基于 Fabric 的跨境汇款追踪平台实现

朱 涛[1,2], 姚 翔[1,2], 许玉壮[1,2], 周 钰[1,2]

[1] 中国银联 上海 中国 201201

[2] 电子商务与电子支付国家工程实验室 上海 中国 201201

摘要 针对“全球速汇”业务场景下对实时信息查询不便的问题, 利用区块链分布式系统架构的特征, 设计并开发了基于 Fabric 的跨境汇款追踪平台。该平台实现将汇款各环节中的流转信息进行共享和存储, 保证信息的不可篡改, 同时兼顾了联盟链的权限控制和数据隐私。结合功能及性能测试结果, 该平台在满足银联跨境速汇业务量需要的同时, 可有效提升业务的透明度, 优化机构业务流程、减少人工操作、提高效率, 并提升用户体验, 为联合机构探索区块链跨境金融应用打下基础。

关键词 区块链; 智能合约; 跨境汇款

中图法分类号 TP311 DOI 号 10.19363/j.cnki.cn10-1380/tn.2018.05.06

Cross-broder Remittance Tracing Platform Based on Fabric

ZHU Tao[1,2], YAO Xiang[1,2], XU Yuzhuang[1,2], ZHOU Yu[1,2]

[1]China UnionPay, Shanghai 201201, China

[2]National Engineering Laboratory of E-Commerce and E-Payment, Shanghai 201201, China

Abstract With the characteristics of distributed system architecture of blockchain, a cross-broder remittance tracing platform based on Fabric has been designed and developed, aiming to solve the problem of inconveniences in real-time information query in the “MoneyExpress” scenario. The platform enables the information flow of remittance to be shared and stored so that not to be tampered. Meanwhile, the permission control and data privacy are also considered in the platform. As is shown from the results of functional and performance test, the platform can meet the needs of “Money Express”, and it can also effectively improve the transparency of the business, optimize the organization's business processes, reduce manual operation, increase efficiency and improve the user experience. This practice will lay the foundation for the joint venture to explore the cross-border financial application of blockchain.

Key words blockchain; smart contract; cross border payment

近年来, 全球大部分国家政府、企业和研究机构均不断加大对区块链技术研究和应用实践的投入力度[1,2]。作为一项迭代性的创新技术, 区块链的显著优势在于优化业务流程、降低运营成本、提升协同效率, 现已延伸至金融服务、供应链管理、知识产权、智能制造、社会公益以及教育就业等众多领域, 为经济社会转型升级提供系统化的支撑。2016 年末, 国务院印发的《“十三五”国家信息化规划》提出, 加快信息化发展, 构建统一开放的数字化市场体系, 满足人民生活新需求。区块链技术首次被纳入国家规划, 这一规划强调了加强区块链等新技术的创新、试验和使用, 实现抢占新一代信息技术的主导权,

自 2014 年起, 国际上首先意识到区块链技术的重要价值, 并将其从比特币、以太坊等虚拟货币应用中剥离, 并开展联盟链技术研究, 形成了联盟化、金融级、全盘布局的特点, 相继出现了 R3 CEV 公司主导的 R3 联盟、Linux 基金会发起的开源项目 HyperLedger 和以太坊企业联盟 EEA 等, 主要参与对象既有大型商业银行、商业机构, 也有科技公司、咨询公司, 意在对产业基础设施进行优化和重构。以 Visa、MasterCard 为代表的卡组织也在积极探索区块链技术在支付清算行业的应用, Visa 在 2016 年 10 月就曾测试一项名为 Visa B2B Connect 的服务, 采用了

通讯作者: 朱涛, 博士, 助理工程师, Email:zhutao2@unionpay.com。

收稿日期: 2018-01-31; 修改日期: 2018-04-28; 定稿日期: 2018-05-02

区块链技术使企业能够更快地处理跨国支付。而 MasterCard 也在 2016 年 10 月份公开了自己的区块链工作, 并推出了针对智能合约和支付结算流程的系统; 2017 年 10 月份, 通过其开发者平台上发布的 API 正式开放区块链技术, 为消费者、商户及银行合作伙伴提供一种全新的交易方式。与此同时, 鉴于区块链所带来的颠覆性技术能力, 国内金融机构自 2015 年起对区块链的研究热度呈现出爆发式的增长, 并在不断的向应用落地演变, 人民银行、工商银行、农业银行、招商银行等均已摸索出了一些颇具特色的应用场景。2018 年 1 月央行推动的数字票据交易平台实验性生产系统上线试运行成功, 完成基于区块链技术的数字票据签发、承兑、贴现和转贴现业务等; 2017 年 9 月, 工行与贵州省贵民集团联合上线首个脱贫攻坚基金区块链管理平台, 实现扶贫资金的透明使用、精准投放和高效管理; 农业银行在 2017 年 8 月上线了基于区块链的涉农互联网电商融资系统, 用于解决农信贷业务信息不对称、管理成本高等问题; 2017 年 3 月, 招商银行将区块链技术应用于全球现金管理, 实现跨境直联清算、全球账户统一视图以及跨境资金归集。

相对于境内百花齐放的应用场景, 信息基础设施较为老朽跨境应用场景的创新脚步较为缓慢, 但也渐渐成为区块链这一创新技术的颠覆对象。“全球速汇(Money Express)”是中国银联是中国银联基于 ISO8583 报文规范和传统银联网络开发的中小额跨境汇款产品, 目前已在美国、日本、新加坡、澳大利亚等 39 个国家和地区开通, 境外汇款人可以方便地向中国工商银行、中国银行、中国建设银行等 13 家境内银行的银联卡进行跨境汇款交易, 具有资金实时入账的优点。但随着该业务量的不断上升, 原有基于中心化系统架构实现的应用已逐渐无法满足用户日益增长的体验需求[3,4], 因无法查询跨境汇款的实时状态, 遭到大量客诉。在整个业务流程中, 由于汇款机构、转接机构、汇入机构、清算机构的数据信息相互独立, 汇款发起、转接、入账、清算的信息被分割, 导致机构间无法直观地看到汇款的整个“流转过程”。一旦汇款人/收款人想要查询汇款的实时状态, 境内外机构间因电子化程度低导致繁琐的人工查询过程往往需要 10-20 天才有回复, 一方面给客户体验造成了不好的影响, 另一方面对汇款机构、转接机构和汇入机构的客服和运营增加了压力。

