Hans Journal of Data Mining 数据挖掘, 2022, 12(3), 272-279
Published Online July 2022 in Hans. http://www.hanspub.org/journal/hjdm
https://doi.org/10.12677/hjdm.2022.123027

Hans汉斯

基于联盟链的安全可信电子病历智能合约设计

廉应生[1]，莫晶亮[2]，邱　钊[1*]，杨子睿[1]，杨　磊[1]，卢本本[1]

[1]海南大学计算机科学与技术学院，海南 海口
[2]海口市妇幼保健院，海南 海口

收稿日期：2022年6月15日；录用日期：2022年7月19日；发布日期：2022年7月26日

摘　要

随着医院信息化的发展，越来越多的医院开始着手重点建设智能医疗化电子病历系统，但是，在电子病历等医疗信息数据的存储、访问与管理方面，传统的医疗系统会存在很多问题。区块链技术中的联盟链具有部分去中心化、可控性较强、数据不会默认公开和交易速度很快等特性，能够保护医疗信息数据安全可信同时又能够实现共享。本文针对传统医疗系统在电子病历信息数据方面的痛点，引用联盟链在数据存储中安全可信的特性，提出了一种合理的基于联盟链的安全可信电子病历智能合约设计方法。这种新型的设计方法可以很好的解决目前医疗行业在信息化过程中遇到的数据安全可信与共享方面的难题。

关键词

区块链，联盟链，安全可信，电子病历，智能合约

Design of Secure and Trusted Electronic Medical Record Intelligent Contract Based on Alliance Chain

Yingsheng Lian[1], Jingliang Mo[2], Zhao Qiu[1*], Zirui Yang[1], Lei Yang[1], Benben Lu[1]

[1]School of Computer Science and Technology, Hainan University, Haikou Hainan
[2]Haikou Maternal and Child Health Hospital, Haikou Hainan

Received: Jun. 15th, 2022; accepted: Jul. 19th, 2022; published: Jul. 26th, 2022

Abstract

With the development of hospital informatization, more and more hospitals begin to focus on the

*通讯作者。

文章引用: 廉应生, 莫晶亮, 邱钊, 杨子睿, 杨磊, 卢本本. 基于联盟链的安全可信电子病历智能合约设计[J]. 数据挖掘, 2022, 12(3): 272-279. DOI: 10.12677/hjdm.2022.123027

construction of intelligent medical electronic medical record system. However, there are many problems in the storage, access and management of medical information data, such as electronic medical record. The alliance chain in blockchain technology has some characteristics, such as partial decentralization, strong controllability, no default disclosure of data and fast transaction speed, which can protect the security and credibility of medical information data and realize sharing at the same time. Aiming at the pain point of traditional medical system in electronic medical record information data, this paper introduces the security and credibility of alliance chain in data storage, and proposes a reasonable design method of secure and trusted electronic medical record intelligent contract based on alliance chain. This new design method can well solve the problems of data security, credibility and sharing encountered by the medical industry in the process of informatization.

Keywords

Blockchain, Alliance Chain, Security and Credibility, Electronic Medical Record, Smart Contract

Copyright © 2022 by author(s) and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 引言

在整个医疗体系中，电子病历是病人医疗信息主要的存储载体，但是拥有这些医疗数据的各大机构和政府等部门在数据共享时存在很大的障碍，除此之外，病人的电子病历中还会包含所属者的个人隐私数据，在没有本人同意的情况下，不适合直接访问交流。很多的病人并不清楚自己的病历信息存储在哪里，会被那些人访问，不同医院的医生和研究人员也不能有效的利用这些信息，主要原因在于病历信息记录存储的方式和各医疗机构对本院数据资产的保护限制。因此，如何构建一个合理的医疗数据共享平台并且实现病人电子病历数据的隐私保护是目前工作的重难点。

本文将研究区块链技术在医疗领域的应用，通过构建医疗机构联盟，搭建支持医疗数据信息共享的平台[1]，设计智能合约来管理病人、医生、医疗机构和研究人员之间的信息交流，同时保护患者隐私以促进信息共享。作为联盟的成员，医疗机构之间共享数据时将自动执行智能合约，获得权限后共享病人电子病历信息数据，设计智能合约过程中将用到椭圆曲线加密算法，这是一种可提供医疗信息访问并避免泄露患者隐私的数字签名算法。医疗数据共享将使跨区域医疗服务更加便捷，在海量医疗数据背景下共享资源，并将医疗数据采集共享提升到一个新的高度。

