Computer Science and Application 计算机科学与应用, 2019, 9(3), 580-587
Published Online March 2019 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2019.93066

Hans汉斯

Research and Application of Food Traceability Based on Blockchain

Mao Yang, Bin Wen*, Dequan Lu

College of Telecommunication Engineering, Chengdu University of Information Technology, Chengdu Sichuan
Email: *474471429@qq.com

Received: Feb. 25th, 2019; accepted: Mar. 7th, 2019; published: Mar. 14th, 2019

Abstract

In recent years, food safety has become the focus of the whole society. Food safety incidents are not uncommon. Now there is an urgent need for a reliable mechanism to strengthen the management and supervision of food safety, improve food safety and ensure people's food health. The rapid development of blockchain technology in the past two years has made its application scenarios widely used in all walks of life. Its decentralization, self-contained trust, data disclosure and transparent traceability can be applied to the traceability of food. Blockchain can be regarded as a distributed account book. Its distributed storage structure can ensure the authenticity and integrity of information. The blocks are connected through a consensus mechanism. In combination with cryptography, information can be effectively prevented from being maliciously tampered in the collecting and transferring process. Therefore, the blockchain technology can solve the pain points of the information centralization management and information asymmetry in the traditional food traceability. This paper will build a traceability system based on blockchain technology. The core of the system is a three-tier architecture, which can effectively trace the extraction, processing and sales process of food.

Keywords

Food Traceability, Distributed Structure, Blockchain Technology, Consensus Mechanism, Three-Tier Architecture

基于区块链的食品溯源研究与应用

杨　茂，文　斌*，卢德全

成都信息工程大学，通信工程学院，四川　成都
Email: *474471429@qq.com

收稿日期：2019年2月25日；录用日期：2019年3月7日；发布日期：2019年3月14日

*通讯作者。

文章引用: 杨茂, 文斌, 卢德全. 基于区块链的食品溯源研究与应用[J]. 计算机科学与应用, 2019, 9(3): 580-587.
DOI: 10.12677/csa.2019.93066

摘　要

近年来，食品安全问题成为全社会关注的焦点，食品安全事件屡见不鲜，现在急需要一个真实可靠的机制来加强对食品安全的管理监督、提高食品安全水平、保证人们的食品健康。这两年区块链技术的快速发展使得其应用场景广泛适用于各行各业，其去中心化、自带信任、数据公开透明全程可追溯的特点可以应用于食品的溯源，区块链可以看作是一个分布式的账本，其分布式的存储结构可以确保信息的真实性与完整性，区块之间通过共识机制联系在一起，再结合密码学原理可以有效地防止信息在收集、流转过程中被恶意篡改。本文将构建基于区块链技术的溯源系统，其核心是三层架构，对食品的采摘、加工以及销售过程都可进行有效溯源。

关键词

食品溯源，分布式结构，区块链技术，共识机制，三层架构

1. 引言

从 20 世纪 90 年代开始，许多国家和地区已经应用可追溯系统进行食品以及农产品质量安全管理。在市场经济高度发达的美国，农产品可追溯系统主要是企业自愿建立，政府主要起到推动和促进作用。美国的行业协会和企业建立了自愿性可追溯系统。由 70 多个协会、组织和 100 余名畜牧兽医专业人员组成了家畜开发标识小组(USAIP)，共同参与制定并建立家畜标识与可追溯工作计划，其目的是在发现外来疫病的情况下，能够在 48 小时内确定所有涉及与其有直接接触的企业。2003 年 5 月 FDA 公布了《食品安全跟踪条例》，要求所有涉及食品运输、配送和进口的企业要建立并保全相关食品流通的全过程记录。

而我国对食品溯源系统也在不断地完善，2016 年 10 月，阿里健康联合天猫医药共同启动“滋补中国”品牌战略，并宣布建立“滋补中国追溯体系”，实现对滋补品“一品一码”的追溯。借助阿里健康“码上放心”平台，可以实现对相关滋补品的溯源，相当于滋补品都有了“身份证”。虽然现在溯源越来越被看重但是传统的溯源方式还是存在很多问题未解决，将食品信息集中存储在一个中心数据库里有被人为篡改的风险，造成消费者或者监管者对食品信息的信息不对称从而带来很多危害，而区块链技术的分布式存储的结构形成了去中心化的数据存储[1]，极大的保证了信息对称性。

