

DOI: 10.13652/j.issn.1003-5788.2020.11.015

数字签名技术在食品产地溯源中的应用研究

Research on the application of digital signature technology in the traceability of food origin

刘 纯 刘柱鸿

LIU Chun LIU Zhu-hong

(湖南安全技术职业学院, 湖南 长沙 410151)

(Hunan Vocational Institute of Safety Technology, Changsha, Hunan 410151, China)

摘要:介绍了数字签名技术,分析了多种数字签名技术的特定和不同的应用场景;对食品产地溯源的基本原理和方法进行了分析和讨论;分析了多种数字签名技术在食品产地溯源中的应用,并对基于不同数字签名技术的食品产地溯源案例的准确性进行对比和研究;展望了数字签名技术在食品产地溯源领域的发展趋势。

关键词:数字签名;产地溯源;食品;数据认证;安全模型

Abstract: Through the introduction of digital signature technology, the specific and different application scenarios of various digital signature technologies were introduced. The basic principles and methods of food origin traceability were also discussed. The application of various digital signature techniques in food origin traceability was investigated, and the accuracy of food origin traceability cases based on different digital signature techniques was compared and studied. The development trend of digital signature technology in the field of food origin traceability was prospected.

Keywords: digital signature; origin traceability; food; data authentication; security model

食品从生产到运输,最后经过加工直到端上餐桌,中间的每一个环节都有可能出现各种问题^[1-2],其中所出现的每一个问题都将严重影响食品的质量,从而对消费者造成伤害^[3]。随着科技的发展和进步,基于大数据数字签名技术在食品产地溯源领域被广泛应用,食品产地溯源技术逐渐成为工业界和学术界的一个重点的研究课

题,并且发展形成了一套完整的技术体系^[4]。多种多样的食品产地溯源技术为中国的食品安全及公共卫生事业作出了重要贡献,有效保护了消费者的根本利益和生命财产安全^[5]。随着移动互联网、智能传感器、新一代无线通信等技术的大规模应用,其为人们提供了记录和分析食品在生产^[6]、流通和制作过程中状态实时变化的能力。食品的各种状态可以通过结构化的数据来描述,如何对这些数据进行建模和分析,发掘其中的重要信息以支撑食品产地溯源技术的发展尤为重要。以区块链技术为代表的数字签名技术,具有去中心化^[7]、不可修改^[8]、保护隐私、安全、高效、成本低等特点^[9],因此非常适合应用于食品的产地溯源等领域中。利用数字签名技术建立起一套完整的视频产地溯源体系,不但可以降低各个监管部门的运行成本,更能够提升食品在生产、运输和制作过程中其状态的透明度和可信度。

文章拟针对数字签名技术在食品产地溯源中的应用展开分析和讨论,对数字签名技术中的“智能合约^[9]”“区块链技术^[10]”在食品产地溯源领域中应用的细节进行介绍;综合比较基于数字签名技术的食品产地溯源技术和基于传统方法的食品产地溯源技术的差异^[11],并总结国内外对数字签名在食品产地溯源领域的最新研究进展,从不同角度对具体的实际应用场景进行探讨和总结,以为食品产地溯源技术的发展提供依据。

1 食品产地溯源的基本概念

食品产地溯源一般包括农产品产地溯源和非农产品产地溯源。目前,这两种类型食品所使用的产地溯源技术差异巨大^[12]。农产品产地溯源最常用的是通过分析食品生产地的特殊性指标间接地完成食品的产地溯源^[13]。目前,该类型食品应用较成熟的技术手段包括光谱检测技术、分子生物学检测技术和质谱分析技术等,这些技术通过产品的具体成分,如挥发性成分、特定同位素含量等指标,并结合相关的物理化学方法对农产品的生产场地

基金项目:湖南省教育厅科学研究项目(编号:18C1238);湖南安全技术职业学院关键科学技术研究项目(编号:HX19Y001)

作者简介:刘纯,女,湖南安全技术职业学院讲师,硕士。

通信作者:刘柱鸿(1972—),男,湖南安全技术职业学院副教授。

E-mail:284769717@qq.com

收稿日期:2020-08-19

进行特征分析,从而完成产地溯源^[13]。

非农产品产地溯源的应用范围比较广泛,包括奶粉、包装类食品、速冻食品等^[14]。这种类型的食品在传统的产地溯源模式中,只能靠产品的标签信息进行信息追溯^[15]。在这种信息严重不对称的情况下,极易容易出现仿冒产品,例如号称是纯进口的奶粉,其实是国内的代工产品;但是在这种情况下,消费者难以界定,有可能被宣传误导,从而造成一定的经济损失^[16]。即使有些产品具有真实的产地等信息,消费者也难以通过标签直接判断食品的质量。

