文章编号：2095-2163(2020)09-0055-06 中图分类号：TP399 文献标志码：A

基于区块链技术的医药可追溯系统的研究

冷泽琪，谭振江，周 伟，刘佳琳
（吉林师范大学 计算机学院，吉林 四平 136000）

摘 要：国内医药的溯源服务存在追溯信息完整性不足、追溯范围覆盖不全、追究责任的主体确认困难等问题。本文针对上述问题，在对国内部分医药市场需求调研和分析各领域与追溯产业结合的案例基础上，提出一种基于区块链技术，实现医药全程可追溯的方法。同时，利用区块链的公开透明，不可篡改，无需信任和去中心等优势，构建了基于区块链的溯源系统；结合 RFID 电子标签等技术，解决了传统溯源过分依赖中心以及容易篡改数据等痛点问题，实现了医药的采购、生产、加工到流通的全程可追踪溯源的功能。本文研究的主要内容有利于医药追溯的发展，助力于提升国内的药物质量，避免假药、劣药事件的频频发生。

关键词：区块链；医药；追溯；药物质量

Research on medical traceability system based on blockchain technology

LENG Zeqi, TAN Zhenjiang, ZHOU Wei, LIU Jialin
(School of Computer Science, Jilin Normal University, Siping Jilin 136000, China)

【Abstract】The traceability service of domestic medicine has the problems such as insufficient information integrity, incomplete coverage of traceability, and difficulty in identifying the subject of accountability. In view of the above problems, based on the case of market demand research and analysis of some domestic medicines combined with traceability industry, a method based on blockchain technology is proposed to realize the full traceability of medicine. At the same time, taking advantage of the openness and transparency of the blockchain, non-tampering, no trust and decentralization, etc., a traceability system based on the blockchain is constructed combined with RFID electronic tags and other technologies, solving the problems of traditional traceability about excessive dependence on the center and tamper with data. The system achieves the procurement of medicine, production, processing to circulation of the entire traceability function. This system is conducive to the development of medicine retrospectively and could help to improve the quality of domestic drugs to avoid the frequent occurrence of counterfeit drugs, bad drugs incidents.

【Key words】block chain; medicine; traceability; drug quality

0 引 言

根据市场需求调研得知，从 2008 年到 2020 年，假药、假疫苗等事件层出不穷[1]。国民对医药的需求逐年递增。假药、劣药不仅给成年人带来了短暂性甚至是终身性的伤害，对老人和儿童也造成不可避免的创伤。因此，医药的质量安全成为国民最关心的问题之一，而基于区块链的溯源服务可以解决这一痛点问题。BlockVerify 自 2015 年开始在伦敦提供对奢侈品、钻石和医药的溯源服务，提供的鉴别类型包括伪造品、调换品、被偷商品以及虚假交易[2]；李娜等人设计了一种对数字证书的追溯平台，能够有效地对数字证书和电子签名进行追溯，从而达到防篡改的目的[3]；刘金鹏等人提出一种基于区块链的二维码技术，应用于食品接触材料中塑料包装的溯源，加深了区块链技术对食品接触材料领域的研究[4]；徐步龙等人对医院门急诊输液药房供应药品进行了统计分析，未标注药品追溯码的药品占 11.8%，进而提出了一种基于区块链的解决建议[5]。

对于医药安全首先考虑的就是医药数据的真实性。医药追溯系统可以实现对药品生产、运输、销售等各个环节有关药品质量安全的数据进行真实可靠地记录和传递[6]。当前我国主要有二种医药追溯方式：一种是药企自己建立的药物追溯系统；另一种是第三方平台提供的追溯服务。无论是哪种溯源方式，数据均来自利益相关方存入的中心数据，那么就存在为了利益篡改数据的风险。同时，第三方服务

基金项目：教育部科技司赛尔网络下一代互联网技术创新项目（NGII20180408）；吉林省教育厅项目（JJKH20200441SK）；吉林省社科项目（2020C048）；吉林省高等教育教学改革研究课题（JLJJ719920190723194557）；吉林省职业教育教学改革研究课题（2017ZCZ045）；吉林师范大学教学成果培育项目（201634）。