本文将区块链与食品溯源相结合构建一个基于区块链技术的溯源系统，其核心是三层架构，能够解决现有溯源系统的部分痛点。该系统架构分为应用层、管理层、网络层三层，实现食品从采摘、加工以及销售过程都可从手机 App 查询进而达到有效溯源。

2. 区块链

2.1. 区块链的意义

区块链技术是密码学、计算机科学、经济学等多个学科发展到一定阶段后的产物，有效融合了多个

学科的杰出成果。区块链技术的出现为解决人类社会的信任问题提供了有力工具，进而将人类社会带入群智时代。

区块链系统本身能产生信用，这种具有信用的产品不是来自第三方，而是来自程序(算法)，因为区块链记录信息的产生需要全网络节点确认，而一旦生成将永久记录，无法篡改。互联网的底层协议是 TCP/IP 协议，实现了信息的低成本高效率传播；区块链可认为是一种新的底层技术，建立了新的信用体系。区块链取代了目前互联网对中心服务器的依赖，使所有数据信息都被记录在一个云系统之上，理论上实现了数据传输中的数据自我证明，从深远意义上讲，这超越了传统和常规意义上需要依赖第三方的信息验证模式，降低了建立全球信用体系的成本。

区块链还创造了一种新的价值交互方式基于“弱中心化”[2]，但这并非意味着传统社会里各种“中心”的完全消失，未来区块链将出现大量的“多中心”体系，以联盟链、私有链或混合链为主，区块链将会进一步提高“中心”的运行效率，并降低其相当一部分成本。

区块链是一种由多方共同维护，以块链结构存储数据，使用密码学保证传输和访问安全，能够实现数据一致存储，无法篡改，无法抵赖的技术体系。这种技术给世界带来了无限的遐想空间，全球对区块链的关注热度持续升温，全球主要经济体从国家战略层面开始对区块链技术及发展趋势进行研究。

可以这样说，第一次工业革命是蒸汽机的发明为标志，第二次工业革命是以电力的产生，第三次工业革命是电脑与互联网信息技术的出现，那么第四次工业革命将是区块链技术的诞生。

2.2. 区块链特点

基于区块链的系统和以往的其他系统有很多的不同之处，以区块链为核心的有以下几大特点：

1) 分布式的(Distributed)：区块链没有中心节点，数据分布式的存储在各个节点上，即使绝大部分节点毁灭了，只要还有一个节点存在就可以重新建立并且还原区块链数据。

2) 自治的(Autonomous)：区块链是一种去中心化的、自治的体系[3]，所有节点是对等的，每个节点可以自由的加入或者离开但不会影响整个区块链系统，并且当系统运作起来可自行产生区块并同步数据，无需人工参与。

3) 按照合约执行(Contractual)：区块链是完全按照合约执行的，各个节点都有运行规则，一旦不符合规则就会被抛弃，其中最重要的便是智能合约，智能合约是一种可程序化的合同条款、规则或规定。

4) 可追溯(Trackable)：区块链中的数据是公开透明的，不能被篡改[4]，并且相关区块之间有一定的关联性，因而和容易被追溯。

若我们把每一个区块看作是一个账本上面记录着所有的交易记录，那不同区块之间的联系也可以看作不同的交易，则其工作的原理如图 1 所示。

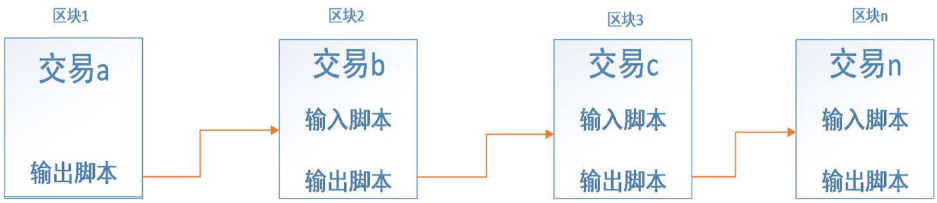

Figure 1. Blockchain schematic
图 1. 区块链原理图

区块链(blockchain)是由多个区块链链接而成的连表结构，除了首区块(“创世区块”)之外，每个区块都由前一个区块的输出脚本控制，如图 1 所示每个区块都可以看成一个账本上面都有对应的交易记录a, b, c...n，每个区块都由前一区块的输出脚本与后一个区块的输入脚本联系起来，此时我们可以形象的把