2. 联盟区块链技术

2.1. 区块链

区块链系统(Blockchain)具有分布式的数据库[2]，是一个开放安全的创新技术区块授权账本网络，架构清晰，可以实时检查和记录所有操作，这可能会改变各医疗行业目前的数据存储与分享处理模式。本文研究的电子病历医疗数据信息共享系统在“互联网 + 医疗”和“大医疗数据”的背景下，采用区块链技术对交易进行存储，具有安全可信、无法篡改的特点。

区块链的基本结构模型由自上而下的六层组成[3] [4]，包括应用层、合约层、共识层、网络层和数据层。应用层是一组功能模块，如医疗数据访问发布、搜索、权限检查等，可以嵌入块链底部的结构中；

合约层具有大量的智能合约开发环境，且实现系统的所有功能智能合约模块；共识层实现了描述节点间协议的共识算法，包括 POW、DPOS 等共识算法[5]；网络层则是包含了各种数据传输协议以及验证机制等功能，确保块网络节点之间的通信；数据层包含了区块链中的数据表示和数据处理规则。

区块链是由加密算法生成的数据块和数据链路组成[6]。由区块头和区块体组成，每个区块的块头包括版本号、时间戳、前一区块哈希值、随机数、目标区块哈希值和 Merkle 根值，记录电子病历的所有操作信息。链上区块的信息可以被前一区块追溯，同时区块信息也可以影响后继区块节点。它的加密方法保证即将到来的恶意攻击不能修改信息，从而确保存储在链上信息的安全可信。在构建区块链时，使用一组共识机制来检查或记录链上的每个节点，当链上大多数的节点都认同此信息记录时，此信息可以被记录在链上，区块链数据结构见图 1 所示。