作者简介：冷泽琪（1996-），女，硕士研究生，主要研究方向：信息安全；谭振江（1956-），男，博士，教授，博士生导师，主要研究方向：计算机应用技术、网络信息安全；周 伟（1979-），女，硕士，助理研究员，主要研究方向：信息资源管理、计算机应用；刘佳琳（1995-），女，硕士研究生，主要研究方向：信息安全。
通讯作者：谭振江 Email：tanzj@jlnu.edu.cn

收稿日期：2020-07-22

与药企存在着企业因技术、人员等问题过于依赖于第三方服务、不能较好约束其行为的弊端。从上述分析可知,在目前大部分的溯源案例中,追溯信息仍存在不完整,且部分有追溯的产品价格比正常产品高出一倍,使得消费者望而却步。药物的安全和国民的健康存在巨大的安全隐患。

区块链是一个数据集,把数据打包成多区块,每一个区块是一个区块链数据集的子集[7]。区块与区块之间的数据相互关联形成逻辑上的链式结构。针对现有的医药安全需求很高,而传统系统数据真实性较低,见表 1。如果将区块链技术应用到医药领域上,能够实现对医药的原料采购、生产、加工、流通等各个环节的全程追溯,能够解决各企业之间“信息孤岛”的问题,从而减轻医药的监管难度。

表 1 传统溯源与区块链溯源对比

Tab. 1 Comparison of traditional traceability and blockchain traceability

系统	系统结构	医药数据真实性	追溯信息完整性	监管方式
传统的溯源系统	单一的中心化管理的数据库	容易被人为篡改	缺少供应链下游节点的录入	以抽样检查为主,消费者投诉为辅
区块链追溯系统	所有节点共同维护的链式结构	不可篡改,公开透明	对采购,生产,流转,销售所有的环节进行录入	所有进入网络的节点共同监督

1 关键技术阐述

1.1 区块链原理

区块链分为块头和块身。块头主要包括:区块编号、时间戳、父哈希和 Nonce 值等元数据,块身的主要功能是存储数据。每一个区块只能以附加的形式加入,新增的区块与上一个区块只能通过哈希值(父哈希)链接,以“链”形式不断增加的区块就形成了区块链。区块链由所有参与节点共同维护,每一个节点可以通过定期与邻居节点交换信息使全局账本保持同步[8]。

1.2 区块链分类

区块链分为 3 类:公有链、私有链和联盟链。公有链对来自互联网的任何人都是公开的,参与者多为匿名,所有人都可以加入公有链网络进行交易,获取完整的账本记录和竞争记账权等权利;私有链由集中管理者管理限制,只有内部少数人可以使用,信息不公开,私有区块链与中心式记账差异并不明显;联盟链通常由多个组织或机构共同参与管理,并事先选取一些预选节点参与其共识过程[9],比较典型的是超级账本项目。联盟链具有交易速度快、可扩展性强等特点。本文选择 Hyperledger Fabric 超级账本 2.0 作为底层开发平台。

1.3 智能合约

智能合约的主要思想是将合约条款转化为计算机协议,在去可信第三方的环境中,让此协议作为合约各方的信任代理,从而高效安全地履行合约[10]。智能合约分为 3 个阶段:合约生成、合约发布和合约执行[8]。具体功能见表 2。

1.4 密码学特性

区块链技术以密码学作为安全保障基础,由二个关键部分组成,即哈希算法和默克尔树。哈希算法是哈希函数去计算区块的头部信息或者交易信息的哈希值,将哈希值存储在区块中,下一区块存储上一区块的哈希值,形成完整的区块链结构[11];默克尔树是一个标准的二叉树,如果树上的一个节点被修改,那么该节点以下的信息将全部更新,拥有可溯源的特点。

