研究论文

量子安全直接通信与区块链网络融合应用

吴永飞[1], 龙桂鲁[2,3], 金建新[4], 王彦博[1*], 王敏[3*], 魏文术[1], 刘曦子[4], 杨璇[4]

摘要 量子计算威胁经典密码体系给区块链网络通信安全带来全新挑战。量子安全直接通信可实现端对端安全,同时具备感知窃听和阻止窃听的能力,将量子安全直接通信应用在基于经典保密通信技术的区块链网络中,有助于区块链网络抵御量子计算攻击,保障区块链网络安全。探索在区块链网络中应用量子安全直接通信的技术方案,并进行了可行性分析和实验验证,实验成功验证了量子安全直接通信与区块链网络融合方案,利用量子安全直接通信技术为区块链网络保驾护航,增强了区块链网络各节点间信息传输的安全性,助力金融行业打造更加安全可信的数字价值网络。

关键词 量子安全直接通信;区块链;量子计算;网络通信安全

2019 年 10 月 24 日,习近平总书记在十九届中央政治局第十八次集体学习时强调要加快区块链和前沿信息技术的深度融合,推动集成创新和融合应用;要推动协同攻关,为区块链应用发展提供安全可控的技术支撑。2020 年 10 月 16 日,习近平总书记在十九届中央政治局第二十四次集体学习时强调加强量子科技发展战略谋划和系统布局。2025 年,国务院《政府工作报告》明确指出建立未来产业投入增长机制,培育量子科技等未来产业。区块链和量子科技作为全球前沿的新兴技术,有望引领新一轮科技革命和产业变革方向,得到全球极大关注。量子科技发展突飞猛进,量子计算可破解公钥密码算法,对以经典密码学为核心的区块链技术体系带来严重威胁,区块链网络中数据、信息和价值传输亦不再安全,区块链可信体系面临极大挑战。庆幸的是,量子安全直接通信(quantum secure direct communication, QSDC)技术作为量子通信研究领域最新成果,为区块链网络体系抵御量子计算攻击提供了可能,探索量子安全直接通信技术与区块链网络体系融合应用具有积极的现实意义。

1. 华夏银行股份有限公司,北京 100020
2. 低维量子物理国家重点实验室,清华大学物理系,北京 100084
3. 北京量子信息科学研究院,北京 100193
4. 龙盈智达(北京)科技有限公司,北京 100020

1 区块链网络技术概述

1.1 区块链网络技术原理及特点

区块链是分布式存储、共识机制、点对点网络、加密算法等计算机技术在互联网时代的创新应用模式,数据由所有节点共同维护,以此构建一套信任机制,保障系统内数据公开透明,实现数据记录可溯源和难篡改[1]。区块链作为一种分布式系统,通过点对点(peer-to-peer, P2P)网络使得区块链网络中每个节点都可以平等、安全地参与共识与记账,实现分布式

收稿日期:2025-03-01;修回日期:2025-07-09
基金项目:北京市科技计划科技金融创新支持项目(Z231100001323001);中国科学技术协会青年人才托举工程资助项目(2022QNRC001);国家自然科学基金项目(62501057, 62471046, 62131002)
作者简介:吴永飞,研究员,研究方向为金融科技、数字金融,电子信箱:zhwyf@hxb.com.cn;龙桂鲁(共同第一作者),教授,研究方向为量子信息、量子通信、量子算法,电子信箱:gllong@tsinghua.edu.cn;王彦博(通信作者),副研究员,研究方向为大数据、人工智能、量子金融科技、光子金融科技、数字金融,电子信箱:wangyanbo@lyzdfintech.com;王敏(共同通信作者),副研究员,研究方向为量子通信、微纳光学,电子信箱:wangmin@baqis.ac.cn
引用格式:吴永飞, 龙桂鲁, 金建新, 等. 量子安全直接通信与区块链网络融合应用[J]. 科技导报, 2026, 44(2): 89-97; doi:10.3981/j.issn.1000-7857.2025.03.00144

网络各节点数据的一致性和可靠性[2]。

P2P 网络中应用了 P2P 协议,该协议构成了区块链网络的基础协议,主要包括如下功能。(1) 区块链节点标识与发现。在区块链网络中,每个区块链节点通过唯一标识符与其他节点区分开,并通过唯一标识符对区块链节点进行寻址。(2) 区块链节点连接管理。实现对区块链节点身份验证,维护各区块链节点之间长连接,对异常连接采取自动断开和自动发起重连。(3) 区块链节点信息通信。在区块链网络中,通过单播、组播或广播等方式完成的区块链节点间的信息通信。(4) 节点同步。完成区块链节点间数据同步,包括交易同步、状态同步等工作。区块链网络常用 P2P 协议算法包括 Gossip、LibP2P、Kademlia 等。以 Gossip 为例,该协议算法由 Demers 等[3]在 1987 年提出。超级账本 Hyperledger Fabric 采用 Gossip 算法作为其网络的传播协议,负责新节点发现、节点监测、剔除离线节点、更新节点列表等(图 1)。

