基于区块链技术的扶贫系统的设计与实现

王方红 黄文彪
(浙江工业大学之江学院 浙江 绍兴 312030)

摘 要 在实际业务需求的基础上设计以区块链作为底层架构的精准扶贫系统平台,完成系统的需求分析、总体设计、详细设计以及编码测试。通过智能合约完成对区块链数据的增删改查,Java 后台向下调用平台提供的 RPC 接口,完成对智能合约方法的调用,向上为扶贫机构等提供 restful 接口,方便系统成员使用区块链平台。为了提供系统的安全性,从多个方面提出解决方案。

关键词 区块链 底层架构 精准扶贫 智能合约

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2023.02.054

DESIGN AND IMPLEMENTATION OF POVERTY ALLEVIATION SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY

Wang Fanghong Huang Wenbiao
(*Zhijiang College, Zhejiang University of Technology, Shaoxing 312030, Zhejiang, China*)

Abstract Based on the actual business requirements, this paper designed a precision poverty alleviation system platform with blockchain as the underlying architecture, and completed the system requirements analysis, overall design, detailed design and coding test. Through the smart contract, it completed the addition, deletion, modification and query of blockchain data. Java background called the RPC interface provided by the platform downward, so as to complete the call to the smart contract method. And it provided the restful interface for the poverty alleviation institutions upward, so as to facilitate the use of blockchain platform by system members. In order to provide the security of the system, this paper proposed solutions from many aspects.

Keywords Blockchain Underlying architecture Precision poverty Smart contract

0 引 言

区块链是一组不可变的带时间戳的数据记录,由不属于任何单个实体的计算机集群管理的分布式数据库[1]。这些块中的每一个块都是按时间顺序连接成链,并使用加密算法来彼此保护并绑定。由于它是一个共享且不可变的分布式数据库,因此其中的信息对任何参与方都可以看到。各个节点之间须要相互监督、协同工作,既没有中心权威节点导致的权利集中,也能够避免在去中心化情况下,个别节点的欺诈行为,从而保证数据的安全。也正因其去中心化、不可篡改、可追溯等属性,区块链技术被广泛应用于相互协作、打通数据孤岛等典型场景,在金融、物流、供应链、物联网等产生了极大影响[2-3]。

目前国内外都在积极开展关于区块链网络的应用和研究,但其在精准扶贫方面的实践和认识还比较少。在此将设计开发基于区块链的金融精准扶贫系统,结合区块链技术的优点来解决传统金融扶贫系统中存在的问题,为“区块链 + 精准扶贫”的发展和推广打下坚实的基础,并探索区块链技术在我国金融精准扶贫领域的应用场景,以期为我国金融扶贫攻坚提供支持[4]。

1 智能合约及 Hyperchain 平台简介

智能合约是一段可以运行在区块链平台的分布式

收稿日期:2020 - 05 - 26。浙江省高校实验室研究项目(YB201942)。**王方红**,实验师,主研领域:区块链与数据挖掘。**黄文彪**,实验师。

计算机程序代码[5]。它能够实现价值的存储、传递、控制和管理,为基于区块链的应用提供了创新性的解决方案[6]。如果说数据、网络和共识三个层次作为区块链底层“虚拟机”分别承担数据表示、数据传播和数据验证功能的话,智能合约则是建立在区块链虚拟机之上的商业逻辑和算法,是实现区块链系统灵活编程和操作数据的基础[7]。

