文章编号：2095-2163(2023)03-0129-05 中图分类号：TP311.13 文献标志码：A

基于可信区块链的网间结算方法研究

裴伦浩，侯青军，朱冠烨
（中国联合网络通信有限公司 济南软件研究院，济南 250000）

摘 要：随着 5G 技术的发展，运营商业务模式愈发复杂，传统的中心化的清结算系统弊端日益明显，数据泄露、篡改的事件时有发生，数据信任无法得到保证。基于此，本文提出了一种基于跨云组网的可信区块链网间结算模式，通过智能合约完成原业务流程的链上处理，解决了数据不一致、数据泄露和篡改的问题，通过投产验证，切实解决了原有业务的痛点问题，为传统清结算系统升级提供了新的思路。

关键词：网间结算；区块链；跨云部署；清结算系统

Research on the inter-network settlement method based on trusted blockchain

PEI Lunhao, HOU Qingjun, ZHU Guanye
(Jinan Software Research Institute of China Unicom, Jinan 250000, China)

【Abstract】 With the development of 5G technology, the business model of operators has become more and more complex, and the drawbacks of the traditional centralized clearing and settlement system have become increasingly obvious. Data leakage and tampering occur from time to time, and the data trust cannot be guaranteed. Based on this, a trusted blockchain inter-network settlement model based on cross-cloud networking is proposed, which completes the on-chain processing of the original business process through smart contracts, and solves the problems of data inconsistency, data leakage and tampering. After verification, the proposed method solves the business pain points and provides new ideas for the upgrade of the traditional clearing and settlement system.

【Key words】 inter-network settlement; blockchain; cross-cloud deployment; clearing and settlement system

0 引 言

随着 5G 时代的到来，运营商业务模式愈发复杂，这一方面促进了市场发展，另一方面对现有的计费清结算模式提出了更高的要求。传统的运营商之间的计费清结算模式存在以下弊端：计费清结算流程冗长、实时性低、数据存储过于中心化、容错性差；人工参与环节较多，审计成本高，缺乏监督和监管不透明，数据存在泄露和篡改的风险。鉴于此，对现有的计费清结算模式进行探索迫在眉睫。本文从国内网间结算项目为突破点，分析现状、设计系统升级方案，为系统整体升级提供试点。

1 网间结算模式现状及挑战

网间结算指的是不同运营商之间互联互通时，由于使用了对方的通信资源或者服务，使用双方会根据协议或者合同对产生的通信费用进行分摊，现有的国内清结算系统仍然沿用中心化的数据库存储架构，网间结算主要采用各运营商各自生成帐单报表、线下交互的方式完成报表交换与对账。传统的网间结算流程如图 1 所示。由图 1 可知，通常先有业务人员进行出账，生成一份结算报表，结算报表需要双方的业务人员进行邮件交互，对于有争议的结算项再次进行修改确认，对涉及调账的结算项目再进行调账结算，生成最终的确认数据，并由双方业务人员确认，业务人员确认后转财务审核，完成最终的结算和支付。从图 1 还可看到，该业务流程反复涉及报表的邮件流转确认，环节冗长复杂，由于双方的出账进度不一致或者审核环节不畅导致的结算周期延长时有发生，难以保证数据的实时性；往来邮件报

作者简介：裴伦浩(1992-)，男，学士，中级软件工程师，主要研究方向：区块链底层链技术研究与应用；侯青军(1971-)，男，硕士，高级软件工程师、通信计费领域专家，主要研究方向：计费领域应用管理、生产运营；朱冠烨(1993-)，男，硕士，主要研究方向：通信软件和区块链应用软件研究。
通讯作者：朱冠烨 Email：zhugy28@chinaunicom.cn

收稿日期：2022-06-23

表流转的过程中存在数据泄露和数据篡改的风险，对某一结算项的结算流程和账目明细难以审计，使得最终的结算结果可信性降低；业务人员在人工审计时时效性低，人工维护的成本高。