就目前而言,农产品在产地溯源问题上虽然难度较小^[17],但是普通的消费者很难使用各种化学检验的方式进行分析;此外,农产品在运输和制作过程中的状态难以记录和分析。非农产品存在严重的信息不对称性,消费者只能通过标签对食品的产地进行溯源。针对食品产地溯源领域中存在的“信息孤岛^[18]”以及“信息壁垒^[19]”等问题,科研人员引入了数字签名技术^[20]。基于区块链的数字签名技术可以建立起一套完整的食品产地溯源体系,食品从生产、运输以及最终的交易信息都可以被完整地保存下来,这些记录一旦生成将无法被更改,极大地提升了食品的信息透明度^[20]。

2 数字签名的基本概念

人类在很长一段时间内都是以手写签名、印章或指模等来确认作品、文件等的真实性,包括认定作品的创作者、文件签署者的身份^[21],推定作品的真伪或者文件内容的真实性。数字签名技术用于在数字社会中实现类似于手写签名或者印章的功能,从而实现数字签名的整个过程。数字签名技术实际上能够提供比手写签名或印章更多的安全保障。一个有效的数字签名能够确保签名的确是由认定的签名人完成,即签名人身份的真实性;被签名的数字内容在签名后没有发生任何改变,即被签名数据的完整性;接收人一旦获得签名人的有效签名后,签名人无法否认其签名行为,即不可修改性。

3 数字签名技术在食品产地溯源中的应用

3.1 智能合约在食品产地溯源中的应用研究

智能合约是数字签名技术的一种,被广泛应用于数字货币等领域^[22]。智能合约是区块链中的一种通用协议,这种协议中包含了一些可执行的代码;不同的智能合约通过自身的可执行程序,可以与其他智能合约进行互动,完成信息的存储^[23]。智能合约主力提供验证及执行合约内所订立的条件。目前,智能合约技术支持去中心化的交易方式,这种交易可以在没有第三方参与的情况下进行,并且交易具有公开性和不可修改性^[24]。

在食品产地溯源领域,可以将智能合约技术应用于

食品生产、流通和交易的各个环节,从而有效地解决“信息孤岛”和“信息壁垒”等问题。文献^[23]以进口食品为例,提出了一种基于智能合约的商品产地追溯方案,在完整的交易流程中,主要是由货物的卖家和货物的买家达成交易协议而带动的一系列的交互过程,从而完成主智能合约。与此同时,其他商家交易方可以使用多个子智能合约,一旦达到交易条件,则可以开始执行该项交易流程,执行过程中,所有的操作都将被记录而无法修改,因此消费者可以通过同一个平台对其中所有的交易和流通环节进行查看。文献^[25]进一步提出了一种改进的食品产地溯源方案,该方案包含多个智能协议,其中包括一个主合约和多个子合约。交易过程中,需要使用主智能合约完成整个交易流程的联动工作,因此所有的子智能合约的交易执行不能违背主智能合约的条款。主智能合约与子智能合约之间存在一种链式关系,所有的交易和执行信息会通过链式的传递方式分级发送;因此,交易双方一旦开始执行,另外的一个账户也会受到交易执行的指令。为了完成智能合约的执行,双方需要同时授权开放,这种多级分布式的合约系统保证了信息记录的可靠性和稳定性,使不法分子难以对食品产地、交易地点等信息进行篡改,保护了消费者的权益。文献^[26]指出建立在block-chain技术的基础上,虽然交易双方互不认识,但是因为block-chain的设计机制,交易双方不必怀疑对方的信息。智能合约与智能合约之间的执行和交易一般是由事件驱动的,其具体结构如图1所示。只有当所有子智能合约验证交易确认完成,主智能合约双方才可以看到一份“合法有效”的交易,且交易被记录于特定区块中,商家可从中获取账户收益数据^[27]。

3.2 链式结构在食品产地溯源中的应用研究

区块链中的链式结构是数字签名中的一项非常重要的技术。链式结构主要分为公有链和私有链,其中私有链式结构可以有效保护交易双方的隐私,并且交易延迟低、速度快,适用于隐私性较强的食品产地溯源。文献^[28]设计了一种基于链式结构的食品产地溯源系统,该系统利用相对于食品交易的银行转账信息更具有难以伪造性,且每一产品都有唯一与其对应的二维码,因此对存在公有链中的数据进行建模,使用KNN^[29]模型来完成食