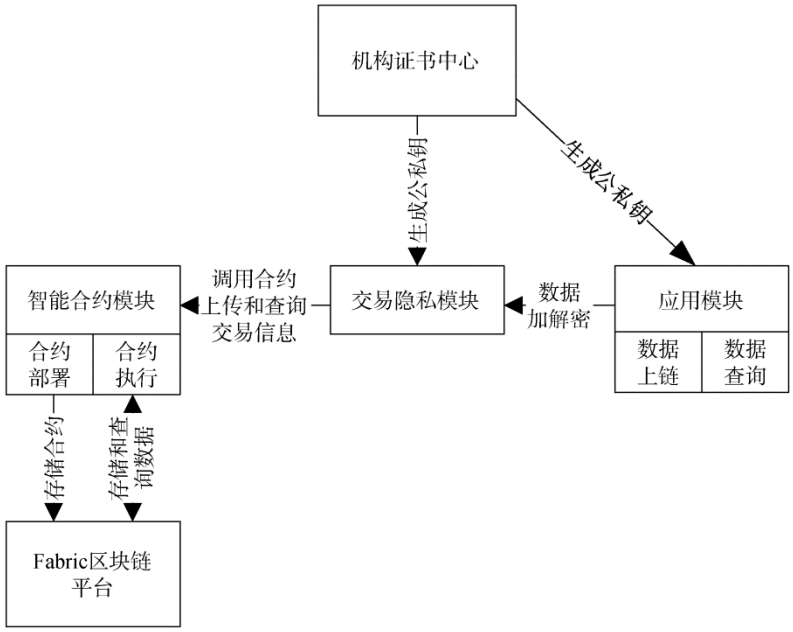

图 1　跨境汇款追踪平台整体架构

Figure 1　The overall architecture of the cross-border remittance tracking platform

针对以上问题, 本实验室基于开源区块链技术 HyperLedger Fabric 开发了跨境汇款追踪平台。在保持原有业务运行不变的基础上, 该平台实现将汇款在各环节中的流转信息进行共享和存储, 针对每一笔汇款: 由汇款机构负责录入包括汇款 ID、汇款人信息、汇款机构、联系方式、汇出时间、附言等信息; 由汇入机构负责录入包括收款人信息、入账时间、交易流水号、币种、金额等信息; 由转接、清算机构负责录入汇款转接和清算时间, 保证信息的不可篡改, 使得任何一个机构都可以通过汇款 ID 查询汇款

的实时流转信息。

1 系统架构

如图 1 所示, 跨境汇款追踪平台包括 Fabric 区块链平台、智能合约模块、交易隐私模块、机构证书中心和应用模块[5]。1)底层区块链平台是整个系统的核心组成, 实现 4 个方面的功能, 一是通过 P2P 组网结构将业务参与主体相连, 并可动态增删节点; 二是根据跨境业务场景, 选择符合国际标准的加密算法对链上数据进行加密, 保证数据传输和访问的安全; 三是采用 Kafka 集群(分布式队列)方式实现交易共识, 保证各个节点的数据一致性; 四是使用关系型/非关系型数据库等保证区块链系统运行过程中的数据保存在各个节点的本地的存储空间中。2)智能合约模块负责向应用模块提供 API, 包括合约的部署、调用、执行及注销, 针对跨境业务, 境内外各参与主体需共同部署相同的智能合约, 其代码将存储于底层区块链模块中, 当外部发来合约调用请求时, 由各参与主体分布式执行智能合约代码。3)交易隐私模块, 对于每一笔交易, 汇款机构、转接机构、汇入机构和清算机构间将分别对上传数据进行加密, 并将加密密钥在交易强相关方间共享, 保证汇款交易的详细信息不会被非相关方获取。4)机构证书中心, 负责为各参与主体的 Orderer、Peer、Kafka 集群、应用服务器等生成公私钥。5)应用模块分为面向机构的跨境汇款数据上链和查询子模块, 通过调用智能合约模块中的程序, 可向区块链模块上传数据和查询数据。

2 Fabric 区块链平台

区块链起源于化名为“中本聪”(Satoshi Nakamoto)的学者在 2008 年发表的文章《比特币: 一种点对点电子现金系统》[6], 主要呈现出“两种结构, 两类算法, 一个合约”的特点, 是基于博弈论、密码学和软件工程等多个领域研究成果的集成创新。通过大规模协作、计算机编码内容、密码技术实现了数据不可篡改、数据集体维护、多中心决策等特征, 可以构建出公开、透明、可追溯、不可篡改的价值信任传递链, 从而为金融与信用服务提供创新可能。

跨境汇款追踪平台中采用的是 HyperLedger Fabric 区块链平台, 该平台的目标是实现一个适合于工程应用的许可链(Permissioned Blockchain)基础框架[7]。采用模块化架构提供可切换、可扩展的组件, 包括共识算法、加密安全、身份管理、智能合约等服务, 其克服了比特币、以太坊等公有链项目的缺陷, 如吞吐量低、无隐私机制、共识算法低效等, 更适用于商业场景, 使用户能够方便地开发商业应用。

2.1 整体架构

跨境汇款追踪平台所采用的是 Fabric 1.0 正式版本, 与 0.6 实验版本相比, 层次更为分明的结构提高了架构的可扩展性和可插拔性, 如图 2 所示:

- 底层由多个节点组成 P2P 网络, 通过 gRPC 通道进行交互, 并利用 Gossip 协议进行同步。
- 账本和交易依赖于链式数据结构、分布式数据库、共识算法等技术; 链码(chaincode)则依赖容器、状态机等技术; 权限管理使用了 PKI 体系、数字证书、加解密算法等技术。
- Fabric 向上层应用提供了 gRPC API 和将 API 进行封装的 SDK, 应用可以通过 SDK 访问账本、交易、链码、事件、权限管理等多种资源。整个平台的核心就是账本, 负责记录平台上所有应用的信息, 而应用通过发起交易来向账本中记录数据, 交易执行的逻辑通过链码来承载。

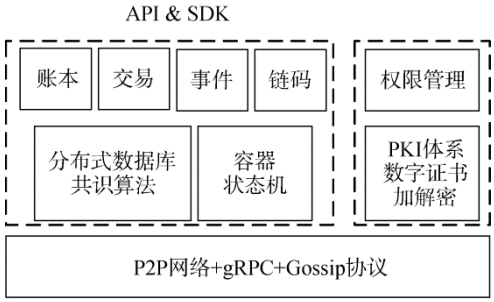

图 2 Fabric 整体架构

Figure 2 The system architecture of Fabric

2.2 网络结构

跨境汇款追踪平台涉及汇款机构、转接清算机构、汇入机构等多种业务角色。针对每一笔汇款: 由汇款机构负责录入包括汇款 ID、汇款人信息、汇款机构、联系方式、汇出时间、附言等信息; 由汇入机构负责录入包括收款人信息、入账时间、交易流水号、币种、金额等信息; 由转接、清算机构负责录入汇款转接和清算时间。该平台通过区块链技术实现将汇款在各环节中的流转信息进行共享和存储, 并保证不可篡改, 使得任何一个机构都可以通过汇款 ID 查询汇款的实时流转信息。多个机构的存在, 使得其网络结构的设计较为复杂, 每一个机构因自身高可用性的需求会包含两个 Orderer 节点和两个 Peer 节点。如图 3 所示, Org1、Org2、Org3 分别为汇款机构、转接清算机构和汇入机构三个组织, 均处于同一个应用通道(business-channel), 并且每个组织中的两个 Peer 负责通过域名的方式与其他组织进行通信。

