软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(6):1594−1613 [doi: 10.13328/j.cnki.jos.005738]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于许可链的 SWIFT 系统分布式架构*

朱建明[1], 丁庆洋[1], 高 胜[1,2]

[1](中央财经大学 信息学院,北京 100081)

[2](粮食信息处理与控制教育部重点实验室(河南工业大学),河南 郑州 450001)

通信作者: 丁庆洋, E-mail: dingqingyang66@163.com

摘 要: 跨境金融通信对于现代金融业务的开展极为重要.环球银行金融电信协会(SWIFT)是跨境金融通信服务的主要提供者.现阶段,报文传输是 SWIFT 系统的主要业务,确保报文传输安全、准确、高效,是 SWIFT 系统的重要目标.但现阶段基于中心架构思想的 SWIFT 系统安全风险突出,传输效率低,成本较高.基于许可链分布式共识机制,提出 BCSWIFT 系统,对现有的 SWIFT 系统进行优化.首先,将 SWIFT 系统的传输网络划分为主网络层和附加网络层;其次,提出了基于双层网络结构的共识算法;第三,介绍了 BCSWIFT 系统的报文交互和传输机制;第四,出于金融业务数据商业保密考虑,提出了一种面向 BCSWIFT 系统的隐私保护机制;第五,对 BCSWIFT 系统的安全性进行了分析.以优化 SWIFT 系统的报文传输业务为例,阐释了基于许可链的跨境金融通信的基本机理,为确保跨境支付、清算、结算的安全、高效、准确和低成本化运作提供了新的思路,也为区块链技术大规模商业应用提供了重要参照.

关键词: 许可链;SWIFT 系统;报文传输;混合式组网;共识机制;信息保护

中图法分类号: TP309

中文引用格式: 朱建明,丁庆洋,高胜.基于许可链的 SWIFT 系统分布式架构.软件学报,2019,30(6):1594−1613. http://www.jos.org.cn/1000-9825/5738.htm

英文引用格式: Zhu JM, Ding QY, Gao S. Distributed framework of SWIFT system based on permissioned blockchain. Ruan Jian Xue Bao/Journal of Software, 2019,30(6):1594−1613 (in Chinese). http://www.jos.org.cn/1000-9825/5738.htm

Distributed Framework of SWIFT System Based on Permissioned Blockchain

ZHU Jian-Ming[1], DING Qing-Yang[1], GAO Sheng[1,2]

[1](School of Information, Central University of Finance and Economics, Beijing 10081, China)

[2](Key Laboratory of Grain Information Processing and Control of Ministry of Education (Henan University of Technology), Zhengzhou 450001, China)

Abstract: Cross-border financial communication is extremely important for the development of modern financial services. The society for worldwide interbank financial telecommunications (SWIFT) is the main provider of cross-border financial communications services. Now, telecommunications message transmission is the main business of SWIFT systems to ensure the transmission of messages. Security,

* 基金项目: 国家重点研发计划(2017YFB1400700); 国家自然科学基金(U1509214, 61602537, 61672104); 中央财经大学"青年英才"培育支持计划(QYP1808); 粮食信息处理与控制教育部重点实验室开放基金(KFJJ-2018-202); 北京市社会科学基金(16XCC023); 内蒙古自然科学基金项目(2016BS0701); 内蒙古数据科学与大数据学会项目(BDY18010)

Foundation item: National Key R&D Program of China (2017YFB1400700); National Natural Science Foundation of China (U1509214, 61602537, 61672104); Central University of Finance and Economics program of the Youth Talent Support Plan (QYP1808); Open fund of Key Laboratory of Grain Information Processing and Control (KFJJ-2018-202); Beijing Municipal Social Science Foundation (16XCC023); Inner Mongolia Natural Science Foundation Project (2016BS0701); Inner Mongolia Data Science and Big Data Society Project (BDY18010)

本文由区块链与数字货币技术专题特约编辑斯雪明教授和陈文光教授推荐.

收稿时间: 2018-06-14; 修改时间: 2018-10-12; 采用时间: 2018-12-18; jos 在线出版时间: 2019-03-27

CNKI 网络优先出版: 2019-03-27 16:40:21, http://kns.cnki.net/kcms/detail/11.2560.TP.20190327.1640.004.html

accuracy, and efficiency are important goals of SWIFT system. However, the current SWIFT system based on the concept of central architecture has outstanding security risks, low transmission efficiency, and high cost. This study proposes a BCSWIFT system based on the permissioned blockchain distributed consensus mechanism, which can make SWIFT system be optimized. First, the transmission network of the SWIFT system is divided into the main network layer and the additional network layer. Second, a consensus algorithm based on the double-layer network structure is proposed. Third, the telecommunications message exchange and transmission of the BCSWIFT system are introduced. Fourth, for the sake of business confidentiality of financial business data, the mechanism of message data privacy protection for financial institutions. Fifth, the security of BCSWIFT system. This article takes the optimization of the SWIFT system's message transmission service as an example, explaining the basic mechanism of cross-border financial communications based on the permissioned blockchain, to provide new ideas for ensuring the safety, efficiency, accuracy and low-cost operation of cross-border paymen , and also provide an important reference for large-scale commercial application of blockchain technology.

Key words: permissioned blockchain; SWIFT system; telecommunications message; hybridnet-working; consensus mechanism; information protection

现代金融行业需要以安全、高效的金融通信系统为支撑.伴随着资本的跨国流动,世界各国之间的金融机构业务往来日益密切,跨境金融通信也更加凸显其重要性.现阶段,诸多机构或组织提供跨境金融通信服务,但处于主导地位的依然是环球银行金融电信协会(Society for Worldwide Interbank Financial Telecom-munications, 简称 SWIFT).该组织成立于 1973 年,旨在实现跨境支付的标准化,其目的在于解决各国金融通信不能适应于国际间支付清算快速增长所引发的效率问题.其业务的实质在于承担起各国银行之间的金融通信中间人角色.在过去的 40 多年间,该组织取得了巨大成功,银行成员数量覆盖了全球 11 000 家银行、证券机构、市场基础设施和企业用户[1].但其交易速度慢、费用高、支撑技术架构僵化也为行业诟病.同时,其安全性也伴随着近年来的黑客攻击事件而备受关注.表 1 为近年来公开数据披露的 SWIFT 安全事件.数据来源根据公开数据整理.

Table 1 SWIFT security incident

表 1 SWIFT 安全事件

时间	地区	事件
2015 年 1 月	南美洲	黑客攻击了厄瓜多尔南方银行,利用 SWIFT 系统转移了 1 200 多万美元
2015 年 12 月	东南亚	越南先锋银行商业银行被黑客攻击,但黑客并没有获得收益
2016 年 2 月	南亚	孟加拉央行的 SWIFT 系统遭受攻击,损失 8 100 万美元

SWIFT 系统所遭受安全性攻击,除本地金融机构防护措施不足以外,中心式系统构架也为攻击者所利用.因而,建立一种安全、高效、低费用成本、技术架构灵活、考量金融机构数据隐私保护的跨国金融通信系统,完成实时跨境信息交互成为世界各国银行的关注点,也成为计算机信息安全领域、金融领域的重要研究课题.

区块链技术最初作为比特币的底层支撑技术进入研究人员的视野,伴随着该技术的不断成熟,逐渐受到社会各界的重视[2],区块链技术逐渐从以数字货币为代表的区块链 1.0 时代,进入以智能合约为代表的区块链 2.0 时代[3].区块链作为一项解决信任问题的普适性技术框架,随着网络信息技术的发展,将被扩展到更多新的应用领域,将来必定会产生更加丰硕的研究成果[4].区块链技术采用分布式架构,利用密码学、共识算法、智能合约等技术,实现信息收集、流转、共享等过程中的信息防篡改、防伪造和可追溯[5],区块链为解决金融行业的问题提供了新的思路[6],其独特的数据安全特性为研究人员解决跨境金融通信,保证跨境支付的安全、准确、高效率以及降低交易成本问题提供新的途径,引发了产业界、学术界以及金融监管的高度重视.基于区块链的跨境支付优化技术,已经成为产业界追踪的热点.一些初创公司为此提出了相应的解决方案,如 Ripple Labs 基于区块链技术推出了名为 Ripple 的数字竞争币.与比特币不同,该数字竞争币以解决跨境以及跨币种的货币转化为主要目标,以 XRP 为各种货币之间的价值中介,基于交易双方信任的网关实现端对端组网的货币转换,并通过消耗 XRP 的方式确保信息安全[7].除 Ripple 币外,初创型企业 Circle 公司推出了名为 Circle 的跨境支付应用产品,该技术在比特币钱包的基础上进行了二次开发,意在解决传统转账业务的低效率、高成本问题,其跨境支付业务的核心机制在于利用比特币充当不同货币之间转换的价值中介,通过锚定比特币制定不同货币之间的汇率.该技术充分发挥了比特币区块链系统的安全性和健壮性,能够提供较为便捷的货币转账服务.2017 年 12 月,该公司推出了 Circle 应用的新版本 CENTRE,后者最大的特点在于该公司用 CENTER Tokens 代替比特币充当货币

价值中介,以解决比特币价值不稳、政策风险大的问题.截止目前,该版本仍然处于概念期,尚未有成熟版本面世.对比现有的区块链跨境支付优化技术方案与现有的 SWIFT 系统,不难发现:基于区块链公链系统的 Ripple 技术和 Circle/CENTRE 技术关注于资金的实时结算,其技术体系并没有完全得到现有金融监管机构的认可,也没有直接涉及到跨境金融通信系统安全保障问题.

基于上述问题,本文提出了一种以现有国际货币清算体系为基础的、以不变革现有国际货币以及金融监管体系为前提的、基于许可链的跨境金融通信优化方案.为清晰说明该方案的运行机理,本文以 SWIFT 系统的报文业务为参照实例进行阐述.在优化过程中,结合当前金融业务实际情况,本文提出双层混合式组网机制,即在由一级金融机构组成的主网络层采用 P2P 组网方式,在由隶属一级金融机构的二级金融机构组成的附加网络层采用星型拓扑网络结构.与此相应,本文提出:在主网络层,部署基于改进的实用拜占庭容错(improved practical Byzantine tolerance,简称 IPBFT)共识机制的联盟链;在附加网络层,部署基于强领导式 Raft(raft of strong leadership,简称 RSL)共识机制的私有链.借鉴原有 SWIFT 系统的报文加密机制,本文提出哈希加密和双重加密相结合的数据保护机制,进而形成双层、多链、分布式、可控匿名的基于区块链技术的 SWIFT 报文传输系统.