Hyperchain 平台架构图如图 1 所示。

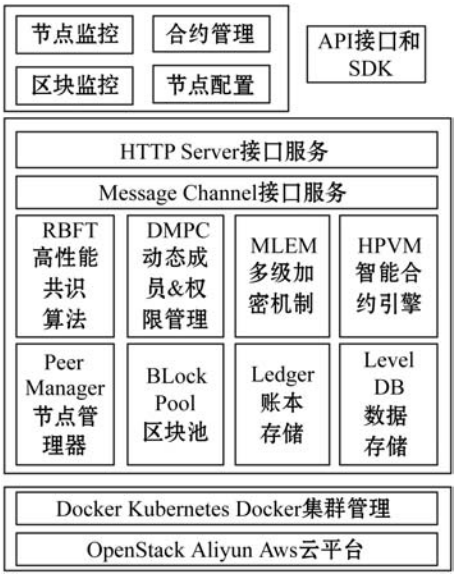

图 1 Hyperchain 平台架构工作流程

2 需求分析与架构设计

2.1 需求分析

用户模块:本系统所涉及到多方协作参与,相关参与方与所能进行的操作如表 1 所示。

表 1 系统角色和相关功能

角色名称	操作描述
平台方	相关信息的审核,服务器监控,及交易线下撮合
申请人	向经办网点申请扶贫贷款或扶贫贴息
经办网点	填写申请信息,上传相关附件,提交相应申请;对通过的贷款信息上传借贷合同
总行零售部	查看贷款申请或贴息申请详情,进行对该申请的审核
市脱贫办	零售部审核通过后的贷款申请和贴息申请会自动转入到脱贫办进行审核
省农业厅	脱贫办审核通过的贴息审核转入省农业厅进行审核
省财政厅	脱贫办审核通过,贴息审核转入省财政厅审核,省农业厅和省财政厅的审核是同级别的,只有两个机构审核全部通过,才会转由省财政厅划拨款项
市财政局	省财政厅确认拨款后,市财政局可以查看该笔拨款和贴息申请详情

权限模块:该系统需要细粒度的权限控制,平台管理员负责审核各个机构注册的管理员,同时分配全量权限,机构内管理员拥有将当前拥有权限再次分配权,如此递推。

扶贫贷款模块:经办网点在页面上填写申请信息,上传相关附件,提交申请,并在页面上查看小额贷款台账列表(列表的数据支持状态筛选和分页浏览),点击单行数据,查看贷款申请详细信息,并查看当前申请状态(如果被拒绝,则显示状态和拒绝理由)。总行零售部登录查看台账详情时,进行对该申请的审核,如果拒绝,须要填写拒绝理由。

扶贫贴息模块:由经办网点成功发起的贴息申请会以贴息人员汇总表的形式呈现给审核机构(总行零售部、脱贫办、省农业厅和省财政厅、市财政局)。点击列表单行,显示贴息详细信息和贴息审核流程。

