

基于区块链物联网的抽样检测平台^①



周寅峰¹, 郁曹一^{2,3}, 梅年松², 张学军¹, 李惠蓉¹, 张自峰¹

¹(盐城市质量技术监督综合检验检测中心 电子电器检验部, 盐城 224056)

²(中国科学院上海高等研究院, 上海 200120)

³(中国科学院大学, 北京 100049)

通信作者: 梅年松, E-mail: meins@sari.ac.cn

摘要: 当前我国的抽样检测平台信息化智能化程度较低导致抽检工作效率低下, 且中心化平台导致了数据可篡改与来源不可信问题. 针对这些问题, 提出了一种面向抽样检测的区块链技术方案, 利用区块链中联盟链多中心化、不可篡改、隐私保护等特点, 结合物联网终端设备对过程的智能感知, 实现了数据安全可信, 过程可追溯可监控的抽样检测平台, 提高了抽样检测的效率与检测结果的可信性, 保障了数据的安全性.

关键词: 抽样检测; 区块链; 物联网; Hyperledger Fabric; 智能合约

引用格式: 周寅峰, 郁曹一, 梅年松, 张学军, 李惠蓉, 张自峰. 基于区块链物联网的抽样检测平台. 计算机系统应用, 2022, 31(6): 75-85. <http://www.c-s-a.org.cn/1003-3254/8517.html>

Sampling and Testing Platform Based on Blockchain and IoT

ZHOU Yin-Feng¹, YU Cao-Yi^{2,3}, MEI Nian-Song², ZHANG Xue-Jun¹, LI Hui-Rong¹, ZHANG Zi-Feng¹

¹(Department of Electrical and Electronic Inspection, Yancheng Quality Supervision Inspection and Testing Center, Yancheng 224056, China)

²(Shanghai Advanced Research Institute, Chinese Academy of Sciences, Shanghai 200120, China)

³(University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: At present, the sampling and testing platforms in China have low degrees of information and intelligence, leading to low sampling and testing efficiency. Moreover, the centralization of such platforms has contributed to data tampering and untrustworthy data sources. In response to these problems, a solution based on Blockchain technology is proposed for sampling and testing. By leveraging the multi-center, tamper-resistant, and privacy-protecting characteristics of the alliance chain in Blockchain and using Internet of Things (IoT) terminal equipment to monitor the process in a smart fashion, this study proposes a sampling and testing platform featuring safe and credible data and a monitorable process, which improves the efficiency of sampling and testing and the credibility of test results and also ensures the security of data.

Key words: sampling and testing; Blockchain; Internet of Things (IoT); Hyperledger Fabric; smart contract

党的十八大以来对政府提出了更高的监管职能要求, 一方面要求政府“放、管、服”, 减轻企业的负担, 另一方面又要求提高对产品质量的有效监管, 实施质量提升工程^[1]. 近年来, 经济的快速发展使得商品的种类数目大大增加, 市场监督抽查规模和抽查范围不断地扩大, 传统依托纸质传输信息的抽样检测模式已无

法满足日益增长的数据量, 无法适应社会发展的要求^[2].

我国目前抽样检测行业整体的信息化程度偏低^[3,4]. 目前国内与抽样检测领域相近的质量管理领域较好地应用了计算机技术、感应技术和数据分析技术等信息技术^[5-7], 但在抽样检测行业信息化程度一直停留在较低的层次, 主要体现在: (1) 抽检效率不高, 检测数据还

① 基金项目: 国家市场监督管理总局科技计划 (2019MK026)

收稿时间: 2021-08-19; 修改时间: 2021-09-13, 2021-09-22, 2021-09-28; 采用时间: 2021-10-14; csa 在线出版时间: 2022-02-21

没有实现自动采集处理,普遍采用人工录入;(2)数据源不可信,采用人工录入数据,出现人为错误的可能性大大增加,另外中心化的系统中管理员权限较大,数据上传后可以被系统管理员轻易地更改。

中国通信标准化协会于2019年11月发布了《“物联网”+“区块链”应用与发展白皮书》指出可利用区块链技术进行数据存储管理,解决传统数据存储模式的中心化、易被攻击篡改等问题^[8]。本文提出了一种基于区块链与物联网技术相结合的抽样检测管理平台,通过物联网终端设备对过程进行智能感知,结合区块链的可溯源、不可篡改等特点,建立数据安全可信,过程可监控的高效抽样检测管理平台。

1 相关工作

1.1 区块链

2008年中本聪在《Bitcoin: A peer-to-peer electronic cash system》中描述了一个去中心化的数字货币系统以及实现它的密码学细节,作为底层技术的区块链开始受到学术界和工业界的追捧。区块链作为分布式的公共账本,具有以下特征:

(1) 去中心化

区块链技术是一个去中心化的信息存储机制,这一特性决定了区块链是由众多节点共同保持和维护数据的。与传统的中心化防伪系统相比,分布式的数据存储使得数据更加安全^[9],即使发生单点故障,通过其他节点保存的副本依旧能维持整个区块链网络,保证数据安全性的同时也保证了完整性。

(2) 不可篡改

数据一旦经由各节点共识后上传至区块链网络,则无法被篡改^[10]。原因在于区块链数据以默克尔树的形式存储在区块体内,数据作为默克尔树的叶节点,两两节点不停进行哈希运算直至只剩一个树根节点,树根节点保存在区块头中,当叶节点保存的数据被篡改时,树根节点发生变化引起区块头的更改,这就导致了整个区块链的变化,而篡改整个网络要付出极大的代价,比如以POW为共识算法的区块链,要掌握全网50%以上的算力才能修改整条区块链。

