DOI:10.13878/j.cnki.jnuist.2019.05.009

杨晓宙[1]　董学文[2]

基于 Fabric 区块链的智能合约协同开发系统

摘要

针对传统协同开发系统普遍采用“中心化”存储架构带来的单点故障、数据不可信、故障难以追责等安全问题,以及传统协同办公系统仅支持单一企业内部办公的问题,本文借助超级账本 Fabric 区块链技术以及业务流程管理和服务组合技术实现了一款基于 Fabric 区块链的智能合约协同开发系统.系统架构中首先结合传统中心化存储技术和区块链去中心化存储技术,通过将系统核心业务数据信息存储在区块链分布式账本中而把业务流程管理等不重要的数据存储在传统数据库中解决了“中心化”存储管理带来的安全信任问题.其次系统通过结合超级账本联盟链技术提供的企业联盟的特点使得系统可以应用于企业联盟办公中,解决了单一办公的问题.

关键词

Hyperledger;Fabric;区块链;智能合约;协同开发

中图分类号 TP39

文献标志码 A

收稿日期 2019-05-08

资助项目 国家重点研发计划(2017YFB1400700)

作者简介

杨晓宙,男,硕士,工程师,主要研究方向为认知无线网络以及区块链应用技术.xd0yxz@gmail.com

董学文(通信作者),男,博士,副教授,硕士生导师,主要研究方向为无线网络安全、大数据隐私保护以及区块链应用技术.xwdong@xidian.edu.cn

1 华为技术有限公司,西安,710075

2 西安电子科技大学 计算机科学与技术学院,西安,710071

0 引言

协同办公系统作为当今时代各企业组织方便快捷办公的最有效方案,在经过十几年的发展和完善之后,现已是国内以及全世界普遍使用的办公技术[1].随着世界诸多公司对其的投资和研发,办公系统得到了质的飞跃.目前办公系统的类型大致可以分为 2 类:第 1 类是 20 世纪八九十年代由纸质方式的办公转向的智能设备比特数据流方式办公[2];第 2 类是就是结合互联网技术并拥有自动化办公流程的协同办公.第 2 类办公方式也是目前最流行的办公系统类型.但是我们通过对现有协同办公系统的分析,发现有许多不足之处需要改进,主要有:

1)系统针对性过强.现有办公系统都属于企业定制,功能单一架构固定,不适用于企业联盟的办公环境.

2)系统过度中心化,缺乏信任.现有办公系统几乎都是中心化的存储架构,缺乏信任[3].

3)系统数据信息容易丢失和被篡改.现有协同办公系统使用的传统架构存储单一,系统数据容易遭到人为恶意破坏或者系统故障导致系统数据丢失或篡改,系统安全不能保证.

近几年,随着中本聪提出的比特币应用的火爆,区块链技术迅速的进入到人们的视野中.现在,区块链技术[4-7]除了应用于数字货币应用以外,还可以应用到其他领域的研究当中.区块链技术本身是使用现有诸多技术的组合,但它们组合起来的新的技术足以颠覆传统系统体系.区块链是分布式存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式,它的最大特点就是其去中心化分布式账本特点[8].目前已有众多领域通过结合区块链的这一特性应用到他们传统的应用架构当中解决了许多安全信任问题.

为了解决现有协同办公系统存在的以上安全和信任的问题,本文通过使用超级账本联盟链技术、业务流程管理技术以及服务组合技术提出了基于 Fabric 区块链的智能合约协同开发系统.系统结合区块链的去中心存储、信息不可篡改、公开透明以及交易可追溯等特性解决了传统办公系统的安全和信任等问题.系统利用 Hyperledger Fabric 联盟链特有的联盟链特点实现了协同办公系统可以应用与企业联盟办公环境.

1 超级账本 Hyperledger 技术

超级账本 Hyperledger 是 2015 年由 Linux 基金会主办的开源协作区块链开发平台项目,致力于推动跨行业区块链技术的发展[9].项目自起步以来就吸引了众多领域的领军者,其中包括金融、银行、物联网、供应链以及制造等.目前为止项目成员已经突破 200 个,其中 18 个高级会员中有中国企业百度,在 100 多个一般会员中包含了大量中国企业,如华为、小米等.在全球众多企业和组织的共同努力下,超级账本项目得到了飞速发展.

