基于 IPFS 和 Merkle tree 存储机制的冷冻面团溯源研究

武 玮[1,2]
WU Wei

摘 要 随着现代生活节奏的加快，冷冻面团因其方便运输、方便存储、保质期长久而受到越来越多的买家认可，但是仍然存在冷冻面团的安全问题。为了应对这些挑战，提出了一种基于以太坊智能合约的冷冻面团追溯模型，设计了基于 IPFS（星际文件系统）和 Merkle tree 的存储机制。实验结果表明，所提出的模型能够实现对冷冻面团全流程的追溯，且在以太坊中的存储成本低于传统的直接存储方式，这无疑为其在实际应用中的推广提供了有力支持。综上所述，基于以太坊智能合约的追溯模型为冷冻面团的安全管理提供了新的解决思路，有助于提高消费者的信心和推动行业的健康发展。

关键词 IPFS；Merkle tree；冷冻面团；数字签名；智能合约

doi：10.3969/j.issn.1672-9528.2024.05.033

0 引言

随着生活节奏加快，冷冻面团产品越来越被客户认可，我国人口中 66.8% 将烘焙食品作为零食进行食用 [1]。然而，由于烘焙食品中的冷冻面团供应链追溯缺乏统一的标准、认证体系和后续管理，冷冻面团的安全问题日益突出，给消费者带来了很大的困扰。为了解决这一问题，越来越多的研究者开始关注食品溯源技术。区块链技术作为当前较为新颖的技术工具，因存在特点可追溯、不可篡改与去中心化 [2]，为食品溯源提供了新的解决方案。本实验旨在利用区块链技术的特性，构建基于以太坊智能合约的追溯模型，解决冷冻面团的安全问题。

1 相关工作

1.1 区块链技术和智能合约

区块链技术与智能合约技术在当前运用的场景越来越多。其中，区块链技术属于分布式数据库技术的一种，其特点是去中心化和不可篡改性，为交易记录提供透明性和安全性。另一个智能合约技术属于区块链技术的一种自动执行合同技术，可以在满足预设条件的情况下自动执行相应的操作，如支付、转移资产等。智能合约的主要特点是自动执行、可追溯和不可篡改。这些特点使得智能合约能够提高交易的效率和安全性，减少欺诈和错误。通过智能合约，交易双方可以在区块链上建立信任，无需第三方介入。

在食品行业中，区块链和智能合约的应用也已经开始显现。例如，一些公司正在使用区块链技术来追踪食品的供应链信息，包括原料来源、生产日期、物流信息等。智能合约则可以用于自动执行食品认证、食品安全检测等方面的操作，提高效率和质量。区块链和智能合约是未来食品行业发展的重要趋势之一，有望给食品供应链管理、食品安全追溯等带来更多的创新和变革。

1.2 研究进展

目前国内外已经有多个研究团队开展了基于区块链技术的冷冻食品、速冻食品溯源研究。其中，Rafi 等人 [3] 利用区块链和 IPFS 来存储物联网设备产生的数据，解决了 IoT 设备数量巨大时数据安全性存储的问题。Saqib Ali 等人 [4] 使用分布式哈希表拓展联盟链的存储，增加了该项目的可持续性。

随着 IPFS 的兴起，区块链存储成为重要的技术手段 [5]，当前的智能合约平台如以太坊，其因较好的延伸性和优异的开放性，被越来越广泛地应用在各类溯源场景之中。本研究将针对冷冻面团的特点和安全问题，构建基于以太坊智能合约的冷冻面团追溯模型。

2 冷冻面团供应链流程分析

2.1 数据准备环节

数据准备需要对准备的产品信息的全流程记录上链。

2.2 原料采购

冷冻面团生产商从供应商处采购所需的原材料，首先对供应商进行筛选，选择信誉良好、质量可靠的供应商，并通过定期评估来维持供应商的质量标准。

1. 北京碧瑞利德食品科技有限公司 北京 101300
2. 中国人民大学信息学院 北京 100089

2.3 生产加工

生产过程中，原料的混合、搅拌和成型是关键步骤，它们决定了最终产品的口感和质地。生产商将采购的原料按照配方进行混合，根据产品类型运用不同的加工技术，生产加工冷冻面团。这种方法可以延长面团的保质期，便于长途运输和储存，同时保持面团的新鲜度和发酵特性。通过这些加工技术，冷冻面团生产商能够生产出多样化的产品，满足不同市场和消费者的需求。同时，这些技术也有助于提高生产效率，降低成本，并确保产品的一致性和可预测性，可划分成冷冻面团法、预烘焙制品冷冻法等，详见图 1。