(3) 去信任化

智能合约是一段运行在区块链系统中的代码,也是一套数字形式的承诺。链上参与方制定智能合约,当合约中条件被触发则合约自动生效并执行,大大减少

中间人为因素所导致的延迟履约甚至不履约,加强诚信合作。

区块链不可篡改的特性可从根本上改变信任方式,解决数据的信任和安全问题。区块链包含3大分支,分别是公有链、私有链和联盟链。公有链项所有节点开放,加入公有链的各个节点都能参与共识,但这会导致Sybil攻击,攻击者大量创建节点干涉整个网络的共识,增加维护系统的开销^[11];私有链仅对个人或单独的实体开放,不具备面向公共的能力;联盟链采用多中心的方式,数据仅在联盟中的机构极其用户中传递,相比公有链的海量节点,联盟链中节点较少,可以较快地达成共识,通过预先设定参与节点、权限控制等方式降低出现Sybil攻击的可能。同时联盟链具备多通道的特点,可将互相信任并可呈现敏感数据信息的节点加入同一通道中,实现隐私保护^[12],种种特点使得联盟链更适合本系统。

1.2 物联网

物联网通过嵌入式计算、嵌入式设备、通信技术、应用程序等基础技术使得普通设备转变为智能设备,实现设备与设备之间、设备与人之间信息交互^[13]。物联网大致可以分为感知层、网络层与应用层。RFID标签、温湿度传感器、全球定位系统等各类物联网终端设备组成的感知层实现对外界的智能感知,采集数据^[14]。然后使用网络层中各类通信技术将感知层采集到的数据传输到应用层。应用层运用大数据、数据挖掘等技术,对海量的感知数据和信息进行分析并处理,实现智能化的决策和控制^[15]。

物联网正将各行各业重塑为以数据分析为导向来制定决策的智能行业,医疗、旅游业、农业等实时数据的获取与分析使得各行各业的从业人员及时有效地制定方案。同时物联网打破一个又一个信息孤岛,以智慧城市为例,城市管理人员和市民可以获取大量城市环境的实时信息,以此为基础综合考量相关数据后采取行动。

1.3 国内外研究进展

自物联网概念提出以来,物联网产业的迅猛发展使得越来越多的物联网设备接入到整个网络中,预计2025年连接数可能达到1000亿,但中心化的数据处理方式使得物联网发展到了瓶颈,万物互联不仅带来了海量的数据还带来了网间协作、隐私与安全、信任机制等挑战,而区块链去中心化、不可篡改、可溯源

等特性,为解决物联网面临的上述瓶颈和挑战提供了新的思路,成为学术界和工业界的焦点。

国内外对于区块链物联网相结合的研究大致分为两类。第一类研究将区块链与物联网相融合,解决物联网发展面临的问题,如海量物联网设备的管理、产生的数据如何存储、不同物联网设备怎样交互数据等,现行物联网架构所采用的中心化管理方式无法有效地处理这些问题。Fakhri等^[16]提出一种基于区块链的物联网设备信息交互方案,将区块链作为信息交互平台实现不同物联网设备的安全交互。Quang等^[17]在研究了海量物联网的管理方式与存在的问题后,提出了基于区块链的可扩展物联网架构以管理大规模物联网设备,结合智能合约实现物联网设备的重配置。Wang等^[18]提出了一种基于分层存储的区块链工业物联网架构以解决物联网数据存储问题,通过区块链连接器与云连接器构建分层存储架构将大部分区块数据存储在云中,而将最新的区块信息存储在工业IoT网络中,实现了在物联网设备中管理与存储区块链。Pavithran等^[19]提出了一种能应用于物联网的基于分层身份加密(HIBE)的保护隐私区块链架构,解决了现存的区块链结构如比特币无法直接融合进物联网中,该方案同时能保证隐私安全。

第二类研究偏向应用领域,将区块链技术 with 物联网技术相结合,取长补短,解决实际生产生活中存在的问题。国内外多数研究人员将目光放在供应链上,将RFID芯片嵌入供应链生产、仓储、运输、销售的全流程中,随时获取当前的数据并监控全流程,同时将数据保存在区块链中以保证数据的可信可溯源。Mo等^[20]选择服装行业作为应用场景,Sun等^[21]选择白酒行业,

Mondal等^[22]以食品供应链为应用场景,结合上述方案实现生产、运输、仓储和销售的全流程透明化管理,保证生产的物品都真实可靠。但供应链监督不只是厂商的责任,需要更有效的监管,且在一些特定的供应链中,如海鲜、农产品等食品供应链对温度环境的要求更为苛刻,所以陈飞等^[23]在设计区块链时引入食品药品监督管理局节点,实现了数据变更服务和食品召回功能。消费者不仅能查询食品的全流程溯源信息,还能在该溯源系统中进行维权投诉。张森等^[12]重点关注冷链运输时的温度信息,提高了冷链物流行业的可信性和数据的安全性。此外, Malik等^[24]引入信誉系统参与整个供应链的管理,再通过智能合约整合资源,提高整个供应链的效率。

2 基于区块链物联网的抽样检测方案设计

2.1 现场抽样

现场抽样环节为抽样检测流程中的先序环节,具体流程为:企业抽样-出证索证-现场取样-现场封样-填写表单-签字盖章-样品运输。在现场抽样环节需要追溯的信息包括:包含企业厂牌、厂名的照片;抽样人员的检验员证、企业营业执照或组织机构代码证等证书;抽样物品的详细信息;抽样单位和检验员信息。在实际过程中,由于沿用纸作为信息传输媒介,不仅效率低下,而且容易在传递过程中丢失。使用NFC标签与区块链技术相结合,在移动端录入抽样单信息的同时,NFC芯片关联样品,最后将所有需要追溯的数据上传至数据库与区块链。在现场抽样环节实现数据来源全部可信,可追溯,提高现场抽样的效率。其现场抽样过程如图1所示。