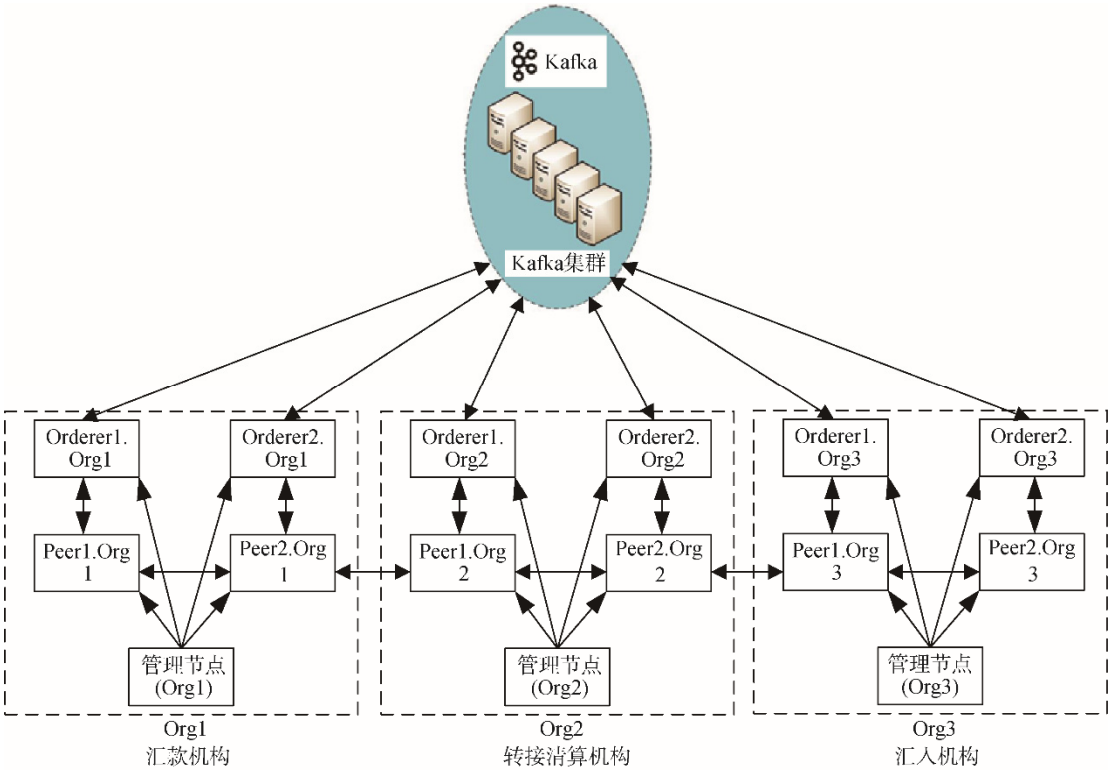

图 3　跨境汇款追踪平台网络结构图

Figure 3　The network structure of the cross-border remittance tracking platform

2.3　交易流程

在公有链的交易流程中, 用户只需要将交易通过服务接口发送到区块链网络中, 再等待网络中的对等节点完成所有的共识和处理过程即可。而对于作为联盟链的 Fabric 来说, 需要更多的考虑网络中节点对交易的执行权限, 因此在逻辑上将节点角色解耦为 Endorser(背书节点)和 Committer(认证节点), 使得不同类型的节点具备不同类型的功能。

典型的交易流程如图 4 所示: 1)客户端从 CA 获取身份证书加入网络内的应用通道; 2)构造交易提案(TX Proposal), 并选择相应的背书策略将交易提交给 Endorser 进行背书; 3)Endorser 节点收到来自客户

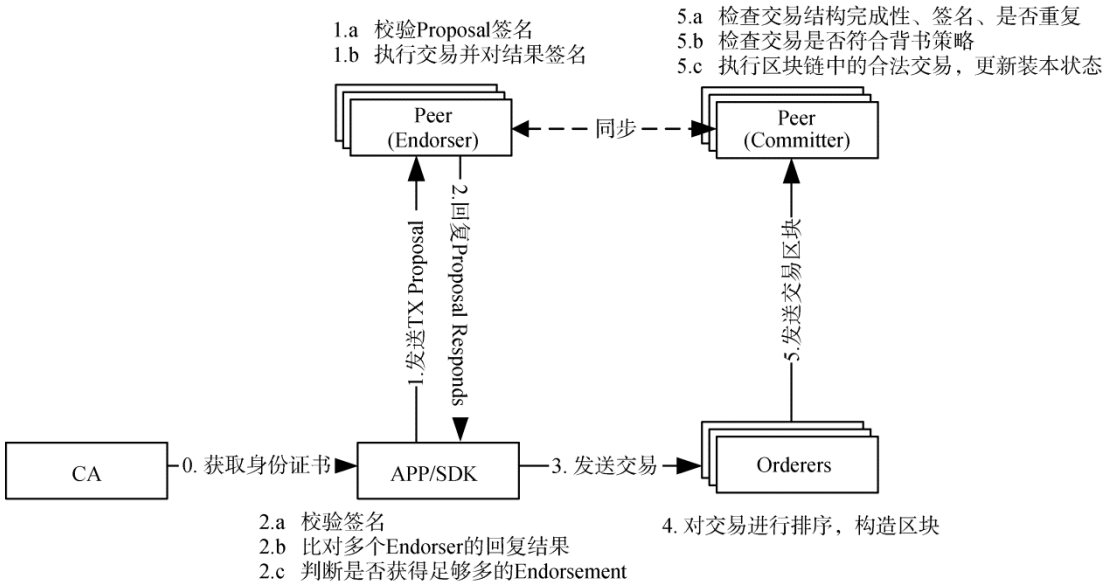

图 4　Fabric 交易处理流程

Figure 4　The transaction process of Fabric

端的交易提案后, 进行交易合法性检查, 检查通过后执行交易, 并对交易结果进行背书返回给客户端; 4)客户端收集到足够的背书支持后可以构造一个合法的交易请求, 发给 Orderer 进行排序处理; 5)Orderer 为网络中的所有的合法交易进行全局排序, 并将一批排序后的交易组合成区块结构; 6)Committer 定期从 Orderer 获取排序后的批量交易区块结构, 对这些交易进行落盘前的最终检查(包括交易消息结构、签名完成性、是否重复、读写集合版本是否匹配等), 检查通过后将结果写入账本。