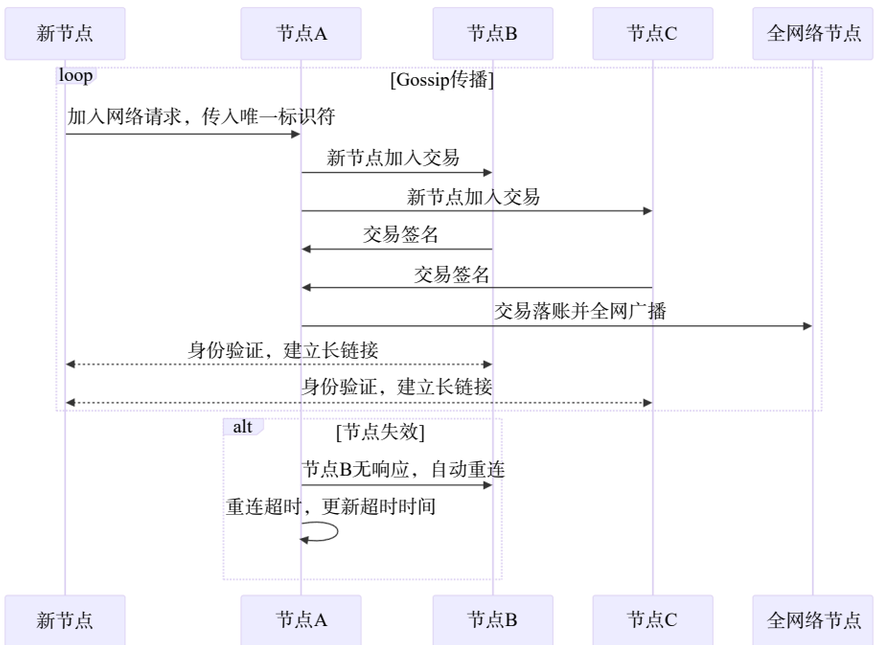

图 1 区块链节点连接管理时序

1.2 区块链网络安全问题现状

区块链主要依托 P2P 协议、SSL/TLS(加密套接字协议层/传输层安全协议)安全通信机制、共识机制等方法为区块链应用提供对等、可信、安全的网络和通信基础[4]。尽管如此,区块链网络安全问题仍不可小觑。

匿名性是公有链的重要特点之一,该特点在保护用户节点隐私的同时带来了相关网络安全风险。公有链网络中,用户不需要身份认证便可轻易创建分布式节点,导致攻击者可以轻易伪造身份加入网络实施攻击。Sybil 攻击(女巫攻击)便是一种攻击方式。Sybil 攻击通过伪造 P2P 网络中大量节点,发出虚假节点信息、误导节点间的正常信息传递,从而破坏网络安全[5]。Eclipse 攻击(日食攻击)通过侵占网络中节点的路由,将足够多的虚假节点添加到某个受害者周围,从而将正常节点限制在隔离网络中并实施欺骗[6]。此外,DDoS 攻击(分布式拒绝服务攻击)利用区块链节点交易同步机制对区块链网络节点发送大量虚假信息,阻塞网络正常运行[7]。

鉴于商业场景对安全、隐私、监管、审计等方面更高的需求,联盟链引入了身份验证机制和网络通信安全协议 SSL/TLS 以保证分布式节点身份可信和数据传输安全。SSL/TLS 协议通过公钥加密算法、数字证书签名等技术手段,进行通信加密、数据签名及校验、身份验证,在保护数据机密性、完整性,以及身份鉴别等方面发挥了重大作用[8]。区块链网络通过 SSL/

TLS 协议,使得不法分子无法通过非法方式窃听、截取和修改网络流量内容,也无法冒充通信者身份,一定程度上确保了区块链节点间共识信息和通信数据传输的安全性和可用性。

然而,SSL/TLS 协议在身份认证和会话密钥协商过程中均涉及签名、验签,以及相应的密钥交换等多种非对称加密算法。若上述加密算法存在潜在后门、漏洞或者弱点,数据传输安全将面临巨大安全风险。从国产自主可控的角度考虑,业界通过对通信消息中的密钥协商部分进行国密化适配,实现 TLS 国密化改造,以保证区块链网络通信安全。

2 量子计算威胁区块链网络通信安全

SSL/TLS 协议应用了 RSA(Rivest-Shamir-Adleman)、ECC(elliptic curve cryptography)、DH(Diffie-Hellman)等公钥密码算法,并在被用于区块链网络中实现了国密化改造,构成确保区块链网络信息安全的底层机制。但随着量子计算技术不断取得突破,对于经典计算机来说足够“困难”的密码算法破解问题在量子计算面前可被轻易破解。由此,量子计算威胁经典密码体系给区块链网络通信安全带来全新挑战。