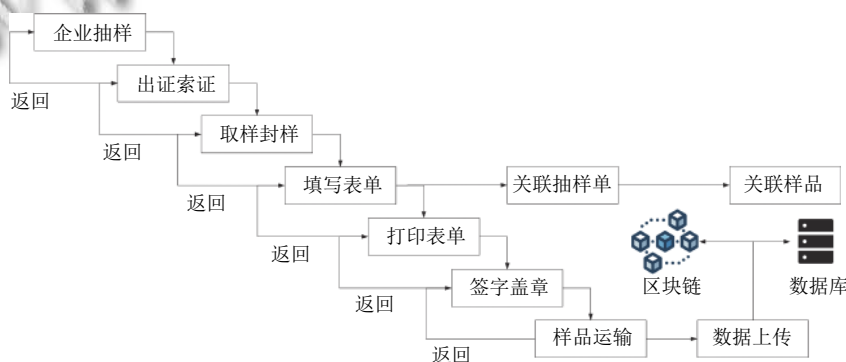


图1 现场抽样过程图

2.2 子样拆分与检验

抽样完成后, 样品会送到当地检验检测机构, 分析样品的成分、结构和性能等. 子样拆分是检验前的必要环节, 样品检验除了对样品整体进行评估检测外, 样品的各个组成部分也需要详细的分析. 因此样品检验

前, 将样品的各个部分依次拆分并通过移动端关联标签, 然后送往不同的检验的部门. 各部门收到子样后读取子样的 NFC 标签, 再读取检验设备的标签, 进入检验记录的界面. 检验完成后在该页面上填写检验项目和检验结构. 其子样拆分与检验过程图如图 2、图 3.

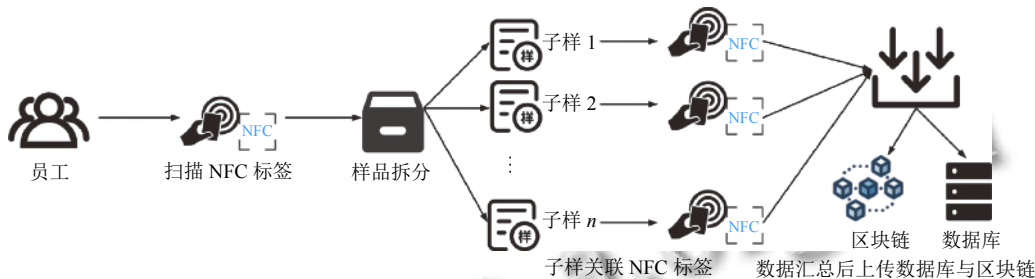


图 2 子样拆分过程图

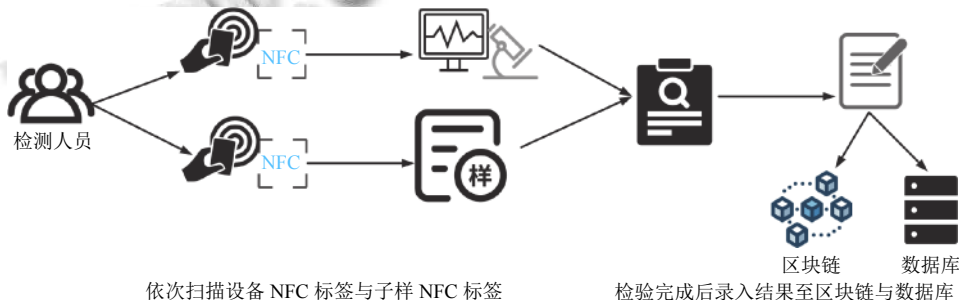


图 3 检验过程图

2.3 人员及设备管理

人员管理在市场监管过程中是很重要的一环. 移动端: 现场抽样, 子样拆分, 检验记录和 设备管理, 各个环节需要安排不同的人员进行操作, 所以要对每个人的权限进行区分. 在 PC 端, 所有人员都可以登录查看检验检测的进度和结果, 但只有管理员可以审核检测结果, 也可以对不同人员的权限进行授权. 人员管理细节分工如图 4 所示.

各子样送到不同部门检测前, 为了保证获取到的检验数据真实可信, 需要扫描检验设备的 NFC 芯片获取仪器的基本信息. 故在仪器正式投入使用前, 需要录入仪器的基本信息: 名称, 规格, 测量范围等, 同时关联到 NFC 芯片, 未关联的设备不能用于检测, 保证检测的结果可追溯. 设备管理过程图如图 5 所示.

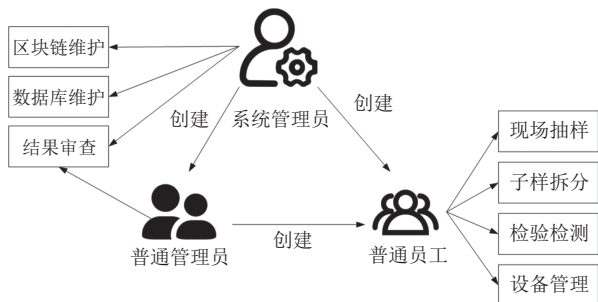


图 4 人员管理分工图

3 基于区块链物联网的抽样检测平台

3.1 存储结构设计

区块链网络的特点决定了无法保存大规模数据, 然而整个抽样检测流程中包含抽样单、详细样品信息、子样信息、检验结果等大量需要存储的数据. 全部存储在区块链中不仅影响上链速度, 而且较高的硬件要求增加了运维成本. 所以在本文中, 将采用区块链与传统关系型数据库相结合的方式^[23], 当各节点采集完数据后, 先将数据经由 SHA256 算法^[25]提取数据摘要并存入区块链网络, 上链成功后区块链网络返回一

个哈希值, 区块链网络中保存该哈希值与数据摘要, 数据库中则存储完整的数据和数据摘要上链后返回的哈希值, 数据库交由市场监管局节点进行维护, 其余节点可以通过区块链中的哈希值在数据库中进行检索来获

取完整数据, 同时根据数据摘要来判断数据库中的数据是否被篡改. 双存储结构不仅能提高整个系统的运行效率, 而且解决了区块链存储数据困难的问题. 存储结构如图6所示.