3 智能合约模块

智能合约是区块链的一项突破性的创新, 可视作一段部署在区块链上可自动运行的程序, 从外部获得的数据信息来识别并判断, 当满足程序设定的条件时, 随即触发系统自动执行相应的合约条款, 实现数据处理、价值转移、资产管理等一系列功能[8-10]。Fabric 的智能合约被称为 chaincode(链上代码, 简称链码), 支持 Java 和 Go 两种图灵完备的编程语言, 采用虚拟机或容器等技术为合约代码提供安全隔离的运行环境。

3.1 技术原理

Fabric 的链码分为系统链码和应用链码。

系统链码是固化在系统中的, 负责处理 Fabric 系统自身的逻辑(包括系统配置、背书和交易等), 运行在节点的进程逻辑中, 通过进程间通信与主进程交互。

应用链码是用户编写的合约代码, 负责执行用户自定义的逻辑, 操作 Fabric 的全局状态。应用链码运行在 Docker 容器中, 通过 gRPC 与节点进行交互, 主要分为注册阶段、初始化阶段、调用阶段和保活阶段, 具体流程如下:

1. 注册阶段

(1) 在调用 shim.Start()方法后, 会向 Peer 发送一个 REGISTER 消息进行注册, 并将其状态标识为 created, 等待 Peer 的回应。

(2) Peer 收到 REGISTER 消息后, 将链码注册到本地, 创建一个 handler 结构处理来自链码的消息, 并返回给 REGISTERED 给链码, Peer 状态更新为 established。

(3) 链码收到 REGISTERED 消息, 将其状态更新为 established。

(4) Peer 向链码发送 READY 消息, Peer 状态更新为 ready。

(5) 链码收到 READY 消息, 将其状态更新为 ready。

2. 初始化阶段

(1) Peer 发送 INIT 消息给链码, 对链码进行初始化。

(2) 链码收到 INIT 消息后, 调用链码 Init()方法执行初始化逻辑。若执行成功, 发送 COMPLETED 消息给 PEER。

3. 调用阶段

(1) Peer 发送 TRANSACTION 消息给链码, 调用链码的逻辑。

(2) 链码收到 TRANSACTION 消息后, 调用 Invoke()方法, 根据消息中的参数, 执行具体逻辑方法。

(3) 链码执行逻辑过程中, 会发送操作全局状态数据库的请求消息给 Peer。

(4) Peer 收到操作数据库消息后, 对相应数据进行增删改查, 返回 RESPONSE 消息给链码。

(5) 链码调用完成后, 发送 COMPLETE 消息 Peer。

4. 保活阶段

在链码注册成功后, Peer 和链码都会定期发送 KEEPALIVE 消息给对方。

3.2 跨境汇款查询合约

跨境汇款查询合约代码采用 Go 语言实现了跨境汇款信息的上链和查询的逻辑。逻辑中主要包括 startRemitMoney()、 changeover()、recorded()、clear()和 getOrder()五个方法来实现跨境汇款全流程数据上链和数据查询功能。

3.2.1 合约主结构

跨境汇款查询合约中具体结构如下, 其中以 main 方法作为合约的入口, 执行 shim.Start()方法, 并使用 Init 方法和 Invoke 方法分别对合约进行初始化和执行交易调用方法。

伪代码 P.1: chaincode 框架

```
//初始化方法
1. func Init(stub shim.ChaincodeStubInterface)
peerResponse { }
//Invoke 方法
2. func Invoke(stub shim.ChaincodeStubInterface)
Peer.Response {
//获取函数名和参数
3. function, args :=
stub.GetFunctionAndParameters()
4. switch function {
//汇出
5. case “startRemitMoney”:
6. result, err = startRemitMoney(stub, request,
requstStr)
```

```
    //转接、汇入、清算、查询...
7. }}
    //合约主函数
8. func main() {
9. err := shim.Start(new(CrossBorderChaincode))
10. }
```

3.2.2 合约方法级权限控制

跨境汇款查询合约的代码可以由汇入机构、汇出机构和银联等多个机构共用, 因此需要限制特定机构可调用的方法, 即合约方法级权限控制。

由于 Fabric 只提供合约级的权限控制, 不能针对不同的方法赋予不同的权限, 因此需要在合约中实现权限控制逻辑。本系统采用签名和验签的方式对合约方法的调用者进行权限控制。机构需要用自己的私钥对合约的调用请求进行签名, 由智能合约根据方法中登记的机构公钥对调用请求进行验签。如果验签通过, 则运行调用; 否则, 返回调用失败。

对跨境汇款查询合约中方法的调用请求需要在机构应用层进行签名, 签名的验证逻辑需要在合约中实现。跨境汇款查询合约中验签的逻辑如下:

伪代码 P.2: 验证签名

Input: the string of public key, *pubKeyStr*; message data, *msg*

```
    //获取公钥并生成 cipher 对象
1. key ← rsa.LoadPublicKeyFromStr(pubKeyStr)
2. cipher ← crypto.NewRSA(key)
    //转码签名
3. signatureBytes ← decodeString(signature, BASE64)
    //验证签名
4. err ←  cipher.Verify([]byte(msg), signature-Bytes, cry.SHA256)
```

4. 交易隐私模块

由于多个汇入行和汇出行共享同一个联盟链网络, 因此, 汇款数据在联盟链中传输和存储过程中, 会面临数据被其他组织或节点拥有者获取的风险[11-13]。例如, 境外机构 A 到境内机构 B 的一笔汇款交易数据可能会被不相关的境内机构 C 获取。因而为了解决链上数据隐私问题, 本平台设计了交易隐私模块。

采用对称加密与非对称加密相结合的方案保证数据隐私, 即对称密钥作为会话密钥对交易进行加密(本系统采用 3DES/AES 算法生成会话密钥及对数据进行加解密), 而非对称密钥用于对会话密钥进行加密, 使加密后的密钥通过联盟链在机构间共享(本系统采用 RSA 算法生成非对称密钥及对会话密钥数据进行加解密), 具体流程如图 5 所示。

对于每一笔汇款, 由汇款机构、转接清算机构(银联)、汇入机构共用一个密钥对上链数据进行加密存储, 保证数据只有交易的强相关方可见。具体流程如下:

(1) 汇出机构生成对称加密的密钥 key, 分别用汇出机构、汇入机构、转接清算机构三方的公钥(*Pkey1*, *Pkey2*, *Pkey3*)进行加密, 形成 *Ckey1*, *Ckey2*, *Ckey3*, 即

$$\begin{cases} Ckey1 = Rsa(key, Pkey1) \\ Ckey2 = Rsa(key, Pkey2) \\ Ckey3 = Rsa(key, Pkey3) \end{cases}$$