本文第 1 节为相关工作介绍.第 2 节为基于许可链的 SWIFT 系统构架介绍.第 3 节为组网机制设计.第 4 节为各层区块链的分布式共识机制.第 5 节为数据交互及查询机制.第 6 节机构数据保护机制.第 7 节为安全性分析与证明.第 8 节为结语及展望.

1 相关工作

现阶段,基于区块链技术对 SWIFT 系统进行优化的相关研究工作主要包括区块链技术在信息安全领域的应用、SWIFT 系统优化及其网络安全事件分析、Ripple 技术及其存在的问题、Ripple 技术与 SWIFT 的对比分析等.刘敖迪等人对国内外的区块链技术及其在信息安全领域的研究进展进行了总结,综述了区块链技术应用于身份认证、访问控制、数据保护等研究领域的进展,并对各类研究的具体情况进行了对比,指出区块链技术应用于信息安全领域面临的挑战[4].Michael 等人通过对一些访谈、会议研讨进行总结和梳理,指出将以区块链技术为代表的分布式账本技术应用于金融数据存储和传输过程中,可以促进金融系统的可持续发展,并可以有效降低业务流程风险和运营成本.但同时也指出,对区块链等分布式技术的预期,可能与企业内部以及企业之间的业务流程协调之间存在不符[8].

环球银行金融电信协会为应对频发的安全事件以及区块链技术兴起对自身的冲击,也展开了相关的研究工作,主要工作包括推出 SWIFT 客户安全控制框架[9].该文件为 SWIFT 用户建立了一套强制性/咨询性的安全控制措施,用以提高本地客户端的安全性,但其并没有触及 SWIFT 系统的底层中心构架.此外,环球银行金融电信协会也开展了一系列将区块链技术应用于自身业务的研究[10],但相关技术方案与现有金融监管框架以及实际业务需求存在较大冲突,仍处于概念构建期和方案实验期,技术方案并不成熟,难以实现大规模应用.

中国人民银行数字货币研究项目组从 SWIFT 系统遭受的网络攻击为切入点,分析了 SWIFT 系统的安全问题,并对孟加拉国 SWIFT 系统遭受攻击进行了详细分析,指出,SWIFT 系统的安全性是基于用户端电脑可信这一假设.并进一步指出,该事件暴露出的核心问题包括两个:一是如何保证信息源头的可信性;二是如何防范对中心节点过度信任所带来的安全问题.最后,研究指出包括区块链技术在内的互联网技术的迅速发展可以实现对网络安全问题的突破[11].

同时,采用区块链技术解决国际金融通信以及价值转换的 Ripple 技术体系也引起了研究者重视.Frederik 等人对 Ripple 系统进行了介绍,指出:Ripple 是一种基于信用网络的分布式支付系统,在该支付系统中主要参与者包括用户、做市商、验证节点、Ripple 协议;指出该系统中的交易类型分为 6 种类型,并对比了 Ripple 和 Bitcoin 的区别;在此基础上,研究者分析了 Ripple 分叉问题,通过数学分析发现,当验证者之间的验证数据集的交叉率超过 40%时才能确保该系统的区块链不发生分叉[6].Marcel 等人以 Ripple 为典型代表,分析了分布式转账支付系统的优势及便利性,同时指出,现有美国境内的监管政策以及措施并不适用于分布式支付系统[12].Adriano 等人对 Ripple 的转账支付系统进行了深入分析,指出,在 Ripple 系统验证节点存在中心化趋势,即,只有少量的节点承

担着整个交易系统的交易验证业务.进一步,研究者对该交易系统的隐私性进行了检验,研究发现,利用某用户的单次交易信息便可以在系统中搜索得到该用户在系统中全部交易信息[13].

除上述研究外,有的研究者对 Ripple 技术与 SWIFT 进行了对比分析,指出 Ripple 在提供便捷支付技术方案的同时,在应用过程中依然面临诸多问题,如:利用交易双方信任的网关作为交易的中介,无法拓展新的信任关系[14];匿名化和去中心化为金融行业的监管带来困难,有可能被用于洗钱等不法活动[15,16];同时,由于该数字币可以在公开市场进行交易,易成为市场炒作标的,币值不稳,导致用户使用的成本波动大等问题.

与 Ripple Labs 类似,初创型企业 Circle 也专注于解决跨境支付问题,其推出的跨境支付技术以比特币作为不同货币之间价值中介,借助比特币在全世界的交易网络,完成法定货币在不同用户之间的结转.但由于近年来比特币炒作氛围浓厚,其与法定货币之间的汇率不稳,锚定比特币充当价值中介,使得不同法定货币之间的转换汇率不稳,为投机者利用该技术进行外汇套利提供了机会;同时,该应用产品设定业务场景较为简单,难以满足跨国银行间的大额货币清算以及金融通信的业务需求;另外,不同国家之间对比特币的监管政策不同,利用法定货币与比特币之间进行直接交易存在巨大政策风险.2017 年 12 月,Circle 公司发布新一代跨境支付产品 CENTRE 的白皮书[17],其突出改进在于提出利用该公司发行的数字代币取代比特币充当不同货币之间的价值转换中介,但该项目尚未落地,所面临的政策性不确定风险突出.

通过上述相关工作回顾不难发现:以 Ripple 和 Circle 为代表,基于区块链技术的分布式转账系统虽然已经相对成熟,但在实际应用以及业务推广过程中依然面临诸多问题.而作为现行国际货币清算体系下的 SWIFT 系统,虽已经开始在相关方面做出探索,但技术方案仍不成熟.因而,鉴于 SWIFT 系统在业务覆盖和合规性审查方面已十分成熟,同时该系统面临的安全性问题、成本问题、效率问题,本文将以 SWIFT 系统为参照实例对基于许可链的跨境金融通信机理进行阐述,以期为后续研究提供参考和借鉴.

2 基于许可链的 SWIFT 系统架构

2.1 SWIFT系统结构框架

SWIFT 系统致力于解决全球金融机构的跨境通信问题,并提供标准化报文,在此基础上助力于建立高效的国际货币清算体系.因而,SWIFT 系统的关键核心在于实现国际金融机构的信息连通.现行的 SWIFT 系统构架基于中心控制-区片存储-区域审核-用户接入的设计构架(具体拓扑结构如图 1 所示).

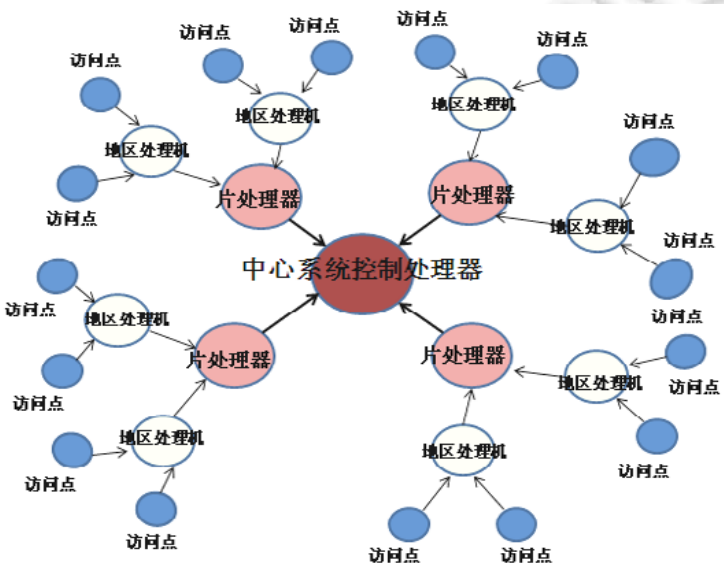

Fig.1 SWIFT system topology

图 1 SWIFT 系统拓扑结构示意图

如图 1 所示,SWIFT 系统拓扑结构由 4 部分组成:处于系统核心位置的是中心系统控制处理器,其他部分由上到下依次分为片处理机、地区处理机、访问点.在该系统中:中心系统控制处理器是整个系统最核心的主控机,对整个系统的运行状态进行检测和控制;片处理器负责整个网络中报文存储转发,目前,世界范围内的报文存储转发由 4 台片处理器负责;地区处理机是系统端的门户,主要负责对用户发送报文的格式、语法、地址代码等进行审核,审核通过的报文才能进一步地向片处理器进行传送,从而分担片处理器的工作负荷;访问点则是被 SWIFT 系统授权的,可以接入到系统中的端口,系统用户利用本地逻辑终端和计算机系统,通过该端口接入系统.

现行的 SWIFT 框架以中心控制系统管理整个系统的运行,参与该系统的金融机构之间交换的报文信息都要经过中心控制系统,一旦中心系统遭受攻击或是攻击者通过骗取中心节点信任的方式,便可轻易地发起对其他金融机构的攻击.而利用中心控制系统进行业务处理模式也导致交易效率低下,如个人利用银行接 SWIFT 系统进行跨境转账到账日期为 3 天,远远长于 Ripple 和 Cricle 的转账时效.

2.2 BCSWIFT框架

基于中心控制思想设计的系统架构在一定时期内保证系统的高效运转.然而,近年来一些安全攻击事件(见表 1)、运营成本高、跨境支付到账时效长的问题引起广泛重视.为解决该系统运行中存在的问题,本文提出基于许可链的 BCSWIFT 构架.

BCSWIFT 构架的核心关键在于不改变现有金融监管体系的前提下对 SWIFT 系统进行优化,将过分依赖于中心节点的中心化架构变革为分布式共识构架.

在 BCSWIFT 系统中,每个节点都参与维护全网的交易账本,因而不存在中心控制节点.考虑到 SWIFT 系统中涉及到世界诸多国家的金融机构,需要对报文进行标准化,同时,世界各国对跨境金融业务具有较强的监管要求,因此,本文将节点类型划分为用户节点和协调节点;进一步地,将用户节点划分为记账节点子群和验证节点子群.用户节点是 BCSWIFT 系统的主体参与者,其中:记账节点子群负责记录本节点与其他节点之间的交易事项,发送报文、接受报文、维护本地账本等;验证节点子群从全体用户节点之中随机选择,负责对系统中的报文进行合规性审查、验证交易,只有通过验证节点验证的报文交易信息才能记录到区块链中;协调节点对整个系统进行维护,制定报文标准、仲裁交易纠纷、负责认证节点的筛选工作、对新近节点进行合规性审查、协调系统与其他监管系统的对接等(详见第 4.1 节的表 2 和表 3).图 2 为 BCSWIFT 系统分布式结构图,图 3 为 BCSWITF 区块链架构图.