2.2 架构设计

逻辑结构:为了保证扶贫系统中数据的安全性和高效性,本扶贫系统结构主要分为四层,如图 2 所示。

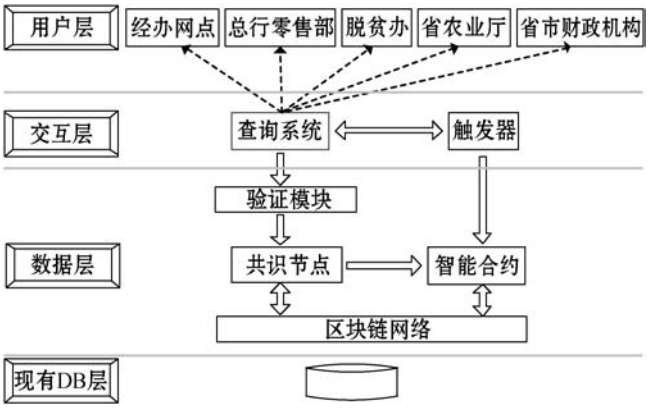

图 2 系统结构模型

物理结构:参与人员通过防火墙接入扶贫系统前置负载均衡器访问应用系统,节点间形成 P2P 网络进行节点间通信,如图 3 所示。

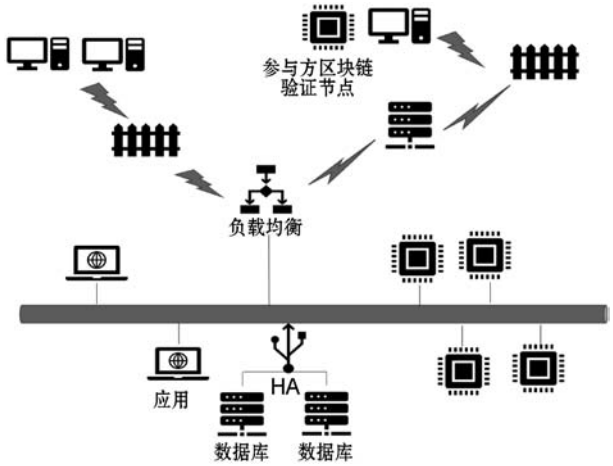

图 3 物理架构图

数据架构:Hyperchain 有关于数据架构的设计图如图 4 所示。

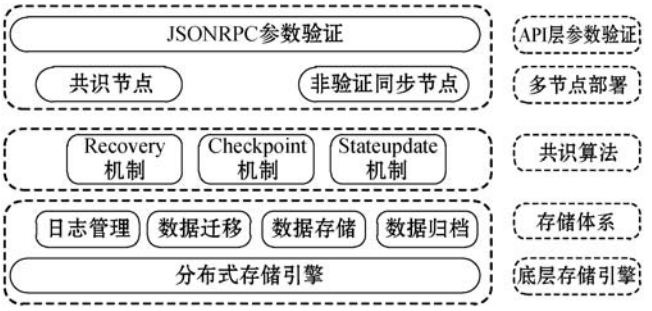

图 4　数据架构图

整个数据架构自底向上可以分为以下几层:

(1) 最底层的存储引擎支持海量存储和数据灾备。

(2) 存储体系保证数据安全存储和历史数据归档。

(3) 强一致的算法保障数据一致性。

(4) 多角色的节点备份及部署支持多用户大并发和数据实时备份和恢复。

(5) 全方面的参数验证支持异常数据过滤。

3　核心模块设计与实现

3.1　智能合约设计

智能合约设计是区块链系统中非常重要的环节,须要确定哪些数据上链以及合约对外接口,并留下数据埋点,用于后续合约升级。类比于数据库,智能合约提供的结构体相当于数据库表,mapping 映射关系相当于外键关联,上链的时候,预留 extra 字段,用于后续的扩展[8]。

1) mapping 设计:类似于 Java 中的 Map,存储的是键值对,表 2 是本系统合约涉及到的部分 mapping。

表 2　合约主要的映射关系

属性	名称	关系说明
_hyperUserAddress2HyperUser	用户信息映射表	用户区块链地址到用户信息结构体的映射
_opId2AuditOperation	审核表操作流水映射表	审核表到操作流水结构体的映射
_auditId2Audit	审核表映射表	审核表 id 到审核表结构体的映射
_discountId2DiscountStaff	贴息人员映射表	贴息表 id 到贴息人员结构体的映射

当需要双方关联且有数据的时候,我们采用两重映射,如贴息状态到趣链用户地址到贴息人员汇总表主键数组映射,mapping(uint => mapping(address => uint[ ]))_loanState2hyperUserAddress2DiscountStaff;即表示该关系类型。

2) 合约方法调用:与合约部署类似,也需要使用公私钥对交易进行签名,然后调用相应的 json-rpc 接口,完成合约方法调用。合约部署和合约方法调用都属于区块链平台上面的一笔交易,需要平台各节点达成共识,才算调用成功。合约方法的调用流程如图 5 所示。

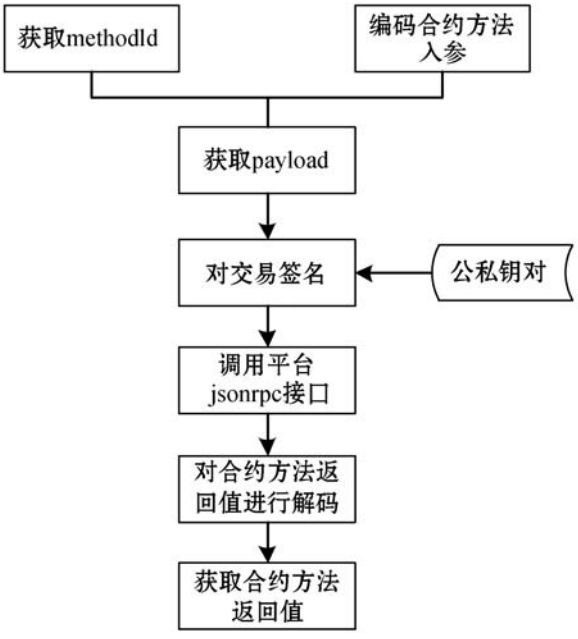

图 5　合约方法调用流程

对要调用的合约方法名做一次 SHA3-256 哈希,取哈希结果的前八个十六进制字符作为 methodId。另外,合约方法的入参也需要经过特殊的处理,按照一定的规则编码成二进制串,用十六进制表示。methodId 和合约方法入参编码而成的十六进制串组合在一起,就是交易信息中的 payload。