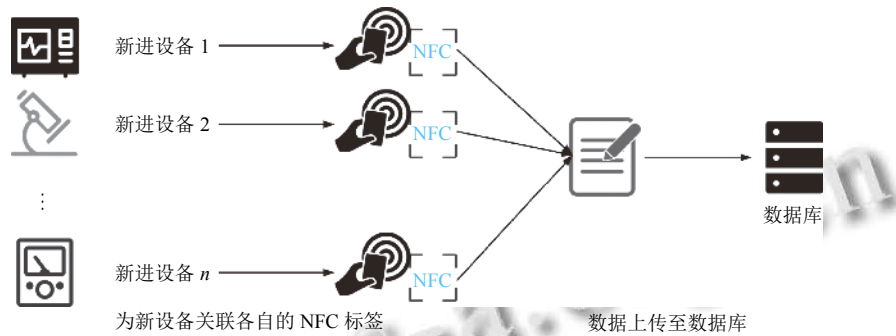


图5 设备管理过程图

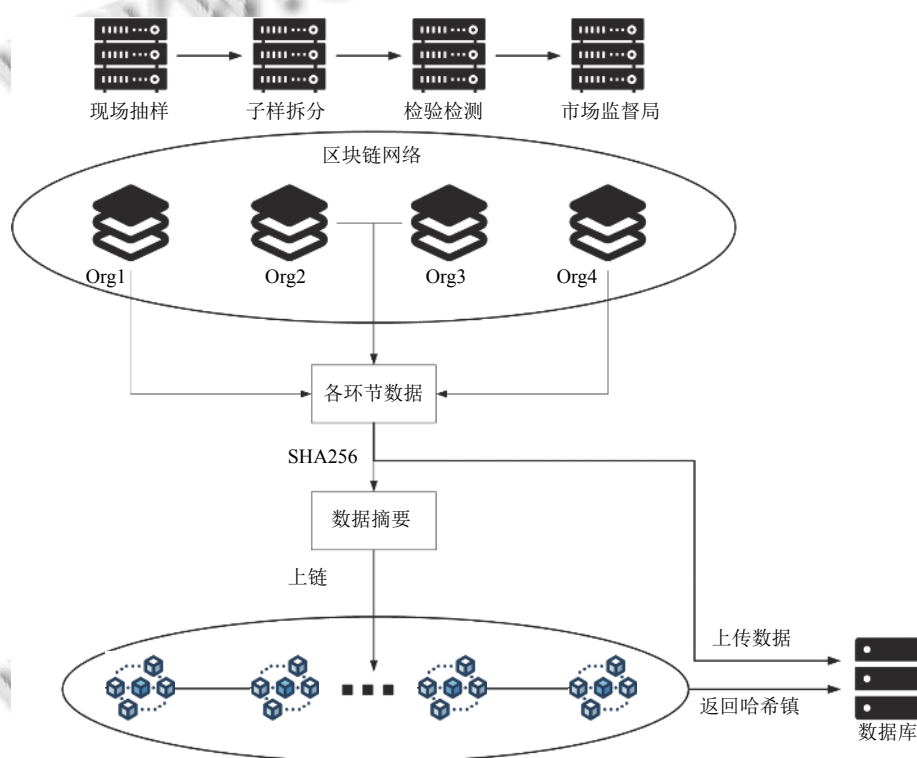


图6 存储架构图

3.2 区块链网络结构设计

抽样检测主要由现场抽样部门、子样拆分部门、检验检测部门和审核结果的市场监管局构成, 每次抽样检测需要四方合作共同完成, 且保证数据可信可追溯. 本系统使用 Hyperledger Fabric 搭建区块链网络, Hyperledger Fabric 是 Linux 基金会下应用最广泛的开

源联盟链项目, 其模块化架构、高度保密性等特点使得用户能够快速搭建联盟链网络^[26], 本系统的网络结构如图7所示.

本平台区块链网络设计中, 以抽样检测的流程作为划分节点方式, 以地级市为例, 各区县检验检测中心以环节划分为现场抽样、子样拆分与检验检测3个部

门, 市场监督管理局除了划分以上 3 个部门外, 单独设置市场监管局节点, 相同部门构成 1 个组织, 市场监管局节点单独构成 1 个组织审核前 3 环节产生的数据. 现场抽样、子样拆分、检验检测与市场监管局 4 个组织处于相互对等的地位, 四方共同参与联盟链的管理. 每个组织内包含多个 Peer, 分别承担背书、与排序服

务节点以及其他组织交互的任务, 但所有节点都需要作为记账节点维护整个账本. 每个组织都有一个为客户生成证书的 Fabric-CA 服务器, 客户端只有向 CA 注册后才能通过 SDK 向 Peer 发起交易. 本系统选择具有高吞吐量易扩展的 Kafka^[27] 作为共识机制, 以提高系统效率.

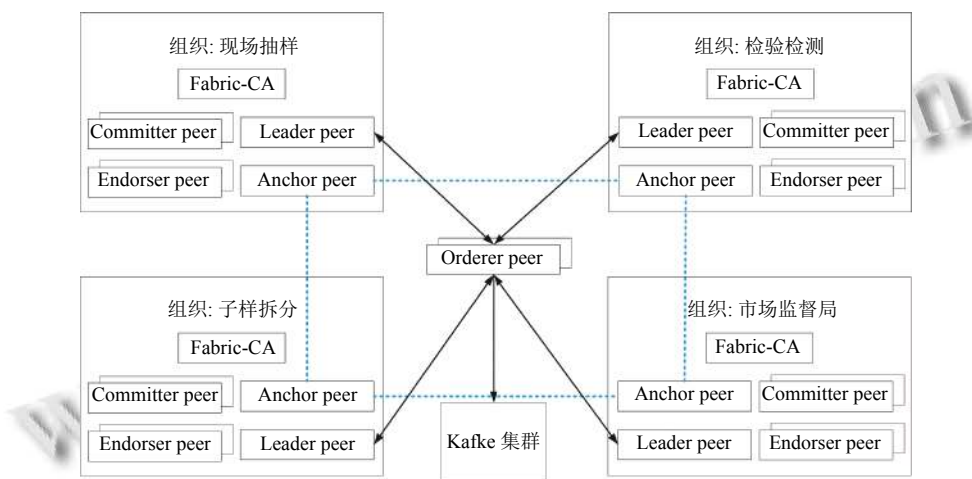


图 7 Fabric 网络结构

3.3 整体系统框架设计

经过第 2 节的抽样检测方案设计与第 3.1 节、

第 3.2 节的存储结构与区块链网络设计, 系统完整框架如图 8 所示.