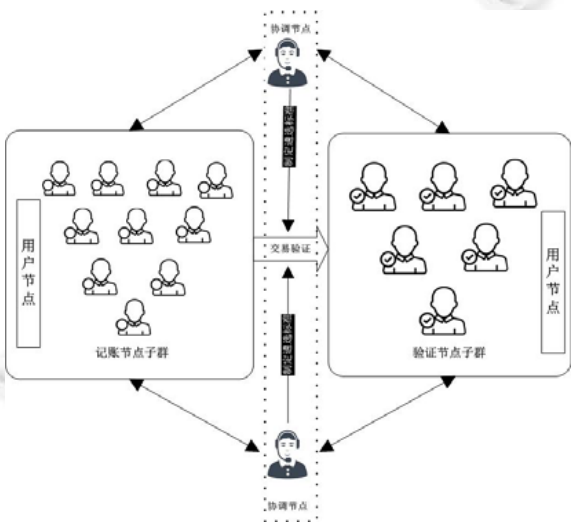

Fig.2 Distributed structure of BCSWIFT system

图 2 BCSWIFT 系统分布式结构图

Fig.3 BCSWITF blockchain architecture

图 3 BCSWITF 区块链架构图

3 组网机制以及区块链结构设计

现有 SWIFT 系统基于中心控制思想进行网络布局,中心控制系统成为各个节点相互连通的信道中转站,是实现世界各国金融机构发送报文进行信息沟通的关键节点.因而,系统的运行效率、信息传播速度很大程度上依赖于中心控制器的处理能力和运转速度.另外,网络中的最低带宽也成为限制全网运行效率和信息传播速度的重要因素.为此,本文提出基于端对端组网方式和星型拓扑网络向结合的混合式组网方式以适应 BCSWIFT 系统的分布式共识机制,并在此基础上提出了各个金融机构及其分支机构的区块链数据结构.

3.1 组网机制设计

当前,根据参与方式的不同,区块链部署形式一般可分为公有链、联盟链、私有链,其中,联盟链和私有链等非公有链又被称为许可链(permissioned blockchain).联盟链是区块链三大部署形式之一,是由若干机构组成利益相关的联盟,共同参与并维护具有准入机制的多中心化区块链.联盟链提供成员管理、认证、授权、审计等管理功能,经过联盟认证的机构才能加入联盟链,对联盟链的写入及查询等操作均可通过联盟授权控制.私有链是指各个节点的写入权限仅有某个机构控制,而读取权限可视需求有选择地对外开放,或被任意程度地进行了限制的区块链[18].进入联盟链的成员具有对等地位,不存在绝对控制中心节点,因而在部署联盟链的过程中,端对端(peer to peer,简称 P2P)的组网方式便成为重要的联盟链网络拓扑结构.而私有链从某种程度上存在着类中心节点,星型拓扑(star topology)网络被视为私有链的重要可参考网络拓扑结构.

现行的 SWIFT 系统为每个加入到该系统中的金融机构提供访问点,并设置相应的机构代码,以保证数据结构的完整、清晰和易于处理.而分布于世界各国的金融机构往往在本国范围内又拥有诸多分支机构和代理机构,这些分支机构和代理机构往往通过专线与主机构联结,当需要利用 SWIFT 系统接发报文时,便借助于主机构拥有的 SWIFT 访问权限进行业务处理.此种方式一方面考虑到不同分支机构或代理机构的数量众多,而且业务量规模分布不均衡,利用主机构统一的系统访问权限可以避免为所有分支机构和代理机构申请 SWIFT 系统访问权限的成本;另一方面,有利于加强主机构对分支机构和代理机构的监管,也便于主机构进行统一的业务核算.基于此,本文提出 P2P 组网方式与星型拓扑网络结构相结合的混合式组网方式.

为便于区分,本文将参与到 SWIFT 系统中的金融机构进行纵向划分,即,按照金融机构是否具有独立的 SWIFT 系统访问权限划分为一级金融机构和二级金融机构.一级金融机构指获得独立 SWIFT 系统访问权限的金融机构,包括各国银行、证券公司以及从属于银行或证券公司但具有独立 SWIFT 系统访问权限的子公司或代理机构;二级金融机构指没有独立的 SWIFT 系统访问权限的金融机构的分支机构、代理机构或是子公司,同时,其对 SWIFT 系统的访问权限需要借助其从属的或者有合作关系的一级金融机构的访问权限.

在一级金融机构中,采用 P2P 的组网方式;而在二级金融机构与其依赖的一级金融机构之间,采用星型拓扑网络.

图 4 为 BCSWIFT 系统混合式组网机制示意图,在该组网机制中,本文将整个网络划分为两层.上层由一级金融机构用户组成,在此层次中,各参与者采用 P2P 的组网方式,以便于为 BCSWIFT 系统分布式共识提供健壮的网络支撑.该层次也是 BCSWIFT 组网的主层,各参与者的跨境报文交换以及金融通信等 BCSWIFT 系统为用户提供的主要业务也在该层完成;下层由二级金融机构用户组成,在此层次中,各参与者采用星型拓扑的网络机制与主层中的相对应的一级金融机构相连接,二级金融机构的跨境报文交换以及金融通信等业务通过向一级金融机构提交申请,借助一级金融机构的 BCSWIFT 系统访问权限的方式完成.该层次是主层次的辅助层,以此扩展 BCSWIFT 系统地域以及受众群体的覆盖范围.

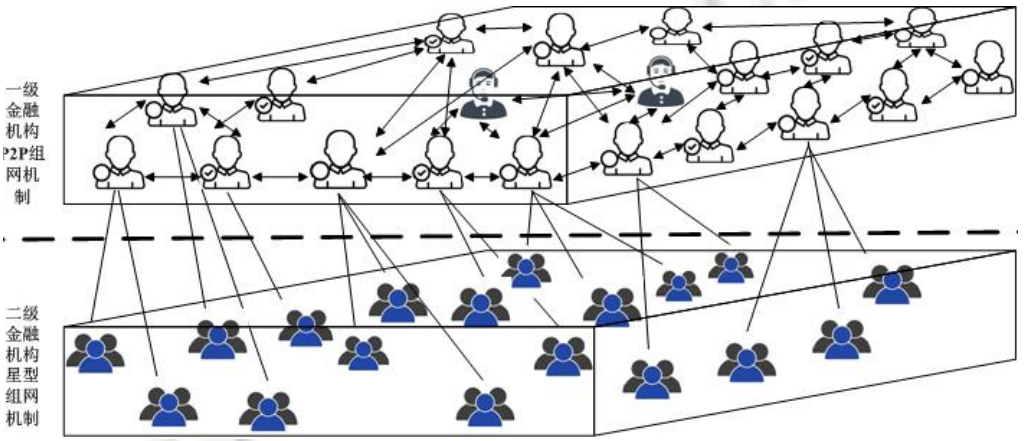

Fig.4 Mixed networking method of BCSWIFT system

图 4 BCSWIFT 系统的混组网方式

3.2 BCSWIFT主层联盟链区块数据结构

根据金融机构实体组织方式以及业务需求,本文提出了基于联盟链的 BCSWIFT 的混合式组网机制.与之相对应,本节提出双层混合式网络中,不同网络层参与者的区块数据结构.具体可以分为主层联盟链区块数据结构和附加层区块数据结构.

主层联盟链的区块主要存储 BCSWIFT 系统中的各参与者报文交换信息,以满足国际间跨境清算的需求.主层联盟链中的区块分为两部分:区块头和区块体.区块头中主要封装当前区块哈希值、前置区块头哈希值、验证子群哈希值、版本号、Merkle 根、时间戳,其中:当前区块的哈希值是对经过验证节点验证之后的区块利用 Hash256 算法计算等到的函数值,前置区块头哈希值为父区块的哈希值,验证子群哈希值是由协调节点选出的验证节点子群中所有验证节点代码组成的代码集合的哈希值,版本号为整个区块链系统的版本编号,Merkel 根则是对区块体中的数据进行 Merkel 计算后得到的,时间戳为经过验证节点共同验证后由协调节点设置;区块体主要封装报文信息,主要包括的事项有发送方代码、发送时间、接受方代码、报文类型、加密方式、报文内容、报文哈希、数字签名、加密算法,其中,发送方代码和接受方代码沿用现有 SWIFT 系统中的代码体系;报文类型的具体分类与现有 SWIFT 系统向一致;加密方式存储报文的加密算法;报文内容存储金融机构之间的交换的报文具体内容;数字签名中存储着报文交换双方的数字签名证书,以保证信息在信道中不被篡改.

具体结构如图 5 所示.

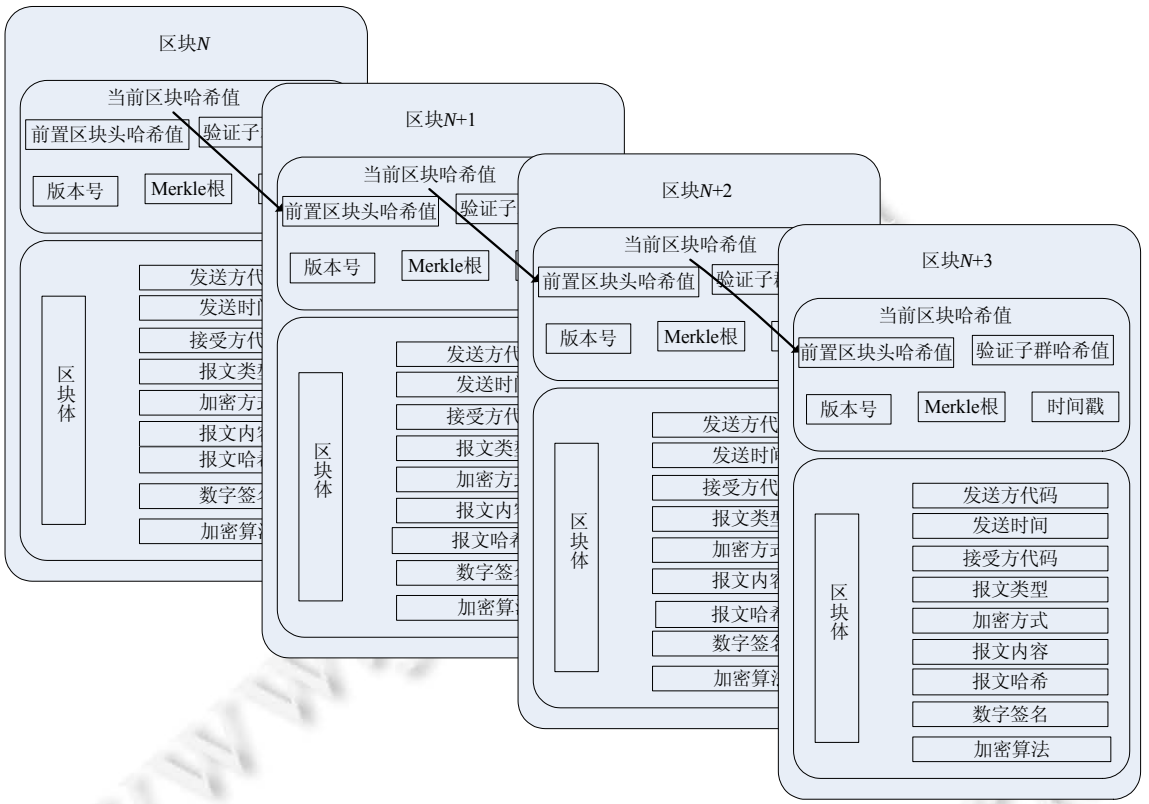

Fig.5 Data structure of BCSWIFT main block

图 5 BCSWIFT 主层区块数据结构图

3.3 BCSWIFT附加层私有链区块数据结构

BCSWIFT 附加层由二级金融机构组成,是主层在地域和服务受众群体范围的扩展.二级金融机构借助一级金融机构的访问权限实现跨境金融通信,二级金融机构处于星型网络拓扑结构的末端位置.根据自身业务的实际需求,一级金融机构可以自行设置其与二级金融机构的数据处理方式,既可以采用中心式数据处理模式,又可以采用私有链或联盟链的数据交互模式.考虑到一级金融机构与二级金融机构之间的组织与业务关系,本文采用私有链的方式实现二级金融机构与一级金融机构之间的跨境信息交互与存储.

