

基于区块链的红黑名单共享管理系统

曾光辉, 高一然

(厦门国信信用大数据创新研究院, 福建 厦门 361009)

摘要: 目前, 从国家到各地市的红黑名单归集采用中心化、层层直报的形式, 存在数据共享不充分、同步性较差、查询应用不方便等问题。为改进当前我国红黑名单在归集应用存在的问题, 基于区块链技术, 构建基于区块链的红黑名单共享管理系统。该系统依托区块链去中心化、可靠数据库、可追溯性等特点, 将国家、各省构建为主链, 省内各地市构建为侧链, 利用消息服务总线解决主侧链之间的互通, 形成覆盖国省市三级的、业务完备的信息化系统。从而解决红黑名单共享难题, 提升红黑名单利用效率, 助力社会信用体系建设。

关键字: 红黑名单; 区块链; 共享管理; 数据库; 信用信息; 数据共享

中图分类号: TP399

文献标识码: A

文章编号: 2095-1302 (2020) 08-0066-05

0 引言

红黑名单本质上是一种名录, 包括红名单和黑名单。具体而言, 红黑名单是指行政机关、司法机关、行业协会、企业等社会组织依照法律、行政法规等法律依据, 将诚实守信、严重违法失信的自然人、法人或其他组织的信息进行归集后形成的, 并向社会公示的名录或数据库。红黑名单为行业的监管起到了示范作用, 是信用监管的有效手段, 对构建社会诚信体系以及促进社会文明进步起到了重要的作用。

当前, 红黑名单信息采用文件报送或名单库形式归集到中心化的信用信息系统, 普遍存在以下问题。

(1) 数据共享不充分。不同的行政管理领域缺乏纵向、横向共享手段, 容易形成“信息孤岛”。

(2) 数据同步性能有待提升。黑名单信息的共享和流转, 因为要人工进行报送操作, 客观上存在时间滞后, 准确性也有影响。

(3) 查询应用不方便。当前红黑名单在“信用中国”或各政府网站上登出, 实际应用时需人工下载并自行查找, 极为不便。

区块链(Blockchain)是分布式数据存储、点对点传输、共识机制、加密算法等多种计算机技术以特定的方式组合的结果。区块链技术的出现, 对红黑名单信息的共享、同步、安全提供了一个新的解决思路。本文以区块链为技术基础, 设计了覆盖国家层面到地市层面的红黑名单共享管理系统。

1 区块链技术

1.1 区块链技术概述

区块链是一种去中心化的、不可篡改的、可信的、分布式账本, 它提供了一套安全、稳定、透明、可审计且高效的记录交易以及数据信息交互的方式^[1]。区块链技术创造了一个不可磨灭的记录, 能抵抗任何一个组织或个人的篡改^[2]。

1.2 区块链技术特点

区块链技术具有去中心化、安全可靠、可追溯性等主要特点。

1.2.1 去中心化

与中心化的系统不同, 在去中心化的结构中, 不存在“主控”地位的节点。区块链系统中, 每个节点都是平等的, 系统决策由所有参与节点在共识机制(Consensus Mechanism)作用下共同决定^[3]。作为区块链的一种部署模式, 公有链网络中所有参与节点的权利和义务都相等, 任何一个节点停止工作都不会影响系统整体的运行。

1.2.2 安全可靠

(1) 存储方面。区块链系统的数据库采用分布式存储, 每个节点都可以记录整个系统的交易, 当需要变动原始数据时, 需要至少修改 51% 的节点数据。正因如此, 参与系统的节点越多, 数据库的安全性越高, 防御破坏和攻击的能力也就越强。另外, 该类存储机制同样也使得数据不可篡改和不可伪造。

(2) 维护方面。区块链系统中的数据块对系统中所有参与记录的节点进行记录。由于有不只一个节点同时记录, 所以当某一节点遭到损坏甚至直接撤出均不会对整体数据有影响。

(3) 安全加密方面。区块链系统对交易进行签名时采用的是非对称加密技术, 该技术使签名不易被伪造。借助分布式系统各节点的工作量证明机制等共识算法形成强大的算法来防御破坏者的攻击, 保证区块链中的区块以及区块内的交易数据不可篡改和不可伪造, 具有极高的安全性。

1.2.3 可追溯性

在区块链系统中, 一个区块拥有前一区块的一个哈希值, 这种形式就像锁链一环扣一环, 任何数据块均无法单独存在。此外, 区块链数据的存储还带有时间戳, 为数据添加了时间维度。可追溯性另一优点在于便于数据查询, 区块链可利用时间节点筛选数据块, 再进行寻址, 使得速度和效率都大大提高。