Hyperledger 项目孵化了很多如区块链分布式账本架构、智能合约执行引擎、客户端库、图形界面、实用程序库等一系列区块链技术框架和工具.目前推出的 Hyperledger[10] 框架有 Fabric、Burrow、Grid、Indy、Iroha 以及 Sawtooth.目前推出的 Hyperledger 工具有 Caliper、Cello、Composer、Explorer、Quilt 以及 Ursa.下面着重介绍 Hyperledger Fabric 框架和 Hyperledger Composer 工具.

1.1 Hyperledger Fabric 框架

Hyperledger Fabric 是超级账本的第一个项目,致力于打造一个全社会共同维护的开源区块链的底层框架,它克服了目前公有链项目中吞吐量低、共识效率低等缺陷,使得用户能够方便的开发商业应用.Fabric 项目采用分层模块化设计、支持插拔式共识算法以及成员管理的模块化架构的区块链实施方案.目前 Fabric 支持 Go、NodeJs、Python 以及 Java 多种语言的链码开发,Fabric 目前已经发布了最新的 1.4 版本.为了系统稳定性,本文使用 Fabric1.0 进行开发.其系统逻辑架构如图 1 所示,Hyperledger Fabric1.0 的设计具有模块插件化、充分利用容器技术、可扩展性以及安全性 4 个特点.

图 1 的 Fabric 系统逻辑架构分别从不同的角度进行了划分,架构上层是从应用程序的角度对区块链进行分析,而底层是对区块链服务进行了细化.上层在封装了 APIs 接口的基础上又向上封装了 Golang、Node.js 以及 Java 等语言的 SDK,这样应用开发人员就可以利用 SDK 进行应用程序的开发.由于区块链节点的信任共识时延比较长,事件模块可以通过回调函数实现异步模式的应用程序开发.从应用上层的角度可以分为身份管理、账本管理、交易管理和智能合约.

1.2 Hyperledger Composer 组件

Hyperledger Composer 是超级账本项目的子项目,是一个广泛的开放式工具集和框架,开发人员使用 Composer 可以更加轻松高效的开发区块链应用程序而不需要考虑 Fabric 底层的各种细节问题.有了 Composer 开发工具集后,应用开发人员就可以花更多的时间去考虑应用程序的业务逻辑实现.Hyperledger Composer 支持现有的 Fabric 区块链的基础架构和运行环境,并且可以与现有系统、数据进行集成.

Hyperledger Composer 的整体架构如图 2 所示,超级账本项目对 Composer 的定位就是在 Fabric 的上层,该架构上层部分就是 Composer 应用开发的 4 个组件,分别是域模型文件、交易逻辑脚本文件、访问控制规则文件以及查询文件.域模型文件用于定义业务网络中的所有资产、参与者、交易处理以及事件.交易处理逻辑文件用于细化域模型文件中定义