附加层私有链中的区块主要存储二级机构借助一级金融机构的 SWIFT 访问权限发送和接受的跨境报文信息.附加层私有链中的区块分为两部分:区块头和区块体.区块头中主要封装当前区块哈希值、前置区块头哈希值、版本号、Merkle 根、时间戳,其中,当前区块的哈希值是对经过验证节点验证之后的区块利用 Hash256 算法计算等到的函数值,前置区块头哈希值为父区块的哈希值,版本号为私有链系统的版本编号,Merkel 根则是对区块体中的数据进行 Merkel 计算后得到的,时间戳由一级金融机构在验证完成后设置;区块体主要封装报文信息,主要包括的事项有发送方代码、发送时间、接受方代码、报文类型、加密方式、报文内容、数字签名、加密算法,其中:发送方代码为私有链系统中的机构代码,接受方代码沿用现有 SWIFT 系统中的代码体系,报文类型的具体分类与现有 SWIFT 系统向一致,加密方式存储报文的加密算法,报文内容存储金融机构之间的交换的报文具体内容.

具体结构如图 6 所示.

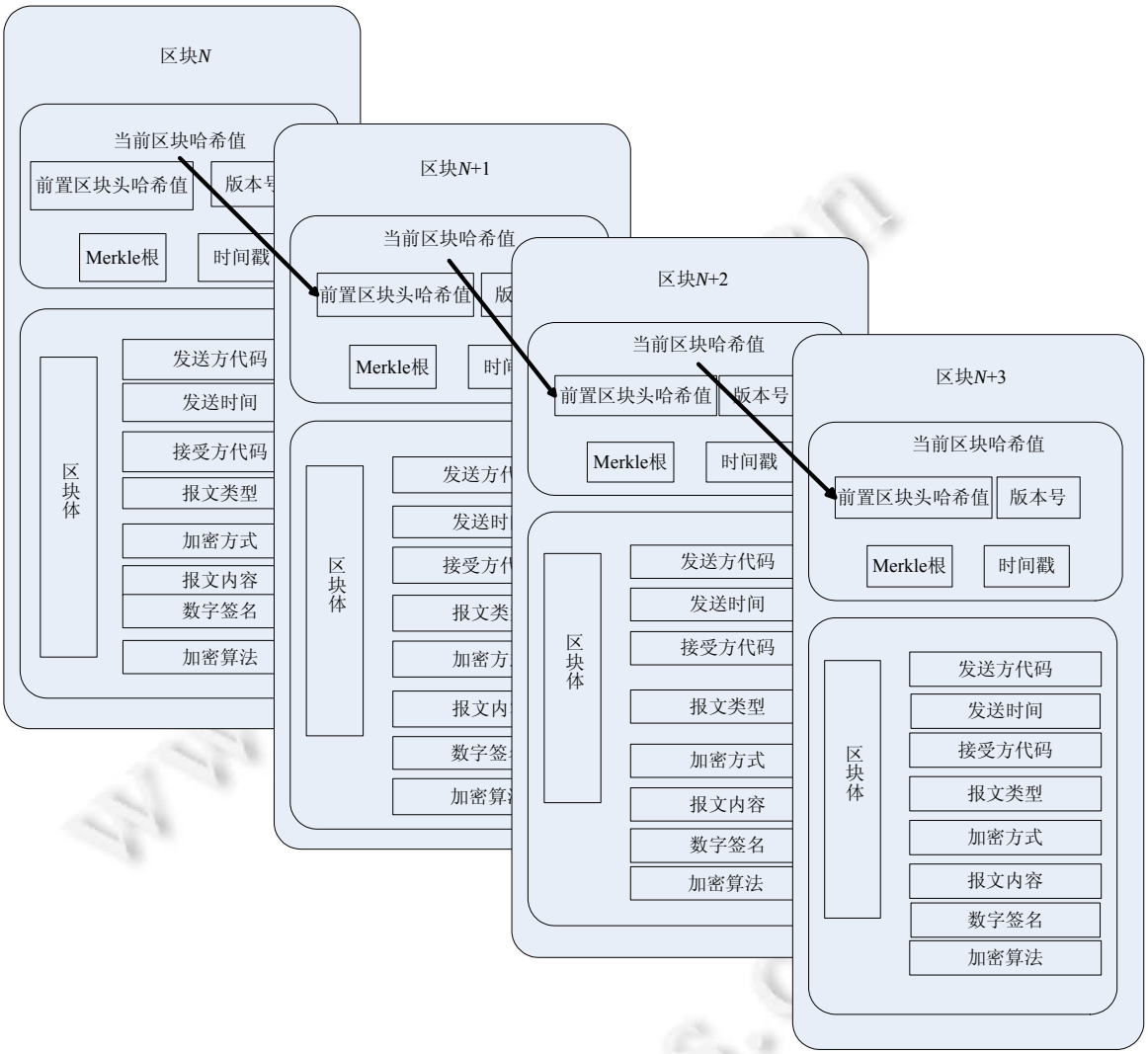

Fig.6 Data structure diagram of BCSWIFT additional layer block

图 6 BCSWIFT 附加层区块数据结构图

4 分布式共识机制设计

考虑到 BCSWIFT 系统用户的组织方式以及业务模式,本文将 BCSWIFT 系统划分成双层结构,即主层和附加层,并分别对应联盟链和私有链.本节将提出主层联盟链以及附加层私有链的共识机制.

4.1 用户角色及职责

BCSWIFT 系统采用双层网络架构:主层基于联盟链建立分布式共识机制,以弱化对现行 SWIFT 系统中心控制节点的依赖程度;附加层考虑到金融机构实体组织结构体系,采用私有链的区块链部署方式以增强系统的健壮性.因而,用户在不同网络层中承担着不同的角色,其拥有的权限与履行的职责也不近相同.表 2 和表 3 列出了 BCSWIFT 主层用户和附加层用户的角色及其职责.

不同的一级金融机构在业务规模和组织方式方面存在差异.对于拥有分支机构或代理机构的一级金融机构,本文提出通过构建私有链的方式,建立分支机构或代理机构与一级金融机构之间的跨境报文传输和存储机制.表 3 为 BCSWIFT 附加层用户角色及职责.

Table 2 BCSWIFT main network layer user roles and responsibilities

表 2 BCSWIFT 主网络层用户角色及职责

角色	用户节点		协调节点
	记账节点子群	验证节点子群	
角色 分配方式	通过签订合约拥有 SWIFT 的 访问权的一级金融机构	由协调节点随机动态 选择 $K>2N/3$ 的用户节点	参与 SWIFT 系统的一级金融机构 共同成立的委员会的代理机构
职责	遵守系统操作规范、按照 标准发送和接受报文、维护 本地账本、遵守本国金融 监管要求和国际通行规范	审查报文信息结构 合规性、对区块 进行交互验证	建立报文信息区块、对系统进行维护、 制定报文标准、仲裁交易纠纷、筛选 验证节点、审核和批准新进节点、 协调系统与其他监管系统的对接
权限	发送和接受报文、查询 区块链数据、进行数据分析	审查报文的合规性、 验证交易	按照委员会规定开展数据增值服务、对新进入 节点进行业务指导、系统最高数据访问权限等

Table 3 BCSWIFT additional network layer user roles and responsibilities

表 3 BCSWIFT 附加网络层用户角色及职责

角色	一级金融机构	二级金融机构
角色 分配方式	按照实体隶属关系、组织 架构体系以及业务流程设置	按照实体隶属关系、组织 架构体系以及业务流程设置
职责	验证报文信息、维护系统安全、保持与主层联结	维护系统安全、维护本地账本
权限	审核新近节点、设置系统操作规则、审核全部报文信息	发送和接受报文

4.2 共识算法设计

4.2.1 相关定义

BCSWIFT 系统中采用双层网络构架,在不同的网络层采用相应的共识机制.本文提出,在主层采用基于实用拜占庭容错[19]的改进的实用拜占庭容错共识机制;在附加层采用基于 Raft[20]的强领导式共识机制.在相关共识机制中定义如下.

定义 1(报文发送方 Sen 和接受方 Rec). 报文发送方是指请求通过 BCSWIFT 系统向其他金融机构发送报文信息的金融机构.报文发送方可以是一级金融机构 $SenF$,也可以是二级金融机构 $SenS$;报文发送方 $SenF_{ID}$ 是一级金融机构在主网络层唯一标识,报文发送方 $SenS_{ID}$ 是二级金融机构在其隶属的星型拓扑网络中的唯一标识.与之类似,可以对 Rec,$RecF_{ID}$ 和 $RecS_{ID}$ 进行定义.对于同一金融机构而言,$SenF_{ID}==RecF_{ID}$ 或 $SenS_{ID}==RecS_{ID}$.

定义 2(报文信息 Tele). 报文信息是 BCSWFIT 系统中传输和存储的主要内容,是指金融机构之间为实现跨境金融信息交互、完成跨境资产清算和结算以加密电文的形式传输的报文.报文信息通过 $Tele_{ID}$(报文信息 ID)全系统唯一标识,每一条报文对应唯一的一个 ID,同时,一个 ID 也只能唯一对应一条报文信息.每一条报文信息在时间切片内只能被传递一次,但每条报文可以包含多项金融交易信息.主网络层的报文主要由两部分组成,即报文头和报文体:报文头主要包括发送方 ID、接收方 ID、发送时间(time)报文类型(type)、加密算法(encryption)、数字签名(signature)、报文哈希值(HAS content);报文体由报文内容(content)组成,同一报文中的发送方 ID 不能等于接收方 ID.在主网络层中,发送方 ID、接收方 ID 为 $SenF_{ID}$,$RecF_{ID}$.二级金融机构发送或接受跨境报文信息,借助其隶属的一级金融机构.因机构数据保护机制不同(见第 6.3 节),附加网络层中的报文头不再包含报文哈希值(HAS content)这一项.