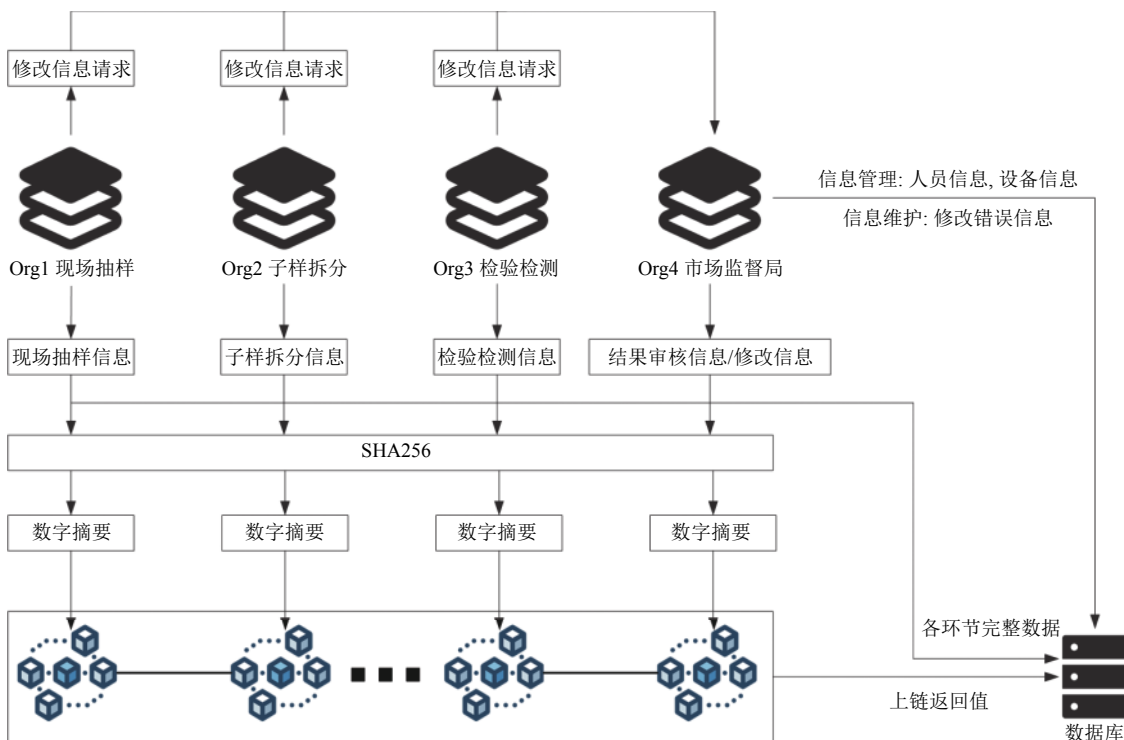


图 8 系统完整架构

引入关系型数据库后解决了区块链存储数据困难的问题,将完整数据存储在数据库中,区块链网络只存储数据摘要。数据库由市场监督管理局节点维护,区块链网络则由各功能对应的节点和市场监督管理局节点一起维护。

现场抽样、子样拆分、检验中心和市场监管局节点信息录入过程相同,以现场抽样为例,将现场抽样环节采集到的数据打包后,先经过SHA256算法获取该数据包的数据摘要并发送到区块链网络,上链成功后返回一条哈希值。此时将返回的哈希值与打包完的数据同属存入数据库中。而市场监管局节点除了录入信息外,还负责处理其余节点更正数据的请求与维护数据库。前3个环节中,由于数据录入量较大,存在操作失误或其他因素导致的信息录入错误,但因为区块链中的数据无法随意更改,所以在本系统框架中将更改数据的权限给予市场监管局节点。若前3个环节中发现录入信息错误,可以向市场监管局节点提交更改信息请求,节点审核通过后由它将更正后的信息上传至

区块链网络与数据库。

本方案基于区块链与物联网技术,将NFC芯片应用于抽样检测流程中的各个方面,从源端采集数据,保证了数据来源可信,数据可追溯。同时减少传统抽样检测过程中人工录入的次数,不仅节约大量的人力成本,而且大大降低了出现人为错误的可能,检验结果审核完成后,相关人员可直接下载检验报告,提高全过程的效率。

4 系统详细设计

4.1 功能模块设计

抽样检测平台是为了保证各环节数据可靠,可追溯,按照抽样检测流程设计满足需求的业务模块。抽样检测平台的业务模块设计如图9所示,分为两大交互端,即移动端和Web端,每端各有4个功能模块,移动端为:现场抽样模块、子样拆分模块、检验记录模块和设备管理模块;Web端为:样品管理模块、检验结果模块、人员管理模块、设备管理模块。每个模块都具备各自的功能,以下对各模块进行简要介绍。