2.1 量子计算

量子计算是利用量子力学的基本特性实现问题求解的新型计算模式。量子计算机是实现量子计算的物理装置。量子计算以量子比特为基本单元,与传统比特一个时刻只能存储一个状态不同的是,量子比特可以是状态的线性叠加,也称为叠加态。量子计算机通过对量子态的操控实现存储和计算,可以实现经典计算机难以比拟的信息携带和并行计算能力。量子计算机的处理能力将随着比特数的增长呈指数级增长,可以解决经典计算机无法解决的大规模计算难题。

2.2 量子计算 Shor 等算法威胁非对称加密算法

量子计算的快速发展导致区块链中的传统密码算法面临着被量子计算机攻击的威胁。其中,Grover 算法对区块链中使用的哈希函数、Merkle 树产生冲击;Shor 算法则直接威胁了区块链中的非对称加密算法。Shor 算法是一种对大数因子分解,离散对数问题解决有着开创性和重大影响的量子算法。该算法于 1994 年被美国科学家 Shor[9]提出,它在理论上展示了利用量子计算机在多项式时间内分解大整数和求解离散对数等复杂数学问题,可以对广泛使用的 RSA、ECC、DSA(digital signature algorithm)、ElGamal 等公钥密码体制进行快速破解。Shor 算法的核心是利用数论的相关定理,将大数因子分解过程转化为求某个函数的周期,可以以极高的效率实现量子傅里叶变换,指数级提高大整数的质因子分解速度,从而对公钥密码造成毁灭性的攻击。2019 年,谷歌公司研究团队指出,理论上通过 2000 万个量子比特量子计算机可在 8 h 内破解 2048 位 RSA 加密算法[10]。2021 年 3 月,巴黎萨克雷大学和吉夫续尔伊凡特理论物理研究所的相关研究发现,可以使用 13436 个物理量子比特在 177 d 内完成 2048 位 RSA 密码破译[11]。2022 年,中国学者提出了量子经典混合算法,有望使用现有的量子计算机破译 RSA[12],该算法的加速性能得到肯定[13],而且最近的实验研究推断该类算法可能给出多项式复杂度[14]。况且,量子计算机的硬件发展迅速。根据谷歌公司和 IBM 公司(国际商业机器公司)量子计算技术路线图,2029 年将会实现百万量子比特。随着量子比特数持续增加,破解公钥密码算法时间将大大缩减,量子计算机对于区块链威胁日益迫近。

2.3 量子计算 Shor 等算法威胁区块链网络传输安全

区块链网络中,存在大量使用公钥加密算法的应用。一方面,区块链网络中应用 SSL/TLS 协议,并通过使用公钥加密算法、数字证书签名等技术手段实现数据加密传输、节点连接认证等;另一方面,公有链应用公钥加密算法实现数字资产确权等。公有链中数字资产的公钥由私钥通过椭圆曲线、哈希等算法生成中间数据,再进一步编码形成。公钥生成过程是不可逆的,即不能通过公钥反推出私钥。

在经典计算机时代,上述过程对公钥加密算法的使用足以保障数据传输通信以及数字资产安全。然而在量子计算时代,Shor 等量子算法能够在多项式时间内解决质因子分解和离散对数问题,攻击者可以利用 Shor 算法破解 SSL/TLS 协议公钥加密算法,获取用户私钥,从而伪造区块链数据信息、签名和转移资产等,导致区块链加密通信和数字资产不再安全,以

经典密码学为核心的可信区块链体系将不再可信,基于区块链的价值网络亦是空中楼阁。

3 量子保密通信技术保障区块链网络通信安全

3.1 量子通信技术

量子通信作为量子信息科学的重要分支,由Bennett等在20世纪80年代提出,它是利用量子态作为信息载体来进行信息交互的一种新型通信技术。量子通信的关键技术有量子密钥分发(QKD)、量子安全直接通信、量子隐形传态(QT)等。量子密钥分发和量子安全直接通信是当前最受关注的2种量子保密通信技术。

3.2 量子密钥分发

量子密钥分发是当前最重要和主流的量子保密通信技术之一。量子密钥分发将量子状态作为信息加密和解密的密钥,以量子态为信息载体,通过量子信道使通信双方共享密钥。现阶段较为通用的是由Bennett等[15]于1984年提出的Bennett−Brassard(BB84)协议。量子密钥分发的安全性基于量子力学的基本原理,通过对单光子的量子态制备、传输和测量,首先在收发双方间实现无法被窃听的安全密钥共享,之后再与传统保密通信技术相结合完成经典信息的加解密和安全传输。量子密钥分发过程中,对密钥的窃听都需要对量子态实施测量,根据量子力学不可克隆原理,任何测量或攻击行为都会导致信息传输载体——量子态本身发生变化,造成高误码率,从而使窃听者被发现并终止通信。量子密钥分发技术可以建立起安全的通信密钥,通过“一次一密”的加密方式实现点对点的安全通信。2021年,中国科学技术大学潘建伟团队首次展现了由700多个光纤量子密钥分发链路和2个高速“卫星—地面”自由空间量子密钥分发链路组成的天地一体化量子通信网络[16]。