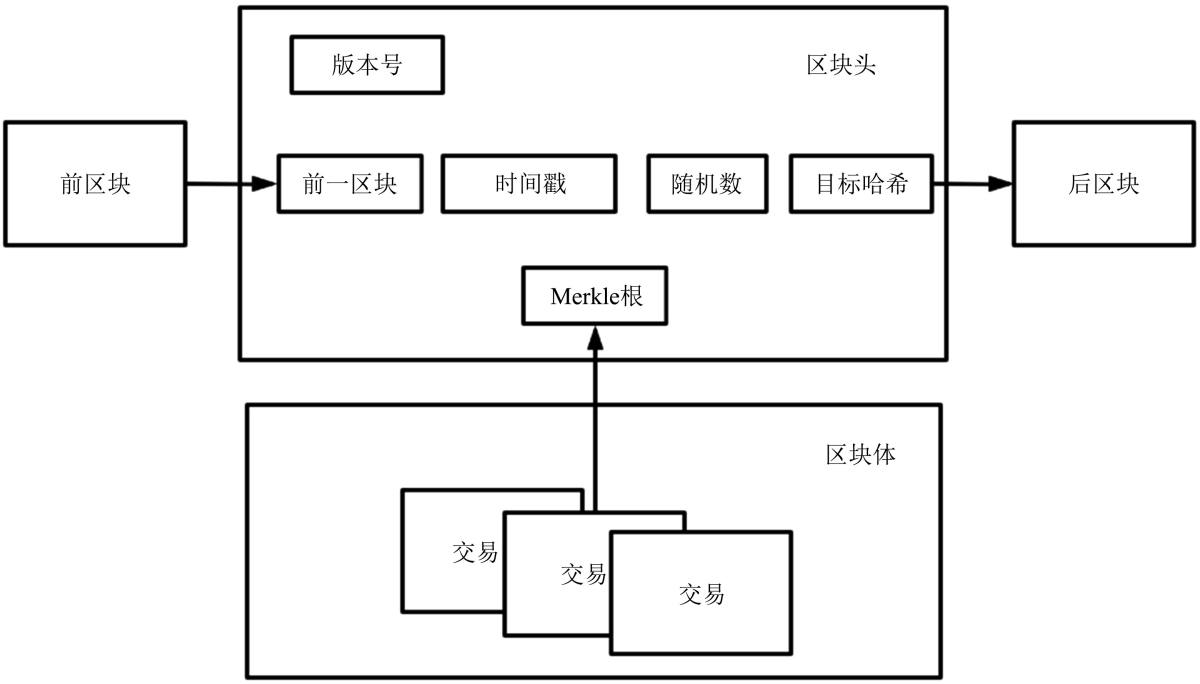

Figure 1. Blockchain data structure
图 1. 区块链数据结构

2.2. 联盟链

联盟链是区块链的一种特殊类型，主要应用于一些具有相同需求的群体，若有额外需要，第三方机构也可通过联盟链的第三方 API 接口来实现查询等限定功能，联盟链的所有成员都要共同决定链中的所有选定节点，这些被选定的节点将会被定为记账节点，在以后的链上区块的生成任务都会有这些选定的节点来完成。除了这些选定节点外，接入联盟链的还有很多的其他节点，这些节点在将来联盟链的运行过程中可以进行交易行为，但是不能进行记账行为。区块链的三种类别本质上没有太大的区别，只是因特性的不同而被应用在了不同的环境而已[7]。对于其他的两种区块链，联盟链具有以下的特性：

1) 部分去中心化

和完全去中心化的公有链不同的是，联盟链主要应用于一些具有相同需求的群体，只被内部的成员拥有，不会随意破坏联盟的整体性，在整个联盟群体中，新的交易发出时，由于成员节点数量较少，交易很容易就会达成一致。

2) 可控性较强

我们都知道，区块链数据具有不可篡改性，数据一旦形成，将无法更改，这是因为，区块链的公有链节点非常多，因此，若是要修改一条数据，则需要链点大多数的同意才能操作，但由于参与节点众多，做出修改操作所付出的代价已远远超过修改数据本身，因此公有区块链保持了链上数据的不可篡改性。但是，在联盟链中，链上内部选定节点较少，做出达成共识的修改操作难度不是特别高，因此，联盟链上的数据具有一定的可操作性。

3) 数据不会默认公开

同样和公有区块链相比，联盟链的数据在被访问时需要访问者被赋予权限，才能进行访问操作。这种链上数据不会默认公开，在一定程度上保证了链上数据的安全。

4) 交易速度很快

同私有区块链相同，联盟链的内部节点较少，在进行交易时节点间共识达成一致所需时间更短，交易速度相比于公有区块链更快，在运行时效率和灵活性更高。

区块链在经过了一段时期的发展后，已经可以很好的应用在不同的场景中了，比如数字货币、产品溯源、税务凭证等等。针对目前医疗行业中电子病历信息共享以及数据隐私安全的问题[8]，区块链中的联盟链给出了一份完美的解决方案。根据联盟链的特性，我们可以设计一种合理的智能合约调用方式来存储电子病历和保护医疗数据隐私的安全。同时，将各大医疗结构联合起来作为联盟链的链上节点，共同维护链上医疗数据，以此搭建一个安全可信的医疗数据共享平台。

3. 智能合约设计

3.1. 智能合约的程序设计机制

智能合约可以理解成一种数字形式的承诺，类似于纸质合同，当条件触发时，合约内容则自动执行，无需监管。主要包括保存机制、事务保存和处理、交易处理和完备的状态机。接受处理合约内容需要状态机来操作，同时，条件符合后，按照合约内容要求，预定的数据将会被传出。

智能合约主要包括函数调用、函数修饰器、事件和合约结构等结构要素，一个具有完整功能的智能合约需要使用这些结构要素来设计，同时，合约的设计过程也会用到 Constant 状态变量、抽象、继承等机制，这为整个设计提供了极大的便利。

本文使用 solidity 语言来设计智能合约，具体机制如下：

1) 数据类型。开发智能合约的数据类型主要包括 bool、struct、mapping、string 和 address 等等。其中，地址 address 是出现次数比较多的一种，主要存储部署的合约地址或者系统使用者的地址，比如系统中的病人、医生、研究人员或者医疗机构。

2) 状态变量。状态变量主要表示智能合约的状态，当状态变量发生变化，则表示智能合约的状态也发生了改变。也可以通过修改状态变量来达到改变智能合约生命历程的目的。

3) 关联和继承。和 JAVA 类似，智能合约相互之间也存在关联和继承关系，但是，由于区块链的分布式存储特点，智能合约间的关系和面向对象方法中的类相比又稍有不同，如果同样采用高内聚、低耦合的方式来构造智能合约的话，可能会降低联盟链内部智能合约的可访问性。