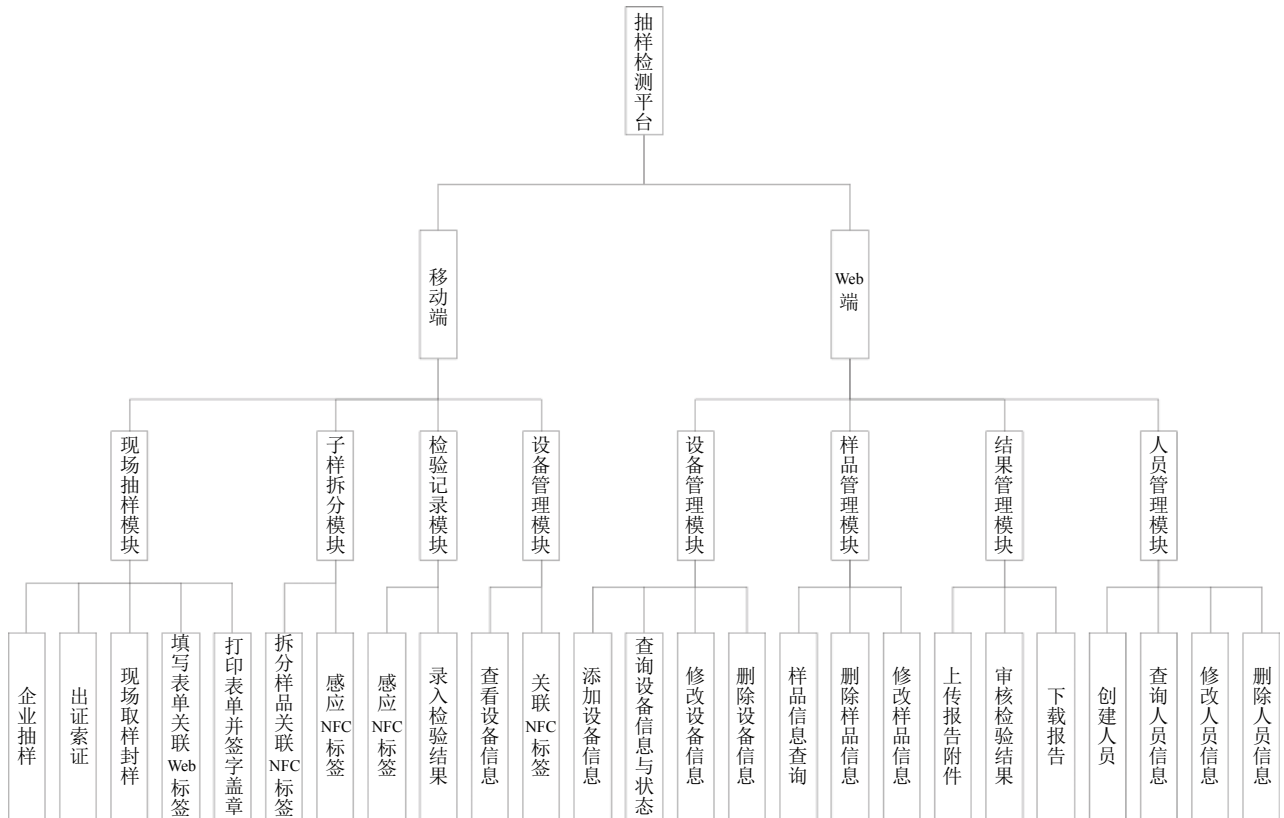


图9 业务模块图

现场抽样模块主要实现现场抽样环节产生的信息录入同时将抽样单关联NFC标签,具体为带有企业厂

牌厂名的照片、抽样人员的检验员证、企业营业执照或组织机构代码证等能够证明单位资质的证书、取样

和封样时的照片、抽样单信息、现场打印后签字盖章的抽样单照片等信息进行录入, 录入抽样单信息后, 需要将该抽样单与 NFC 标签关联。

子样拆封模块主要为拆分后的样品子样关联 NFC 标签, 并将子样名称和 NFC 标签编号录入平台, 便于检验部门后续对样品进行详细分析。

检验记录模块主要是各检验人员收到样品或子样后, 对其进行检验和记录结果, 将结果录入系统中, 检验人员需要依次扫描仪器和样品的标签后, 才能进入检验记录界面, 以保证样品的检验过程都可追溯。

样品管理模块主要对现场抽样后的样品进行管理, 包括对样品信息的查询、修改及删除。在现场抽样环节因为失误造成录入信息有误, 可在这个环节对错误信息进行修改或删除。

检验结果管理模块主要提供给抽样检测管理人员审核流程是否完备, 同时上传报告附件, 报告附件包括检验时的纸质文件, 之后相应人员可以下载检验报告。

人员管理模块主要是对各环节的工作人员进行管理与授权, Web 端管理员创建各环节的工作人员, 并授予权限, 各环节人员只对各自的环节负责, 确保整个过程获取的数据在可追溯的同时可信可靠。

移动端与 Web 端的设备管理模块主要是对检验设备关联 NFC 标签。新设备投入使用前需要管理员在 Web 端录入设备信息, 然后设备管理员通过移动端将设备与 NFC 标签关联, 关联后设备才能投入使用保证所有检验的所有细节都已被追溯。同 Web 端还提供查询、修改和删除功能, 当设备出现问题时, 能立即将设备移除允许使用的序列。

4.2 智能合约设计

(1) 发布修订请求

各组织将数据保存到数据库前, 需要先上传至区块链网络, 然而区块链的特点决定了数据一经上传无法修改。本系统将修改请求通过智能合约实现, 当各个组织发现录入的数据有误时, 调用该合约请求市场监管局节点重新将数据上传至区块链并更新数据库。

修订请求包括修订编号(样品编号+发起组织编号)、发起日期、修改名称、修改内容、监督局节点确认信息、该请求当前状态。将样品编号与发起组织编号合并为一个字段后作为 key, 其余字段作为 value, 具体结构如表 1 所示。

修订请求合约的生命周期如图 10 所示。当发布请求时, 先将 Confirm 值为 false, Current_State 字段置为 Issued。发布修订请求的算法如算法 1。

算法 1. 发布修订请求

输入: 由样品编号与发起组织编号组成的 Issue_ID、合约发布的当前时间 Issue_Time、需要修改的字段 Ex_Name、字段对应的修改内容 Ex_Content

输出: 请求发布成功返回成功标记, 发布失败返回错误信息

1. Function addOrder(Issue_ID, Issue_Time, Ex_Name, Ex_Content)
2. 输入 string 类型的参数实例化结构体 Order
3. orderQuery = GetState(Order.Issue_ID+ Order.Issue_Time)
4. If orderQuery 不为空 then
5. Return 请求已存在, 返回错误信息
6. End if
7. orderkey = CreateCompositeKey("Order", []string{Order.Issue_ID, Order.Issue_Time})
8. orderJSONasBytes, err = json.Marshal(Order)
9. err = PutState(orderkey, orderJSONasBytes)
10. If err != nil then
11. Return 请求提交错误, 返回错误信息
12. Else
13. Return 请求提交完成
14. End if