定义 3(协调节点 Cor). 协调节点是所有股东机构成立的管理委员会的代理机构在 BCSWIFT 系统中的投射.在收集到全网报文数据后,将待验证数据发送到验证群组,对合规数据进行建块,并广播最新联盟链状态.该节点不参与共识,只负责忠实维护系统的安全健壮、准确可靠.对新进节点进行审核,通过在现实世界中签订的合作协议,帮助新进入机构获得系统的接入权,并对其进行业务指导,提供必要的软件以及硬件基础设施.协调节点对验证节点进行动态随机筛选,组织共识验证过程.

定义 4(用户节点 User). 用户节点是除协调节点以外的节点,是金融机构在 BCSSWIFT 的网络投射.从网络结构的角度划分,用户节点分为主网络节点 $UserF$ 和附加网络节点 $UserS$,即 $User=UserF\cup UserS$;从报文发送双方的角度划分,用户节点分为报文发送方和报文接受方,即 $User=SenF\cup SenS\cup RecF\cup RecS$.

定义 5(验证节点 Ver). 验证节点是对报文信息进行审核,参与共识,并将数据写入区块链的用户节点.在主网络层中,验证节点 *VerF* 由协调节点从全部用户节点中选出大于 2/3 组成验证群组.在附加层中,验证节点 *VerS* 为一级金融机构,该验证节点对二级金融机构发送的报文信息进行审核,审核通过后,向主网络层发起报文发送信息,并计入其私有链中.当二级金融机构接收到报文时,也由通过一级金融机构进行验证,并计入其私有链.

定义 6(记账节点 Led). 记账节点是除验证节点之外的节点,在随机动态选出验证节点后,剩余的节点成为记账节点.在主网络层中,记账节点负责将自身以及二级金融机构报文信息进行收集,并向协调节点和验证节点发送报文数据,待数据完成共识,接受联盟链的区块状态,完成自身联盟区块链的数据更新.在主层中,记账节点和验证节点的角色可以互换.在附加层中,记账节点是除中心节点以外的节点,负责自身数据与私有链验证节点的交互,维护本地私有链.

定义 7(并行报文区块链). 在 BCSWIFT 系统中,拥有二级金融机构(SFI)的一级金融机构节点(FIWS)同时维护两条并行的区块链,即主网络层的联盟链(consortium blockchain,简称 CBC)和附加层的私有链(private blockchain,简称 PBC).在主网络层中,通过 IPBFT 共识机制维护主网络层的区块链;在附加层中,通过 RSL 共识机制维护附加层中的区块链.FIWS 将通过验证后的二级金融机构的报文信息写入 BCSWIFTPBC 中;同时,主网络层的验证节点将该条报文信息写入 BCSWIFTCBC 中.

4.2.2 共识算法

BCSWIFT 共识算法的核心思想是:对于不同的网络层采用不同的共识的算法,拥有二级金融机构的一级金融机构参与两种共识机制,并维护两条并行区块链.IPBFT 适用于主网络层,RSL 适用于 FIWS 与其隶属的 SFI 组成的星型拓扑网络中.

(1) IPBFT 算法

算法描述:IPBFT 中,报文数据区块的记账权由协调节点享有;验证节点负责对收集到的数据进行合规性审查,在审查完成后,将全部数据进行哈希运算并将结果返回到协调节点;协调节点在收集到超过全网 2N/3 验证节点的一致性验证后,建立报文数据区块,并将新生成的区块与前置区块相连接,同时将区块的最新高度广播到全网.通过验证后的报文数据区块将被永久记录到 BCSWIFTCBC 中.

算法 1. 验证节点对报文数据进行审核.

输入:全网报文数据集;

输出:通过审核的报文数据集.

Algorithm: *Ver* check *OrgTele*[]

Import: *OrgTele*[];

Outport: *TureTele*[].

for *i* in *OrgTele*[Tele]: //加载全网报文数据

  check($Tele_{ID}$) //查验报文 ID

  check(*Time*) //查验报文发送时间

  check($senF_{ID}$) //查验报文发送方

  check($recF_{ID}$) //查验报文接收方

  check(*Type*) //查验报文类型

  check(*HAS Content*) //查验报文的哈希

  check(*Encryption*) //查验加密算法

  check(*Signature*) //查验数字签名

  if $senF_{ID}$==$RecF_{ID}$:

    then send *Tele*() back to *senF* //如果发送方也为接收方则返回报文

  else if *check*($Tele_{ID}$), *check*(*senF*), *check*(*recF*), *check*(*Type*), *check*(*Encryption*) and *check*(*Signature*)=false:

    then send *Tele*() back to *senF* //如果任意一个被查验项不合规则返回报文

else *append*(*TureTele*[]) //生成合规报文数据集
end if
end for
end

算法 2. 协调节点建立数据区块并向全网广播.

输入:审核通过的报文数据集;

输出:报文区块.

Algorithm: *Cor* generate *block*(*TureTele*[])
Import: *TureTele*[];
Outport: *block*(*TureTele*[]).
for *i* in *Ver*():
Compare *TureTele*[] of *Ver* //对比验证节点的审核结果
K=*i*+1
if *K*>2*N*/3:
then generate *block*(*TureTele*[])
broadcast *block*(*TureTele*[]) //具有相同结果的验证节点数目超过全网 2/3 生成区块并广播
end if
end for

(2) RSL 算法

算法描述:RSL 算法中一级金融机构拥有控制权,并对接收到的二级金融机构的报文传输请求进行审核,审核通过后,将报文信息直接记录到其私有链中,并向其他二级金融机构推送私有链的更新动态.

算法. 一级金融机构对报文数据进行审核.

输入:二级金融机构报文;

输出:一级金融机构报文.

Algorithm: *UserF* generate *OrgTele*[]
Import: *UserS-OrgTele*[];
Outport: *OrgTele*[].
for *i* in *UserS-OrgTele*[]: //加载全网报文数据
check($Tele_{ID}$) //查验报文 ID
check(*Time*) //查验报文发送时间
check($senF_{ID}$) //查验报文发送方
check($recF_{ID}$) //查验报文接收方
check(*Type*) //查验报文类型
check(*Encryption*) //查验加密算法
check(*Signature*) //查验数字签名
if checked *UserS-OrgTele*[]
then *append*(*UserS-TureTele*[]) //生成合规报文数据集
end if
end for
send *block*(*UserS-TureTele*[]) to *UserS*
end
for *i* in *UserS-TureTele*[]:

exchange *UserS-TureTele*[] to *OrgTele*[] //生成一级金融报文数据集

end for

print(*OrgTele*[])

5 数据交互及查询机制

报文传输是 BCSWIFT 系统的重要应用之一,也是本文着重考虑的业务场景.本文提出的 BCSWIFT 系统与现行的 SWIFT 系统基于中心控制的业务处理方式不同,其核心业务处理思想是分布式共识机制.因此,其具体业务流程也存在较大区别.

5.1 报文数据交互机制

报文交互机制从信息传递的角度可以划分为报文发送、报文传输、报文接受这 3 个阶段.依据用户主体的不同,可以划分为一级金融机构与一级金融机构之间的报文传输、一级金融机构与二级金融机构之间的报文传输、二级金融机构与二级金融机构之间报文传输这 3 种类型,这 3 种报文根据其业务的请求发出者可以划分为由一级金融机构发起的报文传输业务和由二级金融机构发起的报文传输业务.

报文传输以金融机构的业务需要为前提,当一级金融机构根据业务需求发送报文时,直接将报文编码向 BCSWIFT 系统发起请求,报文信息通过验证和共识后便会向报文接收方发送,一级金融机构接受到报文后将报文进行解密;如果报文接收方为二级金融机构,则将报文信息传递给二级金融机构,二级金融机构根据报文信息进行业务处理.当二级金融机构收到业务请求时,会向其所隶属的一级金融机构进行报文传输请求,一级金融机构对报文信息进行重新编码后,向 BCSWIFT 系统发送请求,报文信息通过验证和共识后便会向报文接收方发送,一级金融机构接受到报文后将报文进行解密;如果报文接收方为二级金融机构,则将报文信息传递给二级金融机构,二级金融机构根据报文信息进行业务处理.具体流程详如图 7 所示,BCSWIFT 系统报文交互流程图.

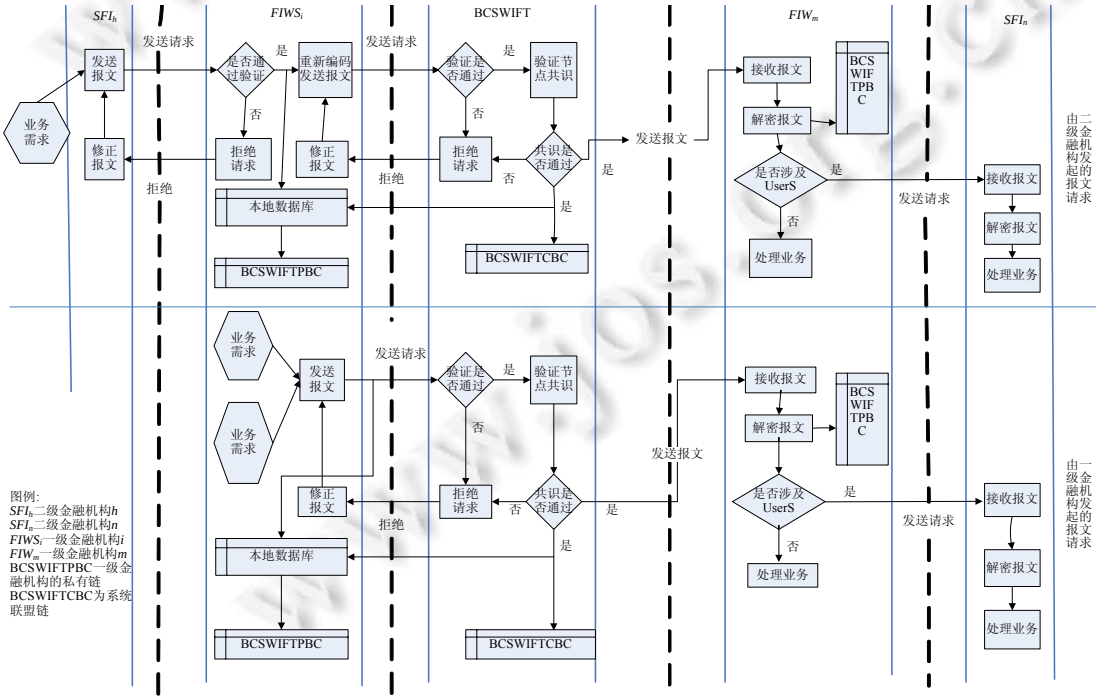

Fig.7 BCSWIFT system message interaction flow chart

图 7 BCSWIFT 系统报文交互流程图

5.2 数据查询机制

金融机构在处理跨境金融业务过程中,除了以报文为载体传输业务信息外,还需要诸如银行对账单等机构业务处理汇总数据,以实现资金或资产的清算、结算和交割.因而,BCSWIFT 系统除为金融机构提供报文传输的交互机制外,还支持金融机构为完成资金或资产的清算、结算和交割等业务活动而向系统发起获得报文记录的查询请求,而基于对金融机构业务数据进行保护的考虑(见第 6 节),数据的公开范围和查询权限受到限制.