3) 合约升级。合约升级分为以下两种情况:

(1) 不须要修改原先已经定义好的数据结构,包括结构体、数组等,而是在已经定义好的成员变量后面新增成员变量,包括或者不包括修改了合约方法。

(2) 修改了合约数据结构。

3.2　操作流水可追溯

不同角色对贷款申请表(或贴息)的每一步审核操作会记录(操作时间、操作用户、操作类型、操作结果)在区块链中,每个用户都能查看到该笔申请(或贴息)的整个操作流水,并在页面上给出直观的体现。

以政府和银行分别为两条主线,可对扶贫资金进行可追溯查询,如图 6 所示,根据每笔扶贫款项的上链 Hash 等数据,可以可视化地精准定位每一笔扶贫款项

的具体流向。

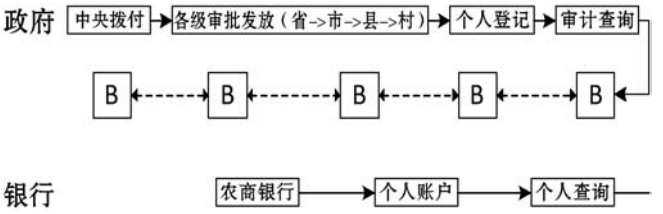

图 6 资产的追溯流程

3.3 数据隔离

不同经办网点上传的数据是相互隔离的，上层机构能看到所有的记录，但是不同经办网点只能看到自己上传的数据，无法看到其他网点的数据。

上一级审核未完成前，数据不会到达下一级。当上一级审核结束，数据同步到其他节点，下一级才有权限读取。

3.4 数据共享和自动同步

当脱贫办贴息审核通过进行确认的同时，相同界面展示多个参与方（省财政厅、省农业厅）的办公电脑同时弹出审核通知，两边办公人员同步进行审批。

省农业厅及省财政厅同时登录查询数据，展示数据详情界面，以及当前审核状态，所作更改流入区块链，分发到其他节点。

传统的办公模式中，每个机构都是独立不互联的，通信通过纸质文件的形式在各个机构之间传递。

接入区块链后，每个机构一个独立节点，各个机构只需要在自己的节点上进行数据的读取和存储，节点之间通过区块链自动进行数据同步和共识，打破了机构之间的通信屏障，既保证了数据一致性，又得到了数据读取的高效性。

4 系统测试

本项目是基于区块链的 Web 应用系统，通过智能合约，改进现有流程和处理逻辑，与传统的 Web 项目的测试流程不同，需要先进行需求分析、评审，确定需求后，开始做系统设计，包括智能合约设计和业务流程设计，同时评审测试用例。