表 1 合约结构

字段	描述
Issue_ID	修订编号
Issue_Time	发布时间
Ex_Name	修改字段
Ex_Content	修改内容
Confirm	监督局节点是否同意
Is_State	修订请求状态

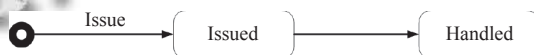


图 10 合约状态图

(2) 审核修订请求

市场监管局节点收到请求后, 核准请求的内容, 如果同意修改, 将 Confirm 字段置为 true, 不同意修改就保持 false, 同时修订请求进入 Handled 状态。

审核修订请求算法如算法 2。

算法 2. 审核修订请求

输入: 由样品编号与发起组织编号组成的 Issue_ID、合约发布的当前时间 Issue_Time、市场监管局节点同意与否 Confirm

输出: 审核通过重新将数据打包上链, 修改数据库内容, 审核不通过返回失败信息

1. Function updataOrder(Issue_ID, Issue_Time, Confirm)


```

2. orderAsBytes = GetStateByPartialCompositeKey ("Order", []string
{Issue_ID, Issue_Time})
3. If orderAsBytes == nil then
4. Return 请求不存在, 返回错误信息
5. End if
6. 将 orderAsBytes 实例化为 Order
7. Order.Confirm = Confirm
8. Order.Is_State = Handled
9. orderkey = CreateCompositeKey("Order", []string{Order.Issue_ID,
Order.Issue_Time})
10. orderJSONasBytes, err = json.Marshal(Order)
11. err = PutState(orderkey, orderJSONasBytes)
12. If err != nil then
13. Return 请求提交错误, 返回错误信息
14. Else
15. Return 请求提交完成
15. End if

```

5 系统测试

在详细设计平台功能模块并编码实现后, 对平台的关键功能进行了测试。如图 11, 图 12 是对于智能合约执行模块的测试, 从发布合约到处理合约, 测试正常; 图 13, 图 14 属于 Web 端的样品管理与测试结果模块,

主要展示抽样样品的详细信息与样品所处的检验环节, 测试正常; 图 15 为移动端主要功能模块, 经测试可以正常使用。

6 结论与展望

本文分析了抽样检测平台的现状, 针对信息化程度不高导致的效率低下问题以及现存的数据篡改与来源不可信问题, 将物联网技术与区块链技术相结合, 设计并实现了一种基于区块链物联网的抽样检测平台。考虑到区块链无法存储大规模数据, 引入传统关系型数据库, 既解决了数据存储问题, 又利用区块链的特点实现了数据的不可篡改。物联网终端设备对于过程的智能感知使得大部分资料不再需要手工摘抄或后补录入, 极大地减少了人为错误出现的频率。即使出现录入数据错误, 通过设计的智能合约发送修改请求, 审核通过后数据再度上链, 兼顾区块链不可篡改的同时保证了数据的正确性。人员权限管理与设备管理使得检验结果的可信程度进一步提高。区块链与物联网技术的结合, 提高了抽样检测工作的效率, 降低了人为错误出现的可能, 也使得检测结果更令人信服。

```

invoke is running addOrder

invoke is running queryOrderByID

query Response:002org120210423 exit
{"Issue_ID":"002org1","Issue_Time":"20210423","Ex_Name":"range","Ex_content":"10000","Confirm":"false","state":"waiting"}

invoke is running updateOrder

invoke is running queryOrderByID

query Response:002org120210423 exit
{"Issue_ID":"002org1","Issue_Time":"20210423","Ex_Name":"range","Ex_content":"10000","Confirm":"true","state":"Handled"}

```

图 11 合约请求通过

```

invoke is running addOrder

invoke is running queryOrderByID

query Response:001org220210422 exit
{"Issue_ID":"001org2","Issue_Time":"20210422","Ex_Name":"I0C","Ex_content":"\u003c100","Confirm":"false","state":"waiting"}

invoke is running updateOrder

invoke is running queryOrderByID

query Response:001org220210422 exit
{"Issue_ID":"001org2","Issue_Time":"20210422","Ex_Name":"I0C","Ex_content":"\u003c100","Confirm":"false","state":"Handled"}