3.3 量子安全直接通信

量子安全直接通信是量子通信的重要模式之一,它是指利用量子态作为信息载体直接进行安全通信的技术。量子安全直接通信自2000年被提出以来,经过25年的深入研究,已经开始走入实用系统研制与推进实用阶段。相比于量子密钥分发,量子安全直接通信将量子通信从量子密钥分发的感知窃听发展成为既感知窃听又阻止窃听。量子安全直接通信通过在量子信道传输信息,可以发现和阻止窃听,不泄露信息,具有高度的安全性。2016年,Hu等[17]在光纤系统中实现了基于单光子频率编码的量子安全直接通信实验演示。2017年,Zhang等[18]完成了基于量子存储的量子安全直接通信演示。同年,Zhu等[19]完成了基于光纤纠缠源的量子安全直接通信演示。2019年,Qi等[20]研制出首台实用化单光子量子安全直接通信样机,并基于Wyner搭线信道理论计算了量子安全直接通信的安全信道容量。2021年,Cao等[21]提出了基于双模压缩态的量子安全直接通信方案。同年,Qi等[22]实现了基于时间−能量纠缠和和频的15个用户量子安全直接通信网络。2022年,Zhang等[23]设计了一种相位量子态与时间戳量子态混合编码的量子安全直接通信新系统,成功实现100 km的量子安全直接通信。2022年,Long等[24]提出了安全中继网络方案并进行了实验演示。2023年,Wang等[25]演示了基于安全中继的三节点量子安全直接通信网络。2024年,Wang等[26]提出了一种基于格密码算法的量子安全直接通信网络的接入认证方案,实现了对量子信道的安全认证,具备双向互认、条件匿名性、数据保密性、数据完整性、不可伪造性和不可抵赖性等安全性,为基于现有技术构建量子安全的量子通信网络提供了新思路。2025年,Pan等[27]提出单向量子安全直接通信方案并成功研制系统,在104.8 km光纤中实现了2.38 kbps的传输速率的世界纪录。同年,Yang等[28]成功实现4节点间300 km级的全连接量子安全直接通信网络。

量子安全直接通信在国外的研究更多侧重于新协议的提出和原理验证实验。2006年,Lee等[29]利用GHZ(Greenberger–Horne–Zeilinger)态量子安全直接通信方案构造了量子身份认证协议。同年,Marino等[30]提出基于连续变量纠缠态的量子安全直接通信协议。2008年,Pirandola等[31]提出基于相干态的连续变量量子安全直接通信协议。2016年,Lum等[32]提出用量子数据锁定进行量子安全直接通信并完成实验演示。2019年,Shapiro等[33]提出了基于量子低截获概率的量子安全直接通信协议并完成实验演示;同年,Massa等[34]提出双向量子安全直接通信方案,并进行了实验演示。2021年,Vázquez−Castro等[35]提出了量子无密钥隐私通信协议。同年,Chandra等[36]提出了

利用含噪纠缠态进行量子安全直接通信的协议。2023 年, Paparelle 等[37]完成了压缩态连续变量量子安全直接通信实验演示。量子保密通信如图 2 所示[38]。

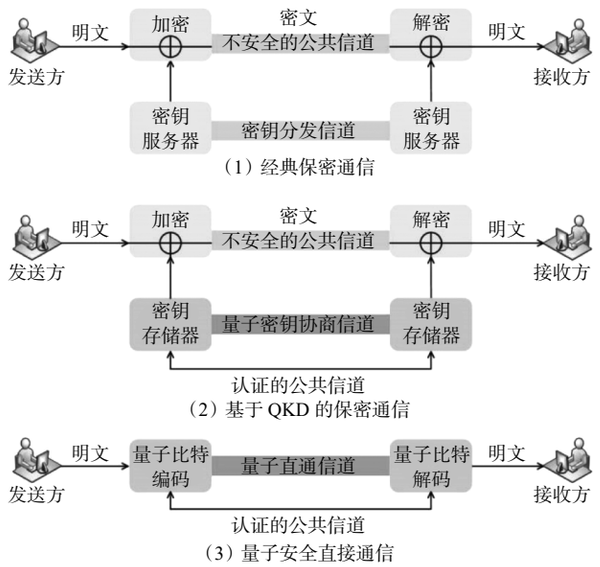

图 2 保密通信

3.4 量子安全直接通信有助于保障区块链网络安全

量子安全直接通信技术基于“海森堡测不准原理”“不可克隆原理”“测量塌缩”等物理特性, 实现了高度保密的量子通信。因此, 面对强大的量子计算对于区块链的威胁, 有必要探索将量子安全直接通信应用在基于经典保密通信技术的区块链网络中, 构建端对端安全、量子窃听感知的区块链量子网络, 以对抗目前已知的量子计算攻击。