输出脚本和输入脚本看作一把锁和钥匙之间的关系，只有正确的钥匙才能打开正确的锁，以区块 1，区块 2 为例如果区块 2 输入脚本是区块 1 的正确的钥匙那么区块 1，区块 2 之间的交易才有效，否则交易无效，交易有效之后交易 b 也会包含一部分交易 a 的信息，这时候我们就可以根据区块 2 溯源到区块 1。

2.3. 共识机制

近几年区块链技术从 1.0 时代发展到 2.0 时代再到正在到来的 3.0 时代，其共识机制扮演着不可或缺的角色，整个区块链网络是靠区块之间的节点通过共识机制维持着稳定。现在主流的共识算法有以下几种[5]：

1) POW 算法：工作量证明算法，是最早提出的一种共识机制，靠参与者(矿工)进行挖矿为区块链网络提供算力，随着矿工的人数增加整个网络就越稳定，系统会给矿工的付出给予一定的奖励机制，以比特币和早期的以太坊为代表。

2) POS 算法：股权证明算法，是根据参与者持有整个系统的代币的数量和时间来确定记账权的算法。

3) PBFT 算法：实用型拜占庭容错共识算法，是根据 BFT (拜占庭容错)改进得到，此算法不像前两种算法会对发行代币，但 PBFT 具有极高的安全性，节点容错率和最终性。以 Hyperledger 的 Fabric 框架为代表。

本文溯源系统为长远打算选取的是根据 POS 改进得到的 DPOS 算法即股权授权算法，是在参与者里通过类似居委会选举制度，选举一部分人为代表人进行投票确定记账权，优化了 POS 算法中可能出现的中心化现象。

DPOS 算法可分两部分：如何选择一群区块生产者及调度区块生产。选择过程要确保利益持有方拥有局面最终控制权，因为当网络非正常运行时，利益持有方的损失最大。由于选择过程本身对实际如何达成共识几乎没有影响[6]。

为更好的解释这个算法，假设有 3 个区块生产者 A，B 和 C。因为达成共识要求 2/3 + 1 多数来裁决所有情况，在这个简化的模型中假设生产者 C 是打破僵局的角色。在现实中，会有 21 个或更多的区块生产者。类似工作量证明，一般规则是链最长者胜出。任何时候，当一个诚实节点看到一个更长的有效链时，它都会从当前分叉切换到更长的这条有效链。当大多数生产者不合格时，DPOS 还是可以继续行使功能的。这样，社区可以投票替换掉不合格的生产者，直到恢复 100%参与率。

说到底，DPOS 之所以有如此强大的安全性，是来自于其选择区块生产者和验证节点质量的算法。赞成投票过程可以确保一个人即使拥有 50%的有效投票权也无法独自挑选指定哪怕一个生产者。DPOS 的设计旨在优化强劲网络连接的诚实节点 100%参与共识的机制。这使得 DPOS 能够在平均只有 1.5 秒的时间内以 99.9%的确定性确认交易，同时以优雅和可检测的方式降级，从降级中恢复到正常也不过是小事一桩。

2.4. 数字签名

数字签名实际上就是非对称加密的算法，即生成公钥和密钥一对密钥，公钥是根据私钥生成的一个地址，所以用私钥对数据进行加密，只有拿到对应的公钥才能进行解密，私钥是只能自己持有，同时生成的公钥由交易发起方公布给交易对象，交易对象通过公钥解密才能看到区块中的信息，从而保证了数据的真实性和可追溯性。

当区块内的信息状态要发生转移时，为保证数据信息的安全性与真实性，区块链节点之间在共识机制的依托之下需要对区块信息进行签名，而交易方必须拿到对应的公钥才能解密才能看到真实的数据信息，验证过程由脚本语言控制其执行的原理如图 2 所示。