4) 合约事件。智能合约设计中，需要着重考虑事件机制的合理性。事件机制设计的准确与否将会直接关系到智能合约是否会被无误的执行，运行效果是否会达到预期的目标。

3.2. 基于联盟链的安全可信电子病历智能合约设计

按照目前医疗行业整体特性，结合联盟区块链在数据隐私保护方面的技术特点，充分考虑对病人电

子病历信息数据的安全保护，我们在设计基于联盟链的电子病历智能合约时合理调整系统的使用者之间的权限关系，以达到预期的目标。设计的智能合约包括联盟链电子病历系统合约、病人合约、医生合约、研究人员合约、病历合约、权限管理合约和医疗机构联盟合约[9]。用合约及合约之间的调用关系来描述联盟链电子病历医疗系统的逻辑结构，电子病历中智能合约调用关系见图 2 所示。

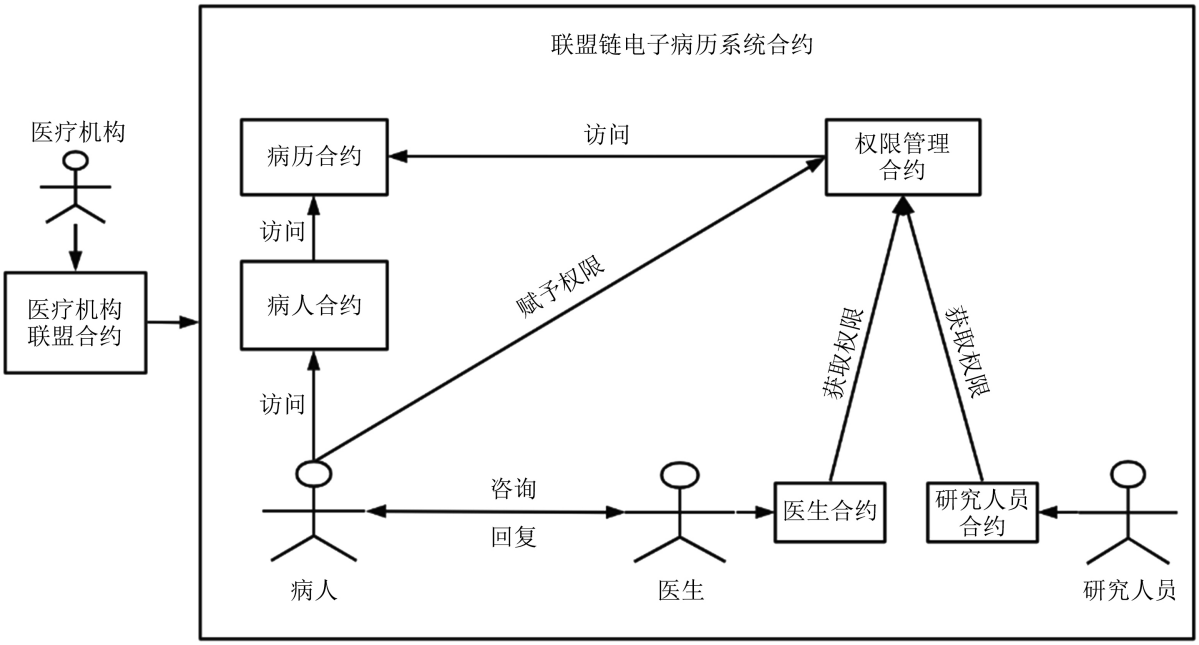

Figure 2. Smart contract calling relationship in EMR
图 2. 电子病历中智能合约调用关系

1) 联盟链电子病历系统合约。联盟链电子病历系统合约设计了整个联盟链电子病历系统的运行机制，管理所有注册到联盟链平台上的用户信息，包括医生、病人和研究人员，同时也为所有访问此系统的用户提供访问机制，为病人提供病历管理、医生咨询、查询权限赋予等操作功能；为医生提供查看病历、获取信息服务、为研究人员提供信息的查询服务。除此之外，医疗机构之间共享医疗信息也将先进入此系统才能进行操作。在系统中在修改电子病历或个人信息数据时，不同于传统直接修改数据，合约只添加新的信息，并且调整合约内部元指针在本地数据库中的指向位置，在查询时访问已添加的新数据，从而修改数据。