4 量子安全直接通信技术与区块链网络融合应用研究

4.1 量子安全区块链网络的国内外研究现状

国内外对量子安全区块链的研究主要围绕抗量子密码与区块链的结合、量子密钥分发与区块链的融合等方面展开。在区块链与抗量子密码的结合方面, 国内外多个研究团队和项目已取得进展。该方法专注于开发和集成后量子密码学(post-quantum cryptography, PQC)算法, 如基于格的加密、哈希签名方案等, 旨在替换现有易受量子攻击的经典加密算法, 确保区块链网络在量子计算环境下的安全性与隐私保护能力。例如, 国外的可验证随机函数(quantum resistant ledger, QRL)项目采用基于哈希的 XMSS 签名算法, Algorand 则通过 VRF(可验证随机函数)和后量子签名算法(如 Falcon)实现了量子安全增强; 国内的长安链和蚂蚁链分别集成了 Dilithium 抗量子签名算法, 为区块链交易提供了量子安全保护。在量子密钥分发与区块链的融合方面, 利用量子密钥分发实现节点间的安全密钥交换, 为区块链提供理论上不可破解的通信保障。国际方面, 2022 年, 摩根大通公司构建了一个量子密钥分发网络, 以保护本公司的生产级点对点区块链网络 Liink。国内方面, 通付盾公司提出了基于量子密钥分发和区块链技术的新一代加密通信系统方案。2020 年, 中国联通研究院、亨通光电公司、问天量子公司等机构在“京雄量子加密干线”上完成区块链 BaaS+量子通信的验证测试。在区块链与量子安全直接通信的结合方面, 主要是提出理论方案与协议。2023 年, Xu 等[39]提出在量子存储网络阶段利用量子安全直接通信等技术实现区块链网络的安全通信。2025 年, Sun 等[40]提出了一种基于量子安全直接通信网络的量子区块链方案。本文提出量子安全直接通信与区块链网络融合技术方案, 并在实验上演示验证了量子安全直接通信增强的区块链网络。该技术方案通过协议适配层实现区块链 P2P 网络与量子安全直接通信设备的无缝对接, 无需重构区块链底层, 实现量子安全直接通信对智能合约全生命周期操作的支持; 此外, 全链路量子安全保障, 现有抗量子密码方案仅保护密钥或签名环节, 而量子安全直接通信直接替代经典通信信道, 实现从数据传输到共识验证的全流程量子安全; 相比量子密钥分发和抗量子密码仅能被动防御, 量子安全直接通信的“测量–塌缩”特性可实时感知并阻断窃听, 结合安全中继网络可突破距离限制构建端到端安全的量子区块链网络。

4.2 量子安全直接通信与区块链网络融合可行性分析

量子计算技术对以经典密码体制为核心的区块链体系和网络通信安全产生了直接威胁, 探索量子安全直接通信技术应用于区块链网络中, 以量子信道代替经典信道, 通过量子态实现信息传递, 以保障数据通信实现无条件安全。鉴于区块链网络技术与实用性量子安全直接通信技术的相关接口技术、协议标准、部署环境、性能指标参数等不尽相同, 有必要对其进行分析。

区块链网络方面。首先,要明确区块链网络协议通信时间相关指标参数。区块链网络采用 P2P 通信协议,主要功能是节点发现、节点连接管理、节点监测、节点同步等。因此,要明确协议中区块链各节点的心跳频率、节点相应超时时间等参数。其次,明确区块链交易中数据通信速率相关指标数据。区块链交易流程一般包括发送提案、背书交易、检查提案响应、发送交易、交易排序、验证和提交交易,涉及共识算法、账本同步、账本读写等多个节点相互通信和账本操作,需要明确不同类型交易的数据传输速率、峰值、数据量等内容以满足量子安全直接通信要求。

量子安全直接通信方面。区块链是分布式系统,由多个分布式节点互联并通过 P2P 协议构建区块链网络,若将量子安全直接通信技术应用到区块链网络中,则量子安全直接通信技术需要具备组网能力。目前,安全中继用量子安全直接通信和抗量子密码结合,可以实现量子通信安全组网。其中,密文在量子信道中传送,具备感知窃听和防止窃听的能力。经典中继的信息在抗量子密码保护下具有可抵抗量子计算攻击的安全性。此外,量子安全直接通信包括量子态制备、窃听检测、信息编码、信息调制、信息解调、信息解码等多个步骤,为满足区块链 P2P 网络正常运行,量子安全直接通信相关通信技术指标、协议和数据接入方式应能够与区块链系统实现适配。当前,量子安全直接通信系统具有较高的稳定性和极低的量子比特误码率(QBER),为接入区块链网络并正常通信奠定基础。

如图 3 所示,本实验将区块链节点间的传统通信信道替换为量子安全直接通信。在该配置下,数据从节点 A 由其量子安全直接通信发送端(Alice)发出,通过量子信道安全传输,由节点 B 的 QSDC 接收端(Bob)接收,最终由 Bob 将数据转发给节点 B 进行处理。