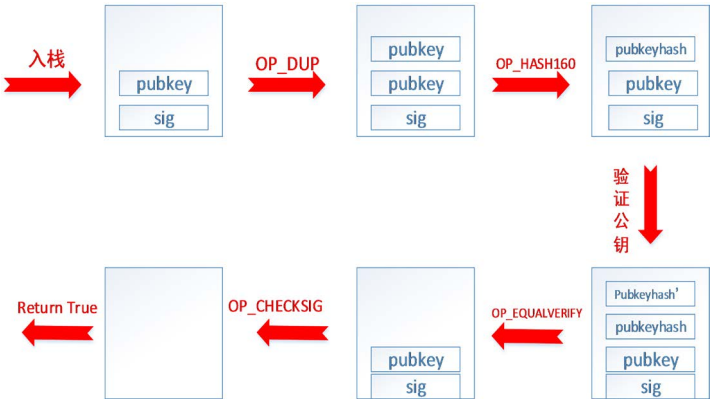

Figure 2. Script execution diagram
图 2. 脚本执行图

我们可以将脚本看作是一个栈，栈是一个后进先出的容器，那么脚本执行过程我们亦可以看成是一个对栈的操作过程[7]，中间过程由相应的合约代码(规则)命令，要成功执行脚本关键点有两个，其一是公钥，公钥实际上就是一个地址，当产生一个交易时就会产生一个公钥，在确认交易合法性是需要出示公钥验证，验证合法交易才能继续。其二是私钥也称作交易签名，私钥也是交易时所必需的，但是私钥只有交易发起人自己拥有，具有唯一性，不可复制性，公钥是交易双方都可拥有的，所有在确保交易的合法性的时候需要公钥和私钥同时验证，均合后法交易才有效，反之无效。

所以脚本执行过程如图 2 所示第一步先将私钥公钥依次入栈，在通过 OP_DUP 命令复制栈顶元素，然后通过 OP_HASH160 命令对公钥进行 hash 算法加密，此过程保证了公钥的安全性，防止恶性攻击偷取公钥。

公钥加密后只有交易双方知道，所以当发起交易者想要进行交易时需要交易的另一方提供同样的公钥，因此第四步<pubkeyhash'>就是交易的另一方提供的公钥，此时脚本需要通过 OP_EQUALVERIFY 命令验证此时两个公钥是否相等，相等则交易继续，否则交易不合法。最后一步就是通过 OP_CHECKSIG 命令检查栈顶元素是否执行签名校验操作，此时的签名一定需要发起交易这提供自己的私钥进行签名，若操作之后相等，则返回 TRUE，否则返回 FALSE。以上所有步骤执行完了也就说明区块之间的交易成功了也就是图 1 的区块 1 到区块 2 的步骤完成了。很显然区块链的这种交易方式是具有极高的安全性，并且是可追溯的。

3. 区块链 + 食品溯源

3.1. 传统的食品溯源

民以食为天，食品安全十三五时期上升为国家重大战略。随着史上最严《食品安全法》的实施，全国各地都在就食品安全采取各项措施。其中食品溯源体系的建设成为食品安全工作中必不可少的项目。随之，食品安全溯源追溯平台市场前景可观，行业将迎来大机遇。食品安全源溯追溯平台的创立保证了食品从田地到餐桌的全程可追溯[8]，在相当程度上遏制了假冒伪劣产品的流通，同时也为消费者提供食品生产全程数据而设立的数字化动态追踪、监控系统。

食品溯源系统在物联网的技术支撑下被越来越多的企业所应用，传统的溯源体系现在主要有利用二维码或者 RFID 技术给食品印上“身份证”，用户可以在手机 APP 上查询食品的生命周期信息做到全面的了解，做到消费更透明，同时食品追溯体系的建立，当发生质量事故时能够提出恰当的应对措施，降低消费者的损失，使得消费者的利益能够得到保障。传统的溯源体系如图 3 所示。

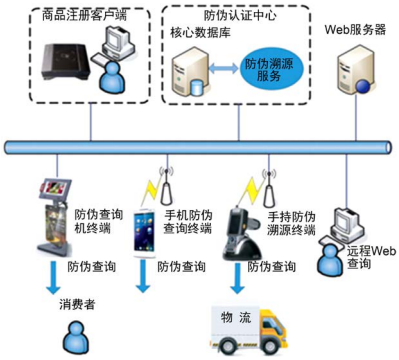

Figure 3. Traceability system diagram
图 3. 溯源系统图

可以看到传统溯源系统中有个特点就是有一个核心数据库，食品的所有信息都存储在这个数据库里，消费者通过手机的 API 接口连接到数据库进行信息查询，但是中心化数据库的内容是可以被更改的，一旦数据库的数据被更改那么消费者看到的数据信息也不一定是真实的，从而发生食品的质量问题，大大的降低了消费者对该食品和企业的信任度，同时传统的溯源系统无法看到食品从生产、加工、销售每一段的情况，中间许多过程也存在个各种风险和隐患。