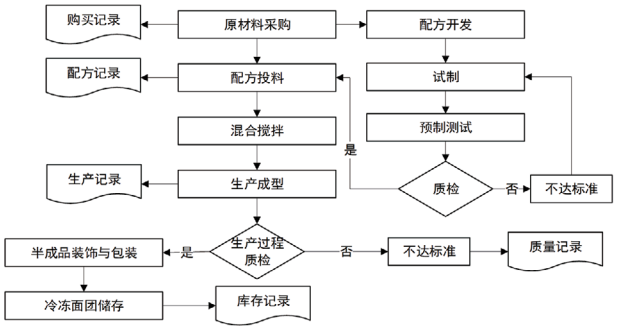

图 1 冷冻面团生产流程图

2.4 冷冻储存

冷冻面团的储存是确保其品质和延长保质期的关键环节。面团在制作过程中会经历物理和化学变化，其质地和结构相对脆弱，容易受到环境因素的影响而老化，导致口感和风味的下降。因此，冷冻面团在生产完成后必须迅速进行冷却处理，以减缓这些变化的速率。

2.5 物流配送

生产商需要将冷冻面团运送到销售商或终端用户手中。在运输过程中，使用专门的冷藏车或冷冻集装箱，这些设备具有良好的保温性能，可以抵御外界温度的影响；通过这些措施，生产商可以确保冷冻面团在运输过程中的品质，减少由于温度变化导致的损失，提高客户满意度，增强市场竞争力，具体见图 2。

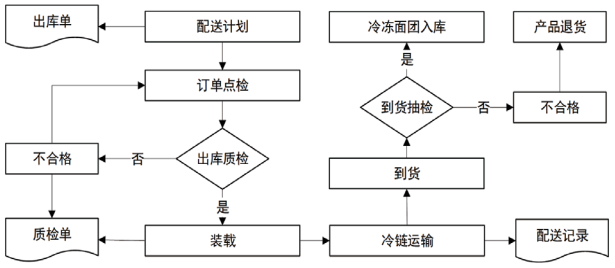

图 2 冷冻面团物流配送流程图

2.6 销售和分销

此环节经过营销策略和分销渠道，生产商通过广告宣传、促销活动、品牌建设、社交媒体营销等提高产品的知名度和吸引力；并通过多种渠道进行分销，生产商需要与这些分销商建立合作关系。根据提供优质的售后服务来提高消费者的满意度和忠诚度，包括产品咨询、投诉处理等。

3 冷冻面团溯源模型设计

3.1 模型角色设计

冷冻面团物流模型，包含生产商、销售商、终端客户、物流公司、政府和第三方认证机构。

生产商：负责生产冷冻面团，控制原料采购、生产加工、冷冻储存等环节，确保产品质量和食品安全。

销售商：负责将冷冻面团销售给终端用户，进行分销和销售管理，提供必要的售后服务和支持。

终端用户：最终使用冷冻面团的客户，向销售商购买冷冻面团，用于制作各种食品。

物流公司：需要确保运输途中的及时性。

政府机构和第三方认证机构：对冷冻面团供应链进行监管和认证，确保产品的质量和食品安全。

这些角色在冷冻面团供应链流程中发挥着各自的作用，共同确保最终产品的品质和食品安全。

3.2 存储机制设计

冷冻面团所包含的环节复杂，每个环节数据量很多，假设本次实验中，将数据直接储存进以太坊，将会导致以太坊在上传速度等环节较慢，产生较高的数据存储的费用支出。

因此，本文设计一种基于 IPFS 和 Merkle Tree 的存储机制。以冷冻面团数据准备环节为例，保存所需要的原材料名称、品种、质量、物料号等。先通过哈希算法处理以上涉及环节的基础数据信息，再通过 Merkle Tree 的储存机制将得到的基础数据进行计算得出哈希值，将运算出来的数据存储 IPFS，最后将 IPFS 地址和 Merkle tree roots 在以太坊中进行存储，见图 3 Merkle Tree 生成图。