4.3 量子安全直接通信与区块链网络融合实验验证

如图 4 所示,在实验室环境下构建区块链网络,各参与机构(如机构 A、B 等)均部署区块链节点。为提高信道安全性,节点间的通信采用单向量子安全直接通信协议[27]实现,机构节点的数据接口与量子安全直接通信发射端/接收端设备(Alice 和 Bob)配对连接,并通过协议适配与接口转换实现数据通信。在本验证实验中,机构 A 与机构 B 之间通过 25 km 标准单模光纤(平均链路损耗 0.2 dB/km)建立量子信道,发送端采用弱相干光作为光源,工作波长为 1550 nm,重复频率为 1.25 GHz,脉冲宽度为 50 ps。系统采用 1 个信号态和 2 个诱骗态,其中信号态平均光子数为 0.6,诱骗态平均光子数为 0.2 和 0(真空态)。接收端采用 InGaAs/InP 单光子探测器,探测效率为 20%,暗计数率 1.2×10^{-6}/gate,如图 5 所示,实验测得系统平均量子比特误码率为 3.84%。基于此配置,首先验证了利用量子安全直接通信技术在 2 个机构间成功进行量子通信的能力。继而,进一步在该融合了量子安全

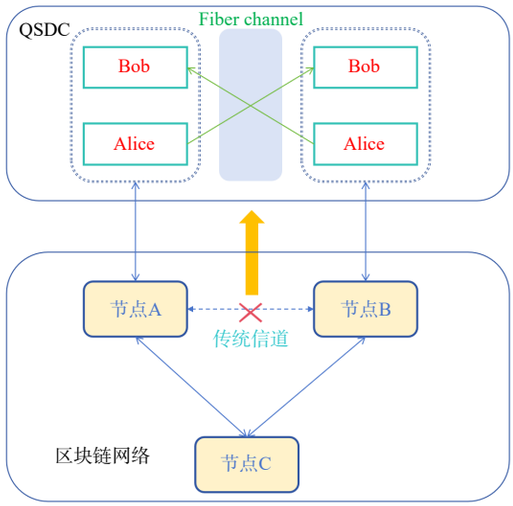

图 3 区块链融合 QSDC 集成示意

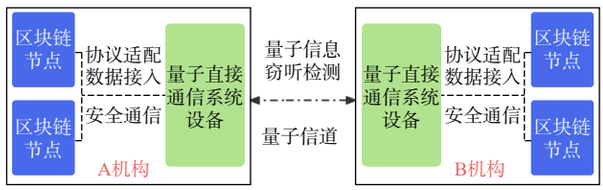

图 4 实验室环境下基于量子安全直接通信的区块链网络示意

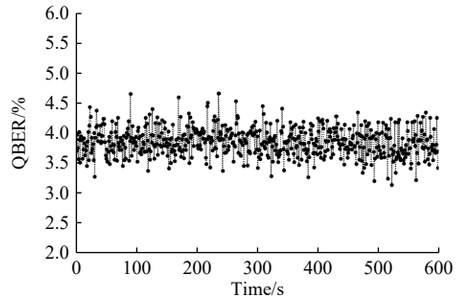

图 5 量子安全直接通信系统量子比特误码率测试结果

直接通信的区块链网络上执行交易功能测试,以验证系统的整体可行性。

验证实施步骤如下。(1)测试环境准备。配置A机构和B机构的区块链节点,并确保其正常运行。配置量子安全直接通信系统设备,确保区块链节点与量子安全直接通信设备之间正常通信。(2)节点共识测试。通过日志观察A机构与B机构节点间的共识过程是否正常完成,验证共识算法正确执行。(3)合约创建部署测试。在A机构的节点上创建和部署智能合约,并在B机构节点上验证其在网络中的正确性和可用性。(4)合约交易测试。发起合约交易操作,在A机构的节点上执行合约的调用操作,并在B机构节点上检查交易是否被正确记录和执行。(5)合约查询测试。在B机构节点上进行合约查询,验证查询结果的准确性和一致性。

通过执行上述步骤,A机构与B机构节点利用量子安全直接通信技术通信时,节点共识、合约创建部署、合约交易,以及合约查询等功能均表现正常,成功验证量子安全直接通信与区块链网络融合方案。实验结果显示,量子安全直接通信在节点共识、合约创建、合约交易及合约查询4个核心场景中均表现出与经典信道相近的流量性能。具体数据如表1所示。

表1 实验室环境下基于量子安全直接通信的区块链核心功能流量指标数据

验证功能	指标	经典信道/kb	量子信道/kb
节点共识	5 min总量	5.75	6.62
合约创建	交易峰值	7.75	8.74
合约交易	交易峰值	8.03	9.20
合约查询	交易峰值	10.20	14.38

上述结果验证了量子安全直接通信在保持安全特性的同时,能够支撑区块链基础通信需求。该实验为构建基于量子通信技术的安全区块链网络提供了重要的数据参考。理论上,多机构节点之间所有信道都可以替换为量子信道,由此建立一个能够抵御量子计算攻击的区块链网络体系,并利用量子安全直接通信技术感知窃听和防止窃听能力,实现端对端的安全通信。当然,在实际生产面临高频次交易场景需求时,一方面,需要对区块链进行分流分层优化改造处理,以满足高标准的业务需求通过设置流量分级管理机制;另一方面,通过提升量子硬件性能参数,包括提升弱相干光光源的重复频率、单光子探测器的探测效率、量子态的调制解调速率和优化编解码方案等措施,使量子信道的数据传输速率和有效吞吐量逐步提升。

