cn/report>.
- [3] 丁勇, 相恒奎, 罗得寸, 等. 一种结合Fabric技术的电子存证方案[J]. 西安电子科技大学学报, 2020, 47(5): 113-121, 158.
- [4] 吕伟龙, 魏松杰, 于铭慧, 等. 面向可信联盟的区块链账本可验证修改方法研究[J]. 计算机学报, 2021, 44(10): 2016-2032.
- [5] 郑慧颖. 联盟链数据访问控制与高效存储研究[D]. 南宁: 广西大学, 2022.
- [6] 任芳. 区块链技术在京东物流领域的应用[J]. 物流技术与应用, 2018, 23(5): 88-90.
- [7] 曹颖. 基于区块链的个人征信系统设计与实现[D]. 西安: 西安电子科技大学, 2019.
- [8] 刘小东, 黄哲, 陈玉文. 药品追溯体系建立中区块链技术的应用研究[J]. 中国药事, 2022, 36(3): 241-250.
- [9] 陆一鸣, 丁姝萌, 江舒涵, 等. 基于链区块链的电子数据存证技术研究[J]. 网络安全技术与应用, 2022(11): 118-121.
- [10] MITTAL P, WALTHALL A, CUI P C, et al. A blockchain-based contactless delivery system for addressing COVID-19 and other pandemics[C]//2021 IEEE International Conference on Blockchain (Blockchain). Melbourne, Australia: IEEE, 2021: 1-6.
- [11] LONG Y X, CHU D J, WANG H L, et al. Blockchain-Based trace the source system for Chinese medicinal materials[C]//2022 14th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA). Changsha, China: IEEE, 2022: 1007-1010.
- [12] 戚燕芳, 高法钦, 蒋路草, 等. 区块链下的个人快递隐私保护系统研究[J]. 软件导刊, 2022, 21(4): 208-213.
- [13] 杨艳梅, 刘心如, 邓朝军, 等. 区块链在公益活动平台中的应用研究[J]. 软件导刊, 2022, 21(4): 203-207.
- [14] 王健, 张蕴嘉, 刘吉强, 等. 基于区块链的司法数据管理及电子证据存储机制[J]. 信息安全, 2022, 22(2): 21-31.
- [15] 易先颖, 林绍福, 贾晓丰, 等. 基于区块链的商业性短信监管方法研究[J]. 软件导刊, 2023, 22(8): 124-129.

作者简介:

王九九, 毕业于北京交通大学, 硕士, 主要从事网络技术、业务IT一体化相关工作; 马永亮, 毕业于北京邮电大学, 硕士, 主要从事业务IT支撑相关工作; 沈超, 毕业于北京邮电大学, 学士, 主要从事行业短信业务平台建设相关工作。