1.3 联盟链

联盟链通常会为一个特定的组织或群体所使用。联盟链一个最显著的特点就是各个节点都对应一个实体机构, 任何实体机构节点想要加入联盟链, 需要得到联盟的许可^[4]。联盟链具备区块链多节点运行的通用结构, 适用于多个机构的业务协作。

鉴于红黑名单共享管理系统技术要求的特点: 需要数据库、存在多方写入且利益不一致、不信任第三方、需要系统控制权, 本系统选取联盟链作为底层技术支撑。

2 系统整体架构

2.1 红黑名单管理系统架构

红黑名单共享管理系统的架构包含 5 个层级: 基础资源、

数据源、区块链支撑平台、数据分析应用层服务、服务对象。红黑名单管理系统架构如图 1 所示。

基础资源: 系统的最底层, 包含整个系统部署的物理资源。

数据源: 主要来源于各个政府部门机构提供的可信数据, 区块链支撑系统提供接口接入。

区块链支撑平台: 系统核心部分, 整个数据的流转通过数据支撑层实现, 包括数据源的接入、数据的整合规则制定等。

数据分析应用层服务: 对业务封装, 包括数据的分析引擎、根据信用模型实现的智能合约, 以及提供的黑名单查询。

服务对象: 通过系统提供的接口, 获取黑名单共享数据。

2.2 区块链网络架构

考虑到我国城市众多, 如果国家、省、市均构建一个区块链网络, 将使得整个网络拥挤不堪, 数据过度膨胀, 节点不堪重负。为此, 本系统采用“多联盟链级联”的方式, 搭建区块链网络。

本系统以“多联盟链级联”的形式, 搭建覆盖“国家—省—市”三级的区块链网络。其中, “国家—省”包括了国家级的节点、各个省节点, 形成一个联盟链; “省—市”包含省级节点、省内各地市节点, 形成一个联盟链。这两个联盟链以省级节点作为关联节点, 以消息服务总线技术进行跨链数据同步, 如图 2 所示。以此形成完整的黑名单共享系统。

国家级节点: 该节点拥有最高权限, 可汇聚、查询其他节点的黑名单数据, 并将数据落地。



图 1 红黑名单管理系统架构

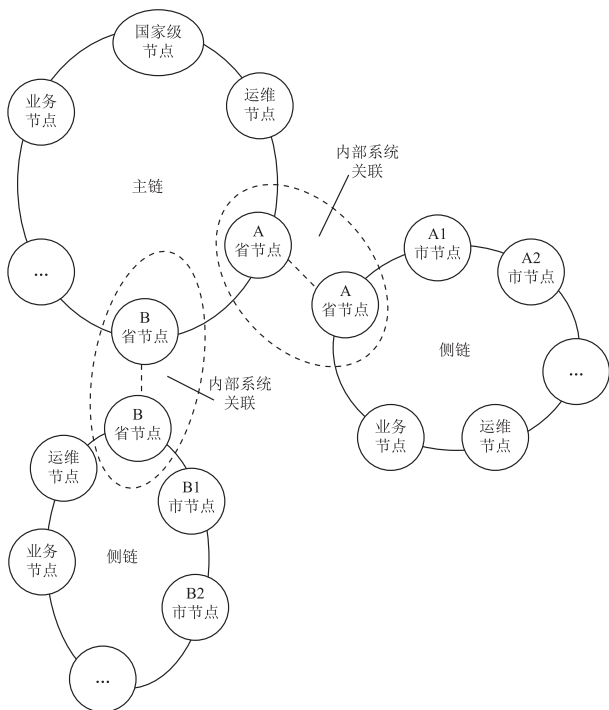


图2 区块链节点架构

省级节点：省级节点具有三重身份。一是在“国家—省”联盟链中，省级节点作为业务节点进行数据上传、查询工作；二是在“省—市”联盟链中，省级节点拥有最高权限，可汇聚、查询其他节点的黑名单数据，并将数据落地；三是作为“国家—省”联盟链和“省—市”联盟链的连接点，部署专用服务器，用作消息分发服务，省级节点内部要将数据落地，并将数据和业务需求转发到另一联盟链上。