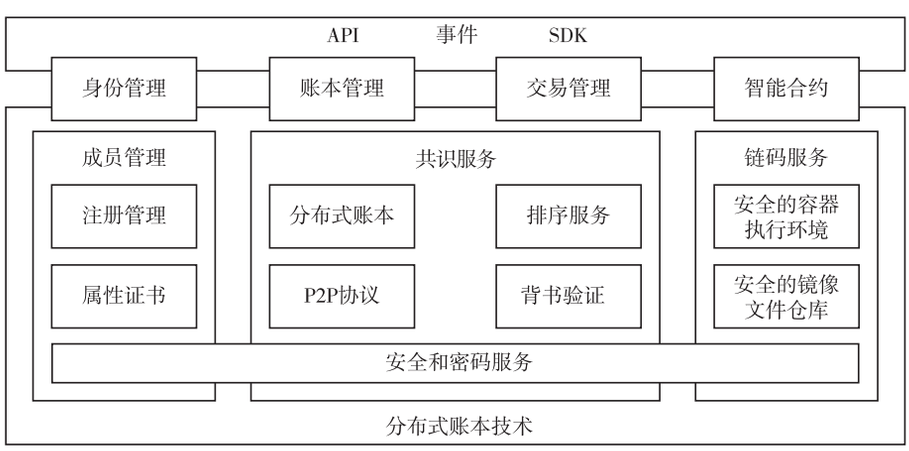

图 1 Fabric1.0 系统逻辑架构

Fig. 1 The logic architecture of Fabric1.0

的交易处理,对具体交易的业务逻辑进行实现,即智能合约中的逻辑处理.访问控制规则文件使用 Hyperledger Composer 提供的访问控制语言来约束用户、参与者对于区块链业务网络、资源、域模型实例的访问权限.查询定义文件使用 Hyperledger Composer 提供了类似 SQL 的 Query Language 来进行符合特定条件的查询.

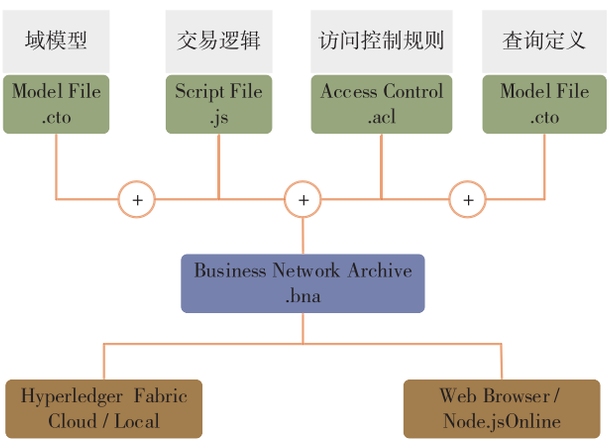

图 2　Composer 架构

Fig. 2　Composer architecture

业务网络通过 4 个组件实现之后打包成业务网络归档文件部署到 Fabric 网络中,然后业务网络中定义的业务逻辑就可以在区块链中稳定调用执行.业务网络归档文件最终会在 Fabric 底层编译转换成智能合约运行在区块链网络中.

2　基于 Fabric 区块链的智能合约协同开发系统架构设计

根据现有区块链应用系统架构并结合现有协同办公系统的平台架构,设计了去中心化群智合约协同开发系统,其整体架构如图 3 所示.系统架构分为 3 层,上层为界面层也称用户交互层,中层是业务网络开发的业务逻辑层,底层则是最重要的数据存储访问层.系统采用如此的分层架构是为了把用户交互与数据存储分离开来,用户交互过程中的用户体验与传统中心化架构一样,只需要通过浏览器登录访问即可而无需考虑底层数据如何存储等.这种结构划分使的整个系统结构清晰、层次分明,可以借鉴到其他的区块链应用系统的设计中.