当前,量子安全直接通信最大支持距离为100 km,若机构彼此之间距离超过100 km,则可考虑建立量子安全直接通信安全中继,实现长距离量子安全直接通信。为保障安全中继节点数据安全性,在量子信道传输和安全中继节点中,采用抗量子密码算法对数据进行加密,以抵御量子计算机对安全中继节点数据的破译和攻击。根据量子安全直接通信网络技术指标参数情况,调整区块链节点P2P网络模块相关参数进行适配,保证节点之间正常通信。

5 结论与展望

基于“海森堡测不准原理”“量子不可克隆定理”“测量塌缩”等物理特性,量子安全直接通信可实现端对端安全,同时具备感知窃听和阻止窃听的能力。本文探索在区块链网络中应用量子安全直接通信技术方案,利用量子安全直接通信技术为区块链网络保驾护航,增加了区块链网络各节点间信息传输的安全性,助力金融行业打造更加安全可信的数字价值网络。当然,量子安全直接通信与区块链网络融合应用落地还面临传输距离受限(最大仅支持100 km传输)、通信速率相对较低无法适配高频区块链交易场景等难点。针对这些挑战,未来可通过量子中继网络和卫星通信扩展传输距离,采用高维量子编码提升通信速率,开发量子适配中间件实现协议兼容。随着量子通信技术快速发展,量子安全直接通信局域网、城际网及全球量子网络将逐步成为现实,建立在量子安全直接通信之上的区块链将有助于构建无条件安全、信息可信的数字基建底座,赋能数字经济发展。

致谢: 华夏银行股份有限公司贾蒴,龙盈智达(北京)科技有限公司李广龙、郑宏、阳少杰、张月、高新凯对本文亦有贡献。

参考文献(References)

[1] 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, 2017, 44(4): 1−7.
[2] 刘敖迪, 杜学绘, 王娜, 等. 区块链系统安全防护技术研究进展[J]. 计算机学报, 2024, 47(3): 608−646.
[3] Demers A, Greene D, Houser C, et al. Epidemic algorithms for replicated database maintenance[J]. ACM SIGOPS Operating Systems Review, 1988, 22(1): 8−32.
[4] 倪雪莉, 马卓, 王群. 区块链P2P网络及安全研究[J]. 计算机工程与应用, 2024, 60(5): 17−29.
[5] Platt M, Platt D, McBurney P. Sybil attack vulnerability trilemma[J]. International Journal of Parallel, Emergent and Distributed Systems, 2024, 39(4): 446−460.
[6] Dai Q Y, Zhang B, Dong S Q. Eclipse attack detection for blockchain network layer based on deep feature extraction[J]. Wireless Communications and Mobile Computing, 2022, 2022: 1451813.
[7] Shah Z, Ullah I, Li H L, et al. Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey[J]. Sensors, 2022, 22(3): 1094.
[8] 刘新亮, 杜瑞颖, 陈晶, 等. 针对SSL/TLS协议会话密钥的安全威胁与防御方法[J]. 计算机工程, 2017, 43(3): 147−153.
[9] Shor P W. Polynomial−time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Review, 1999, 41(2): 303−332.
[10] Arute F, Arya K, Babbush R, et al. Quantum supremacy using a programmable superconducting processor[J]. Nature, 2019, 574: 505−510.
[11] Gouzien , Sangouard N. Factoring 2048−bit RSA integers in 177 days with 13436 qubits and a multimode memory[J]. Physical Review Letters, 2021, 127(14): 140503.
[12] Yan B, Tan Z, Wei S, et al. Factoring integers with sublinear resources on a superconducting quantum processor[J]. arXiv, 2022: 2212.12372.
[13] Campbell R, Diffie W, Robinson C. Advancements in quantum computing and AI may impact PQC migration timelines[J]. arXiv, 2024: doi: 10.20944/preprints202402.1299.v1.
[14] Tesoro M, Siloi I, Jaschke D, et al. Quantum inspired factorization up to 100−bit RSA number in polynomial time[J]. arXiv, 2024: 2410.16355.
[15] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing[J]. Theoretical Computer Science, 2014, 560: 7−11.
[16] Chen Y A, Zhang Q, Chen T Y, et al. An integrated space−to−ground quantum communication network over 4, 600 kilometres[J]. Nature, 2021, 589: 214−219.
[17] Hu J Y, Yu B, Jing M Y, et al. Experimental quantum secure direct communication with single photons[J]. Light, Science & Applications, 2016, 5(9): e16144.
[18] Zhang W, Ding D S, Sheng Y B, et al. Quantum secure direct communication with quantum memory[J]. Physical Review Letters, 2017, 118(22): 220501.
[19] Zhu F, Zhang W, Sheng Y B, et al. Experimental long−distance quantum secure direct communication[J]. Science Bulletin, 2017, 62(22): 1519−1524.
[20] Qi R Y, Sun Z, Lin Z S, et al. Implementation and security analysis of practical quantum secure direct communication[J]. Light, Science & Applications, 2019, 8: 22.
[21] Cao Z, Wang L, Liang K, et al. Continuous−variable quantum secure direct communication based on Gaussian mapping[J]. Physical Review Applied, 2021, 16(2): 024012.
[22] Qi Z T, Li Y H, Huang Y W, et al. A 15−user quantum secure direct communication network[J]. Light: Science & Applications, 2021, 10: 183.
[23] Zhang H R, Sun Z, Qi R Y, et al. Realization of quantum secure direct communication over 100 km fiber with time−Bin and phase quantum states[J]. Light: Science & Applications, 2022, 11: 83.
[24] Long G L, Pan D, Sheng Y B, et al. An evolutionary pathway for the quantum Internet relying on secure classical repeaters[J]. IEEE Network, 2022, 36(3): 82−88.
[25] Wang M, Zhang W, Guo J X, et al. Experimental demonstration of secure relay in quantum secure direct communication network[J]. Entropy, 2023, 25(11): 1548.
[26] Wang M, Long G L. Lattice−based access authentication scheme for quantum communication networks[J]. Science China Information Sciences, 2024, 67(12): 222501.
[27] Pan D, Liu Y C, Niu P H, et al. Simultaneous transmission of information and key exchange using the same photonic quantum states[J]. Science Advances, 2025, 11(8): eadt4627.
[28] Yang Y L, Li Y H, Li H, et al. A 300−km fully−connected quantum secure direct communication network[J]. Science Bulletin, 2025, 70(9): 1445−1451.
[29] Lee H, Lim J, Yang H. Quantum direct communication with authentication[J]. Physical Review A, 2006, 73(4): 042305.
[30] Marino A M, Stroud C R. Deterministic secure communications using two−mode squeezed states[J]. Physical Review A, 2006, 74(2): 022315.
[31] Pirandola S, Braunstein S L, Mancini S, et al. Quantum direct communication with continuous variables[J]. Europhysics Letters, 2008, 84(2): 20013.
[32] Lum D J, Howell J C, Allman M S, et al. Quantum *Enigma* machine: Experimentally demonstrating quantum data locking[J]. Physical Review A, 2016, 94(2): 022315.

