文章编号: 2096-1618(2019)03-0267-07

基于区块链的药品溯源追踪方案研究设计

范 硕[1], 宋 波[1], 董旭德[2], 韩天齐[1]
(1.成都信息工程大学网络空间安全学院, 四川 成都 610225; 2.成都信息工程大学软件工程学院, 四川 成都 610225)

摘要: 结合区块链相关技术,针对药品行业的安全、流通管理、溯源追踪、监督等问题,提出了一种药品溯源追踪查询的参考方案及参考实现。以区块链技术解决药品行业存在的安全问题,所需要的主要工作包括: 对参与各方的业务流程通过智能合约实现; 对参与各方成员信息和药品数据信息的通用定义; 对参与各方权限身份的区分约束等。区块链的核心价值之一在于解决信任问题。通过把可共享的数据以区块链共享账本的形式保存到区块链网络上,多方共同参与、维护及监督区块链网络生态,可以实现共享数据的不可篡改、可追溯等需求。相对于传统的中心化溯源形式,基于区块链技术的应用是对解决药品行业安全、溯源等问题的一种有益的尝试。

关 键 词: 区块链; 药品安全; 智能合约; 共享账本; 溯源; 监督管理
中图分类号: TP311.13 文献标志码: A
doi: 10.16836/j.cnki.jcuit.2019.03.011

0 引言

近年来,关于药品、食品等相关领域的安全事件时有发生,如禽流感、苏丹红、瘦肉精、三聚氰胺、疫苗造假等事件[1],其中存在生产环节的数据造假、流通环节的信息封闭、管理失控等问题。由于信息的封闭性,公众及第三方组织机构等难以介入监督。传统的药品追溯管理体系一般采用的是中心化存储模式,一般由企业、渠道商或者政府负责维护管理,这种模式下,数据被少数机构掌控,当出现问题时,需要对所存储的药品记录数据追溯查询时,如果数据维护管理方为利益相关方,则管理者可能对数据进行篡改[2-3]。现有药品领域生产及流通环节的问题主要有: 企业擅自篡改产品生产记录及检验记录,销售商伪造销售记录,药品流通过程难以追溯,信息不对称,监管信息不公开等。

区块链技术可应用于诸多领域,有广阔的应用前景[4],区块链本身具有去中心化和不可篡改的特性[5],不依赖于某个组织或者个人。区块链网络的核心是一个分布式共享账本,分布式共享账本本质上是历史记录不可篡改的分布式数据库技术,在这个账本中记录了网络中发生的所有交易信息,账本中的历史数据,是无法被篡改的,因此可以有效地解决溯源问题。同时,由于区块链的分布式架构特性,任一节点的损坏,都不会导致数据的丢失,区块链仍然能够正常运行,没有哪个单独的机构可以完全破坏它,所有信息公开记录在共享账本中,由多方参与维护共享账本[6-10]。基于区块链的架构可以为药品、食品等商品的生产、流通、监督等构建一个更公开、透明的环境和可追溯查询的商品管理体系[11-12]。对于药品行业可以将药品生产厂商、药品经销商、各级医院及疾控中心、药店以及药品生产审批机构、第三方监督机构和消费者等都纳入到这个链上系统,实现数据信息共享和信息不可篡改以及信息可追溯等应用需求,可以有效地改善现有药品、食品等行业供应链的安全性和可追溯性。

收稿日期: 2018-11-28

1 相关概念

由于区块链属于新兴行业,对区块链的架构还没有权威的标准定义,文献[13]定义区块链是一种按照时间顺序将数据区块以链条的方式组合成特定数据结构,并以密码学的方式保证其不可篡改、不可伪造的去中心化共享总账,能够安全存储简单的、有先后关系、能在系统内验证的数据。文献[14]认为区块链技术是利用加密链式区块结构来验证和存储数据、利用分布式节点共识算法来生成和更新数据、利用智能合约来编程和操作数据的一种全新的去中心化基础架构和分布式计算范式。文献[15]从层次结构划分上将区块链分成3层: 网络层、交易层、应用层,文献[16]将区块链分成6层: 存储层、基础区块链层、缓存层、API层、链上代码层、应用层。