系统界面层也即用户交互层,主要包含系统各功能模块业务逻辑的浏览器端页面,用户在浏览器

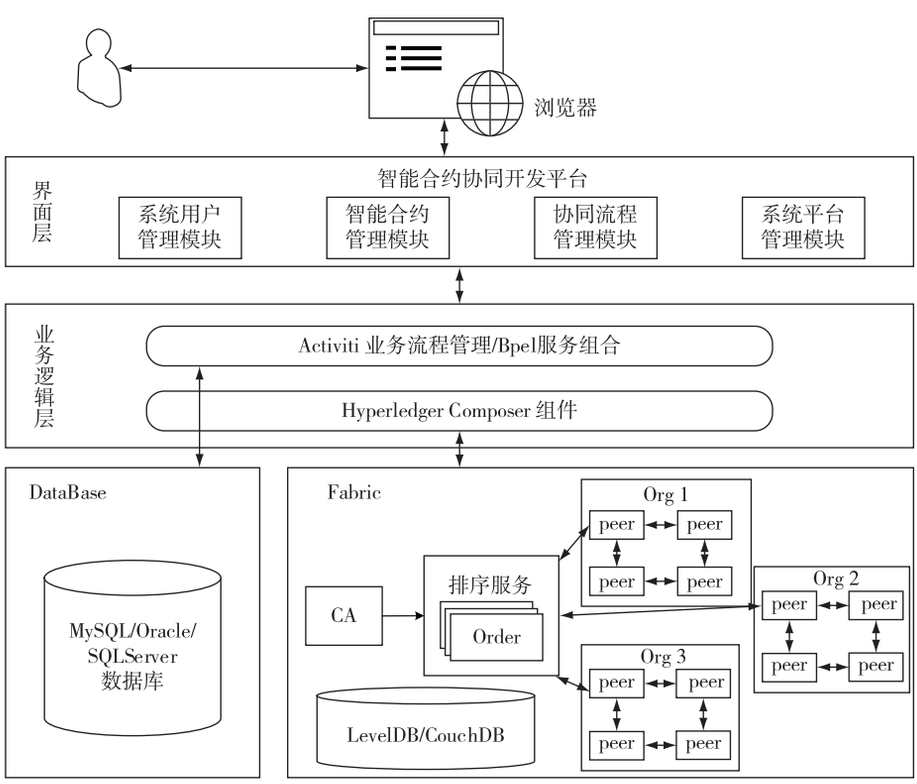

图 3　系统架构

Fig. 3　System architecture

端操作就可以实现底层的业务逻辑服务.用户交互层可以将用户在浏览器端操作的数据转换成虚拟资产或者交易等存储在底层区块链账本中.用户在页面的增删改操作对应底层数据的增删改,但是操作记录会被永久保存;用户在页面的查找操作则是通过系统底层接口获取底层存储信息在前端进行展示.

系统中间的业务逻辑层是系统平台的核心业务层,界面层展示的所有功能模块的业务逻辑需要在该层进行实现.该层主要涉及到两个方面,业务流程管理和区块链业务网络.本层首先基于底层 Fabric 网络使用 Hyperledger Composer 的一系列组件工具对底层业务网络进行设计最终向上提供 REST APIs 服务接口,然后再使用传统业务流程管理以及服务组合技术对业务网络服务接口进行服务编排组合以及流程管理等业务的实现.整个系统属于异构的系统,是 Fabric 区块链与 Web Service 技术等的异构系统.

系统底层是数据存储访问层.DataBase 用于存储系统协同流程管理数据的传统中心化数据库,它可以存储管理不重要的系统工作流程数据,为 Fabric 区块链层减少数据存储压力并提高系统办公效率.Fabric 区块链层主要包括联盟节点的部署以及利用其去中心化存储特性存放系统主要业务数据信息等.

系统用户拥有两种访问区块链的方式,第一种方式是通过 Web 应用平台进行智能合约协同开发操作,这些操作可以实现将智能合约存储在区块链中以及对智能合约的增删改查等;第二种方式可以通过使用 Hyperledger Composer 工具提供的 RESTFul API 服务接口进行操作区块链底层.本系统平台通过对 RESTFul API 服务接口进行集成,为用户提供统一的 Web 系统平台进行区块链操作.

3 基于 Fabric 区块链的智能合约协同开发系统功能模块设计与实现

通过对智能合约协同开发系统业务功能需求的分析,本节对系统业务功能模块进行划分,智能合约协同开发系统的功能结构如图 4 所示.

协同开发系统有 4 个核心功能模块:系统成员模块、协同流程模块、智能合约模块和系统管理模块,其中系统成员模块、智能合约模块和系统管理员模块关联底层 Fabric 区块链存储机制而协同流程模块关联传统中心化数据库存储协同流程资源信息.

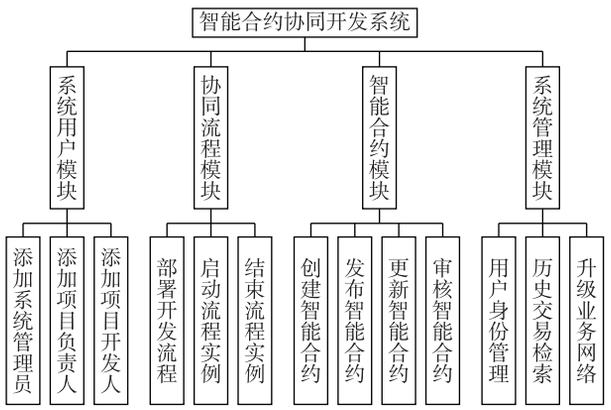

图 4 智能合约协同开发系统功能结构图

Fig. 4 Functional structure of smart contract collaborative development system

1)系统用户模块主要用来向系统中添加系统管理员、项目负责人员和项目开发人员的个人基本信息,包括用户 ID、姓名、所属组织、电话、邮箱以及地址等,同时系统通过设置访问控制规则对系统各类用户进行权限控制.