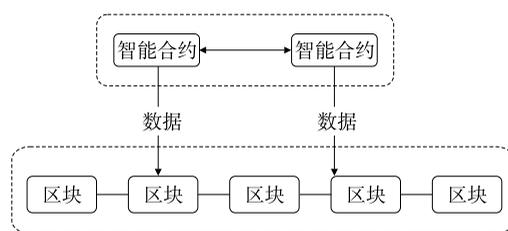


图1 智能合约的交易架构

Figure 1 The transaction structure of the smart contract

品的产地溯源任务。文献[30]则以进口乳制品为例,设计了一种基于公有链和私有链的混合食品产地溯源技术,首先,各个产品生产企业将交易信息以时间戳方式进行记录,例如乳制品生产时间、生产数量、原材料产地、交易的具体信息等录入企业的私有链中;其次,商家还需要将私有链中所记录的有关商品交易的具体信息再次上链至公有链中,保持对外公开透明,其流程如图2所示。产品的买卖双方均需要对产品的具体交易信息进行记录和上传,并在区块中进行记录;对于其他的隐私数据可以记录至私有链中,既实现了信息公开,也保证了交易双方的隐私。实践显示,基于混合链的食品溯源系统可以更好地保存所有交易的细节信息,更加有助于食品产地的追溯^[31]。



图2 基于混合链的食品溯源系统

Figure 2 Food traceability system based on hybrid chain

3.3 数字签名结合生物技术在食品产地溯源中的应用研究

非农业食品的产地溯源领域中,最大的问题是“信息壁垒”和“信息孤岛”,但是这一问题在农产品中并不存在。农产品在食品产地溯源领域中最大的问题是存储和流通之间产生的问题^[32]。一旦农产品出现质量问题,具体的责任方无法落实,最后只能由消费者买单。为了解决这一问题,文献[33]提出了一种基于数字签名技术和生物技术的食品产地溯源技术,该技术将分子生物学技术与数字签名技术结合,共同完成了农产品的产地溯源。分子生物学溯源技术主要是运用脱氧核糖核酸(DNA)技术进行溯源,DNA的本质是脱氧核糖核酸,由于其分子结构排列组成的多样性,使不同生物具有不同的DNA结构。DNA是生物的特有属性,不会因环境的变化而改变,因其独特性与稳定性,可作为溯源的依据。根据获取研究对象特征DNA,经数据处理建立数学模型,是一种准确、灵敏的溯源技术。将生物学技术检验出的结果上传至区块链中,形成完整的数字签名,消费者和各级监管部门可以通过数字签名技术和生物检测技术的结合更加全面地对食品产地进行溯源。文献[20]提出了使用核磁共振技术和数字签名技术完成对白酒、水果、食用油等的产地追溯。

3.4 多种混合技术在食品产地溯源中的应用研究

随着检测技术的不断发展以及农产品内部成分的复杂化^[34],依靠单一的技术已无法实现有效的产地溯源,越来越多的研究者开始关注多种溯源技术的联用^[35],以

提高食品产地溯源的准确率^[36]。不同溯源技术之间可以通过多参数多指标多技术融合的方式进行结合,对数字签名食品溯源技术^[37]、同位素指纹溯源技术^[38]、矿物质元素指纹溯源技术^[39]、拉曼光谱指纹溯源技术、核磁共振指纹溯源技术、高光谱指纹溯源技术等进行结合使用,充分利用每一种溯源技术的优点,在提高食品产地溯源的准确性上具有广阔的应用前景。文献[39]通过提出联合数字签名技术和化学分析的方法对樱桃产地进行追溯,结果显示,基于混合技术的食品产地溯源方法在判别准确率上远优于传统方法。

4 结论

数字签名技术是一种全新的技术体系,该技术具有去中心化、不可修改、保护隐私、安全、高效、成本低等特点,因此非常适合应用于食品的产地溯源等领域中。基于数字签名技术的食品产地溯源技术,可以对食品的交易流程进行全方位的记录。由于数字签名本身具有去中心化等特点,因此可以防止所记录的数据被修改,保证记录的安全可靠。文章从数字签名技术在食品产地溯源领域的应用为出发点,介绍了多种基于数字签名技术的食品产地溯源方法,分析了各个方法的优缺点和使用场景。