一个完整的区块链生态包括一系列的技术组合: P2P网络、加密签名技术、数据存储技术、分布式算法等方面。根据应用场景和架构体系的不同,一般分为

公有链、联盟链和私有链，其中联盟链一般由授权组织机构共同参与维护区块链系统的运转，方案研究在联盟链的基础上实现。从具体应用的角度看，主要关注区块链的智能合约、共享账本以及加密、签名算法等方面的内容。

1.1 智能合约和共享账本

智能合约及应用是区块链技术架构[17-18]的重要组成部分及未来重要发展趋势之一，智能合约是企业、组织或个人等认可并参与的业务逻辑流程操作，区块链参与成员通过智能合约操作区块链共享账本数据。共享账本可以看作是业务流程的日志，账本被联盟、团体或个人等组织成区块链或者交易链，形成不可更改和抵赖的数据结构，在各个参与方之间形成一个统一的状态账本。区块链技术通过支持各种业务合约，在相关参与者间共享交易账本和流程状态。不同的区块链架构的账本设计有所区别，图 1 为一种简化的账本模型结构。

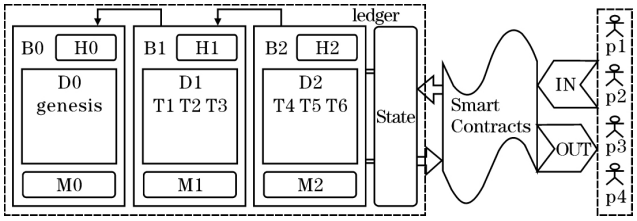

图 1 区块链账本模型结构简图

其中 B0，B1，B2 为区块结构，B0 称为初始区块，B1 中的 D1 部分保存具体的状态转换记录或者称为交易记录 T1、T2、T3，M1 为区块的元数据信息包括时间戳、证书信息等，H1 为区块头，头信息包括对本区块数据 D1 的数字摘要(哈希)以及上一个区块 B0 的哈希等。后续的区块向前链接，形成一条不可变更不可分割的链式结构。参与成员 p1 ~ p4 等通过智能合约(smart contracts)和账本数据库交互。

1.2 数字签名

区块链利用数字签名算法[19]来保证数据在整个系统中不可篡改，并保证参与成员身份的真实可靠。数字签名使用了非对称加密技术和数字摘要(哈希)技术，保证了在传输过程中的数据完整性、发送者身份真实不可假冒等。非对称加密技术包括一对公钥和私钥，私钥只保存在所有者手中，公钥对外公开，数字签名即是用私钥加密用公钥解密。在应用中对成员身份管理验证以及数据信息的验证都可以通过数字签名算法来实现，数字签名流程如图 2 所示。

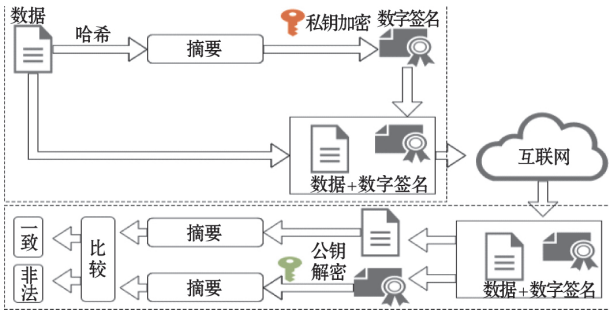

图 2 数字签名流程图

发送方通过哈希算法生成摘要信息，通过发送者的私钥对摘要进行加密生成数字签名，把签名信息和数据信息一起发送给接收方。接收方通过发送方的公钥对签名进行解密，还原出签名摘要，对发送的数据信息进行哈希，生成数据摘要，比较两个摘要，如果相等证明信息无篡改，否则信息被篡改过。