2)协同流程模块主要用于设计、部署、启动和结束协同开发智能合约的流程,整个系统的协同特性就体现在该模块,系统流程管理数据存储在传统数据库中为系统减压.

3)智能合约模块是系统功能实现的重点,该模块结合协同流程模块实现项目负责人员创建智能合约、发布智能合约的开发任务、项目开发人员更新智能合约以及项目开发人员审核验收智能合约,智能合约模块主要实现智能合约的功能需求完善工作.

4)系统管理模块的功能主要是对系统注册用户进行身份管理、当系统出现问题追责时对系统历史交易信息进行检索查询以及对业务网络进行版本升级等.

通过以上 4 个模块的功能实现了智能合约协同开发系统,整个系统的核心目的就是在各企业组织组成的企业联盟环境中由不同的工作人员组成一个智能合约开发项目组,可以实现协同开发智能合约的任务.通过分析智能合约协同开发系统的整体业务流程,归纳出的系统业务功能用例图如图 5 所示.

根据以上系统业务功能用例图,系统功能可以归纳如下:

1)系统用户可以通过输入用户账户信息进行系统登录.

2)系统业务网络管理员可以注册添加项目负责

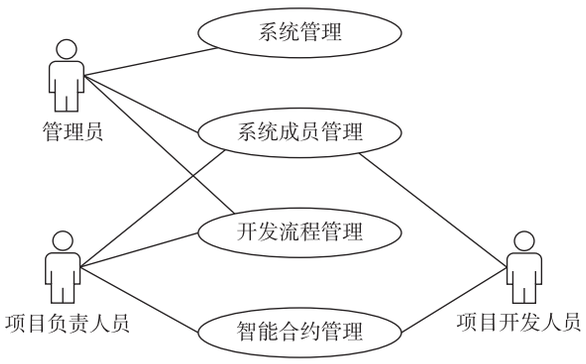

图 5　系统业务功能用例图

Fig. 5　The use case diagram of system business function

人或者开发人员等系统用户.

3)业务管理员可以对系统用户、系统资源等区块链中数据进行增删改查,同时这些操作记录也会记录到区块链中.

4)管理员或者项目负责人用户可以设计、部署或者启动智能合约协同开发流程.

5)项目负责人可以创建智能合约、指定智能合约设计要求以及可以启动一个协同开发流程来发布智能合约开发任务.

6)开发人员通过登录系统查看自己当前开发任务,如果有任务就要根据智能合约详细需求进行合约的开发.

7)项目负责人需要随时查看当前任务并进行任务审核.如果开发人员均按照合约设计要求完成了协同开发任务,则审核通过并且任务完成;如果没有符合要求,则审核不通过并继续协同开发流程.

智能合约系统平台的开发过程广义上分为两部分.第一部分是区块链网络中业务网络的设计,同使用 Composer 工具集实现业务网络定义文件并提供出 RESTFul API 如图 6 所示,该部分主要实现功能模块中的系统用户模块、智能合约模块以及系统管理模块的服务接口.第二部分是使用 Web 应用程序开发框架结合业务流程管理技术和服务组合技术封装组合业务网络 REST API 接口实现系统平台,该部分串联整个系统功能并完成了协同管理模块功能.协同开发智能合约工作流如图 7 所示.