2) 病人合约。病人合约用于病人管理自己的个人信息，病人可增添自己的个人信息，也可通过病人合约调用病历合约，查询或修改自己的病历信息。病人也可以通过此合约来给其他医生或者研究人员赋予查看自己电子病历信息的权限。还能通过联盟链电子病历系统向医生发出请求，医生用户可根据通过病人赋予的权限查看病人的相关病历，并按照请求信息中的患者地址返回响应内容。

3) 病历合约。病历合约主要用来管理病人的病历信息，其中包含了大量的元指针信息，通过元指针可查询到存储在部门节点的本地数据库中最终的病历数据信息，根据访问者的权限不同提供不同等级的元指针信息，同时向访问者提供增删改查等操作。

4) 医生合约。医生合约用于管理医生的个人信息。同时，医生可通过联盟链电子病历系统来查询系统中已储存的医生信息或者患者个人信息，可以为前来咨询的病人提供相应的医疗服务或者与其他的医疗机构医生成员进行医学交流。

5) 研究人员合约。研究人员合约用于管理研究人员的个人信息。同时研究人员可以在被赋予权限之后查看病人的电子病历信息，以供医学研究。

6) 权限管理合约。权限管理合约定义了所有系统中的权限操作，包括电子病历的访问查询、公开和非公开数据的显示等。

7) 医疗机构联盟合约。医疗机构联盟合约用于管理所有联盟链上的医疗机构信息，医疗机构之间构成了整个的数据分享平台，医疗机构联盟合约可以用来管理医疗机构的沟通合作。

本文的智能合约设计主要包含用户身份和病历数据两个部分。其中针对用户身份主要包含系统使用者：病人、医生、研究人员和医疗机构。每个用户在注册时会被分配唯一用户 ID，在登陆时由系统确认其身份合法性，且每个唯一 ID 都由以太坊地址表示，地址私钥由用户保管；针对病历数据主要包含病人的就诊信息等相关医疗信息数据，以病历数据为重点，以上传数据的哈希值和联盟链链上数据属性来保证数据安全可信。

3.3. 智能合约数据设计验证方法

智能合约内部的方法即为将来执行时的一个个功能单元，维持着系统的正常运行。智能合约部署到链上后，合约代码无法修改，在事件被触发后开始执行，因此，在部署智能合约之前，要严格的对智能合约的功能设计进行验证。以下是验证智能合约数据设计安全有效性的方法。

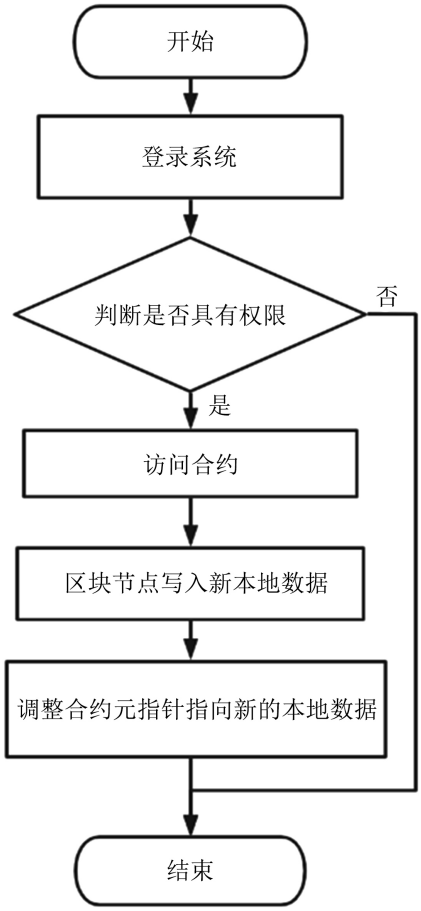

Figure 3. Flow chart of data modification
图 3. 修改数据的流程图

1) 添加数据的方法。我们可以进行病人病历的数据添加、医生或者研究人员的信息数据添加、新的医疗机构的信息数据添加。根据联盟链电子病历系统合约内容，每增加一条个人数据或者电子病历数据，都会产生一个新的合约来对其进行数据管理。

2) 修改数据的方法。由于联盟链的自身特性，修改数据会存在巨大的困难，我们在设计系统的时候也考虑到这一情况，设定为在执行修改电子病历或个人信息数据时，合约直接添加新的信息，且对旧的信息做已修改说明。同时将智能合约中的元指针调整指向新的本地数据，根据访问者在合约中查询数据所具有的权限的不同，智能合约中的元指针会指向规定的本地数据，系统对其显示的信息也不同，从而达到不篡改数据而修改数据的效果。修改数据时的流程图见图 3 所示。