市级节点：在智能合约的基础上，进行数据上传、查询工作的节点。该类节点一般是业务部门。

运维节点：对黑名单具有目录控制、有效期限、公开属性、数据校验及加密等信息控制的节点。该类节点一般是系统管理单位中的运维部门。

业务节点：链接对黑名单有业务需求的第三方机构，为其提供查询服务的节点。

3 功能设计

3.1 数据上链流程

数据上链共享流程如图3所示。

数据于部门业务系统生成，通过共享平台 SDK 送到本系统，系统接收到数据后，再进行跨链同步。整个流程具体包括：

- (1) 业务部门生成黑名单数据，按照要求进行打包；
- (2) 调用 SDK，按照预先设定的数据提交方法，向节点传入主体 ID；
- (3) 区块链节点根据主体 ID 查找对应的公钥，并返回 SDK；
- (4) SDK 用公钥加密数据，并用私钥对主体 ID 和加密数据签名；
- (5) 区块链节点收到数据并记账，同时数据也同步至省级节点；
- (6) 省级节点利用消息服务总线同步至主链，使国家主管机构获得黑名单更新信息，至此流程结束。

3.2 数据共享查询

该功能用于向用户提供一个全面的、多角度的黑名单查询功能。可查询当前及历史黑名单、黑名单的历史变动、黑名单的发布情况等。区块链数据共享查询流程如图4所示。

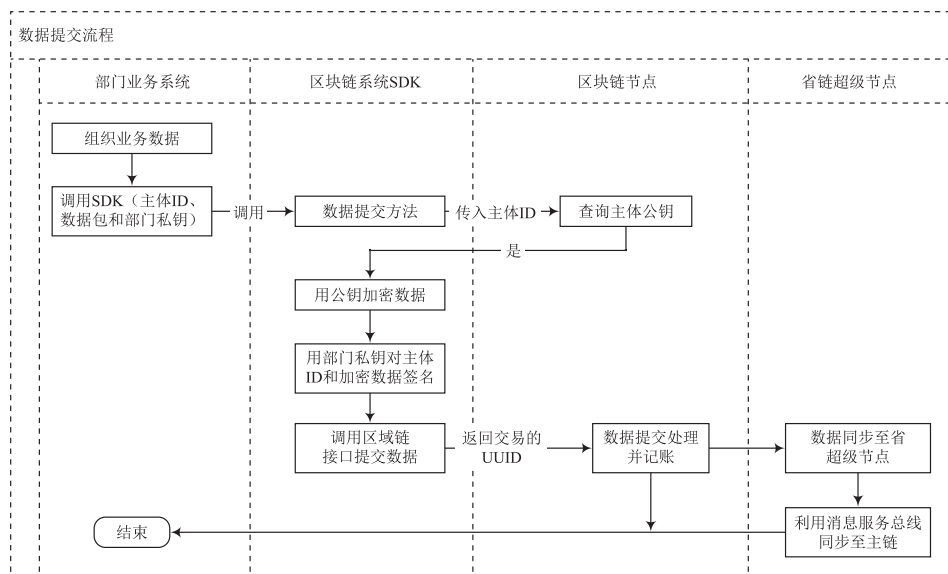


图3 数据上链共享流程

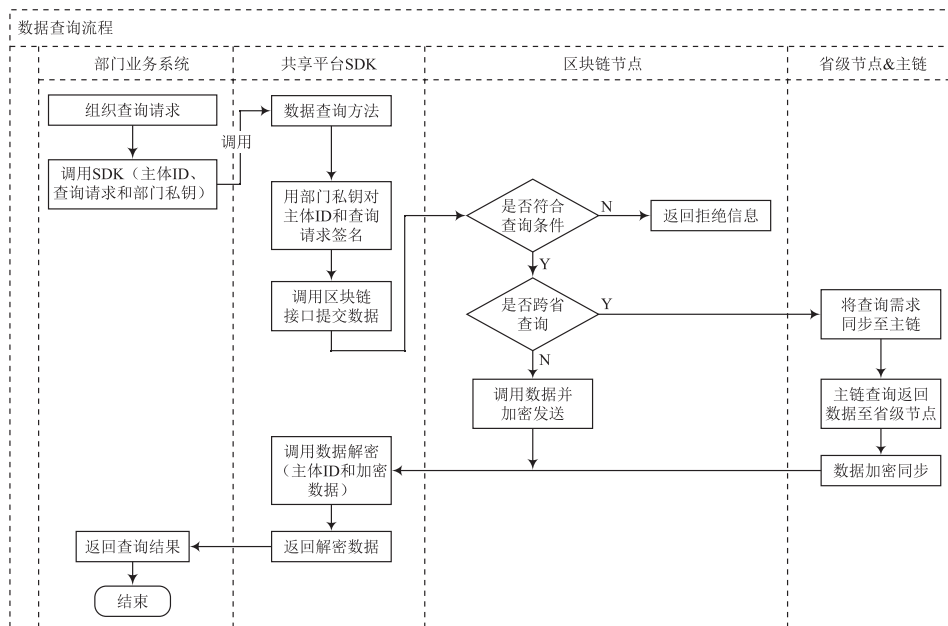


图4 区块链数据共享查询流程

第三方机构通过业务节点查询黑名单数据时，需要用到该功能。一般地，区块链节点在接收到查询需求后，先判断该需求是否符合查询条件，若符合，再判断是否跨省查询，查询到数据之后，将数据返回业务节点。整个流程具体包括：