2 方案研究及实现

区块链底层平台系统可由政府主导组建，由厂商、行业联盟或相关机构共同实施贡献节点并参与维护，消费者及第三方机构可以对链上数据进行查询反馈，同时各方可对链上相关机构进行监督，对链上数据的操作权限取决于区块链管理员对参与者在区块链系统中的角色和职能定位。从区块链应用的角度来看，主要是对业务流程的逻辑实现即智能合约的实现，以及对业务数据的定义，接入网络的授权成员通过智能合约操作区块链上的业务数据。尽管不同行业的参与成员各有不同，但从对业务数据的共享、溯源追踪、监管等需求出发，业务流程是具有相似性的，在实际的应用场景中，可以针对某一类商品定义标准化的数据结构格式以及参与成员的数据结构信息，在智能合约中实现对数据操作的封装以及用户权限管理验证等操作，根据参与方用户的不同角色定位，通过智能合约控制用户对数据的操作。

下面以某一类药品比如疫苗作为溯源追踪的实体进行详细的方案分析。以区块链技术实现疫苗药品生产流通的全流程追溯，每一支疫苗要有独立的药品识别 ID 或标签，药品的防伪识别措施应由生产厂商提供，药品经生产检验合格准备投放市场之前，生产厂商首先将药品信息入链，伴随药品的流通，可以由生产商、销售商、医院及医疗机构、药店等当前药品持有机构更新药品的状态记录，对应每一步的流转记录即被记入区块链账本保存。药品行业的相关参与方如图 3 所示，包括生产厂商、医院、诊所、医疗机构、药店、销售者以及消费者、监管者等。

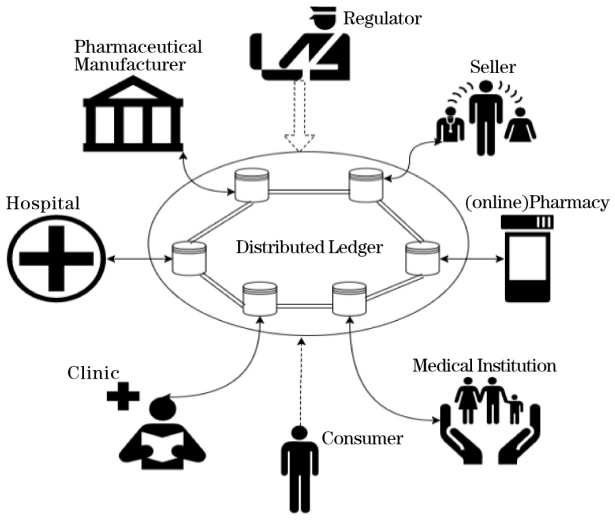

图 3　区块链网络上的业务参与网络图

2.1　方案流程说明

区块链管理者可以由政府或行业联盟及第三方机构共同参与构成，管理者不参与链上数据的更新维护，只负责维护区块链成员的信息，入链的网络参与成员均由管理者授权并向管理者申请数字证书，由区块链系统管理者对链上组织成员的公钥及相关信息加密生成数字证书分发给成员，网络成员私钥只由成员自己持有保存，网络成员公钥公开保存。针对疫苗行业的区块链网络参与成员可包括厂商、销售商、医院及医疗机构、药店等，成员根据不同角色定位对链上数据有不同的更新操作权限，消费者及第三方机构等非直接参与方可以对链上数据进行查询。区块链上保存药品的当前状态记录和历史记录，历史记录不可更改，由历史记录可以正向推出药品的当前状态记录，反向追溯药品的历史流转记录，药品的当前状态记录由药品当前的拥有者负责维护更新，初始拥有者为生产厂商。