3) 删除数据的方法。联盟链电子病历系统中的数据并不能进行删除操作，但在系统中存在两种类似的删除行为，一是智能合约本身的注销，在设计智能合约时，提前设计了智能合约注销事件，满足条件时即可销回智能合约；二是病人其他系统使用者将自己的信息访问权限设置为禁止访问。且不对外开放，系统对外可表示为无此用户信息。以表现出类似删除的操作。

4) 查询数据方法。查询数据时根据访问者的访问权限级别不同，可访问的数据也不同，通过管理权限分配来达到控制数据查询的目的。

4. 总结与展望

本文研究讨论了区块链技术中的联盟链的特性，并将之应用在传统医疗行业中，将各医疗机构视为联盟链的节点，组成一个庞大的医疗数据共享平台，并且通过设计联盟链电子病历系统的智能合约，进行访问权限管理，完成对病人电子病历信息、用户个人信息的隐私保护，确保数据的安全可信。除此之外，本文在智能合约设计中创新性的加入元指针来管理本地数据，在智能合约中可以找到部门节点本地数据库的元指针，然后程序通过这个元指针可以查询访问到最终的数据。通过智能合约中元指针的设计，相比于传统联盟链系统，避免了联盟链链上数据过于庞大，导致系统运行响应慢等一系列问题。病人、医生、研究人员和医疗机构在智能合约的合理调度下可以进行安全的交流咨询合作，同时链上数据也可以追溯，方便后续的研究治疗。

区块链技术在医疗上的应用发展缓慢，主要障碍在于各医疗机构对于病人的病历数据严格管控，且视为自己医疗机构的资源，不愿意将数据公开。本文所讨论的智能合约设计在解决这一障碍上给出了一个可供思考的解决方法：各医疗机构的医疗数据信息仍然存储在本地数据库，只是当机构本身成为联盟链节点后，由智能合约中的元指针来指向本地数据库，数据还存储在本地，但可控制元指针的访问权限来保护本地数据库的数据安全。在智能合约的设计上还有很长的路要走，还有更好的方法等着我们去探索研究。

基金项目

海南省重点科技计划项目“基于区块链的联盟业务协同关键技术研究与应用”(编号：2020018)；海口市科技计划项目“基于区块链技术建立安全可信的电子病历研究”(编号：2020-049)；海南省教育厅项目资助(项目编号：Hnjg2021ZD-10)。

参考文献

[1] 张圣垚. 基于区块链的电子病历系统的设计与实现[D]: [硕士学位论文]. 哈尔滨: 哈尔滨工业大学, 2018.

[2] 尹慧子, 张海涛, 刘雅姝, 等. 国内外医疗信息共享研究进展[J]. 情报理论与实践, 2020, 43(1): 177-181+162.

[3] Azaria, A., Ekblaw, A., Vieira, T., *et al.* (2016) MedRec: Using Blockchain for Medical Data Access and Permission Management. *Repot on Health Information Blocking*, **11**, 25-30.

[4] Daniele, M., Peter, M. and William, N. (2017) Validation and Verification of Smart Contracts: A Research Agenda. *Computer*, **50**, 50-57. https://doi.org/10.1109/MC.2017.3571045

[5] 戴钰涵. 基于互联网的个人医疗解决方案——传统医疗服务的改良与升级[J]. 中国管理信息化, 2016, 19(2): 227-228.

[6] 任天宇, 王小虎, 郭广鑫, 等. 基于多级身份验证和轻量级加密的电力物联网数据安全系统设计[J]. 南京邮电大学学报: 自然科学版, 2020, 40(6): 12-19.

[7] 胡凯, 白晓敏, 高灵超, 等. 智能合约的形式化验证方法[J]. 信息安全研究, 2016, 2(12): 1080-1089.

[8] 孙学波, 姜金希. 基于区块链的医疗信息系统及智能合约设计[J]. 辽宁科技大学学报, 2020, 43(2): 135-145.

[9] 高健博, 刘宏义, 李青山, 等. 智能合约安全漏洞检测技术研究[J]. 保密科学技术, 2020(1): 22-25.