- (1) 部门业务系统打包查询需求数据；
- (2) 调用 SDK，按照预先设定的数据查询方法，用私钥对主体 ID 和查询需求进行签名，并通过区块链接口提交数据；
- (3) 区块链判断是否符合查询需求，若不符合，则返回拒绝信息，若符合，继续判断是否跨省查询；
- (4) 若非跨省查询，则直接在当前区块链内查询数据，并返回 SDK；
- (5) 若跨省查询，则由省级节点同步至主链，主链查询完成后加密返回至省级节点，进而返回 SDK；
- (6) SDK 返回查询结果至业务系统。

3.3 数据同步应用

该功能用于实现省、市节点和业务节点之间的数据同步。

假定节点 A 产生了数据变动事件，以图 5 所示流程阐述了节点 B 如何正确同步这些数据变动。

3.3.1 智能合约设计

按照需求，本文设计了一套智能合约，该合约维护黑名单数据共享账本，账本记录共享黑名单的最终状态（Status）及事件日志（Event Logs）。在最终状态中记录每条黑名单数据的最新 Hash 值，用于同步节点进行数据对比，从而防止黑名单数据不一致。同时，事件日志记录了所有黑名单数据的变动记录，一条黑名单最终状态数据可能对应多次事件日志。

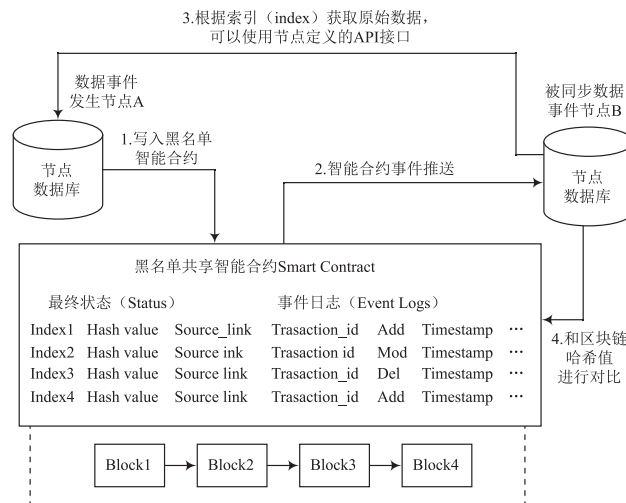


图5 数据同步应用流程

所有节点可以在第一时间获得合约事件推送，用于同步节点数据库，也可以主动到账本定期对账，保证各个节点数据库和区块链账本一致。

3.3.2 标准协作流程

(1) 节点 A 产生了对某条黑名单的数据变动操作，该节点首先生成该黑名单数据的校验 Hash 值，通过智能合约 API 接口写入智能合约中。

(2) 智能合约将这条黑名单状态记录（包括但不限于索引号、校验 Hash 值、原数据获取地址 Source_link 等）写入到一致性账本中，并同步记录了一条操作日志 Event Log。该操作日志被同步到所有区块链网络节点。

(3) 节点 B 收到了这个事件推送，通过原数据获取地址 Source_link，在区块链外通过系统接口获得原数据，并通过

标准的 Hash 算法对原数据计算 Hash 值。

(4) 节点 B 向合约请求这条黑名单数据的最终状态 (Status), 检查与其校验值 Hash 是否一致, 如果一致则说明数据无误; 反之则说明数据状态存在异常, 可能要进行对账处理。

3.3.3 对账处理流程

在某种情况下, 比如某条黑名单数据由多个节点多次修改, 节点 B (同步节点) 未获得最终状态的数据, 此时 Hash 值校验将不一致。节点 B 需要向合约账本追寻与这条黑名单相关的所有事件, 并确定是否遗漏了某次数据变动记录的同步, 此时仅需要按照 3.3.2 节步骤 (3) 和步骤 (4) 操作即可完成状态同步。