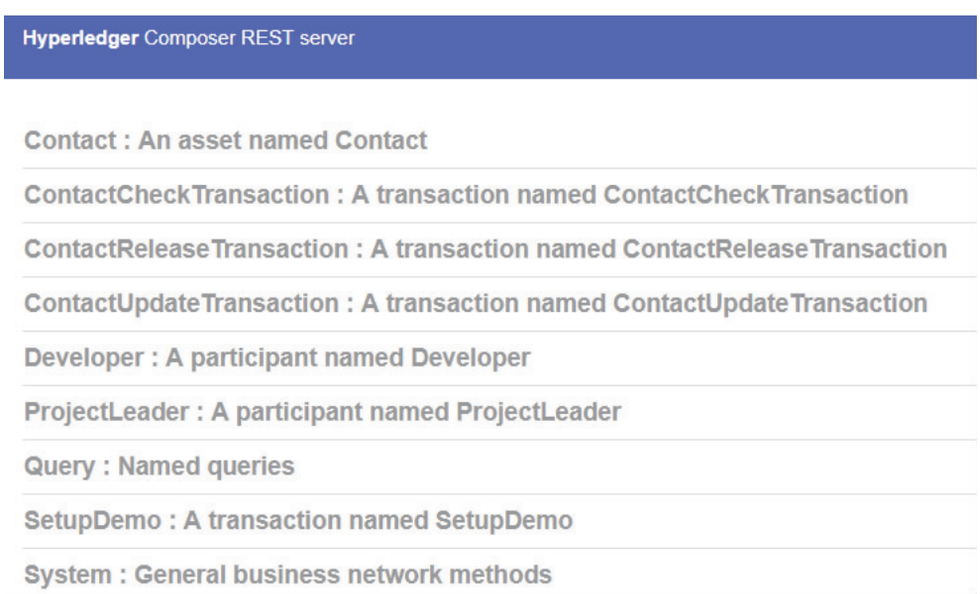

图 6　业务网络 RESTFul API 接口

Fig. 6　The RESTFul API interfaces of business network

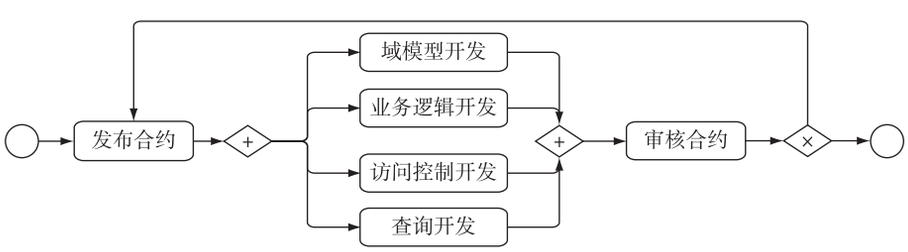

图 7　协同开发智能合约工作流

Fig. 7　Workflow of smart contract collaborative development

4 系统测试

本文通过对智能合约协同开发功能和流程进行测试并且对 Fabric 区块链网络运行情况进行监测和分析,最终证明了本文实现的智能合约协同开发系统的完整性.

4.1 系统功能测试

本节通过模拟实例场景对智能合约协同开发系统的功能协同开发智能合约进行功能和流程测试.如图 8 所示,首先本系统在部署区块链网络时分别设置了 3 个组织(组织可以动态添加),同时在每个组织中部署了 Peer 节点供用户接入;然后通过系统可以由管理员为各组织中的员工进行用户信息注册,图中展示了 3 个组织 Org1、Org2 和 Org3,Org1 中注册了 2 个用户 a 和 b,Org2 中注册了 3 个用户 c、d 和 e,Org3 中注册了两个用户 f 和 g.由于不同用户对系统具有不同的访问权限,而且在智能合约协同开发过程中需要有两种角色,一种是协同开发项目负责人,另一种是智能合约开发人员.图中展示的 Org1 中的用户 a 是项目负责人,3 个组织中的其他用户均为开发人员.

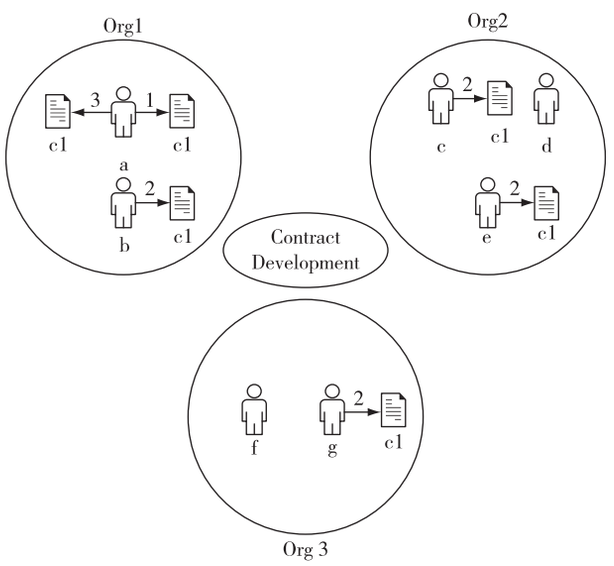

图 8 智能合约协同开发实例

Fig. 8 Example of smart contract cooperative development

智能合约协同开发流程实例以及功能通过图 8 中的编号表示,智能合约协同开发步骤如下;