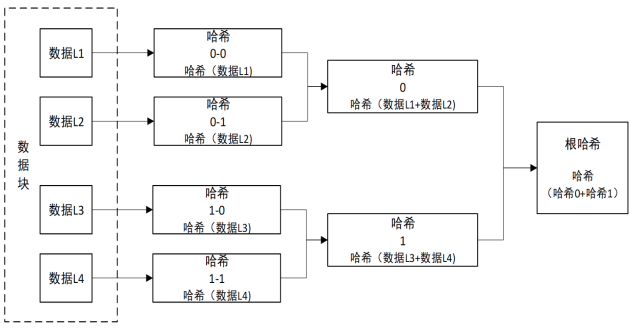

图 3 Merkle Tree 生成图

3.3 数字签名设计

一般情况下，在生成 Merkle Tree 之后，使用私钥对根哈希值进行加密，生成一个数字签名。这个数字签名是与 Merkle Tree 相关联的，可以证明 Merkle Tree 的根哈希值是由私钥持有者生成的。但在冷冻面团溯源模型中涉及研发、生产、质量、仓储、物流、销售等众多环节，每个环节所产生

的数据量也非常大，例如产品的物料清单（bill of material，BOM）、生产工艺、生产版本等等，将很难保证数据的有效性、准确性。综上所述，本文将以太坊和椭圆曲线数字签名算法（elliptic curve digital signature algorithm，ECDSA）相结合，因此可以对其进行双重认证，具体流程见图 4。ECDSA 算法的流程如下。