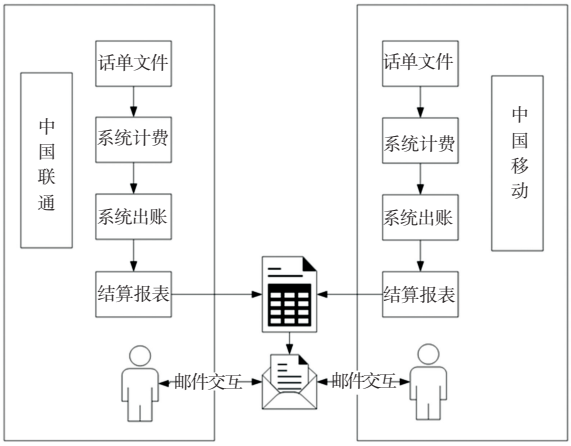

图 1 传统的网间结算流程

Fig. 1 Traditional inter-network settlement process

2 区块链助力网间结算升级

区块链技术是由区块构成的链式数据处理系统[1]，是通过去中心化和去信任化方式集成维护的可靠数据存储方案。区块链技术的核心优势是去中心化，能够通过数据加密、时间戳、分布式共识等方式，在分布式系统中实现去中心化信用的点对点交易、协调和写作，进而解决中心化机构普遍存在的高成本、低效率和数据存储不安全等问题。区块链按照功能划分可以分成公有链、私有链、联盟链。其中，公有链的目标群体为所有用户，例如比特币、狗狗币等场景；私有链只能给某个企业内部单独使用，无法进行多方组网；联盟链可以以“组织”的方式进行若干单位联合构建，形成小规模、低成本、灵活性高、多方参与的区块链网络，目前企业级应用大部分还是以联盟链为主。

针对目前国内网间结算业务中存在的业务痛点，联盟链技术为解决这些问题提供了新的思路。针对中心化存储的问题，联盟链基于分布式的存储结构，降低了中心化数据库故障而造成业务停滞的风险；针对业务流程冗长的问题，可以借助智能合约进行实现，全流程通过智能合约自动触发，减少了人工参与的环节；将结算报表通过加密的方式进行上链，数据不会直接暴露给业务人员，有效杜绝数据篡改和数据泄露的问题，借助区块链分布式[2]的特点，解决中心化存储的弊端。网间结算业务-区块链技术改造点如图 2 所示。

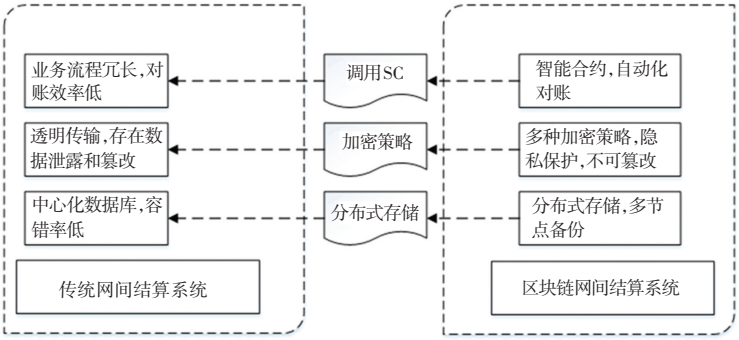

图 2 网间结算业务-区块链技术改造点

Fig. 2 Inter-network settlement-business transformation points for blockchain

3 基于跨云组网的可信区块链网间结算系统设计

3.1 整体设计

天宫区块链 BCS 系统（以下简称 BCS）是基于联通链底层架构搭建起的区块链平台，本文以 BCS 为基础进行联合组网。引入区块链后，系统的交互示意如图 3 所示。由图 3 可知，出账结束后，报表直接被送到链上，经过链上各环节流转后，交付业务人员审核。由于各节点部署在 2 个云环境中，因此首先需要解决网络交互的问题；其次，需由中国联通、中国移动双方进行区块链节点的部署，通过进行网络配置、节点配置[3]等手段，实现双方节点之间交互；再由双方共同编辑并部署智能合约，实现全业务链上自动流转；由双方各自开发自己的客户端，通过客户端调用智能合约访问区块链中的数据。

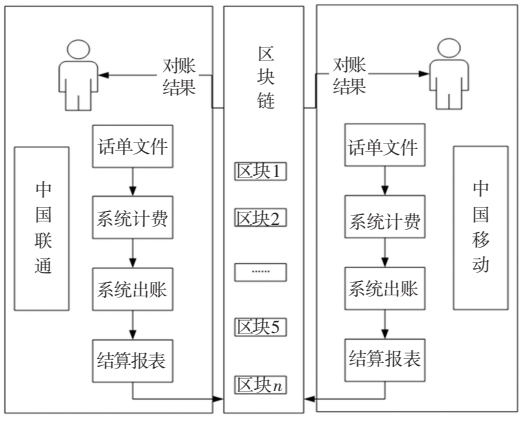

图 3　基于区块链的网间结算系统交互示意图

Fig. 3　Schematic diagram of the interaction of the inter-network settlement system based on blockchain