表 2 智能合约各部分功能

Tab. 2 Functions of each part of the smart contract

智能合约	功能
合约生成	确定合约的规范和功能,最终开发得到合约代码
合约发布	将合约发给每个节点,最终达成共识的合约写入区块中,并扩散到整个链上
合约执行	通过具体的“事件”,执行相应的合约

(1) Hash 算法。哈希算法是一种单向密码算法,把长度不一的明文以不可逆的方式映射为长度固定的密文,密文即哈希值。常用的哈希算法有 SHA-256、SHA-512 等。大部分区块链使用的是 SHA-256 算法。

(2) Merkle 树。由一个根节点、若干非叶子节点和叶子节点组成。它的叶子节点存储的是当前区块体中每一笔交易的哈希值,非叶子节点是对应子节点哈希值链接之后再进行哈希运算的哈希值[12],非叶子节点之间两两组合并重复运算,最终得出 Merkle 根。其优点见表 3。

表 3 Merkle 的优点

Tab. 3 Merkle advantages

哈希树优点	大量数据对比快	查找高效性
具体内容	只需对比根节点数据,相同则下面节点内容一致,否则不一致	某个节点发生改变,从该节点至以下节点全部改变。可快速定位被修改的点

2　可行性分析

从四川省“毒胶囊”事件、山东省非法疫苗案、再到天津市假药的“鬼市”和扬州假药事件，医药安全是目前最重要的问题之一。对于医药安全，首先考虑的是医药数据的真实性。传统的溯源系统的中心数据存在因利益等因素而被人为篡改的风险，很难保障医药数据的完整性和真实性。而区块链技术的分布式存储、账本公开透明等优势，能够保证所有节点共同监督与维护，为追溯数据提供了可靠性。国内成熟的基于区块链技术的医药追溯系统寥寥无几，区块链技术应用到医药领域具有很好的适用性与广阔的发展前景。

落地的区块链追溯案例很多，但大部分存在数据不完整的问题，在医药的供应链下游节点，很少参与到记录追踪中，从而缺失了医药的追溯的必然环节。本文提出的医药追溯区块链包括提供安全性的块头和存储医药数据信息的块体。区块头包括版本号、上一医药块的哈希值、当前的时间戳、Nonce 等信息，每一个医药区块按照时间戳的顺序链接成医药区块链，链囊括了所有的历史交易记录，因此提供了完整的医药追溯。

3　基于区块链技术的医药追溯系统的设计

3.1　整体流程

本文采用区块链技术与 RFID 电子标签技术相结合，整体上来说，消费者通过扫描 RFID 标签得到溯源全程的数据。医药追溯系统的验证流程如图 1 所示。

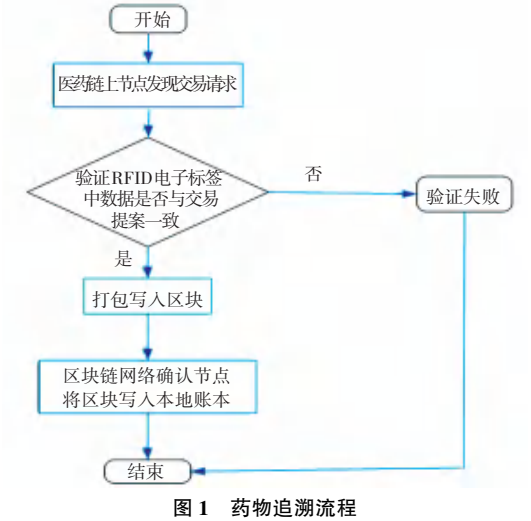

图 1　药物追溯流程

Fig. 1　Drug traceability process

3.2　追溯范围的确定

改变传统的溯源模式有助于提高医药安全性，结合区块链技术不可篡改、开透明等特点，本文建立了新型追溯系统组织架构。如图 2 所示。以医药为例，从药材原料厂、制药企业、运输、存储和销售全程记录追踪，让消费者不再觉得追溯只是“噱头”。