```

图 12 合约请求未通过

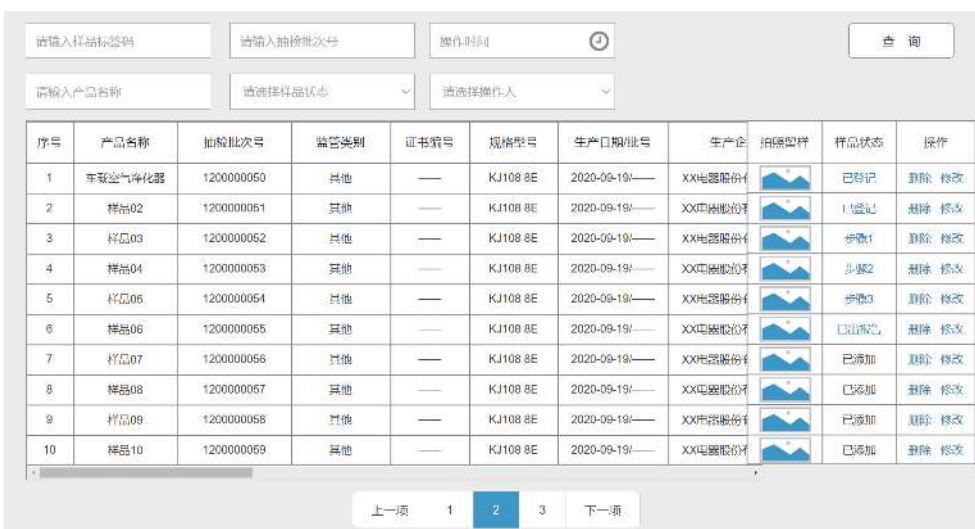


图 13 样品管理界面



图 14 检验信息界面



图 15 移动端主要功能

参考文献

- 1 吴行惠, 康笃刚, 梁娜, 等. 区块链技术在产品质量监管中的应用研究. 网络空间安全, 2018, 9(4): 7–12, 15. [doi: 10.3969/j.issn.1674-9456.2018.04.002]
- 2 盛晓骏. 产品质量监督抽查智能数字化的分析与研究. 价值工程, 2018, 37(28): 1–3.
- 3 高建民. 以技术为支撑实现科学监管和质量提升. 中国市场监管研究, 2018, (8): 21–23. [doi: 10.3969/j.issn.1004-7645.2018.08.006]
- 4 张严方. 我国食品安全监管研究. 中国市场监管研究, 2019, (6): 45–48. [doi: 10.3969/j.issn.1004-7645.2019.06.013]
- 5 张万红, 李斌. 物联网技术在产品质量管理中的应用探究. 物联网技术, 2015, 5(9): 78–79. [doi: 10.3969/j.issn.2095-1302.2015.09.029]
- 6 滕伟黎. 物联网技术在消防装备质量检验中的应用. 消防界, 2016, (6): 164.
- 7 Alam FB, Zohura FT. Automated IoT-based water quality measurement and analysis tool. Proceedings of 2020 IEEE Region 10 Symposium. Dhaka: IEEE, 2020. 1523–1526.
- 8 中国通信标准化协会. “物联网+区块链”应用与发展白皮书. https://res-www.zte.com.cn/bigmediafiles/zte/Files/PDF/white_book/201911071548.pdf.
- 9 陈新林, 王政铭. 一种基于区块链和 NFC 芯片的动态信息防伪技术. 物联网技术, 2018, 8(3): 67–69.
- 10 Dutta P, Choi TM, Somani S, *et al.* Blockchain technology in supply chain operations: Applications, challenges and research opportunities. Transportation Research Part E: Logistics and Transportation Review, 2020, 142: 102067. [doi: 10.1016/j.tre.2020.102067]
- 11 Bamakan SMH, Motavali A, Bondarti AB. A survey of Blockchain consensus algorithms performance evaluation criteria. Expert Systems with Applications, 2020, 154: 113385. [doi: 10.1016/j.eswa.2020.113385]
- 12 张森, 叶剑, 李国刚. 面向冷链物流的区块链技术方案研究与实现. 计算机工程与应用, 2020, 56(3): 19–27. [doi: 10.3778/j.issn.1002-8331.1908-0453]
- 13 Al-Fuqaha A, Guizani M, Mohammadi M, *et al.* Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 2015, 17(4): 2347–2376.
- 14 张玉清, 周威, 彭安妮. 物联网安全综述. 计算机研究与发展, 2017, 54(10): 2130–2143. [doi: 10.7544/issn1000-1239.2017.20170470]
- 15 孙其博, 刘杰, 黎彝, 等. 物联网: 概念、架构与关键技术研究综述. 北京邮电大学学报, 2010, 33(3): 1–9. [doi: 10.3969/j.issn.1007-5321.2010.03.001]
- 16 Fakhri D, Mutijarsa K. Secure IoT communication using Blockchain technology. Proceedings of 2018 International Symposium on Electronics and Smart Devices. Bandung: IEEE, 2018. 1–6.
- 17 Quang LD, Tho LN. Scalable Blockchain-based architecture for massive IoT reconfiguration. Proceedings of 2019 IEEE Canadian Conference of Electrical and Computer Engineering. Edmonton: IEEE, 2019. 1–4.
- 18 Wang G, Shi ZJ, Nixon M, *et al.* ChainSplitter: Towards Blockchain-based industrial IoT architecture for supporting hierarchical storage. Proceedings of 2019 IEEE International Conference on Blockchain. Atlanta: IEEE, 2019. 166–175.
- 19 Pavithran D, Al-Karaki JN, Shaalan K. Edge-based Blockchain architecture for event-driven IoT using hierarchical identity based encryption. Information Processing & Management, 2021, 58(3): 102528.
- 20 Mo B, Su KR, Wei SJ, *et al.* A solution for internet of things based on Blockchain technology. Proceedings of 2018 IEEE International Conference on Service Operations and Logistics, and Informatics. Singapore: IEEE, 2018. 112–117.
- 21 Sun WR, Zhu XH, Zhou T, *et al.* Application of Blockchain and RFID in anti-counterfeiting traceability of liquor. Proceedings of the 2019 IEEE 5th International Conference on Computer and Communications. Chengdu: IEEE, 2019. 1248–1251.
- 22 Mondal S, Wijewardena KP, Karuppuswami S, *et al.* Blockchain inspired RFID-based information architecture for food supply chain. IEEE Internet of Things Journal, 2019, 6(3): 5803–5813. [doi: 10.1109/JIOT.2019.2907658]
- 23 陈飞, 叶春明, 陈涛. 基于区块链的食品溯源系统设计. 计算机工程与应用, 2021, 57(2): 60–69. [doi: 10.3778/j.issn.1002-8331.2007-0324]
- 24 Malik S, Dedeoglu V, Kanhere SS, *et al.* TrustChain: Trust management in Blockchain and IoT supported supply chains. Proceedings of 2019 IEEE International Conference on Blockchain. Atlanta: IEEE, 2019. 184–193.
- 25 Sanadhya SK, Sarkar P. A new hash family obtained by modifying the SHA-2 family. Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. Sydney: ACM, 2019. 353–363.
- 26 Hyperledger. Hyperledger fabric. <https://hyperledger-fabric.readthedocs.io/en/latest/>.
- 27 Kreps J, Narkhede N, Rao J. Kafka: A distributed messaging system for log processing. Proceedings of NetDB. Athens: ACM, 2011. 1–7.