其中 *Rsa* 为所用的非对称加密算法。

(2) 汇出机构将汇款信息 *Remdata* 用 *key* 进行加密, 生成加密后的汇款信息 *CRem*, 并发送到智能合约进行处理, 即

$$CRem = Dec(Remdata, key)$$

其中 *Dec* 为所用的对称加密算法。

(3) 智能合约将加密后的<*CRem*,*Ckey*1,*Ckey2*, *Ckey3*>存入数据库;

(4) 转接机构向智能合约请求并获得密钥 *Ckey2*。转接机构用自己的私钥 *Prvt2* 将 *Ckey2* 进行解密, 获得对称密钥 *key*, 并用 *key* 将转接信息用 *key* 进行加密, 发送给智能合约进行存储, 即

$$key = DRsa(Ckey2, Prvt2)$$

和

$$DTrans = Dec(TsData, key)$$

其中 *DRsa* 为所用的非对称加密算法对应的解密方法。

(5) 汇入机构向智能合约请求并获得密钥 *Ckey3*。汇入用自己的私钥 *Prvt3* 将 *Ckey3* 进行解密, 获得对称密钥 *key*, 并用 *key* 对汇入信息进行加密, 发送给智能合约进行存储, 即

$$key = DRsa(Ckey3, Prvt3)$$

和

$$DRec = Dec(RecData, key)$$

(6) 清算机构用 *key* 将清算信息用 *key* 进行加密, 发送给智能合约, 并由智能合约将清算信息存入数据库, 即

$$key = DRsa(Ckey2, Prvt2)$$

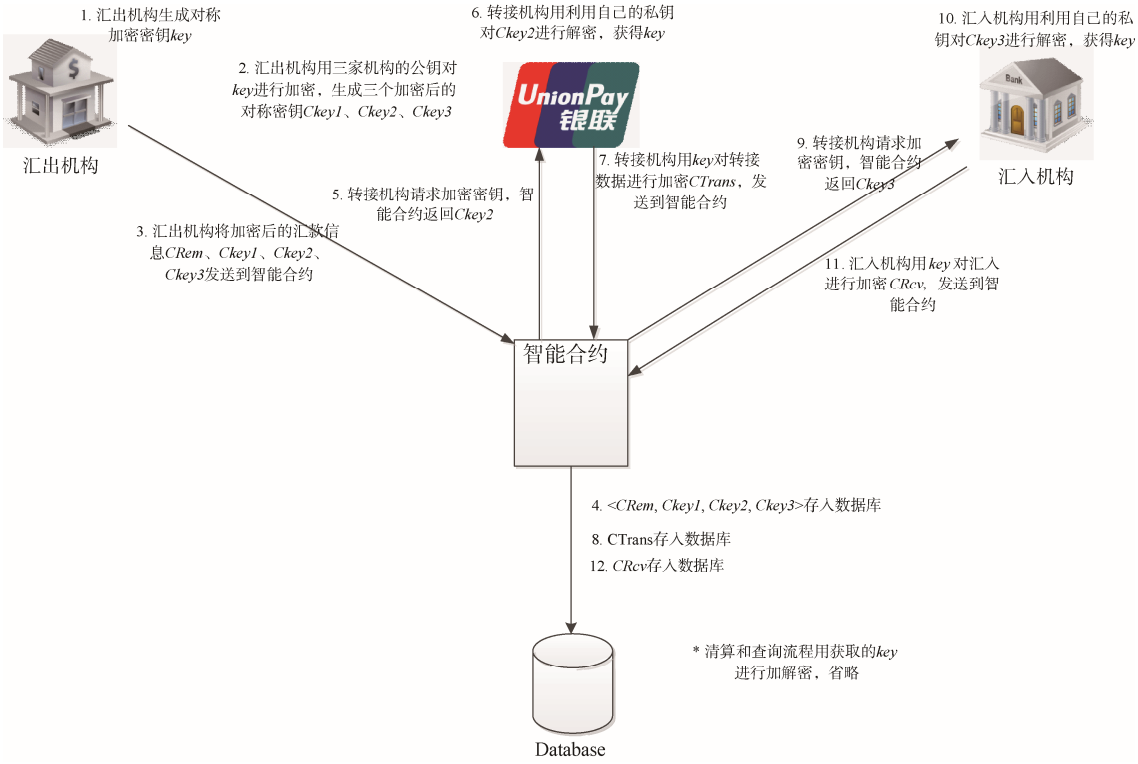

图 5　跨境汇款交易隐私示例

Figure 5　The transaction privacy mechanism of cross-border remittance

和

$$DClr = Dec(ClrData, key)$$

(7) 查询: 向智能合约查询汇款信息, 智能合约返回加密的数据, 与汇款信息相关的三方可以用 key 进行解密, 而其他机构无法解密, 从而保证了汇款数据的隐私性。

5　机构证书中心

机构证书中心用于产生机构的 MSP (Membership Service Provider)。MSP 模块用于 Fabric 底层的加密、签发和校验证书, 及用户验证。一般来说, 一个组织拥有一个 MSP, Fabric 提供模块化的成员操作及不同成员管理标准和框架的可操作性。为了实现一个默认的 MSP, 需要提供符合 RFC5280 标准的参数[14]。

Fabric 的 MSP 可以有多种方式生成——传统的 CA 证书中心、Fabric 证书和软件生成。本系统为了降低各个组织间证书的耦合性, 采用各自独立生成证书的方式, 并利用 cryptogen 工具生成证书。一个组织如果包含了 orderer 节点和 peer 节点, 需要生成 orderer 组织的证书和 peer 组织的证书, 生成的证书文件需要包含如下几个目录:

(1) admincerts 目录: 包含与管理员证书对应的 PEM 证书文件;

(2) cacerts 目录: 包含与 CA 根证书对应的 PEM 文件;

(3) intermediatecerts 目录(可选的): 包含与中间 CA 证书对应的 PEM 文件;

(4) config.yaml 文件(可选的): 包含 OUs(Orgnization Units)的信息;

(5) crls 目录(可选的): 包含废止证书的列表;

(6) keystore 目录: 节点签名私钥的 PEM 文件;

(7) signcerts 目录: 包含节点 X.509 证书的 PEM 文件;

(8) tlscacerts 目录(可选的): 包含 TLS CA 根证书对应的 PEM 文件;

(9) tlsintermediatecerts 目录(可选的): 包含中间 TLS CA 证书的 PEM 文件。

以 Peer 组织的证书为例, 生成一个 MSP 证书目录的伪代码如下:

伪代码 P.3: 生成 MSP 证书

Input: *caDir, orgName, etc.*

```
//创建签名 CA
1. signCA ← new_ca(caDir, orgName,
orgSpec.CA.CommonName)
//创建 TLS CA
```