详细业务流程如图 4 所示。生产厂商每生产一个批次的药品并检验通过后，首先用私钥签名监管或质检部门对该型号或批次的药品批文及药品相关信息，然后厂商把药品信息和签名数据一同更新到区块链上; 当药品由厂商向销售商或医疗机构流转时，双方达成交易共识后，首先由销售商或医疗机构对准备购买的药品签名信息进行验证，验证通过后用私钥签名对应药品信息，把签名数据发送给生产商，由生产商更新药品状态记录、药品当前所有者及所有者签名信息等; 当药品由销售商或医疗机构向子销售商或下级机构流转时，链上数据更新方式同上，由当前药品持有者负责更新数据; 当药品由销售商或医疗机构直接向最终消费者或其他非链上成员流转时，由销售商或医疗机构把药品最终去向及受众信息更新到链上药品信息中并更新药品状态。

生产厂商可以通过链上数据追踪本厂药品的流向及流通情况，销售商和医疗机构可以通过链上数据验证需要采购的药品，消费者及第三方机构等均能够对链上药品信息进行指定查询，同时药品流转的下级机构、成员或第三方监督机构通过对历史记录溯源可形成对整个行业生态的监督机制。若药品出现问题，根据链上记录可以很方便地查询流转过程，以及在哪一个环节可能出现问题。如果在药品流通环节出现造假等问题，可以根据链上记录和厂商提供的防伪机制对中间商或机构进行鉴别追责处理; 如果是在药品源头出现造假等问题，可以根据链上记录和厂商提供的防伪机制对厂商进行追责处理。

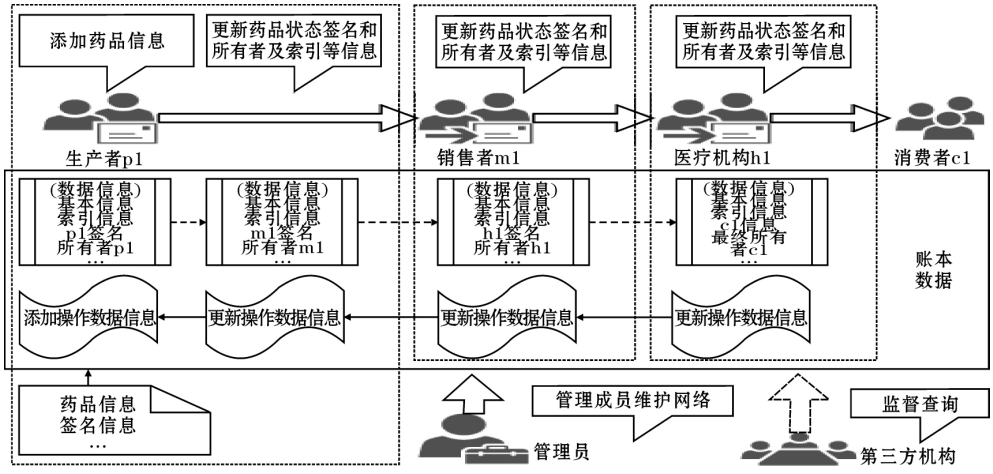

图 4　业务流程图

2.2　参考实现

2.2.1　架构说明

方案采用联盟链 Hyperledger Fabric 架构实现，Fabric 的账本系统包含一个哈希值链接的区块链结

构，以及一个状态数据库（称为世界状态），状态数据库记录当前的 Fabric 网络上的数据状态。区块链结构中保存所有状态转换记录，状态转换记录是参与各方对当前状态记录操作结果，相当于日志记录，通过日志记录可以导出目前状态，区块以文件形式保存在节点文件系统中，区块记录只能追加。图 5 是一个简化的 Fabric 底层架构，由 peer 节点集群验证处理用户请求并处理响应，orderers 集群对处理数据排序，排序后的数据由 peer 节点通过调用智能合约把数据写入账本。