为了解决以上问题，本文提出了将区块链技术融入互联网的溯源系统。因为区块链具有分布式共享总账、去中心化共识机制、智能合约、时间戳不可篡改等特征，将其融入基于互联网的溯源系统中就能使消费者看到自己食品从生产、加工到销售的每一步情况，并且能保证每一步自己所查询到的信息都是真实有效的，使得溯源系统更加数字化、智能化、规范化。

3.2. 基于区块链的食品溯源系统

为解决基于传统食品溯源系统的缺陷，可以构建基于区块链的食品溯源系统，区块链中可以任意添加或者减少区块而不影响整个系统可以使得系统更具有动态性和实效性，每生成一个区块都由唯一的不可更改的时间戳保证了其不可篡改[9]、不可复制性。将各类信息都放在区块链上，其公开透明的数据可以使用户直观的看到，使得消费者对食品，基于以上特点本文设计出如图 4 所示的基于区块链的溯源系统框架。

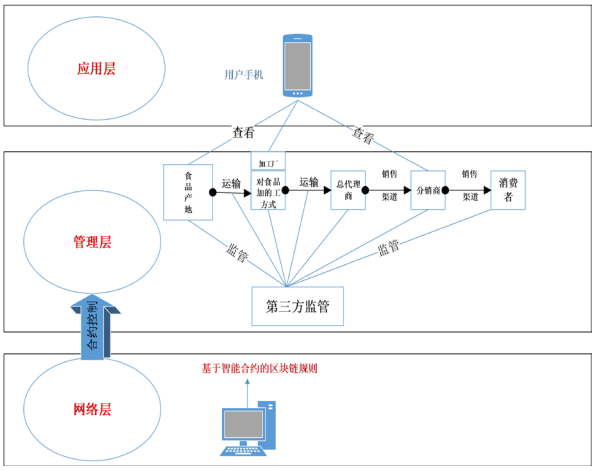

Figure 4. Traceability frame
图 4. 溯源框架图

将该系统架构分为应用层、管理层、网络层三层，其应用层是消费者通过手机 APP 直观的看到食品的原产地，食品加工厂的加工状态再到各大食品代理商以及他们的销售渠道等所有过程，每一个环节都会有一个区块记录着相同的账本，并且这个账本只允许追加而无法修改，每个区块之间都是通过满足共识机制的节点维护者整个网络不需要人为的介入，加上每个区块信息都包含有唯一的时间戳更加保证了信息的安全性[10]。区块上的信息内容是通过 hash 加密保存在默克尔树上，在极大的保证了数据真实性的情况下还防止了数据的泄露，因为只有交易方的公钥才能解密看到信息，也就是说只有交易双方能看到信息，也凸显一定的隐私性。

对于管理层第三方的监管则只需要监管者加入区块链系统并且拿到相应的公钥便能查询，但即便是监管者也是无权、无法篡改信息内容的，也避免了监管者在食品出现质量问题进行食品溯源追责的时候出现徇私舞弊的情况。

网络层

此处的网络层亦可称作是合约层，其包含了脚本代码、智能合约、共识算法等机制共同制定了控制管理层的规则，利用脚本代码使每个区块连接起来并且使其可追溯，共识算法是一种去中性化机制，提高了该系统的可信任性，智能合约则是通过代码控制输出日志记录，对于后面的溯源和监管起着至关重要的作用。

3.3. 实现机制

在溯源系统中，每一样商品在区块链网络中都是数字化的，包括其各种参数信息。数字化后形成的电子文档在区块链中是只能追加但不可修改的形式。利用相应的信息文档，认证授权中心可以通过智能合约的方式自动对商品当前担责节点开放权限，保证数据维护的有序性与可靠性，防止相关节点违规操作，实现系统有序、严谨、全面的跟踪商品。

针对本文的食品溯源而言，图 4 里的管理层的每一个环节都是被授权参与者，当被授权的参与者要维护食品的信息文档时，必须需要此参与者的私钥连接网络后，进行数据信息的输入，在进行数字签名。系统要收集一系列的信息，包括但不限于商品当前状态、产品类型、行业标准等。一旦参与者发起了产品转移，通过智能合约对数据进行审核、验证，之后将信息打包录入。被授权的节点在与另一节点进行“交易”时，两节点之间需要达成统一的协议并进行数字签名。数字签名此处采用 ECDSA (非对称数字加密)技术，保证了信息不被篡改且两节点之间信息无需公开。当“交易”在区块链网络中被核心层节点公证并进行全网广播之后[11]，包含交易信息的区块按照时间戳顺序成为区块链上的最新环节。双方交易信息的加密通过非对称加密完成的，即用私钥加密在用相应的公钥解密，保证了信息无法被恶意篡改，解决了交易过程中的诚信问题。