数据查询的种类根据发起金融机构的种类不同,可以划分为由一级金融机构发起的查询和由二级金融机构发起的查询:一级金融机构发起的查询可以分为附加层网络的查询和主网络层的查询,即对 BCSWIFTPBC 的数据查询和对 BCSWIFTCBC 的数据查询;二级金融机构发起的查询可以分为附加层网络的查询和主网络层的查询,即对 BCSWIFTPBC 的数据查询和对 BCSWIFTCBC 的数据查询.

一级金融机构在附加网络层具有最高权限,可以随时调取 BCSWIFTPBC 的全部数据,而不需要经过二级金融机构的同意.一级金融机构虽具有数据访问的最高权限,却无法对 BCSWIFTPBC 中的数据进行修改,从一定程度上可以避免一级金融机构的道德风险和操作风险.一级金融机构对 BCSWIFTCBC 的数据查询则需要经过协调节点的审证,协调节点作为全体参与者组成的管理委员,在网络中的投射可以很好地代表全体参与者的意愿,由其对查询请求进行审证可以体现全部参与者的意愿,符合 BCSWIFT 系统金融机构商业联盟的根本运营性质.通过审证后,BCSWIFTCBC 系统将返回查询结果.审证标准包括两个方面,即合理性和合规性:合理性是指一级金融机构请求查询的数据在 BCSWIFT 联盟中规定的数据查询业务场景提供的数据范围内;合规性则是指一级金融机构数据查询的请求指令应该符合 BCSWIFT 联盟的统一规范,同时请求指令发送的频率在安全阈值范围内.审证环节意在防止恶意节点通过数据查询窥探其他节点的商业信息,也防止利用数据查询进行“粉尘”攻击,而并非赋予协调节点某种类中心化的权限.审证环节的主要流程也围绕审证标准的 3 个方面展开:首先是合理性审查,其次是合规性审查,再者是查询次数限定.

二级金融机构发起对 BCSWIFTPBC 的数据查询请求,由其隶属的一级金融机构负责审核.通过审核后,系统向二级金融机构返回查询结果.二级金融机构对 BCSWIFTCBC 的数据查询请求由其隶属的一级金融机构审核,并重新以一级金融机构的名义向协调中心发送查询请求,审证通过后,将 BCSWIFTCBC 返回的查询结果向二级金融传递.具体流程如图 8 所示.

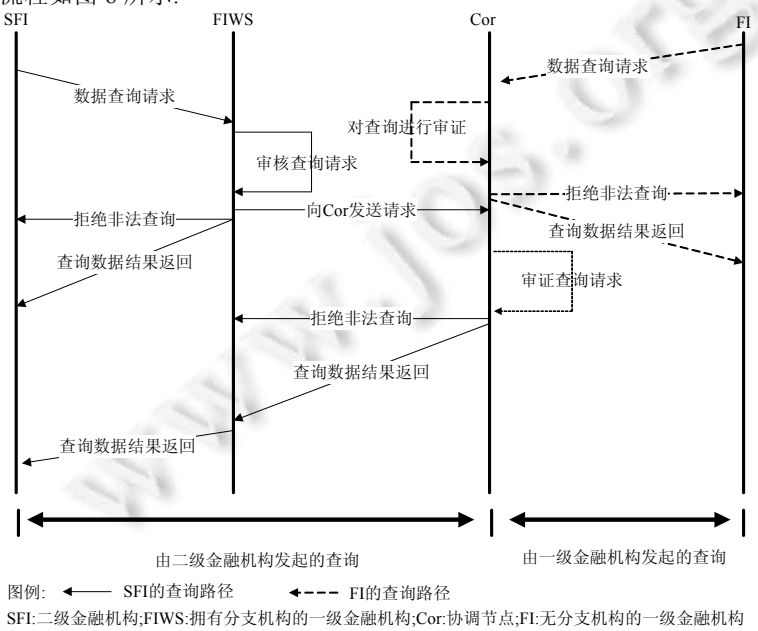

Fig.8 BCSWIFT system data query mechanism

图 8 BCSWIFT 系统数据查询机制

6 机构业务数据私密性保护

跨境金融通信是金融机构处理跨境业务的必要条件,便捷、安全、准确的跨境金融通信体系,是金融机构在跨境金融业务领域的核心竞争力之一.同时,金融机构在业务处理中积累的大量业务数据,也成为其重要的数据资产,甚至一些重要的数据信息成为了金融机构的核心商业机密.因而,保护包括跨境报文信息在内的业务数据,是金融机构保持其竞争力的重要途径.其数据保护机制按照BCSWIFT系统的报文处理流程可以划分为3个方面,即报文传输过程中的信息私密性保护、报文验证过程中的信息私密性保护、报文存储以及查询过程中的信息私密性保护.

6.1 报文传输过程中的信息私密性保护

借鉴现有SWIFT系统中报文传送的加密机制,除广泛应用的对称加密算法外,本文提出采用非对称密码、数字签名、哈希加密的方式保证数据在传输过程中的信息安全性.

- 非对称密码体制(asymmetric cryptosystem)在密钥分配、密钥管理以及实现不可否认方面相较于对称密码体制具有较大优势[18],因而在区块链技术体系,如比特币[21]中被广泛应用.利用非对称密码体制,报文发送方在发送报文之前首先要获取报文接收方发布的公钥.利用该密钥将明文加密成为密文,接收方解密时,使用私钥对密文进行处理以获得明文.利用私钥可以计算得出公钥,但是利用公钥却难以计算得到私钥,使得非对称密码体制在加密方面具有极高的安全性.在BCSWIFT系统中采用非对称密码体制,可以较好地解决现有SWIFT系统中报文加密密钥的分配问题,防止报文被截取以及报文接发过程中的抵赖问题;
- 数字签名(digital signature)[22]主要用于对数字消息进行签名,以防止消息的冒名伪造或篡改,也可以用于通信双方的身份鉴别.在BCSWIFT系统中,报文发送方利用签名密钥对报文信息进行签名加密,接受方利用验证密钥对报文内容进行解密.通过采用数字签名技术,BCSWIFT系统可以防范攻击者假冒发送方发送报文信息或是对报文信息进行伪造;同时,加之以报文ID号和时间戳,BCSWIFT系统可以防止报文重放,也可以有效防止发送者抵赖曾经签署过的报文信息;
- 哈希加密也被称为哈希函数(Hash function)[23],是一种从明文到密文的不可逆映射.利用哈希函数可以将任意长度的信息加密为固定字符长度的输出,且一旦明文数据出现微小的变动,整个加密后的哈希值将发生巨大变动.在BCSWIFT系统中,哈希函数可以对报文区块进行加密,并存储于后一区块中,进而形成前后相连的链式数据结构.同时,利用哈希函数对整个报文进行加密,生成的哈希值放置于报文头,以防止攻击者对报文数据的恶意篡改.

6.2 报文验证过程中的信息私密性保护

在主网络层,报文验证过程中,报文信息保护主要考虑各个金融机构在报文传输中的数据不被恶意窃取和集中化收集,以窥探其运营状况.其主要的安全风险在于协调节点以及验证节点在收集到全网报文数据后,构建报文数据区块的过程中以及验证节点在收到协调节点发送的数据区块后,在完成共识前,对金融机构报文数据的窃取和集中化收集.

通过对报文数据进行加密传输,让报文数据以密文的形式在全网中进行传输,只要确保密码算法的安全性,就可以保障数据的安全性.但密文传输使得协调节点在审核报文消息是否合规的处理过程中面临巨大问题,因为验证节点并不允许对报文数据进行解密,无法直接查看报文的具体信息.

为解决报文审核以及共识过程对数据公开性的要求与金融机构报文数据隐私保护之间的矛盾,需要在验证内容上寻找平衡阈值,既可以不妨碍分布式共识机制的运行,也可以最大限度地降低其道德风险.本文提出对报文中的信息进行分类审核,同时采用双重加密的技术手段加以解决.

本文研究认为:报文信息与数字资产不同,只存在重放而不存在“双花”,因而不验证信息的具体内容也可以实现对报文的合规性审查.将验证节点的报文审核内容限定在报文ID、发送时间、发送方ID、接受方ID、报文类型的合规性审查、报文哈希、报文数字签名的完整性“报文头”中的内容进行审核,而不对报文的具体内容,

即“报文体”进行审查是最合理的平衡阈值.该种审核机制类似于将一条报文信息看做是一封信,验证节点可以便捷地实现对信封上的公开信息进行校验,而无法探知信纸中记录的具体内容.不仅可以提高审核效率,还可以保证报文的信息机密性.通过审核和共识的报文信息将会被打包成为数据区块,并记录到 BCSWIFTCBC 中.

为确保报文数据不被恶意收集和窥探,本文提出采用双重加密的方式.所谓双重加密,是指报文在传输过程中利用非对称加密算法(诸如 RSA 等)和对称加密进行双重加密:第一重加密是利用非对称加密算法对报文体进行加密,发送方利用接受收方的公钥进行加密,接收方通过其私钥进行解密,便可以得知报文体内容;第二重加密是利用对称加密算法对报文头和加密后的报文体进行加密,报文发送方将经过双重加密的报文数据进行广播,广播接收方包括报文接收方、报文验证方、记账节点、协调节点等.但在此过程中,真正可以查看报文完整信息的只有报文接收方,而其他各方虽接受到报文,但只限于查看报文头,验证节点利用报文头信息进行验证,形成共识.通过共识验证后的报文数据将被打包进入主层联盟链以及相应的附加层私有链.进一步地,双重加密过程中采用两种不同的非对称加密算法和对称加密算法可以进一步提高数据的安全性,增加攻击者破译难度.