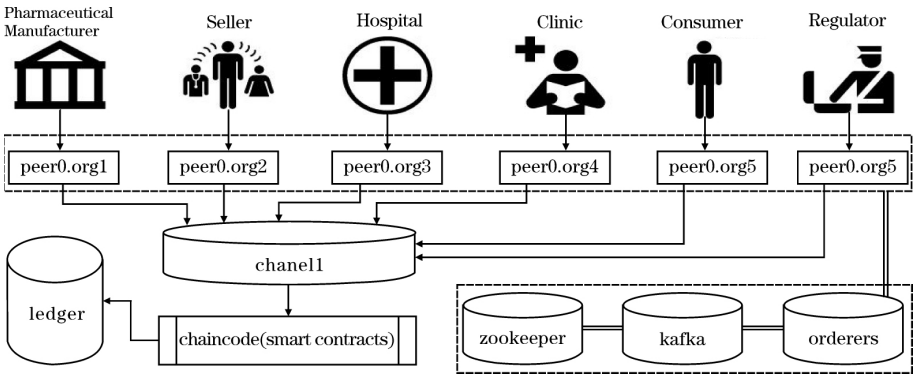

图 5 Fabric 底层架构简图

2.2.2 智能合约实现

在 Fabric 架构上，业务逻辑部分主要是智能合约和数据结构设计以及应用程序接口实现等。智能合约即是对上一节中方案流程的功能实现，区块链应用通过智能合约实现对账本数据访问和控制，实现业务流程。

从智能合约的实现角度看，如图 6 所示主要包括 3 部分逻辑实现：链上数据结构的定义，包括成员信息、药品信息、药品索引信息等；数据操作的逻辑实现，包括对药品数据相关信息的查询、添加、更新、删除等操作实现，对药品索引信息的操作实现；成员权限管理的实现，包括管理员对网络参与成员的添加、更新、删除等操作，成员对药品信息及其他相关数据信息的操作权限验证等。智能合约实际上是一段部署到区块链网络上的操作区块链数据的业务逻辑代码，可由政府、联盟组织或授权管理机构等制定行业业务逻辑规则，通过智能合约封装并对外开放调用接口。

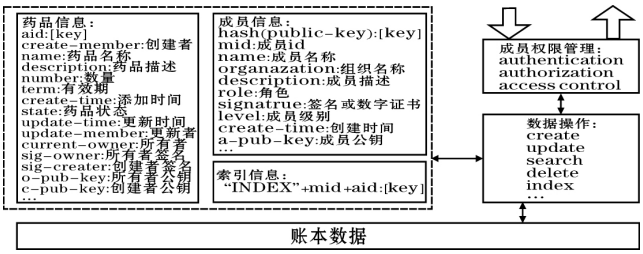

图 6 智能合约部分数据结构及功能定义

其中成员权限管理模块采用公钥密码体系实现，权限验证分两个层次的授权验证，包括参与者参与区块链网络的授权和验证，参与者操作区块链账本数据的授权和验证，如图 7 所示。

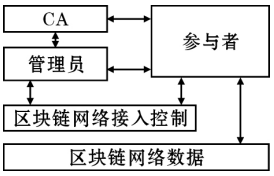

图 7 权限管理逻辑

由管理员通过 CA 机构向区块链网络参与者分发不同级别的授权密钥包括公钥、私钥。参与者的私钥只由参与者自己保存，参与者通过分发的私钥接入区块链网络并进行授权内的操作，有权限进行更新操作的区块链参与者，更新数据时，通过私钥对所更新的数据签名，签名信息和数据信息一同保存到区块链数据账本中。在对数据进行再次更新时，首先通过上次更新者的公钥验证用户身份和数据信息，通过后在通过当前用户私钥进行本轮更新操作。