[33] Shapiro J H, Boroson D M, Ben Dixon P, et al. Quantum low probability of intercept[J]. Josa B, 2019, 36(3): 41−50.

[34] Massa F, Moqanaki A, Baumeler , et al. Experimental two−way communication with one photon[J]. Advanced Quantum Technologies, 2019, 2(11): 1900050.

[35] Vázquez−Castro A, Rusca D, Zbinden H. Quantum keyless private communication versus quantum key distribution for space links[J]. Physical Review Applied, 2021, 16: 014006.

[36] Chandra D, Cacciapuoti A S, Caleffi M, et al. Direct quantum communications in the presence of realistic noisy entanglement[J]. IEEE Transactions on Communications, 2022, 70(1): 469−484.

[37] Paparelle I, Mousavi F, Scazza F, et al. Practical quantum secure direct communication with squeezed states[J]. arXiv, 2023. 2306.14322.

[38] 龙桂鲁. 量子安全直接通信原理与研究进展[J]. 信息通信技术与政策, 2020(7): 12−19.

[39] Xu M R, Ren X X, Niyato D, et al. When quantum information technologies meet blockchain in web 3.0[J]. IEEE Network, 2024, 38(2): 255−263.

[40] Sun Z Z, Cheng Y B, Wang M, et al. Quantum blockchain relying on quantum secure direct communication network[J]. IEEE Internet of Things Journal, 2025, 12(10): 14375−14385.

Research of the application of quantum secure direct communication combined with blockchain networks

WU Yongfei[1], LONG Guilu[2,3], JIN Jianxin[4], WANG Yanbo[1*], WANG Min[3*], WEI Wenshu[1], LIU Xizi[4], YANG Xuan[4]

1. Huaxia Bank Co., Ltd., Beijing 100020, China
2. State Key Laboratory of Low-dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing 100084, China
3. Beijing Academy of Quantum Information Sciences, Beijing 100193, China
4. Longying Zhida (Beijing) Technology Co., Ltd., Beijing 100020, China

Abstract Quantum computing threatens classical cryptographic system and brings new challenges to the security of blockchain network communications. Quantum secure direct communication can achieve end−to−end security and has the ability to detect and prevent eavesdropping. Applying quantum secure direct communication in blockchain networks based on classical confidential communication technology can help blockchain networks resist quantum computing attacks and ensure blockchain network security. This paper explores the technical solution of applying quantum secure direct communication in blockchain networks, and conducts feasibility analysis and experimental verification. The experiment successfully verifies the integration of quantum secure direct communication and blockchain networks, uses quantum secure direct communication technology to safeguard blockchain networks, enhances the security of information transmission between nodes in blockchain networks, and helps the financial industry build a more secure and reliable digital value network.

Keywords quantum secure direct communication; blockchain; quantum computing; network communication security

（责任编辑　王微）