1)Org1 中的项目负责人 a 新建智能合约 c1,然后设置开发者人员列表为(Org1_b,Org2_c,Org2_e,Org3_g),指定合约开发详细规则并发布智能合约启动智能合约协同开发流程实例.如图 8 中步骤 1 所示.

2)开发者人员列表中的 Org1_b、Org2_c、Org2_e、Org3_g 分别根据合约 c1 开发详细规则更新属于自己开发部分的智能合约代码.如图 8 中步骤 2 所示.

3)当所有开发者用户更新完智能合约 c1 的代码之后就需要 Org1 中的项目负责人 a 对开发完成的合约 c1 进行功能以及漏洞等审核验证.如图 8 中步骤 3 所示.如果审核通过则智能合约 c1 开发完成可以部署到区块链网络中运行,如果审核未通过则需要项目负责人 a 重新执行智能合约开发流程.

通过对智能合约协同开发功能流程以及其他辅助功能的测试,最终验证了系统的功能完整性.

4.2 Fabric 网络监测

智能合约协同开发系统是基于 Fabric 区块链实现的,Fabric 区块链网络中各节点组成大的组织,组织再组成一个联盟.随着系统的运行会伴随着区块链交易的产生,通过在 Fabric 网络之上部署一个 Fabric 区块链浏览器,测试开发人员可以随时查看区块链中的各种信息,例如节点运行信息、区块数量、成功的交易以及区块链网络中部署的智能合约等,图 9 展示了 Fabric 区块链浏览器界面图,测试开发人员可以根据浏览器上的不同标签查看区块链网络中的信息,对 Fabric 网络进行监测.

5 结束语

随着比特币应用的出现以及近几年来区块链技术的发展,区块链已经深入到各行各业的应用当中.目前区块链应用的领域有金融、医疗、物联网、供应链、法律、教育等,但由于区块链技术的发展处于起步阶段,短期内存在落地困难的问题,但长期而言,区块链技术会深刻变革现有的生产关系.当下国内外已经存在了不同领域的区块链应用,它们充分的结合了区块链技术的去中心化、信息不可篡改、公开透明、可追溯等特性,使得应用产品也具有了相关特性,提高了安全可靠性等.本文在国家重点研发计划项目的驱动下提出基于 Fabric 区块链的智能合约协同开发系统,将区块链技术与协同办公系统结合,避免了传统协同办公系统中心化结构带来的诸多安全隐患,系统操作数据以交易的形式存储在区块链账本中保证了数据的安全完整性.