2.2.3 应用程序业务功能划分

应用程序即前端和用户、管理者、参与者等交互的程序，应用程序通过调用智能合约的接口来查询或更新区块链的数据。

应用程序的业务功能可以分为 4 部分：管理员模块，由管理员负责对区块链上成员的管理维护，管理员不参与链上数据的维护；生产厂商模块，由生产商负责对所生产的药品信息及签名信息入链并更新药品初始状态信息，根据药品索引记录可以查询本厂商所有生产药品记录，药品由厂商流转向销售商等下级机构时由厂商负责更新药品状态信息；中间商模块，销售商、医院及医疗机构、药店等均可看作是药品流转环节的中间商节点，可对不同机构赋予不同的级别以区分机构权限或类型等，药品由中间商向下级机构或最终消

费者流转时由药品持有机构负责更新药品状态信息; 开放查询模块,可对消费者、第三方机构、监管机构等非链上直接参与成员提供对应权限的可共享数据的查询接口。由成员权限管理模块对参与操作的管理员和用户进行功能划分并授权对应的操作,如图 8 所示。

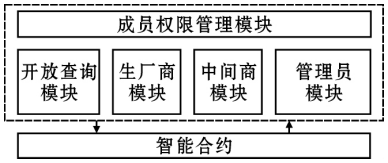

图 8　业务功能模块

2.2.4　整体实现架构参考

智能合约实现了所有业务逻辑功能和成员权限管理操作,根据参与者角色定位控制相应的业务逻辑操作权限。在智能合约中实现上述模块功能并封装 API 接口,可供外部应用程序调用,Website 站点可作为一种外部应用方式实现业务功能划分,提供用户和区块链数据的交互功能,实现业务展现层的封装,通过 SDK 调用后台智能合约; 智能合约实现业务逻辑及成员权限管理的封装,控制用户权限,并通过底层 API 操作区块链数据库,实现数据的存取。整体实现方案架构如图 9 所示。Website 站点以 MVC 模式封装应用程序业务功能,普通参与者通过 Website 应用和区块链数据交互,区块链管理员可通过 Website 对区块链网络进行常规管理,同时当区块链网络底层架构需要重大更新变动时管理员也可以通过 HyperLedger Fabric 框架的接口对区块链网络进行重新配置、更新、升级等。

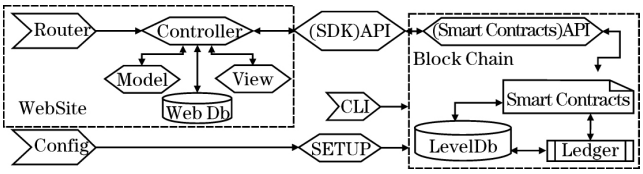

图 9　方案整体架构简图

3　方案讨论分析

3.1　业务逻辑核心

方案是以药品信息及药品状态信息为核心构建的,区块链账本记录了药品历史流转记录,区块链状态数据库除保存当前链上成员信息、索引信息及其他相关结构信息外,主要存储的是药品信息及药品状态信息,可以根据区块链参与者的角色限制查询更新权限。只有生产厂商可以在链上添加新的药品信息,只有药品当前所有者可以更新药品的状态信息,状态数据库中只维护当前流通中的药品记录。药品流转到最终成员或用户时由最后一级的拥有更新权限的链上成员对药品状态进行更新后删除状态数据库中的药品信息及相关索引记录等(删除状态数据库数据信息的操作及删除的信息都会被记录到账本) ,以保证状态数据库的大小可以动态调整而不至于无限增大。药品的历史流转记录即对状态数据库所有的添加、更新、删除操作记录可以通过账本进行查询。方案中可以尽量把智能合约和数据结构的耦合度降低,使智能合约不必关心具体的数据结构定义。智能合约中只要实现对数据结构的所有逻辑操作以及成员管理验证等操作,成员管理可根据成员数据结构中定义的信息分派不同的操作权限。对于其他类别的药品或食品等类似相关行业的商品可以同样构建以该类药品或食品为核心的数据信息格式,通过类似的智能合约处理流程实现相应的业务逻辑。