3.2　跨云组网的可信联盟链

3.2.1　网络设计

运营商系统网络具有较高的网络安全要求，因此，各运营商内网具有封闭性、低接入性、高安全性的特点，解决区块链网络组网的第一件事情，就是网络的打通问题。常见的运营商与外部联动的系统有如下几种方案：

（1）专线网络方案。该种方式具有极高的安全性、低时延以及可靠传输性，但是成本较高。

（2）通过 DMZ 主机映射方式。各运营商内部均有用于外部网络交互的 DMZ 集群，可以通过 Nginx 转发的方式进行网络交互。该方式安全性高，传输可靠性高，存在部分时延。

由于网间结算响应时间比较集中，出账期间系统交互频繁，其他时段网络需要较低，故而采用第二种方案。

中国移动与中国联通的底层链架构具有一定的相似性，节点类型[4]分成如下 3 类：

（1）CA 节点。用于证书生成和鉴权。

（2）Order 节点。用于对交易进行排序和打包，对交易进行广播。

（3）Peer 节点。用于背书和记账，主节点用于与 order 节点进行通信。

基于以上各类节点作用，本文基于各自的 CA 节点生成证书，通过公网网络达成各运营商 order 节点和 peer 节点能够通信的目的，从而形成可跨云交互的联盟链[5]，网络的拓扑结构如图 4 所示。

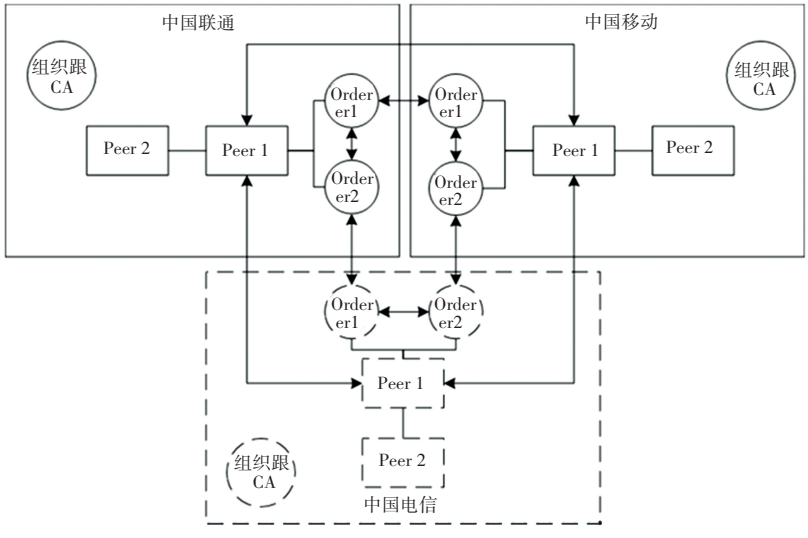

图 4　跨云组网的联盟链节点网络拓扑图

Fig. 4　Node network topology diagram of cross-cloud blockchain

3.2.2　国密信息互通

按照通信部对加密的要求，区块链参与各方均使用基于国密改造过的底层链镜像组网。因代码库和具体改造方式等不同，双方节点无法在同一网络中进行通信，因此需要进行国密算法的改造工作。对于该部分内容，选择重点工作，简单罗列改造点具体如下：

（1）将各国密算法代码名称规范统一。

（2）将 TLS 单双证书方式统一为单证书认证。

（3）交易哈希、区块哈希算法使用统一开发后的版本。区块链的搭建均使用以上改造代码编译的镜像和工具，包括但不限于 peer、orderer、ccenv、tools、cryptogen、configtxgen 等。

3.2.3　联盟链搭建及验证

在完成网络交互的连通性测试之后，进行联盟链的跨云组网[6]，整体流程如图 5 所示。首先，由联通、移动各自生成证书，该证书用于对区块链的交易进行鉴权、校验；双方进行证书交换，并进行底层联盟链的配置，包括状态数据库、出块策略、共识策略、