在双重加密中,第 1 重加密是为了确保报文体的数据隐私性,将报文体以密文的形式在系统中传输,在报文发送方发送报文以后,只有报文接收方可以解密得到相关报文体的明文;第 2 重加密主要用于保证报文广播中的安全性和便于验证.具体而言:首先是为防止报文在传输信道中被截取以后可以轻易获得报文,只要确保第 2 重加密中采用的加密方法具有密码学意义上的安全性,就可以确保报文被截取以后的安全性;其次,对第 2 重对称加密进行解密以后得到的明文是一致的,即报文头和采用第 1 重加密后的报文体密文,便于进行共识.

双重加密中,密钥的管理也较为便捷.第 1 重加密和第 2 重加密采用不同种类加密方法,系统中每一个节点保存有第 1 重非对称加密方法的公钥 P 和私钥 S,和第 2 重对称加密算法的密钥 K.非对称加密算法的私钥由节点自身保存,公钥由节点进入系统之初向全网节点发送.报文发送方在发送报文时,利用接收方的 P 对报文体加密,利用第 2 重对称加密算法对报文头和加密后的报文体进行加密.报文接收方接收到报文后,利用自身的 K 先对报文头和加密后的报文体进行解密,再用自身的 S 对采用非对称加密算法加密后的报文体进行解密,进而得知全部报文信息.非报文接收方节点只利用自身节点保存的密钥 K 对报文头和加密后的报文体进行解密,数据查看范围限于报文头的明文和报文体的密文.

其过程中主要的安全威胁来源于报文在小概率范围内被截取和破译之外,攻击者基于相同的报文内容重写报文,发起的重放攻击.重放攻击会使整个报文系统记录的跨境金融数据出现巨大偏差,将迫使参与节点耗费巨大的人力和算力寻找重放信息,造成的损失不可估计.为此,本文提出在报文头中加入报文信息整体的哈希以及非对称加密算法对报文体信息进行加密的方法避免重放攻击.当攻击者基于相同的报文体内容进行重放攻击时,报文 ID 号必须是唯一且区别于其他任何一条报文信息的.报文 ID 的不可重复性致使攻击者进行重放攻击时,报文信息哈希值会发生巨大变化,因而验证者可以轻易识破重放攻击.同时,采用双重加密机制不仅可以保证数据私密性,也为攻击者破译报文体信息增加了难度,也进一步降低了重放攻击成功的概率.

在附加网络层中,FIWS 可以对报文的全部信息进行校验,通过审核的报文将利用其自身的 BCSWIFT 系统访问权限向主网络层发送报文,待到主网络层完成共识,再将 SFI 的报文信息记入到 BCSWIFTPBC 中.

6.3 报文存储以及查询过程中的信息私密性保护

利用非对称密码体制、数字签名、属性加密以及哈希函数,使得报文数据在 BCSWIFT 系统中的传输和流转完全以密文的形式存在,即使攻击者获取了 BCSWIFTCBC 中的全部数据,只要加密算法具有安全性,也难以实现对数据的暴力解密,更无法实现对数据的篡改.同样,参与 BCSWIFT 系统的金融机构在未取得其他金融机构授权(私钥)的前提下,也无法探知其他金融机构报文数据.

同时,为保证金融机构的业务清算和结算,每个金融机构也维护本地数据库,该数据库只记录与其自身有关的报文.因而,即使该数据库遭到攻击,其数据流失范围仅限于其自身业务数据和部分与其有报文交互记录的其他金融机构的数据,而不会威胁到全网.但需要提出的是:本地数据库遭到攻击,会造成附加网络层中的一级金融机构和其所辖属的二级金融机构的报文数据泄露.因而,一级金融机构仍要采用诸如物理隔离、安全防护墙

等技术手段和管理方法确保本地数据库的安全性.

数据查询是必要的,是用户节点确保本地数据库与全网保持一致的重要方式,也是实现仲裁的重要手段.在主网络层,数据查询的请求要经过协调节点的审证,通过审证后的查询请求将会被返回查询结果.在附加网络层,如果只是涉及附加网络层的内部查询,则有一级金融机构进行审核,通过审核后的查询请求将会被返回查询结果;如果涉及主网络层的查询,则由一级金融机构向协调节点提交查询请求,通过审证后的查询请求将会被返回查询结果,并进一步返回到二级金融机构.此种机制设计是为了加强对攻击者恶意伪装成为诚实节点对系统进行 DOS 攻击的识别,并有效降低 DOS 攻击的概率.

7 安全分析与证明

安全性对于金融通信至关重要,也是许可链在构建 SWIFT 系统中的重要优势之一.基于许可链的 BCSWIFT 系统面临的信息安全风险主要包括两个方面:一是原有 SWFIT 系统中固有的信息安全风险,二是 BCSWIFT 系统分布式共识过程中隐含的风险.本节将集中对这两个方面安全性进行分析并给出证明.

7.1 对原有SWFIT系统信息安全风险的分析

现阶段,SWFIT 系统中面临的信息安全隐患包括假冒、报文被截取(读取或复制)、修改、重播、报文丢失、报文发送方以及接收方否认等.同时,采用中心控制的报文系统对中心控制系统依赖程度过高,中心控制点的操作风险和道德风险较大.对于信息安全的防范应以安全目标为导向,采用相应的安全措施解决现有的安全威胁.BCSWIFT 系统的安全目标与其他基于计算机技术的信息系统安全目标一致,其核心要点分为 4 个:信息保密性、完整性、可用性以及可追溯性[24,25].考虑到 BCSWIFT 系统中不同网络层的重要性不同,本文将该部分的安全分析限于主网络层中.表 4 对 BCSWIFT 系统中的安全风险、安全目标与安全措施之间的关系进行了梳理.

Table 4 Correspondences between security objectives, security risks and security measures in BCSWIFT

表 4 BCSWIFT 系统中的安全目标、安全风险与安全措施之间的对应关系

信息安全目标	信息保密性	信息完整性	信息可用性	信息可追溯性
信息安全隐患	报文被截取、读取或复制	报文被修改	假冒报文发送方、重放	报文丢失及否认
	中心控制点的操作风险和道德风险			
信息安全措施	非对称密钥体系、双重加密	数字签名、哈希加密	数字签名、报文哈希、利用报文 ID 对报文进行标识	数字签名、非对称密钥体系、链式联结
	分布式共识机制			

定理 1. 采用非对称密钥体系、双重加密可以确保报文信息的保密性.

证明:非对称密钥体系为报文数据的全网广播实现共识提供了密码学技术支撑,在主网络层报文广播过程中,每一个节点保有全网其他节点的公钥,在发送报文过程中,利用接收节点的公钥对报文体进行加密,接收节点利用其自身私钥对报文体进行解密.解密得到的报文头和报文体密文足以确保验证节点完成验证实现共识,同时也确保了数据的分布式存储.对报文体利用非对称加密算法进行的数据加密,使得报文的全部信息只有接受方可以探知,保护了数据的隐私性.综上可知,采用非对称密钥体系和双重加密可以确保报文信息保密性. □

定理 2. 数字签名技术、哈希加密可以确保报文信息的完整性.

证明:数字签名技术、哈希加密使得数据一旦被修改就会发生巨大变化,因而报文被修改以后信息就会作废,无法通过共识.攻击者修改过的报文会轻易被诚实节点探知,其攻击意图会被识破,无法达到攻击意图,信息完整性得以确保. □

定理 3. 数字签名技术、报文标识技术可以确保信息的可用性.

证明:数字签名是发送节点的标识,攻击者在无法得到全网节点数字签名的前提下无法实现假冒.报文采用唯一的报文 ID 进行标识,重放的报文其 ID 会在系统中出现重复,而一旦出现重复 ID 报文会被判定无效,重放攻击便宣告失败;同时,报文哈希也使得攻击者难以在报文 ID 不可重复的前提下,通过分解报文、复制报文体实现重放攻击.以上使得报文信息可用性得以确保. □

定理 4. 数字签名技术、非对称密钥体系、链式联结可以确保信息的可追溯性.

证明:每一个发送节点都具有特定的数字签名,使得发送方难以否认.而一旦报文数据经过验证和共识便被记录到区块链中,前后联结的数据区块使得数据极易被发现,也不易发生丢失,协调节点仲裁机制也使得接受节点难以否认曾接受到报文信息.因而,数字签名、非对称密钥体系、链式联结使得信息具有可追溯性. □

定理 5. 分布式共识机制可以最大化降低中心控制节点的操作风险和道德风险.

证明:分布式共识机制大大降低了中心控制节点在报文传输过程中的数据权限,中心节点被协调中心所取代,协调节点的行为处于全网监督中,其不诚实行为将轻易地被全网节点所发现,降低了其操作风险和道德风险的发生概率和危害性. □

7.2 分布式共识机制中的安全风险分析

本文所提出的 BCSWIFT 系统基于许可链技术体系,除 SWIFT 系统中面临的固有信息安全风险外,分层网络组网方式、分布式共识机制中也面临着共识机制可信度、网络不可信、篡改报文数据、区块分叉等问题.本节将对此进行安全性分析.

定理 6. 验证共识机制是可信的.

证明:在 BCSWIFT 系统中采用“审核即验证”的模式,验证节点即审核节点,通过审核的报文即为通过验证的报文.主网络层采用改进的拜占庭共识机制,多于 $2N/3$ 的验证节点返回的报文验证合格数据集具有一致性时,共识即达成.而同时加入到系统的主体通过合约等方式规定了权利与义务,节点具有高可信度.进而,主网络层的共识机制具有可信性.在附加网络层中,一级金融机构和二级金融机构为利益共同体,同时,考虑实体机构的组织构架方式,一级金融机构节点具有权威性,其通过审核的报文即可以向主网络层发送请求,进而附加网络层的共识机制具有可信性.综上可以证明,BCSWIFT 系统的验证共识机制具有可信性. □

定理 7. 网络环境具有可信性.

证明:一方面,基于许可链的 BCSWIFT 系统中节点,无论是在主网络层还是附加网络层,实体组织之间都具有高度的相互信任机制,主网络层中新近节点进入系统,都要经过严格的审核,只有确认新近节点具有高度可信性后,节点才会被批准加入到系统中;附加网络层中,二级金融机构是一级金融机构的下属机构,其进入附加网络中以二级金融机构服从一级金融机构管辖为前提;另一方面,各个金融机构之间的业务通信往往通过网络专线,确保了网络传输的安全性. □

基于以上两点,本文认为 BCSWIFT 系统网络环境具有可信性.