2. tlsCA ← new_ca(tlsCADir, orgName, "tls"+orgSpec.CA.CommonName)
　//创建 MSP 证书
3. err ← generate_verifying_MSP(mspDir, signCA, tlsCA)
　//创建 Peer 节点证书
4. generate_nodes(peerDir, orgSpec.Specs, signCA, tlsCA)
　//创建用户证书
5. generate_nodes(usersDir, users, signCA, tlsCA)
　//将管理员证书拷贝到组织 MSP 的 adminCerts
6. err ← copy_admin_cert(usersDir, adminCertsDir, adminUser.CommonName)

组织的 MSP 证书(包括根 CA 证书、中间 CA 证书和管理员证书)会登记在创世区块中(创世区块是指跨境汇款追踪平台底层区块链的第一个区块, 其中记录了各组织节点间网络、身份等配置信息)。对于系统通道, 登记的是 orderer 组织的证书, 用于在创建应用通道时对请求进行验证; 对于应用通道, 登记的是 peer 组织的证书, 用于在获取、加入通道、发送交易等操作时对请求进行验证。MSP 发布流程如图 6 所示。

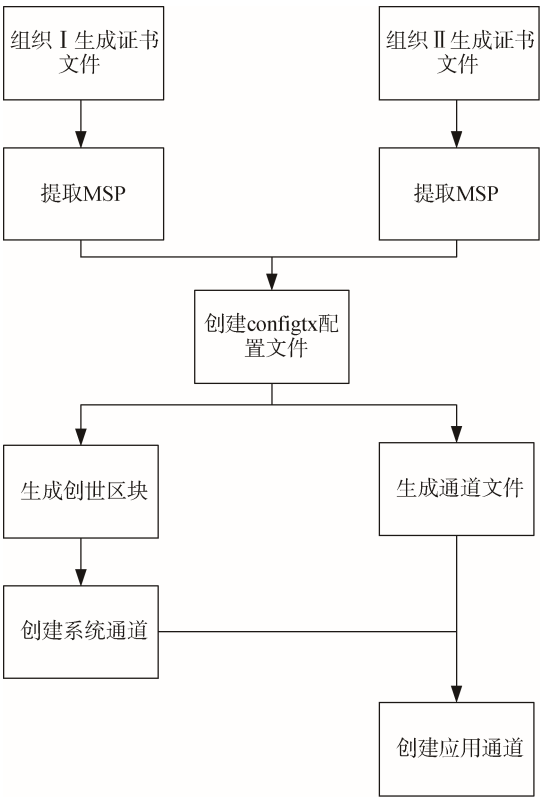

图 6　MSP 发布流程图

Figure 6　The release process of MSP

6　应用模块

应用模块分为面向机构的跨境汇款数据上链和查询子模块, 通过调用智能合约模块中的程序, 可向区块链模块上传数据和查询数据。

6.1　跨境汇款数据上链

在跨境汇款业务流程中, 汇款机构、转接清算机构和汇入机构需要上传的信息是不同的, 分别通过调用智能合约中的 startRemitMoney()、changeover()、recorded()和 clear()四个接口完成数据上链。

汇出机构方法用于设置汇款交易中汇出机构的信息, 如汇款人、汇出国家、汇出机构、汇出地址等, 其伪代码为:

伪代码 P.4: 汇出机构上链数据

Input: an *orderer* indicate by *order_id*
1. result ← ∅
　//生成会话密钥, 并设置 order 属性
2. symKey ← generate_random_key()
　//设置汇出机构名
3. cryptRmtName ← encrypt(rmtName, symKey)
4. set_rmt_name(result, cryptRmtName)
　//设置汇出国家
5. cryptCountry ← encrypt(country, symKey)
6. set_country(result, cryptCountry)
　//设置汇出时间
7. cryptRmtTime ← encrypt(rmtTime, symKey)
8. set_rmt_time(result, cryptRmtTime)
　//设置汇出结果
9. cryptRmtRes ← encrypt(rmtRes, symKey)
10. set_rmt_res(result, cryptRmtRes)
11. ……

转接机构方法用于设置转接信息, 主要为转接的时间和转接的结果, 其伪代码为:

伪代码 P.5: 转接机构上链数据

Input: an *orderer* indicate by *order_id*

1. result ← ∅
　//生成会话密钥, 并设置 order 属性
2. symKey ← generate_random_key()
　//设置转接时间
3. cryptChangeTime ← encrypt(order_change_time, symKey)
4. set_clear_time(result, cryptChangeTime)
5. ……

汇入机构方法用于设置收汇机构的信息, 包括收款人、收款货币类型、汇入金额、汇入结果等, 其伪代码为:

伪代码 P.6: 汇入机构上链数据

```
Input: an orderer indicate by order_id
1. result ← ∅
   //生成会话密钥, 并设置 order 属性
2. symKey ← generate_random_key()
   //设置汇入人
3. cryptPayeeName ← encrypt(order_name, symKey)
4. set_payee_name(result, cryptPayeeName)
   //设置汇入币种
5. cryptCurrency ← encrypt(order_currency, symKey)
6. set_currency(result, cryptCurrency)
   //设置汇入金额
7. cryptAmount ← encrypt(order_amount, symKey)
8. set_amount(result, cryptAmount)
9. ……
```

清算机构方法用于设置清算信息, 主要为清算时间, 其伪代码为:

伪代码 P.7: 清算机构上链数据

```
Input: an orderer indicate by order_id

1. result ← ∅
   //生成会话密钥, 并设置 order 属性
2. symKey ← generate_random_key()
   //设置清算时间
3. cryptClearTime ← encrypt(order_clear_time,
symKey)
4. set_clear_time(result, cryptClearTime)
5. ……
```

6.2 跨境汇款数据查询

跨境汇款追踪平台的各参与主体可通过调用智能合约中 getOrder()接口查询区块链系统中的跨境汇款数据, 比如汇款信息、转接信息、入账信息和清算信息等。伪代码为:

伪代码 P.8: 从链上查询信息

```
Input: an order indicated by order_id
1. request ← ∅
   //设置查询请求
2. set_type(request, "invoke")
3. set_public_key(request, PUBLIC_KEY_TYPE)
4. set_contents(request, order_id)
   //将请求结果转换为 JSON 格式, 并构建交易
5. request_json ← ∅
6. to_json(request, request_json)
7. transaction ← create_f_transaction(request_json)
8. queryResult ← que-
ry_contract(fabricAPI(transaction))
   //用私钥解密数据, 获取会话密钥
9. encryptSymKey ←
get_encrypt_sym_key(queryRequest)
10. symKey ← decrypt(encryptSymKey, PRIV_KEY)
   //解密数据获取汇款交易的相关信息
11. cryptRmtName ←
get_crypt_rmt_name(queryResult)
12. remitterName ← decrypt_asym (cryptRemName)
13. ……
```