参考文献

- [1] 鹿保鑫, 马楠, 王霞, 等. 大豆有机成分辅助矿物元素指纹特征产地溯源[J]. 食品科学, 2019, 40(4): 348-354.
- [2] 刘静, 管晓, 易翠平. 近红外光谱技术结合支持向量机对食用醋品牌溯源的研究[J]. 食品与机械, 2016, 32(1): 38-40.
- [3] 鹿保鑫, 马楠, 王霞, 等. 基于电感耦合等离子体质谱仪分析矿物元素含量的大豆产地溯源[J]. 食品科学, 2018, 39(8): 295-301.
- [4] 李明佳, 汪登, 曾小珊, 等. 基于区块链的食品安全溯源体系设计[J]. 食品科学, 2019, 40(3): 288-294.
- [5] 杨雪菲, 郑东, 任方. 一种基于QC-LDPC码的数字签名算法[J]. 计算机科学, 2019(6): 30-36.
- [6] 马雪婷, 张九凯, 陈颖, 等. 燕窝多元素的分布及溯源信息研究[J]. 食品与机械, 2019, 35(2): 66-71.
- [7] 刘元林, 龙鸣, 李儒, 等. 脂肪酸检测在食品工业中的应用研究进展[J]. 食品与机械, 2019, 35(11): 223-228.
- [8] KHAN M A, KHALED S. IoT security: Review, blockchain solutions, and open challenges[J]. Future Generations Computer Systems Fgcs, 2018, DOI: 10.1016/j.future.2017.11.022.
- [9] CONG L W, HE Z. Blockchain disruption and smart contracts[J]. Social ence Electronic Publishing, 2018, 21(4): 92-103.
- [10] CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and smart contracts for the internet of things[J]. IEEE Access,