4.1 用例测试

基于测试用例的开发模式，有助于在编写时的逻辑判断，以及开发人员的自测，好的测试用例需要覆盖各种边界问题，便于检测系统可能存在的问题。

图 7 为系统部分测试用例的展示，以思维导图的形式对外提供，方便测试流程和验收。

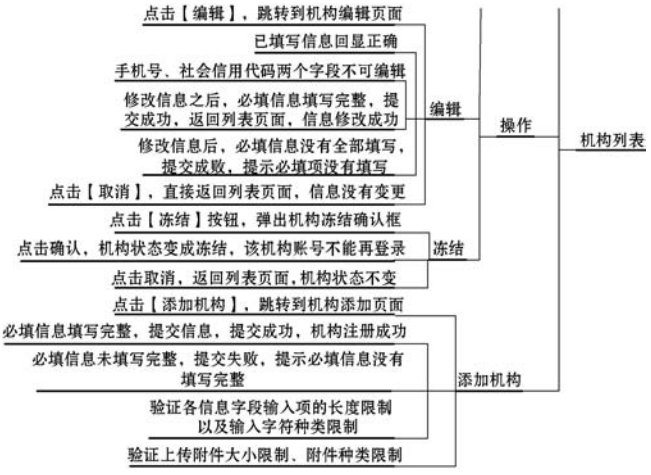

图 7 区块链精准扶贫平台部分测试用例

4.2 压力测试

合约测试和接口测试之后，须要对系统进行一轮压测，检测系统的吞吐量。压测工具选择的是 jmeter，Apache 的一个顶级开源项目，功能很强。下面展示的是录入交易确认信息接口的压测数据。应用服务采用 4 核 8 GB 配置，区块链节点同样采用 4 核 8 GB 配置。压测时开启 200 个线程，持续时间是 2 分钟。图 8 是报价信息录入接口的压测数据，可以看出，在这种情况下系统的 TPS 是 73.3，吞吐量并不高。

# Samples	Average	Median	90% Line	95% Line	99% Line	Min	Max	Error %	Throughput	Received K...	Sent KB/sec
5287	4681	3405	5405	10178	40311	368	40645	0.00%	41.9/sec	12.09	0.00
5287	4681	3405	5405	10178	40311	368	40645	0.00%	41.9/sec	12.09	0.00