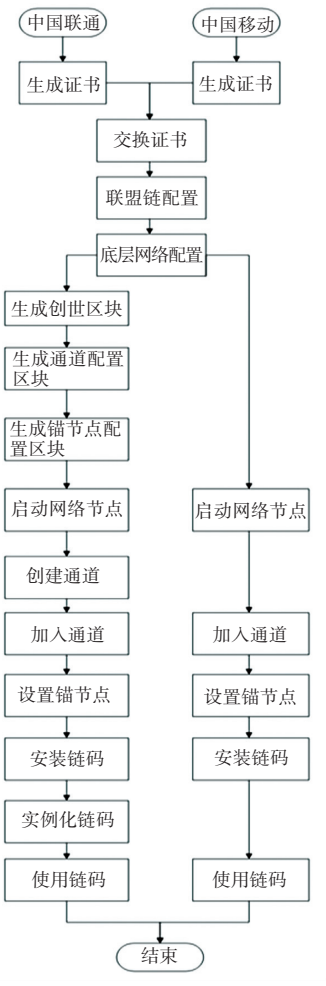

图 5 区块链网络组网及测试流程

Fig. 5 Blockchain networking and testing process

节点个数以及密码策略。通过反复的性能测试,区块超时时间设置为 1 s,块内存储为 100 MB,块内交易数为 50; 共识策略选取 raft 共识,节点个数需要满足 $2f + 1$, 双方约定背书节点 2 个,共识节点 5 个,密码策略启用国密。

完成以上配置后,由双方任何一方生成创世区块、通道配置区块[5]以及锚节点区块,并启动本方的网络节点,另一方则仅需启动本方网络节点并加入通道,双方设置各自的锚节点后,进行智能合约的安装,最后需任意一方进行链码实例化[7]。此时,联盟链组网完毕,双方可各自通过自己的客户端进行合约调用,查看是否成功出块,双方核对块内交易是否一致。

3.3 业务流程优化

原有的业务流程冗长、复杂,涉及到诸多人工审核的环节,优化后的流程如图 6 所示。由图 6 可知,出账结束后,出账报表由结算系统自动封装数据,调用智能合约将报表数据传到区块链上。为保证数据隐私,任何一方在上传报表时均会通过 aes 方式进行加密[8],将密钥保存在本地服务器,待双方报表数据均上传后,双方将各自密钥上链,通过链上解密完成自动化对账,生成准终结算数据。此时,业务人员会接收到短信提醒,对该数据进行链上审核,如果对该数据需要做进一步调账,则可将调账数据进行上链,上传方将调账数据上传后,另一方收到审核通知,审核完成后于链上进行调账,生成终结算数据。终结算数据对接财务系统,完成支付。

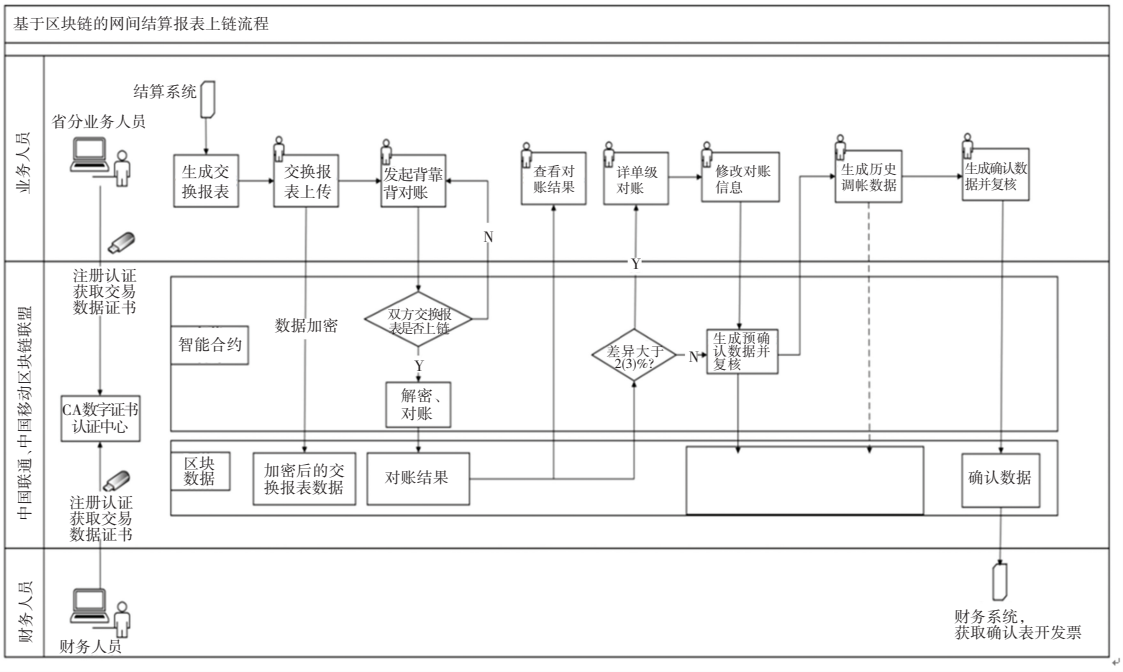

图 6 基于区块链的网间结算业务流程

Fig. 6 Inter-network settlement business process based on blockchain

(下转第 142 页)