图 2　追溯范围改进

Fig. 2　Improvement of traceability scope

3.3　各层架构的设计

追溯系统的区块链网络共分为 4 层：数据层、合约层、业务层和应用层，如图 3 所示。数据层中提供分布式账本维护、私有数据库维护，合约层即智能合约层，设计了现医药在供应链上下游流转过程中的追溯，对医药数据结构体和智能合约功能接口，包括医药生产合约、医药运输合约、医药销售合约等调用功能。业务层是应用程序的后端服务，设计了 RESTful 的接口、用户管理、Node.js.jdk，提供医药监测管理服务。应用层包括发布医药信息、用户登记、查询和节点注册等功能，可以实现用户账户管理和业务操作的功能。

3.4　隐私服务的设计

除了药企自建的追溯系统外，第三方平台掌握着录入追溯系统的全部药物信息，一旦发生数据泄露事件，将严重影响到药企之间的公平竞争。为防止将系统内部的药物数据外泄，本文提出了多链业务架构，进行了授权节点和未授权节点账本对比，如图 4 所示。当同行企业存在隐私需求时，非授权节点 PEER1 不可访问该隐私数据，而授权节点则可以在不被影响的情况下继续访问该医药数据。本文设计的多链业务架构可以实现不同权限的节点访问的副本隔离，从而达到同行企业的隐私要求。

4　基于区块链技术的医药追溯系统的实现

本文提出的基于区块链的医药追溯系统实现了一个原型系统。本文以复方氯酚烷胺片为例，实现的功能包括：药厂发布医药生产信息，发布医药的运输信息，发布医药的销售信息。消费者查询医药的生产信息和运输信息以及销售信息。