定理 8. 报文数据在 BCSWFT 系统中难以被篡改.

证明:在 BCSFIT 系统中,报文数据在经过哈希加密、非对称加密、双重加密后,以密文的形式在系统中进行流转,其安全机制已在第 7.1 节证明.另外,共识通过的报文信息一旦写入区块链,由区块链的基本特性可知,其数据具有不可篡改性.因而,报文在 BCSWIFT 系统中难以被篡改. □

定理 9. BCSWIFT 系统不存在分叉风险.

证明:在主网络层中,BCSWIFT 系统采用 IPBFT 共识机制,BCSWIFTCBC 的记账权由协调节点享有,协调节点在对区块状态更新后将区块链数据摘要发送到各个节点.各个节点的区块链实时与协调节点相一致,故在 BCSWIFTCBC 中不存在分叉问题.在附加网络层,BCSWIFTPBC 的记账权由一级金融机构享有,一级金融机构对数据进行审核后,将二级金融机构的请求记录到该链中,向其他节点发送区块摘要,故在 BCSWIFTPBC 中不存在分叉问题.因而,双层多链的 BCSWIFT 系统不存在分叉风险. □

定理 10. BCSWIFT 系统可以有效防止攻击者通过攻击协调节点选取验证子群进行作恶.

证明:协调节点所承担的职责中包含筛选验证节点的角色职责,但协调节点的筛选结果并非是由其自身主观决定,而是通过随机动态的筛选过程得出的随机筛选结果.在得出验证子群的筛选结果之前,协调节点并无法进行预测,也无法改变筛选结果,除非所有参与者一致通过改变筛选结果的决议.因而在攻击者在小概率范围内对协调节点成功实施攻击后,其自身依然难以通过选取特定的验证子群进行作恶. □

8 结语及研究展望

本文以 SWIFT 系统的安全、成本和效率问题为切入点,介绍了相关工作以及现有 SWIFT 系统的中心式架构,聚焦于报文传输这一基本业务场景,提出了 BCSWIFT 框架,并对该框架进行了详细说明.结合实际运营环境对报文传输的参与者进行重新分类,介绍了报文传输的区块结构、共识机制、业务流程、数据保护措施等,最后对框架的安全性进行了证明.本文提出的双层架构和多链融合思想以及多种共识机制并存和数据保护措施具有通用性的实践指导意义;同时,聚焦于报文传输这一基本业务场景,为实现基于区块链技术的国际跨境支付业务的优化打开了新的突破口,为进一步推动区块链技术在国际跨境金融业务中的应用奠定了坚实的基础,也为包括国际跨境金融业务在内的现代金融也的发展提供了巨大助力.

本文的不足之处在于以报文传输业务作为参照实例,尚未涉及 SWIFT 系统中的其他增值业务(如跟单信用证、信用担保等),未来可以进一步探索基于区块链以及智能合约技术优化 SWIFT 系统增值业务以及完善国际跨境金融业务监管.另外,BCSWIFT 系统的效率问题也是未来的重要研究方向.本文提出的 BCSWIFT 系统是基于许可链,许可链包括私有链和联盟链,是一种多中心化体系结构,而并非是完全的去中心化体系,虽然会在一定程度上降低效率,但是可以提高系统信任.而且许可链效率不是很低,Vukolic 指出,BFT 类投票共识每秒可达到上万笔交易[26].根据联盟链 HyperLedger Farbic 白皮书,其所采用的 PBFT 共识能实现每秒约 2 000 笔交易[27].本文所提出的 BCSWIFT 系统的共识机制中,主层联盟链的 IPBFT 共识算法正是以 BFT 类共识机制为基础,并加以改善的共识算法.因而,我们谨慎地认为,系统的交易效率并没有呈现断崖式下降.

限于本文的写作目的主要在于研究和论述基于许可链的 SWIFT 系统与共识机制,强调其中的技术方案以及实现机制,有关 BCSWIFT 系统交易效率检测以及优化问题可以基于本文的研究成果,同时结合 SWIFT 运营的实际情况开展进一步的研究.

References:

[1] SWIFT. Wikipedia. https://en.wikipedia.org/wiki/Society_for_Worldwide_Interbank_Financial_Telecommunication

[2] Jesse YH, Deokyoon K, Sujin C, Sooyong P, Kari S, Houbing S. Where is current research on blockchain technology?—A systematic review. Plos One, 2016,11(10):1−27.

[3] Yuan Y, Wang FY. Blockchain: The state of the art and future trends. Acta Automatica Sinica, 2016,42(4):481−494 (in Chinese with English abstract).

[4] Liu AD, Du XH, Wang N, Li SZ. Research progress of blockchain technology and its application in information security. Ruan Jian Xue Bao/Journal of Software, 2018,29(7):2092−2115 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5589.htm [doi: 10.13328/j.cnki.jos.005589]

[5] Ding QY, ZHU JM. The product information traceability and security model of B2C E-platform from the perspective of blockchain. China Business and Marke, 2017,12:41−49 (in Chinese with English abstract). [doi: 10.14089/j.cnki.cn11-3664/f.2017.12.005]

[6] Tsai WT, Blower R, Zhu Y, Yu L. A system view of financial blockchains. In: Proc. of the 2016 IEEE Symp. on Service-Oriented System Engineering (SOSE). IEEE, 2016.

[7] Armknecht F, Karame GO, Mandal A, Youssef F, Zenner E. Ripple: Overview and outlook. In: Proc. of the Int'l Conf. on Trust and Trustworthy Computing. Cham: Springer-Verlag, 2015. 163−180.

[8] Mainelli M, Milne A. The Impact and Potential of Blockchain on Securities Transaction Lifecycle. Social Science Electronic Publishing, 2016. 1−81.

[9] SWIFT customer security programme Ver.1.0. https://www.swift.com/myswift/customer-security-programme-csp/security-controls

[10] SWIFT on distributed ledger technologies. http://www.ameda.org.eg/files/SWIFT_DLTsposition_paper_FI NA L1804.pdf

[11] People's Bank of China Digital Money Research Project Team. Seeing financial network security from SWIFT hacking events. China Finance, 2016,17:43−44 (in Chinese with English abstract).

[12] Rosner MT, Kang A. Understanding and regulating 21st century payment systems: The Ripple case study. Michigan Law Review, 2016,114(4):649−682.

[13] Luzio AD, Mei A, Stefa J. Consensus robustness and transaction de-anonymization in the Ripple currency exchange system. In: Proc. of the IEEE Int'l Conf. on Distributed Computing Systems. IEEE, 2017. 140−150.

[14] Wang CY, Zheng BG. RIPPLE in Internet finance: Principles, models and challenges. Shanghai Finance, 2015,3:46−52 (in Chinese with English abstract).

[15] Shan KJ. Comparative analysis of Ripple and SWIFT. Financial Theory and Practice, 2016,447(10):105−107 (in Chinese with English abstract).
[16] Yan M, Xiao L. Virtual currency: Operational mechanism, trading system and governance strategy. China Industrial Economy, 2014,4:110−121 (in Chinese with English abstract).
[17] Circle corporation. CENTRE.2017. https://www.centre.io/
[18] Zhu JM, Gao S, Duan MJ. Blockchain Technology and Application. Beijing: Mechanical Industry Press, 2017. 211−213 (in Chinese).
[19] Lamport L, Shostak R, Pease M. The Byzantine generals problem. ACM Trans. on Programming Languages and Systems (TOPLAS), 1982,4(3):382−401. [doi: 10.1145/357172.357176]
[20] Woos D, Wilcox JR, Anton S, Tatlock Z, Ernst MD, Anderson T. Planning for change in a formal verification of the raft consensus protocol. In: Proc. of the ACM SIGPLAN Conf. on Certified Programs & Proofs. ACM Press, 2016. 154−165.
[21] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. Consulted, 2008.
[22] Merkle RC. A certified digital signature. In: Proc. of the Conf. on the Theory and Application of Cryptology. New York: Springer-Verlag, 1989. 218−238.
[23] Bellare M. Keying Hash function for message authentication. Crypt Proc., 1996,1109:1−15.
[24] Bishop M. Computer Security: Art and Science. Boston: MA Press, 2002. 62−68.
[25] Ding QY, Wang XL, Zhu JM, Song B. Information security protection framework of information physics fusion system based on blockchain. Computer Science, 2018,45(2):32−39 (in Chinese with English abstract).
[26] Vukolić M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In: Proc. of the Int'l Workshop on Open Problems in Network Security. Springer-Verlag, 2015. 112−125.
[27] Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, Enyeart D, Ferris C, Laventman G, Manevich Y, Muralidharan S, Murthy C, Sethi M, Singh G, Smith K, Sorniotti A, Stathakopoulou C, Vukolić M, Cocco SW, Yellick J. Hyperledger abric: A distributed operating system for permissioned blockchains. In: Proc. of the 13th EuroSys Conf. (EuroSys 2018). 2018. 1−15.

附中文参考文献:

[3] 袁勇,王飞跃.区块链技术发展现状与展望.自动化学报,2016,42(4):481−494.
[4] 刘敖迪,杜学绘,王娜,李少卓.区块链技术及其在信息安全领域的研究进展.软件学报,2018,29(7):2092−2115. http://www.jos.org.cn/1000-9825/5589.htm [doi: 10.13328/j.cnki.jos.005589]
[5] 丁庆洋,朱建明.区块链视角下的 B2C 电商平台产品信息追溯和防伪模型.中国流通经济,2017,12:41−49. [doi: 10.14089/j.cnki.cn11-3664/f.2017.12.005]
[11] 中国人民银行数字货币研究项目组.从 SWIFT 黑客事件看金融网络安全.中国金融,2016,17:43−44.
[14] 王朝阳,郑步高.互联网金融中的 RIPPLE:原理、模式与挑战.上海金融,2015,3:46−52.
[15] 单科举.Ripple 与 SWIFT 比较分析研究.金融理论与实践,2016,447(10):105−107.
[16] 祁明,肖林.虚拟货币:运行机制、交易体系与治理策略.中国工业经济,2014,4:110−121.
[18] 朱建明,高胜,段美姣.区块链技术与应用.北京:机械工业出版社,2017.211−213.
[25] 丁庆洋,王秀利,朱建明,宋彪.基于区块链的信息物理融合系统的信息安全保护框架.计算机科学,2018,45(2);32−39.

朱建明(1965－),男,山西太原人,博士,教授,博士生导师,主要研究领域为信息安全,电子商务安全,区块链技术.

丁庆洋(1991－),男,博士生,CCF 学生会员,主要研究领域为区块链应用,信息安全,数字经济.

高胜(1987－),男,博士,副教授,CCF 专业会员,主要研究领域为数据安全与隐私保护,区块链技术及应用.