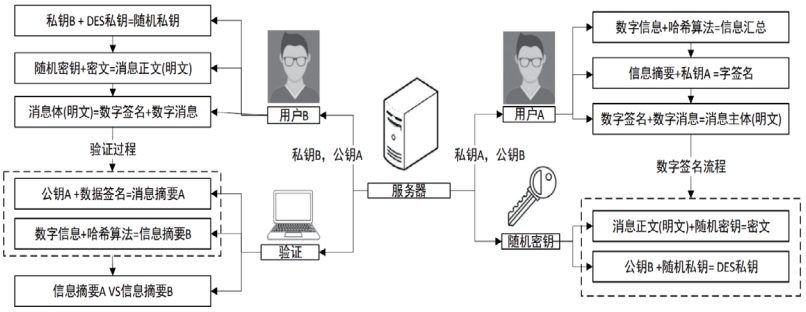

图 4 ECDSA 算法模型图

（1）下列为椭圆曲线公式：

$$F(x)=x^2+ax+b(\mathrm{mod}\ p) \tag{1}$$

式中：a、b 为圆曲线参数，p 为大质数，并满足条件：$8a^3+54b^2\neq 0$。

（2）随机生成一个 k 作为私钥：s_{kA}，并将基点 G 和随机数 k 计算得到公钥 p_{kA}：

$$p_{kA}=k\times G \tag{2}$$

（3）数字签名计算过程如下。

（a）使用上链的数据（明文）通过哈希函数转换成固定长度且不可逆的哈希值：$h=Hash(\mathrm{message})$。

（b）随机选一个数 v（$0<v<n$，n 为椭圆曲线的价）。

（c）计算对应椭圆曲线点对：

$$p=v\times G=x_p+y_p \tag{3}$$

（d）通过运算获得数字签名的 r、s 值：

$$r=x_p \bmod n \tag{4}$$

$$s=(v^{-1}\times(h+k\times r)) \bmod n \tag{5}$$

（4）将溯源的数字签名进行正确性验证。

（a）对数据进行哈希处理 $h=Hash(\mathrm{message})$。

（b）将 s、h、r 进行计算得到 u_1 和 u_2：

$$u_1=h\times s^{-1} \bmod n \tag{6}$$

$$u_2=r\times s^{-1} \bmod n \tag{7}$$

（c）通过以下公式运算得到曲线点 (x_1, y_1)：

$$(x_1, y_1)=u_1\times G+u_2\times p_{kA} \tag{8}$$

（d）若 $r=x_1 \bmod n$，则证明签名是符合要求的。

3.4 冷冻面团溯源模型设计

（1）确定溯源目标：首先需要明确溯源的目标，例如是追踪冷冻面团的原料来源、生产过程、物流配送等信息，还是仅关注某一特定环节的追溯，有助于设计溯源模型。

（2）数据采集与整理：采集冷冻面团从原料采购到生产、储存、运输等各环节的数据，包括原料信息、生产日期、批次号、物流信息等，确保数据的准确性和完整性。

（3）建立数据库：建立冷冻面团溯源数据库，将采集到的数据整理后储存到数据库中。数据库应具备数据存储、查询、更新等功能，以便对数据进行管理和分析。

（4）设计溯源流程：根据冷冻面团的生产和流通特点，设计合理的溯源流程。从原料采购开始，到生产加工、储存、运输等环节，确保每个环节的信息能够清晰地追溯和呈现。

（5）开发追溯系统：基于数据库和溯源流程，开发冷冻面团追溯系统。系统应具备数据录入、查询、分析、可视化等功能，使用户能够方便地进行冷冻面团追溯操作。

（6）测试与改进：对开发的追溯系统进行测试，确保其功能和性能满足设计要求，提高系统的可靠性和易用性。

（7）部署与实施：将追溯系统部署到实际生产环境中，进行实际操作和运行。根据实际使用情况，持续监控和优化系统的运行状态，确保其能够为冷冻面团的生产和流通提供有效的追溯支持，详细流程见图 5。

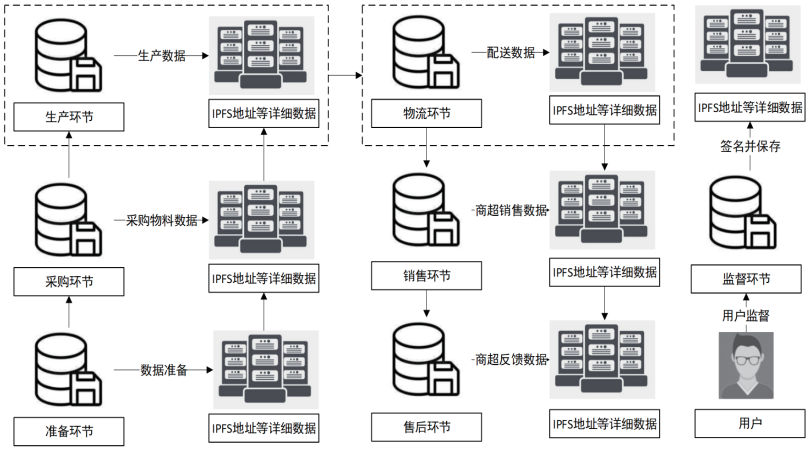

图 5 冷冻面团模型部署图

4 实验设计与实现

4.1 实验环境

本次实验中，运行的是 64 位的 Windows 11 操作系统，是由 AMD 制造的处理器，属于 Ryzen 5000 系列，3.30 GHz 频率，16 GB 大小的存储器。实验中使用的是 solidity 语言，智能合约的框架基于 Node.js 的命令行工具和开发环境的 hardhat，涉及的相关模型部署在以太坊私链当中。

4.2 模型部署

对于本次实验的模型，通过之前的流程在部署智能合约之前需要生成模型角色，部署在以太坊私链中，模型角色分

为准备工作环节、采购冷冻面团原料环节、生产冷冻面团环节、成品配送物流环节、冷冻面团销售环节、售后环节、用户 / 会员环节、监督环节，共计 8 个。

通过以太坊的 Hardhat 开发环境框架，输入 npx hardhat node 命令，启动对应 8 个本地的区块链节点，详见图 6。

```
Account #1: 0x0a2f385b6d79b7124e435c7e1f80435b
Account #2: 0x9c8376e1524a53858c536b179cb43022
Account #3: 0x7e50349b1375b3239815541d265c4c02
Account #4: 0x48f0c8b76b28fe9847a9c14679d570df
Account #5: 0x283f485c6e719d9a9cba1eaf3be99a24
Account #6: 0x9a2a4c77a3af04d015a591b2f67ec9ad
Account #7: 0x7a16e0d9d2af2ed89e290df37c36f296
Account #8: 0x1e66b7fbdcd6cee4b9dcd0fbbefc45fd
```