7 测试分析

跨境汇款追踪平台目前已经在测试环境中运行, 由 10 台服务器组成, 其中 4 台搭建了 Kafka 集群, 部署了 2 台 Orderer 和 2 台 Peer, 1 台应用服务器和 1 台证书服务器。服务器的 cpu 为 4 核 Xeon 处理器, 内存为 8G, 操作系统为 CentOS 7.2。软件包括 Fabric V1.0.2、Java V1.8、Jmeter V3.2。具体功能测试和性能测试结果如下:

7.1 功能测试

如图 7 所示, 针对每一笔汇款, 业务各参与主体分布式上传汇款信息: 由汇款机构负责录入包括汇款 ID、汇款人信息、汇款机构、联系方式、汇出时间、附言等信息; 由汇入机构负责录入包括收款人信息、入账时间、交易流水号、币种、金额等信息; 由转接、清算机构负责录入汇款转接和清算时间。通过交易隐私模块, 使用交易强相关方之间共享的密钥对数据进行加密存储到区块链平台。应用模块中的跨境汇款数据查询子模块面向机构端开放, 通过调用智能合约可以实时查询到机构自身相关联的汇款信息。

本应用实现了整个业务流程中数据的上传、存储、查询、加解密等功能, 数据多方维护、可追溯且不可篡改, 解决了境内外机构间信息不对称、权限控制和交易隐私保护等问题, 实现跨境汇款全流程自动化处理。

7.2 性能测试

在内网测试中, 如图 8 所示, 经多次测试后, 系统的每秒交易数量平均值为 370, 方差为 10。平均时延的平均值为 104ms, 方差为 4.43ms。

在广域网测试中, 如图 9 所示, 经多次测试后, 系统的每秒交易数量平均值为 77.3, 平均时延的平均值为 261.5ms, 满足银联跨境速汇业务的需要。最

图 7　应用功能测试图

Figure 7　The application function test

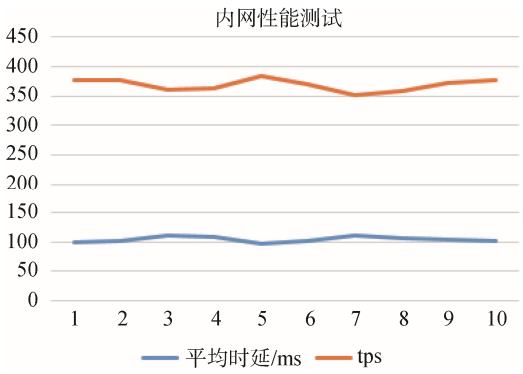

图 8　应用性能测试图(内网)

Figure 8　The application performance test

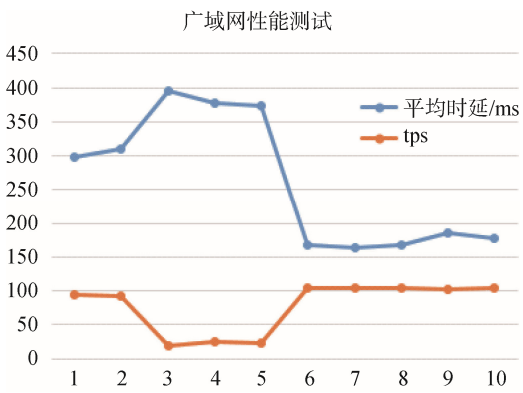

图 9　应用性能测试图(广域网)

Figure 9　The application performance test

终产品将由各方各自部署节点，并基于互联网连接。在预生产测试中，性能的主要瓶颈主要受制于网络带宽，呈现出忙闲时段的显著差异。

在目前“全球速汇”业务中，一旦收款人声称未收到汇款或者希望查询汇款来源等信息时，需要通过银联跨境差错平台(CDRS)提交查询，查询请求会由银联转交至相应汇款机构和汇入机构，由于商业银行非一体化管理的原因，往往会由总行到省行、省行到分行、分行再到支行，由于各层级银行间信息的不对称，导致对于交易查询都会很高的时间成本，虽然业务规则约定时间是 5 天，但往往整个流程需要 10 天才可回复汇款信息，使消费者具有较差的汇款体验。此外，繁复的人工流程也增加了汇款机构、转接机构和汇入机构的客服和运营的压力。

基于区块链的跨境汇款查询应用通过汇入机构、汇出机构、银联、银联国际共建区块链网络，实现对跨境汇款流转过程中的信息进行存储，使得汇款信息在各级银行间实时同步，而且是汇款的全量数据，这样一旦用户想查询交易，国内银行可以不依赖于银联、不依赖于境外银行，从自有数据库中直接读取数据，大大降低了运营成本；如果采用普通的分布式技术，虽然在一定程度上缓解多地查询的问题，但依然无法避免金融风控制度和审核机制，同时利

用传统的分布式技术构建数据平台带来更多的业务沟通和系统对接成本。

7.3 安全性分析

本系统通过 fabric 底层的证书体系和加密机制保证交易和节点的数据安全, 另外, 在应用层通过对称加密与非对称加密结合保证应用数据安全。

交易数据安全: fabric 的成员管理, 保证了只有拥有由特定根证书签发的证书的节点才能加入区块链, 保证了节点的可信性; 同时, 通过 fabric 的多通道机制实现了数据隔离, 保证交易数据只在与业务相关的组织内传输, 因此, 在一定程度上保护了数据隐私。

存储安全: 由于落盘的业务数据是通过会话密钥进行加密的, 而链上的会话密钥又是由业务方应用层的公钥加密的。在最坏的情况下, 不是业务相关方的机构或节点只能绕过区块链系统直接从底层数据库拿到加密后的会话密钥和加密后的业务数据。因为不是业务相关方的机构或节点没有加密会话密钥对应的私钥, 因此无法获得会话密钥的明文, 因此也无法解开业务数据。

传输过程中安全: 在传输过程中, 业务数据和会话密钥也是加密的, 因此可以保证传输过程中数据不会被窃取; 同时, 客户端到节点、节点之间的传输采用 tls 加密机制进一步保证了传输过程中数据的安全。

7.4 应用创新性及不足

本项目运用区块链技术, 创新性地解决了现有跨境汇款业务中由于信息不对称导致用户体验差的问题, 相比于其他项目, 其创新点主要体现在以下方面:

(1) 应用创新性

中国银联自 2017 年 3 月起, 对跨境汇款的路径追踪问题开始研究, 基于区块链技术搭建全球跨境支付追踪平台, 解决跨境支付中过程不透明, 信息不流畅的问题, 实现高效的资金实时追踪, 向银行和支付机构提供易接入、低成本的全球网络, 为其客户创造更优质的跨境支付服务。而在国际上与以上工作比较类似就是 SWIFT 于 2017 年启动的 SWIFT GPI(Global Payment Innovation)项目, 该项针对现有汇款速度慢、体验差、资金流动性差的问题, 基于分布式账本技术同样构建了一个平台, 面向 SWIFT 的成员机构提供相关接口, 使机构在处理每一笔汇款的同时上传汇款的处理时间, 从而实现监控每一笔汇款端到端的路径追踪, 并已完成相关概念验证, 但目前并没有在现有的系统中进行应用。