4 结 语

随着国内外对区块链的研究与应用, 区块链在金融、服务业等行业的应用更加广泛。本文利用区块链的分布式、可靠数据库、安全可信等特点, 构建了基于区块链的红黑名单共享管理系统, 解决了以往中心化系统中数据共享不充分、同步性较差、安全性较差等缺陷。本文主要介绍底层架构, 实际应用中, 前端功能可视具体需求进行开发利用。

作者简介: 曾光辉 (1982—), 男, 江西抚州人, 经济学硕士, 厦门国信信用大数据创新研究院院长。

高一然 (1990—), 男, 福建厦门人, 工学硕士, 厦门国信信用大数据创新研究院研究员。

(上接第 65 页)

现了自动跟随行李箱的整体设计, 从而为后续样机制作及试验调试提供了有力保障。

注: 本文通讯作者为刘凯磊。

参 考 文 献

- [1] 叶伟慧, 舒秀兰, 林桂盛, 等. 多模式可载儿童智能行李箱装置优化设计 [J]. 智能计算机与应用, 2019, 9 (1): 127-130.
- [2] 张丰, 李顺霖, 陈仁, 等. 基于自动跟随系统的智能行李箱 [J]. 智能计算机与应用, 2019, 9 (3): 163-165.
- [3] 申耀武, 吴进程, 徐亦昌, 等. 基于单片机控制的智能行李箱设计研究 [J]. 自动化与智能化, 2019, 48 (7): 114-116.
- [4] 赵艳妮, 马顺, 张书源, 等. 基于视觉传感器的自动跟随行李箱

作者简介: 彭秋洁 (1998—), 女, 广西南宁人, 本科, 主要研究方向为机械设计制造及其自动化。

刘凯磊 (1988—), 男, 甘肃嘉峪关人, 工学博士, 讲师, 硕士生导师, 主要研究方向为机电液一体化与智能控制。

参 考 文 献

- [1] 黄步添, 蔡亮. 区块链解密: 构建基于信用的下一代互联网 [M]. 北京: 清华大学出版社, 2016.
- [2] SCOTT Brett. How can cryptocurrency and blockchain technology play a role in building social and solidarity finance? [R]. UNRISD: Working paper, 2016.
- [3] 孙国茂. 区块链技术的本质特征及其金融领域应用研究 [J]. 理论学刊, 2017 (2): 58-67.
- [4] 周辉, 王丽丹, 钟成跃. 区块链助力电子医疗数据共享 [J]. 解放军医院管理杂志, 2019, 26 (7): 645-647.
- [5] 韩家平. 关于加快社会信用立法的思考与建议 [J]. 征信, 2019, 37 (5): 1-6.
- [6] 和亚娟. “黑名单”制度的属性、功能及其边界控制 [J]. 贵州警官职业学院学报, 2019, 31 (5): 27-35.
- [7] 马佳悦. 信用监管视角下的黑名单制度研究 [D]. 苏州: 苏州大学, 2017.
- [8] 佚名. 工信部信息化和软件服务业司参加 2016 云栖大会 [J]. 电子世界, 2016 (20): 4.
- [9] 李仪. 大数据下个人信息共享的风险及其知识治理对策 [J]. 管理现代化, 2019 (6): 79-82.
- [10] 陈平刚, 蔡利华, 王玲丽. 政务大数据支撑的政府舆情预警研究 [J]. 现代商贸工业, 2019, 40 (34): 141-142.
- [11] ELTAYIEB Nabeil, ELHABOB Rashad, HASSAN Alzubair, et al. A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud [J]. Journal of systems architecture, 2020, 102: 101653.

设计 [J]. 智能城市, 2017 (8): 23-24.

- [5] 丁世豪, 李光顺, 刘鹏坤, 等. 基于蓝牙 4.0 的自动跟踪智能行李箱设计 [J]. 电子技术, 2018, 47 (5): 47-49.
- [6] 陈文康. 基于单片机的直流电机调速系统设计探讨 [J]. 电脑编程技巧与维护, 2018 (10): 53-54.
- [7] 陶冶. 基于 Arduino 和 WiFi 的温室监控系统 [J]. 物联网技术, 2019, 9 (3): 23-26.
- [8] 蔡磊, 周亭亭, 郭云鹏, 等. 基于超声波定位的智能跟随小车 [J]. 电子测量技术, 2013, 36 (11): 76-79.
- [9] 曾金, 雷建云. 基于 Arduino 的果园基地环境 Web 监测系统 [J]. 物联网技术, 2016, 6 (8): 60-61.
- [10] 汉俊梅, 郑艳, 张锦枫. 轮罩翻边机变频器定位和跟随控制系统的研究 [J]. 汽车工艺与材料, 2015 (11): 67-72.