(1)药企发布医药的生产信息。发布医药信息是录入系统的重要环节之一，药企在发布信息时，将根据某一医药编号来补充完善。发布医药的生产信息界面如图 5 所示。

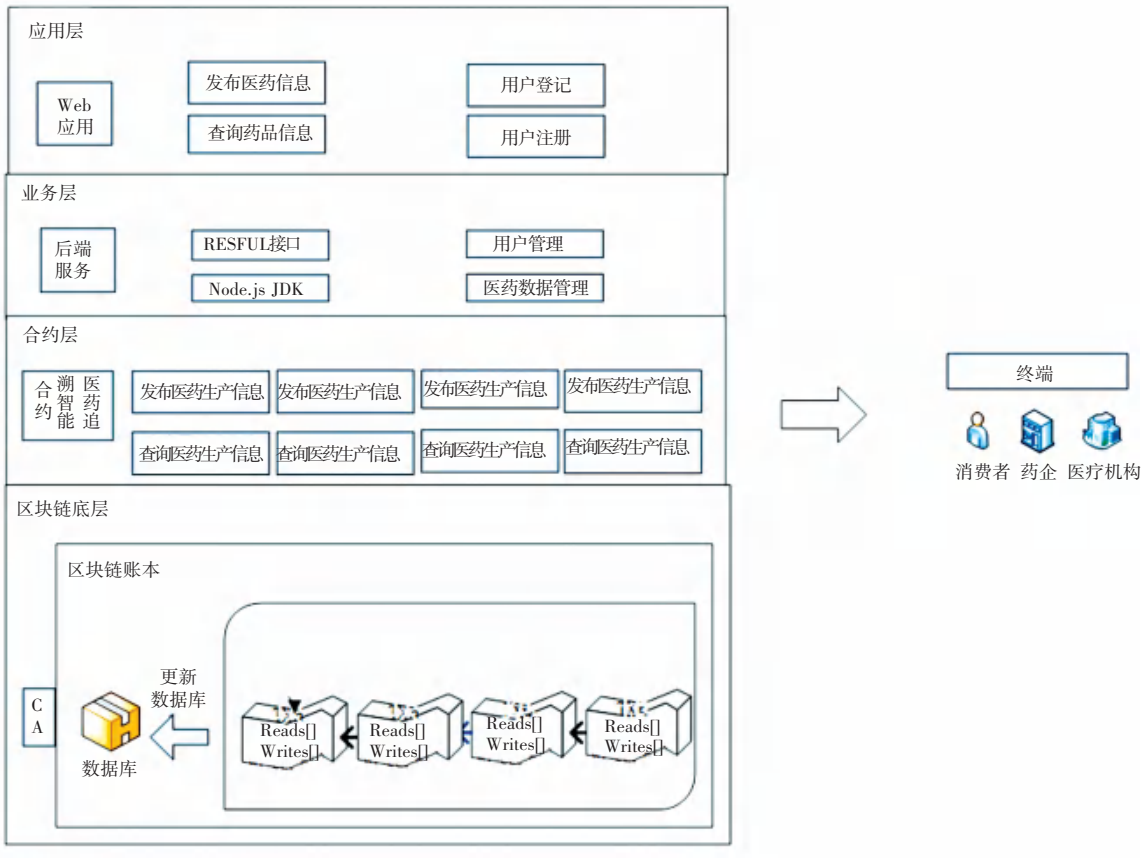

图 3 区块链网络各层架构

Fig. 3 The architecture of each layer of the blockchain network

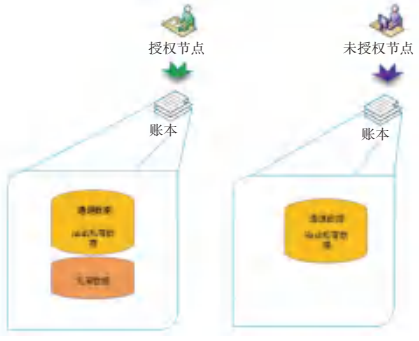

图 4 多链业务授权与未授权节点对比

Fig. 4 Comparison of multi - chain business authorized and unauthorized nodes

(2)药企发布医药的运输和销售信息。本文提供追溯全程服务,包括录入生产、流通和销售的信息。在每个录入环节中提供了相关工作人员证明的新服务点,目的是当出现问题时,责任可以落实到个人。发布医药的运输和销售信息界面如图 6、图 7 所示。

(3)消费者查询医药的生产信息。在为消费者提供的查询服务中,只需输入医药编号,即可查到该药物生产、流通、销售数据等的全部信息。可以具体到生产日期、厂商和地址等,查询医药的生产信息界面如图 8 所示。

图 5 发布医药生产信息界面

Fig. 5 Interface for publishing pharmaceutical production information

在查询医药的流通和销售中,包括追溯到的发货方、出库证明人员、物流和药店地址等数据信息。利用区块链技术对医药全面记录,有利于消费者对医药质量的信任,如图 9 和图 10 所示。

图 6　发布医药流通信息

Fig. 6　Release of medical circulation information

图 7　发布医药销售信息

Fig. 7　Release of medical sales information

图 8　查询医药生产信息

Fig. 8　Querying pharmaceutical production information

图 9　查询医药流通信息

Fig. 9　Querying medical circulation information

图 10　查询医药销售信息

Fig. 10　Querying medical sales information

5 结束语

区块链技术赋予了追溯行业新的活力。利用联盟链的数据公开透明与隐私保护,本系统通过数据的同步验证,更新状态数据库,再通过每个交易请求的身份验证和有效的加密机制,能够将追溯的全部过程信息落实到个人,以便追责。它保障了追溯到的信息安全可靠,解决了一直以来的“难追溯”、“追溯信息不全”等问题。具有很高的扩展性,在医药以及其他领域中可以发挥更好的作用。