3.2　验证机制

方案可实现对链上成员及数据的双重验证机制,包括对成员信息的验证和对药品信息的验证。由政府或行业联盟联合 CA 机构为区块链参与成员分发数字证书,区块链网络参与成员、消费者及第三方机构等均可通过 CA 机构的公钥对参与成员信息的数字证书解密以验证证书持有人信息及持有人公钥信息,以防止冒用及欺诈,成员验证可直接通过 Fabric 平台的成员服务实现。生产厂商对新生产并检验通过的药品用私钥对药品信息及相关信息进行签名,把药品生产者签名数据和药品信息一同入链,下级销售商或最终消费者及第三方机构等可用厂商的公钥对签名数据解密和药品信息及实际药品进行验证。药品流转过程中,销售商或医疗机构等在更新药品状态信息的同时需要对当前药品信息进行签名,把药品当前拥有者签名数据和药品状态信息同时更新,下级机构或最终消费者等可用上一级药品持有机构的公钥对药品拥有者签名数据解密以确认药品来源。

3.3　防伪机制

通过数字签名及身份验证方法可以实现链上数据的不可篡改、保证真实有效。然而,对于像食品、药品以及其他实体性质的行业产品进行数字化信息处理时,必然要考虑对于实体商品数字化并且保证数字化后的数据信息和实体严格对应的问题,即造假问题。造假又可分为两种,一是恶意造假,即第三方假冒原厂生产同样批次或型号的商品; 二是故意造假,即原厂故

意生产假冒伪劣商品。对于第一种情况,如果假冒商品入链必然导致链上记录出现分支,根据分叉情况可以追溯到商品的部分流通线索;第二种情况,直接通过链上记录可以溯源到厂商。而实际应用场景中,可能是两种情况并存,导致不能确定哪一环节出现问题。从商品流通的角度看,应由厂商提供对本厂产品的防伪验证机制,当出现问题时根据链上记录和厂商防伪机制联合进行溯源及追责处理。目前,比较通用的二维码、电子标签等方式,对防伪有一定的效果。防伪机制本质上是提高对该产品的造假成本,更好地解决造假问题需要多方的努力。一是监管方面的制度及措施落实,二是防伪措施的升级,三是提升产品的工艺、降低产品的可复制性。

3.4 部署实施

对方案实施参与各方可以选择搭建一个全新的业务系统来处理区块链数据,或者结合现有的业务模式对现有流程中可以入链的数据和业务接入区块链网络,作为现有模式的补充。传统的业务流程模式如果是各方独立维护本方的业务数据,则存在参与方协作与数据融合问题,可能存在数据不兼容,不能有效协作等问题,需要政府或行业联盟等机构指定相关数据标准及处理链上数据的通用业务逻辑;如果是由政府或机构主导采取的中心化数据存储管理方式,可以由主导方对基础平台进行改造,然后把行业相关参与方及机构纳入新的系统平台进行扩充。

4 结束语

引入区块链技术的核心价值在于它所构建的信任机制,将区块链技术和传统药品溯源管理场景相结合,通过制定标准化的智能合约流程以及不可篡改的账本数据,可以有效地降低参与各方的信任成本,将机构和社会运作透明化,从而提高效率,而去中心化模式则是区块链信任机制的衍生特质。区块链技术应用前景广阔,但也并非万能。将区块链技术引入监管系统中并不能完全解决传统中心化溯源系统中存在的作假掉包等问题,只能做到改善目前的状况而已。如何将药品等实体物品映射到链上,同时保证链上数据与实体药品本身严格对应仍需要进行研究,不能指望区块链应用到药品监管系统后能够解决所有问题。但区块链对于推动药品监管系统的发展进步是有实际意义的,以不可篡改的共享数据为基础,引入社会、消费者的共同监督,从而实现生产厂商、消费者、监管部门的交叉验证,从而提高各环节的造假成本,改善医药领域的生态环境。

参考文献:

[1] 厉曙光,陈莉莉,陈波.我国2004-2012年媒体曝光食品安全事件分析[J].中国食品学报,2014,14(3):1-8.