图 6 区块链节点生成图

接下来，将数据准备环节、采购环节、生产环节、冷冻面团（销售）环节、物流环节部署到以太坊，详见图 7。

```
  Test Contract
    function
Data preparation contract address: 0x1a93f0c2e556f9b40e9c65752e274b17
Procurement node contract address: 0x9198d75a33847b3380356cfe65f2b94c
Production node contract address: 0x6b4f31b936c658492ee2438d41d5d807
Frozen dough contract address: 0x14d1d68b19eac7129321d42d60b4b74a
Logistics Contract Address: 0x5790a6d5b91e33f8f462809ef9a8102c
```

图 7 合约明细

4.3 计算结果

通过上述的实验，得到数字签名时间用时、密钥用时、验证用时，并进行测试分析。

由图 8 可知，当本文运算 1400 多时，此时的密钥用时为 700 ms，签名时间用时为 3780 ms，验证时间用时为 14 560 ms。

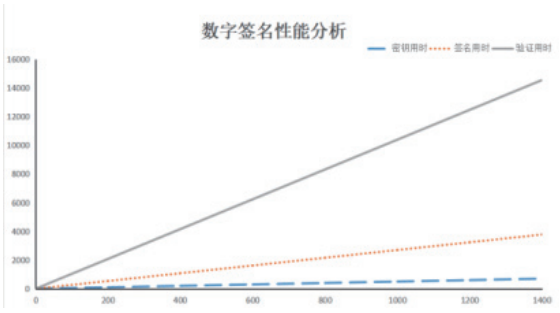

图 8 性能分析

综上所述，因为数字签名中验证时间很高，所以本次计算时间都在正常范围内。接下来，本文对主要的功能、对应消耗的时间进行了测试。各环节数据上链需要时长详见图 9。由于证明模型对应需要的耗时，是在可接受范围之内，由此可知本次实验的模型提出的存储机制，与直接存储相比较，效果更良好。

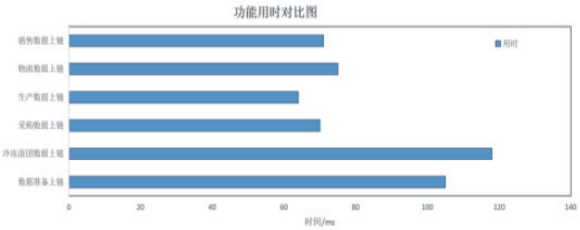

图 9 模型功能用时图

5 结语

综上所述，由于当前社会对冷冻面团产品没有统一的监管制度，其包含的采购、生产、质检、仓储、物流、销售等涉及环节较多，仍然存在难以溯源等问题。本实验通过发挥区块链的去中心化、可追溯性和数据不可篡改特性，来解决在冷冻面团供应链环节中存在的中心化等问题。

本次实验中，将智能合约引入了用户监督环节，这样能对所涉及的各冷冻面团供应环节产生的数据进行监管。在本次实验中可以看出，当收到监督的数据时，利用区块链技术及时进行溯源跟踪，同时将处理的数据存储在以太坊中，可以确保监督结果的公开、公正性。

结合实验结果，通过利用 IPFS 和 Merkle tree 的存储机制，能够减少冷冻面团模型在存储过程中所需要的用时。基于实验，结合当前迅速发展的互联网区块链技术，将来要考虑到涉及多品类多渠道的数据交互传递问题，因此，后续研究将在冷冻面团供应链环节上，提高数据交互的安全性。

参考文献：

[1] 张毅 .2022 年中国烘焙行业发展趋势报告 [R]. 北京 : 中国焙烤食品糖制品工业协会 ,2022.

[2] 张志威 , 王国仁 , 徐建良 , 等 . 区块链的数据管理技术综述 [J]. 软件学报 ,2020,31(9):2903-2925.

[3]RIFI N, RACHKIDI E, AGOULMINE N, et al.Towards using blockchain technology for IoT data access protection [C]//2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband. Piscataway:IEEE,2017:1-5.

[4]ALI S, WANG G, WHITE B, et al. A blockchain based decentralized data storage and access framework for pinger [C]// 2018 17th IEEE International Conference on Trust , Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/ BigDataSE). Piscataway: IEEE , 2018: 1303-1308 .

[5] 孙知信 , 张鑫 , 相峰 , 等 . 区块链存储可扩展性研究进展 [J]. 软件学报 ,2021,32(1):1-20.

【作者简介】

武玮（1996—），男，河南安阳人，硕士研究生，研究方向：大数据、区块链、人工智能。

（收稿日期：2024-03-06）