综上，上述的每一步都可通过区块链来记载操作日志，时间戳技术与非对称加密技术保证了基于区块链技术的食品溯源系统的可靠性和防篡改性[12]。

数据访问

在此系统中还涉及第三方的监管，就需要对区块链系统进行数据访问，因为商品的每条信息的输入都有相应的时间戳并且有相应的参与节点的数字签名。每个环节的数据都是通过参与者的私钥进行非对成加密的，那么第三方监管想要访问数据是需要拿到相应参与者的公钥进行解密，获取相应的权限之后就能看到食品信息，这种方式有利于发生食品安全问题的时候监管部门访问此类信息进行追责。

4. 结语

如今，我国对区块链的研究也是很重视，许多区块链的公司企业应声而起。随着区块链 2.0 甚至 3.0

的到来，区块链+的应用也蓬勃发展，其中基于区块链的食品溯源与防伪是国家重点支持的项目[13]。而人们对食品品质的要求越来越高，“绿色”、“健康”、“天然”、“口感佳”逐渐成为人们挑选商品和食物的标准。影响这些标准的根本就在于食品从生产、加工再到销售这一系列的供应链的操作是否安全。根据本文的方案设计的基于区块链的三层架构能够有效地保证食品从农田到餐桌的每一步的可追溯性。该系统包含了区块链技术的去中心化、不可篡改的特点，将数据进行存储，保证数据的可靠性[14]。本系统有较好的扩展性和可移植性，为用户提供方便的 App 手机查询，现在主要提供食品的数字信息的溯源查询，以后将加入图片信息的查询，使得此系统更智慧化。后期同样需要对系统的吞吐量、溯源效率等方面进行优化，实现更加有效、智能的食品溯源系统。

参考文献

[1] 冯翔, 等. 区块链开发实战: Hyperledger Fabric 关键技术与案例分析[J]. 北京: 机械工程出版社, 2018.

[2] 申屠青春. 区块链开发指南[J]. 北京: 机械工业出版社, 2017.

[3] 邹均, 等. 区块链技术指南[J]. 北京: 机械工业出版社, 2016.

[4] 林小驰, 胡叶倩雯. 关于区块链技术的研究综述[J]. 金融市场研究, 2016(2): 97-109.

[5] 罗格瓦唐霍费尔. 区块链核心算法解析[J]. 陈晋川, 等, 译. 北京: 电子工业出版社, 2017.

[6] 沈政启. 基于区块链的食品溯源系统的存储设计[J]. 通讯世界, 2019, 26(2): 304-305.

[7] 张宁, 王毅, 康重庆, 程将南, 贺大玮. 能源互联网中的区块链技术: 研究框架与典型应用初探[J]. 中国电机工程学报, 2016, 36(15): 4011-4023.

[8] 张延华, 杨兆鑫, 杨睿哲, 金凯, 林波, 司鹏搏. 基于区块链的农产品溯源系统[J]. 情报工程, 2018, 4(3): 4-13.

[9] 傅俊, 曹春益. 基于物联网的农产品质量溯源系统设计[J]. 软件, 2014(3): 9-10.

[10] 郭彬, 于飞, 陈劲. 区块链技术与信任世界的构建[J]. 企业管理, 2016(11): 110-113.

[11] 钱卫宁, 邵奇峰, 朱燕超, 金澈清, 周傲英. 区块链与可信数据管理:问题与方法[J]. 软件学报, 2018, 29(1): 150-159.

[12] 汪登, 曾小珊, 白倩兰, 孙耀杰. 基于区块链的食品安全溯源技术[J/OL]. 食品科学, 1-9.

[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] Alireza, B. and JooSeok, S. (2015) Trend of Centralization in Bitcoin’s Distributed Network. *IEEE/ACIS International Conference on Software Engineering*, *Artificial Intelligence*, *Networking and Parallel/Distributed Computing*, Takamatsu, 1-3 June 2015, 1-6.