图 8 区块链精准扶贫平台部分测试

压测前，应用服务器内存使用率 60.4%，CPU 使用率 1.1%。区块链服务器内存使用率 60.8%，CPU 使用率 1.5%。

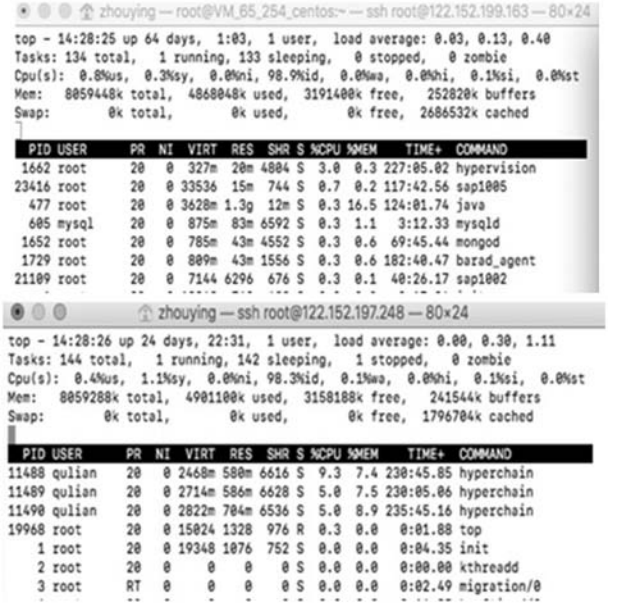

图 9 压测前服务器内存、CPU 使用情况

压测时，应用服务器内存使用率 61.2%，CPU 使用率 38.8%。区块链服务器内存使用率 98.4%，CPU

使用率47.1%。

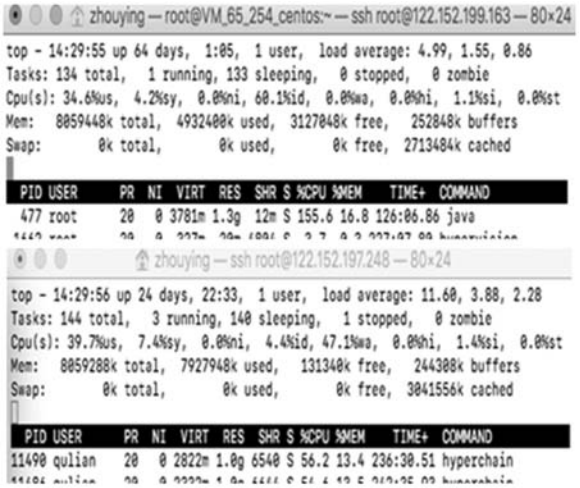

图 10　压测时服务器内存、CPU 使用情况

所以,压测使用的区块链服务器的内存大小是主要瓶颈,如果使用16 GB 大小的内存,压测的 TPS 将有一定程度的提高。

4.3　区块链扶贫系统与同类型系统对比

将区块链扶贫系统与同类型系统对比,如表3 所示。

表 3　区块链扶贫系统与同类型系统对比

扶贫方式	资金全程监管程度	扶贫流程透明度	贫困户隐私保护度	系统稳定性	系统高效性	系统成本
区块链精准扶贫	高	高	高	高	高	低
银行扶贫	中	低	低	中	中	高
政府政策扶贫	低	中	中	低	低	低
互联网扶贫	中	高	中	高	高	中
公益扶贫	高	高	中	中	低	低

由表3 可知,区块链精准扶贫方式保证金融数据不易被修改、系统流程透明、扶贫用户隐私难被泄露、扶贫资金全程监管、金融服务效能高等。尤其是在对贫困户的隐私保护上,由于将对每个贫困户的操作转为对一个地址的操作,可以有效保证贫困户隐私不被泄露。

5　结　语

本系统为了解决传统扶贫系统中存在的数据风险和信息流动问题,创新地采用区块链作为信息的载体。区块链是近几年流行起来的一种分布式数据存储技术,具有可追溯、防篡改、隐私保护、数据透明且安全性高的特点。通过得到的数据分析结论以及与同类型系统对比,得出了本系统具有效率高、易监管、隐私保护强的特点。由于区块链较高的金融属性,金融行业逐步会加大对区块链技术应用部署的投入,未来会看到区块链与更多的金融场景结合落地。但区块链始终只是技术,只有当技术应用到实地场景的时候,才能最大限度地发挥其价值。

参　考　文　献

[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] 胥爱欢,李红燕. 区块链技术在我国金融精准扶贫领域的应用[J]. 金融理论探索,2017(5):22 – 28.

[3] 周立群,李智华. 区块链在供应链金融的应用[J]. 信息系统工程,2016(7):49 – 51.

[4] 孙建钢. 区块链技术发展前瞻[J]. 中国金融,2016(8):23 – 24.

[5] Pilkington M. Blockchain technology: Principles and applications[J]. Research Handbook on Digital Transformations, 2016,32(2): 235 – 233.

[6] Swan M. Blockchain: Blueprint for a new economy[M]. Sebastopol:O'Reilly Media,Inc.,2015.

[7] 钱卫宁,邵奇峰,朱燕超,等. 区块链与可信数据管理:问题与方法[J]. 软件学报,2018,29(1): 150 – 159.

[8] Naceur S B, Zhang R X. Inequality and Poverty: Some international evidence[J]. Financial Development,2018,14(3):18 – 27.

(上接第 258 页)

[22] Hochreiter S, Schmidhuber J. Long short-term memory [J]. Neural computation, 1997, 9(8): 1735 – 1780.

[23] Cho K, Van Merrienboer B, Gulcehre C, et al. Learning phrase representations using RNN encoder—decoder for statistical machine translation[C]//Empirical Methods in Natural Language Processing, 2014: 1724 – 1734.

[24] Greff K, Srivastava R K, Koutnik J, et al. LSTM: A search space odyssey [J]. IEEE Transactions on Neural Networks and Learning Systems, 2017, 28(10): 2222 – 2232.

[25] Shen Y,Tan S,Sordoni A,et al. Ordered neurons:Integrating tree structures into recurrent neural networks[C]//7th International Conference on Learning Representations, 2019.

[26] Mirsamadi S, Barsoum E, Zhang C, et al. Automatic speech emotion recognition using recurrent neural networks with local attention[C]//International Conference on Acoustics, Speech, and Signal Processing, 2017: 2227 – 2231.

[27] Bahdanau D,Cho K,Bengio Y. Neural machine translation by jointly learning to align and translate[EB]. arXiv:1409.0473,2014.

[28] Lin Z H,Feng M W,Santos C N,et al. A structured self-attentive sentence embedding[EB]. arXiv:1703.03130,2017.