- 2016(4): 2 292-2 303.
- [11] 韦银. 大数据下计算机信息技术在食品企业食品安全管理中的应用[J]. 食品与机械, 2016, 32(2): 226-228.
- [12] 禹忠, 郭畅, 谢永斌, 等. 基于区块链的医药防伪溯源系统研究[J]. 计算机工程与应用, 2020, 56(3): 35-41.
- [13] 孙晓明, 陈小龙, 余向阳, 等. 基于近红外光谱分析技术的水蜜桃产地溯源[J]. 江苏农业学报, 2020, 36(2): 507-512.
- [14] 王静静, 房芳, 周晓明, 等. 基于矿物元素含量的葡萄干产地溯源[J]. 新疆农业科学, 2020, 57(1): 69-77.
- [15] 吴鹏, 李颖, 刘瑀, 等. 基于 PCA-SVM 的仿刺参产地溯源在线系统研究[J]. 光谱学与光谱分析, 2019, 39(5): 282-287.
- [16] 李水芳, 朱向荣, 单杨, 等. 中/近红外光谱技术结合化学计量学在蜂蜜快速检测中的应用研究进展[J]. 食品与机械, 2009, 25(5): 121-124.
- [17] 陈柔含, 古淑青, 钮冰, 等. 水产品真伪鉴别与产地溯源检测研究进展[J]. 分析测试学报, 2020, 39(2): 287-294.
- [18] 刘耀宗, 刘云恒. 基于区块链的 RFID 大数据安全溯源模型[J]. 计算机科学, 2018, 45(2): 367-368, 381.
- [19] 张利, 童舟. 基于区块链技术的农产品溯源体系研究[J]. 江苏农业科学, 2019, 47(13): 245-249.
- [20] 成映波. 转基因食品安全: 基于研究事实与逻辑分析的评述[J]. 食品与机械, 2019, 35(1): 103-110.
- [21] 阙梦菲, 张俊伟, 杨超, 等. 物联网中基于位置的数字签名方案[J]. 计算机研究与发展, 2018, 55(7): 1 421-1 431.
- [22] 范硕, 宋波, 董旭德, 等. 基于区块链的药品溯源追踪方案研究设计[J]. 成都信息工程学院学报, 2019, 34(3): 267-273.
- [23] NATHAN Jin. Can blockchain connect food? [J]. Food Processing, 2018, 79(3): 10.
- [24] BUMBLAUSKAS D, MANN A, DUGAN B, et al. A blockchain use case in food distribution: Do you know where your food has been? [J]. International Journal of Information Management, 2019, 52: 12-43.
- [25] 尤瑶, 孔兰菊, 肖宗水, 等. 一种支持区块链交易溯源的混合索引机制[J]. 计算机集成制造系统, 2019, 25(4): 192-198.
- [26] 唐甜甜, 解新方, 任雪, 等. 稳定同位素技术在农产品产地溯源中的应用[J]. 食品工业科技, 2020(8): 22-29.
- [27] 焦彧, 冯兰平, 李百蝉, 等. 镉同位素在葡萄酒产地溯源中的研究进展[J]. 中国酿造, 2019, 38(8): 9-13.
- [28] 陈柔含, 古淑青, 钮冰, 等. 水产品真伪鉴别与产地溯源检测研究进展[J]. 分析测试学报, 2020, 39(2): 287-294.
- [29] 吴鹏, 李颖, 刘瑀, 等. 基于 PCA-SVM 的仿刺参产地溯源在线系统研究[J]. 光谱学与光谱分析, 2019, 39(5): 282-287.
- [30] 张诚, 刘守臣. 区块链中电商冷链溯源系统 Petri 网建模与分析[J]. 企业经济, 2020(1): 48-55.
- [31] 齐婧, 李莹莹, 姜锐, 等. 矿物元素和稳定同位素在肉类食品产地溯源中的应用研究进展[J]. 肉类研究, 2019, 33(11): 67-72.
- [32] 童成英, 何守阳, 丁虎. 茶叶产地与品质的元素、同位素鉴别技术研究进展[J]. 生态学杂志, 2018, 37(5): 1 574-1 583.
- [33] 陶启, 崔晓晖, 赵思明, 等. 基于区块链技术的食品质量安全管理系统及在大米溯源中的应用研究[J]. 中国粮油学报, 2018, 33(12): 110-118.
- [34] 赵政杰, 赵原爽. 大数据背景下对葡萄酒产地溯源的研究[J]. 科技资讯, 2018, 16(1): 77-78.
- [35] 熊丽君, 袁明珠, 吴建强. 大数据技术在生态环境领域的应用综述[J]. 生态环境学报, 2019(3): 13-19.
- [36] 赵嘉承, 郑新立, 陈浩, 等. 基于大数据挖掘的进口食用农产品质量安全数据开放共享研究[J]. 信息通信, 2020(4): 13-15.
- [37] 王靖会, 臧妍宇, 曹威, 等. 基于机器学习方法的吉林大米产地确证模型研究[J]. 中国粮油学报, 2018, 33(9): 123-130.
- [38] 唐甜甜, 解新方, 任雪, 等. 稳定同位素技术在农产品产地溯源中的应用[J]. 食品工业科技, 2020(8): 11-20.
- [39] 卢丽, 刘青, 丁博, 等. 元素含量分析应用于櫻桃产地溯源[J]. 分析测试学报, 2020, 39(2): 219-226.

(上接第 73 页)

参考文献

- [1] 王利明. 法治: 良法与善治[J]. 中国人民大学学报, 2015(2): 114-121.
- [2] 马怀德. 行政程序法的价值及立法意义[J]. 政法论坛, 2004(5): 4-10.
- [3] 刘兆彬. 《食品安全法实施条例》的制度价值[J]. 中国市场监管研究, 2020(2): 26-30.
- [4] 姜明安. 行政法与行政诉讼法[M]. 6 版. 北京: 北京大学出版社, 2015: 267.
- [5] 孙娟娟. 《食品安全法实施条例》中的行政处罚规定与评析[J]. 中国食品药品监管, 2020(1): 32-34.
- [6] 杨丹. 综合行政执法改革的理念、法治功能与法律限制[J]. 四川大学学报(哲学社会科学版), 2020(4): 138-149.
- [7] 毛伟旗, 毛睿涵. 对《食品安全法实施条例》的实务解读[J]. 中国食品药品监管, 2019(12): 20-27.
- [8] 何晖, 郭富朝, 郭泽颖. 新《食品安全法实施条例》评述[J]. 食品科学, 2020(11): 336-343.
- [9] 毕玉谦. 论庭审过程中法官的心证公开[J]. 法律适用, 2017(7): 46-53.
- [10] 安勇华. 新《食品安全法》中行政处罚纠纷的化解向度[J]. 食品与机械, 2019, 35(4): 68-71.
- [11] 于航宇, 樊永祥, 王家祺. 我国现行食品安全地方标准分析[J]. 中国食品卫生杂志, 2019(5): 485-489.