[2] 孙志国,李秀峰,王文生,等.区块链技术在食品安全领域的应用展望[J].农业网络信息,2016(12):30-31.

[3] 温川飙,赵姝婷,陈菊,等.基于区块链的第三代中药追溯平台构建研究[J].中国现代中药,2017,19(11):1519-1522.

[4] Aste T,Tasca P,Matteo T D.Blockchain Technologies: The Foreseeable Impact on Society and Industry[J].Computer,2017,50(9):18-28.

[5] Nakamoto S.Bitcoin: A peer-to-peer electronic cash system [EB/OL]. https://bitcoin.org/en/bitcoin-paper.

[6] 中国区块链技术和应用发展白皮书[M].北京:中国工业与信息化部,2016:5-38.

[7] 黄征,李祥学,来学嘉,等.区块链技术及其应用[J].信息安全研究,2017,3(3):237-245.

[8] 朱建明,付永贵.区块链应用研究进展[J].科技导报,2017,35(13):70-76.

[9] 李董,魏进武.区块链技术原理、应用领域及挑战[J].电信科学,2016,32(12):20-25.

[10] 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.

[11] 汪登,曾小珊, 白倩兰,等.基于区块链的食品安全溯源技术[J].大数据时代,2018(3):30-36.

[12] 张夏恒.基于区块链的供应链管理模式优化[J].中国流通经济,2018(8):42-50.

[13] 袁勇,王飞跃.区块链技术发展现状与展望[J].自动化学报,2016 42(4):481-494.

[14] Beck R,Stenum Czepluch J,Lollike N,et al. Blockchain-The Gateway to Trust-Free Cryptographic Transactions[J].ECIS 2016 Proceedings,2016:1-14.

[15] 祝烈煌,高峰,沈蒙,等.区块链隐私保护研究综述[J].计算机研究与发展,2017,54(10):2170-2186.

[16] 蔡维德,郁莲,王荣,等.基于区块链的应用系统开发方法研究[J].软件学报,2017,28(6):1474-1487.

[17] 邵奇峰,金澈清,张召,等.区块链技术: 架构及进展 [J].计算机学报,2018(5):969-988.
[18] 董宁.区块链技术演进及产业应用展望 [J].信息安全研究,2017,3(3):200-210.
[19] 张先红.数字签名原理及技术 [M].北京: 机械工业出版社,2004: 12-31.
[20] Pilkington M. Blockchain Technology: Principles and Applications [J]. Social Science Electronic Publishing,2016.
[21] Zhang C. The Technology Principle, Application and Suggestion of Block Chain [J]. Computer Engineering & Software,2016.

Research on Tracing Scheme of Medicine based on Block Chain Technology

FAN Shuo[1], SONG Bo[1], DONG Xude[2], HAN Tianqi[1]
(1.College of Cybersecurity, Chengdu University of Information Technology, Chengdu 610225, China; 2.College of software engineering, Chengdu University of Information Technology, Chengdu 610225, China)

Abstract: Aiming at the problems of safety, circulation management, traceability and supervision of drug industry, based on the block chain technology, a reference scheme and its implementation of drug traceability query are proposed. To solve the safety problems in drug industry by block chain technology, the main work include three parts: to implement the logic of business processes through block chain smart contracts, to define the drug data format and related data of all participant, and to distinguish and restrict the authority and identities of participants. The core value of block chain is to solve the problem of trust. By the shared ledger data letting multi-party participate in the maintenance and supervision, which can realize the goal of immutable data, traceability and some other requirements. Compared with the traditional centralized traceability, the application of block chain technology is a beneficial attempt to solve the safety and traceability problems of the drug industry.

Keywords: block chain; drug safety; smart contracts; shared ledger; traceability; supervision