参考文献

[1] 杨春松,张伶俐,高山,等. 区块链技术在我国医药领域的应用现状评价[J]. 中国药房,2020,31(17):2060-2064.
[2] 杨保华. 区块链原理, 设计与应用[M]. 北京:机械工业出版社,2017.
[3] 李娜,周熹丽,胡敏. 基于区块链技术的数字证书溯源防伪系统的设计[J]. 中国计量,2020(9):101-102.
[4] 刘金鹏,赵红,刘新星,等. 区块链在食品接触用塑料包装溯源系统的应用[J]. 包装工程,2020,41(17):165-170.
[5] 徐步龙,施芳红,李浩,等. 门急诊输液药房注射制剂追溯体系现存问题及对策分析[J]. 中国药业,2020,29(2):10-12.
[6] 薛丹. 基于区块链的药品供应链追溯系统设计与实现[D]. 西安电子科技大学,2019.
[7] 唐盛彬. 以太坊智能合约开发实战[M]. 北京:机械工业出版社,2019.
[8] 徐文玉,吴磊,阎允雪. 基于区块链和同态加密的电子健康记录隐私保护方案[J]. 计算机研究与发展,2018,55(10):2233-2243.
[9] 闻胜莲. 基于区块链的医疗数据共享方案研究[D]. 重庆邮电大学,2020.
[10] 方燚飚,周创明,雷晓莉,等. 基于区块链技术的供应链交易系统设计[J/OL]. 计算机工程:1-10[2020-12-28].https://doi.org/10.19678/j.issn.1000-3428.0058450.
[11] 余攀. 基于区块链的电子病历隐私数据保护共享研究[D]. 江西理工大学,2020.
[12] 陈云龙. 基于区块链的电子处方追溯系统的设计与实现[D]. 重庆邮电大学,2020.

(上接第 54 页)

其中,I_i 为第 X_i 个基本事件的结构重要度系数;N_{ij} 为第 i 个基本事件所在 K_j 内的基本事件总数;j 指第 j 个最小割集。

由此结构重要度排序如下:

$$I(X_{20}) = I(X_{19}) = I(X_{18}) = I(X_{14}) = I(X_{13}) = I(X_{12}) = I(X_{11}) > I(X_{22}) = I(X_{21}) = I(X_6) = I(X_5) > I(X_7) = I(X_{16}) = I(X_{15}) > I(X_{10}) = I(X_9) = I(X_8) I(X_7) = I(X_4) = I(X_3) = I(X_2) > I(X_1).$$

由以上计算结果知,如果不考虑基本事件发生的概率,仅仅从其在事故树结构中所占地位分析,基本事件 X_{20}、X_{19}、X_{18}、X_{14}、X_{13}、X_{12}、X_{11} 最重要,其次是基本事件 X_{22}、X_{21}、X_6、X_5,次之是 X_7、X_{16}、X_{15},再次是 X_{10}、X_9、X_8、X_7、X_4、X_3、X_2,最不重要的是 X_1。可以根据结构重要度,对基本事件逐一改进。

3 结束语

(1)通过对造成钻井井塌事故的原因进行分析,找出导致井塌的基本事件,建立钻井井塌故障树模型。

(2)对钻井井塌事故进行定性分析,得出影响井塌的全部路径。在钻井过程中,要对概率高的因素进行控制,减少井塌事故的发生。

(3)计算结构重要度并排序,找出对顶上事件发生影响最大的事件,即井斜、井身质量差、严重狗腿、钻井液入侵地层、钻井液失水量大、流变性差、抑制性差。对此类基本事件要重点关注,最大程度减少事故发生的可能性和危害。

基于故障树分析,为钻井井塌风险的预防以及安全管理工作提供了可靠的依据。

参考文献

[1] 卢亿. 地铁火灾的事故树分析[J]. 城市轨道交通研究,2011,14(2):95-97,102.
[2] 阮存寿.基于事故树模型的井喷事故原因分析及预防对策[J]. 石油工业技术监督,2020,36(1):60-63.
[3] 刘刚,贾国玉,杨锡亮. 风险树分析在钻井工程事故中的应用[J]. 断块油气田,2006(3):69-70,93.
[4] 袁智,汪海阁,王海强, 等. 基于事故树分析的钻井井漏事故危险评价研究[J]. 中国安全科学学报,2010,20(3):107-112.