相比于 SWIFT 业务, 本论文所述平台对于汇款路径上的关键数据进行收集, 包括汇款人信息、汇款机构、联系方式、汇出时间、收款人信息、入账时间、交易流水号、币种、金额、附言、汇款转接和清算时间等信息, SWIFT 的 POC 功能相对简单, 仅仅是对汇款路径的追踪, 虽用了区块链技术, 但是逻辑上的去中心化, 而本项目将要实现的是各机构间的信息去中心化。目前, 中国银联已与中国银行、上海银行基于开源区块链技术完成跨地域、跨机构的联盟链搭建以及跨境汇款查询应用验证, 未来将引入境外机构实现应用扩展。

(2) 物理分布式网络

现有联盟链项目, 部分是将共识节点部署在统一的云平台, 部分是将共识节点部署在统一的机房, 但各自属于不同的参与方(所谓物理上统一, 逻辑上隔离), 极少有各方独立部署节点, 并通过互联网或专线打通的。本项目各家机构均在本地部署与自己业务系统打通的共识节点, 目前节点分布在境内外三个城市, 通过互联网构建区块链网络, 保证了业务合规, 增加系统可控性。

(3) 许可链中的权限及隐私保护

跨境汇款信息涉及个人用户隐私, 在项目实施过程中, 除对上链数据脱敏外, 还通过密码学技术, 严格保证机构无法获取到与本机构无关的汇款信息明文, 最大限度地在许可链中保护用户隐私。

除此以外, 在项目运行过程中同样反应出了一些区块链的不成熟之处。

(1) 集成和可配置性差

项目实施过程, 反映出主流联盟链技术 Fabric 与现有系统集成及配置上的不足。由于金融机构不可能直接将业务系统的机器暴露给外部参与共识, 一般是添加一层前置作为业务系统机器的反向代理与其他机构机器进行通信, 这无疑增加了网络系统的复杂度。而 Fabric 的网络配置大多是登记在创世区块中, 为各个机构所共用, 因此, 造成了各方网络和系统配置耦合性强的问题, 增加了系统配置和部署的复杂度。

(2) 权限管理缺陷

目前, Fabric 只支持合约级的权限控制, 而不支持合约方法级的权限控制。因此, 当需要对具体方法限制其操作者时, 需要合约开发人员对权限控制进行实现。另外, 应用层也需要进行权限管理相应的实现。

(3) 运维问题

由于联盟链的节点分布于各个组织机构, 而且

在权限管理、网络配置等方面的耦合性, 使得联盟链系统在运维过程中也面临许多挑战。

首先, 由于机构间节点的隔离, 运维人员或运维工具无法获取全部节点的状态, 需要各个机构对自己的节点分别进行运维, 为系统监控和排错带来了挑战。

当前 Fabric 动态添加组织和节点需要复杂的操作, 且缺少系统运维和监控的成熟的工具, 对系统运维人员的要求较高。另外, 在智能合约升级方面, Fabric 联盟链需要各个机构分别进行操作, 为机构的投产窗口及相应的应用升级方面提出了较高的要求。

8　结论

中国银联采用开源联盟区块链技术 Fabric, 以各家独立部署、借助互联网通信的方式, 与汇款机构共同搭建了跨境汇款追踪平台。该平台可支持跨境汇款信息的实时追踪查询, 提升了用户汇款体验, 降低银行客诉成本; 并保证只有汇款的强相关方才能查询到汇款信息, 保证了用户的安全。项目基于区块链技术, 保证了各参与方的可信平等合作, 具有国际前瞻性, 同时也反映出现有区块链技术在系统集成性、权限控制、隐私保护、运维管理上的不足。

参考文献

[1] 李岩玉, 吴强, “区块链与金融服务升级”, *中国金融*, 2016,(24): 40-41.

[2] 王硕, “区块链技术在金融领域的研究现状及创新趋势分析”, *上海金融*, 2017(9): 26-29.

[3] 潘闻闻,“区块链与国际金融中心建设”, *中国金融*, 2016(16): 78-79.

[4] 张锐,“基于区块链的传统金融变革与创新”, *西南金融*, 2016(10): 18-23.

[5] 叶小榕, 邵晴, 肖蓉, “基于区块链、智能合约和物联网的供应链原型系统”, *科技导报*, 2017, 35(23): 62-69.

[6] Nakamoto Satoshi, Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008.

[7] 杨保华, 陈昌, 《区块链原理、设计与应用》, 机械工业出版社, 2016.

[8] N. Szabo, “Smart Contracts,” http://szabo.best.vwh.net/, 1994.

[9] V. Buterin, “A next-generation smart contract and decentralized application platform,” https://github.com/ethereum/white paper, 2014.

[10] 刘德林, “区块链智能合约技术在金融领域的研发应用现状、问题及建议”, *海南金融*, 2016(10): 27-31.

[11] F. Reid and M. Harrigan, “An analysis of anonymity in the bitcoin system,” Security & Privacy, 2013:197-223.

[12] I. Miers, C. Garman, M. Green and A.D. Rubin, “Zerocoin: anonymous distributed E-cash from bitcoin,” Proc. Security & Privacy, 2013: 397-411.

[13] 朱岩, 甘国华, 邓迪, “区块链关键技术中的安全性研究”, *信息安全研究*, 2016, 2(12): 1090-1097.

[14] R. Housley, W. Polk, W. Ford, et al. “Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile,” 2002.

朱涛　于 2016 年在上海大学微电子学专业获得博士学位。现任中国银联股份有限公司电子支付研究院助理工程师。研究领域为区块链、数字货币, 研究兴趣包括区块链技术应用。Email: zhutao2@unionpay.com

姚翔　于 2015 年在北京邮电大学计算机技术专业获得硕士学位。现任中国银联股份有限公司电子支付研究院助理工程师。研究领域为区块链、数字货币。研究兴趣包括: 密码学。Email: yaoxiang@unionpay.com

许玉壮　于 2017 年在北京航空航天大学计算机科学与技术专业获得硕士学位, 现任中国银联电子支付研究院技术研究员, 研究领域为区块链技术, 研究兴趣包括区块链、密码学、分布式系统。Email: xuyuzhuang@unionpay.com

周钰　复旦大学通信技术专业硕士。现任中国银联电子支付研究院高级主管。研究领域为智能卡、智能终端、区块链和数字货币。Email: zhouyu@unionpay.com