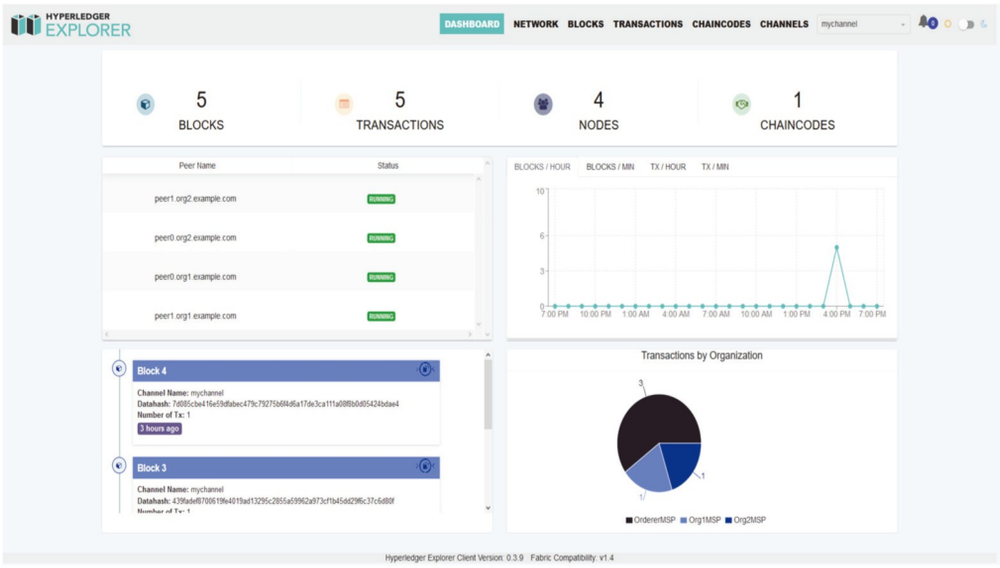

图 9　Fabric 区块链浏览器

Fig. 9　Browser of fabric blockchain

参考文献

References

[1] 陈强,张睿,郑环,等.协同办公平台设计与实现[J].医学信息学杂志,2019,40(1):41-46
CHEN Qiang, ZHANG Rui, ZHENG Huan, et al. Design and implementation of the collaboration office platform [J]. Journal of Medical Informatics, 2019, 40(1): 41-46

[2] 崔娟.浅析 OA 协同办公系统在企业中的应用[J].信息通信,2018(3):181-182
CUI Juan. Brief analysis application of OA cooperative office system in enterprises[J]. Journal of Information and Communications, 2018(3): 181-182

[3] 李展.基于 J2EE 的高校协同办公系统的设计与实现[D].西安:西安电子科技大学,2016
LI Zhan. Design and implementation of college collaborative OA system based on J2EE [D]. Xi'an: Xidian University, 2016

[4] 谢辉,王健.区块链技术及其应用研究[J].信息网络安全,2016(9):192-195
XIE Hui, WANG Jian. Study on blockchain technology and its applications [J]. Netinfo Security, 2016 (9): 192-195

[5] Underwood S. Blockchain beyond bitcoin[J]. Communications of the ACM, 2016, 59(11): 15-17

[6] Dwyer G P. The economics of bitcoin and similar private digital currencies [J]. Journal of Financial Stability, 2015, 17: 81-91

[7] Bonneau J, Miller A, Clark J, et al. SoK: research perspectives and challenges for bitcoin and cryptocurrencies[C]//2015 IEEE Symposium on Security and Privacy, 2015. DOI: 10.13140/rg.2.1.4179.5605

[8] 邹均,张海宁.区块链技术指南[M].北京:机械工业出版社,2016
ZOU Jun, ZHANG Haining. Blockchain technology guidelines[M]. Beijing: Machinery Industry Press, 2016

[9] Cachin C. Architecture of the hyperledger blockchain fabric[C]//Proc of Workshop on Distributed Cryptocurrencies and Consensus Ledgers, Ruschlikon, Switzerland, 2016

[10] Hyperledger Working Group. Hyperledger members[EB/OL]. [2018-03-02]. https://www.hyperledger.org/members

Research and implementation of smart contract collaborative development system based on Fabric blockchain

YANG Xiaozhou[1]　DONG Xuewen[2]

1　HUAWEI Technologies Co., Ltd, Xi'an　710075

2　School of Computer Science and Technology, Xidian University, Xi'an　710071

Abstract　Aiming at the security problems such as single point of failure, data untrustworthiness, failure untrace-

ability caused by centralized storage architecture and the problem that traditional collaborative office system only supports single enterprise internal office,this paper uses hyperledger fabric blockchain technology,business process management technology and service combination technology to implement a smart contract collaborative development system based on fabric blockchain.Firstly,the system architecture combines the traditional centralized storage technology and the blockchain decentralized storage technology.By storing the core business data information in the blockchain distributed ledger and the unimportant data such as business process management in the traditional database,the problem of security and trust brought by centralized storage management is solved.Finally,by combining the characteristics of enterprise alliance provided by hyperledger fabric blockchain technology,the system can be applied to enterprise alliance office,and solve the problem of single office.

Key words Hyperledger;Fabric;blockchain;smart contact;collaborative development