**2.2.1 区块链+传统数据库的建立**

研究了区块链存储方式和传统数据库存储方式的融合，实现了对过去传统Web数据库所存储数据的增量式兼容，通过存储方式的融合，比只用区块链存储具有更高的查询效率。根据稻米食品生产各环节的生产时间关联各区块链节点的时间戳，实现了不可篡改、不可抵赖、不易丢失，提高了数据的可靠性。

经过深入调研糙米制品全产业链生产管控过程和已有的ERP系统后，从质量安全追踪溯源的角度，整理抽取安全相关信息，完成了区块链上的数据库结构设计。然后，对其进行了区块链改造，使得传统数据库的查询方便性和区块链的安全性优势结合。

**2.2.1.1 食品质量安全可追溯核心数据集的设计**

首先，我们是在育秧和种植过程中，为了完成质量安全溯源，我们主要管控了生产过程中的批次号转换环节和药品的使用环节，如下图：

图1 药品使用的数据库实体-关系图（ER图）

由上图，种子的批次ID（种子ID）是第一个关键信息，这是每批种子在生产过程管控中的唯一标识，也是HACCP标准中的第1个关键控制点，产生第一个种子ID即为区块链上记录的第一笔生产过程中的用户交易。种子的品种和类型等相关信息绑定在种子ID上。

第2个和第3个关键控制点是种子的浸泡和喷药处理，药品信息已记录在区块链上，农药、肥料和灌溉用水均作为药品记录，包括唯一标识即药品批次（药品ID），和生产标准、名称、剂量、作用等附加信息。浸泡和喷药的过程，则分别记录了日期和浓度、用量等信息。

然后是种子批次到秧苗批次的转换，这是第4个关键控制点，种子处理过后送进育秧工厂，产生新的秧苗批次号，批次转换是在真实性溯源中最重要的溯源信息。

在上图中，还显示了一个与药品相关的后续关键控制点（第7个关键控制点），即种植过程中的用药，包括除虫、施肥、浇水（按施肥处理）等流程管控，记录了日期、用量和目的（作用）等信息。

接下来是育秧过程中的质检、插秧过程中的批次转换，和收割过程中的批次转换，如下图：

图2 种植过程的数据库实体-关系图（ER图）

在上图中，可以看见在前述第4个关键控制点，即种子批次到秧苗批次的转换中，每添加一个秧苗批次ID（秧苗ID）时，同时记录相关信息（育秧地点、育秧起始日期）和来源的种子批次ID。

育秧是在育秧工厂中进行的，添加秧苗批次时，秧苗实际上还只是处于刚播种的状态，外表形式是一盘一盘的托盘，以一定的高度层叠放在育秧架上，经过一段时间之后才能破土，长成秧苗。在此过程中，进行秧苗质检（第5个关键控制点），记录检测的秧苗批次、质检时间以及质检内容（长势、种植密度、虫害），这是关键的秧苗质量信息。

从秧苗到大田种植的批次转换（第6个关键控制点），即是秧苗经过插秧机分散到大田的过程，存在着从秧苗批次到种植批次的转换，转换过程中存在着合并和分叉，在插秧过程中人工记录并存入区块链，除了种植ID以外，需要记录种植地点，这是溯源需要的关键信息。种植过程中需要用药（第7个关键控制点），记录在图1中。

接下来是收割和入库时的批次转换操作（第8个关键控制点），从种植ID到入库ID的转换，过程中记录日期和产量，以及下图中的入库时间。



图3仓储过程的数据库实体-关系图（ER图）

入库时的质检是第9个关键控制点，对每个入库批次（入库ID）进行检测，记录霉变、虫害、水分含量等管理安全关键质检信息。

入库过程是第10个关键控制点，这里的关键信息，是从入库ID到仓库ID的转换。仓库信息也是在生产过程之外预先添加在区块链上的数据，包括仓库号（编号ID）、容量、地点表示、仓库建设标准等关键信息。

仓库检测是第11个关键控制点，包括检测日期、稻谷水分含量、虫害情况、粮堆温湿度、仓库空气温度等关键信息。接下来是出库和进料过程，见下图：



图4加工过程的数据库实体-关系图（ER图）

出库和进料过程，是指稻谷进入大米生产流水线的运输过程，存在从仓库号（仓库的编号ID）到进料编号（ID）的批次转换，这是第12个关键控制点。除了进料编号外，还记录了时间戳和进料重量信息。

初加工过程，即从稻谷进料到大米出料之间，没有批次的合并或分叉，直到深加工成为糙米制品产品时，才产生到产品批次（产品ID）的批次转换（第13个关键控制点），附加记录转换过程中的质量安全信息，包括初加工质检信息，如大米水分含量、碎米率、黄米率等，以及产品信息，如产品名称、规格、口味、日期等。

深加工过程除了需要大米原料外，还需要其他从外部采购的原料，其他原料批次到产品批次的转换是第14个关键控制点。原料信息也在生产过程之外记录在区块链上，包括唯一标识（原料ID）和附加信息如日期、种类、来源、重量等。接下来的关键控制点是深加工过程中的质检，如下图：



图5深加工质检过程的数据库实体-关系图（ER图）

在深加工的质检过程中，共有三个关键控制点，即烘烤质检（第15个关键控制点）、冷却/灭菌质检（第16个关键控制点）和内包质检（第17个关键控制点），分别记录烘烤过程中的温度、时间、烘烤之后的重量，冷却质检中的温度和时间，以及内包质检中得含氧量、内包膜材质信息和日期。

以上17个生产流程中的关键控制点，以及前述的药品采购、仓库信息和其他原料采购等3个重要质量安全相关信息，一起构成本系统基于区块链的数据库结构设计，总体ER图如下：



图6食品质量安全可追溯核心数据集实体-关系图（ER图）

**2.2.1.2 区块链+传统数据库的结合**

传统数据库是中心化数据库，有被人为故意篡改的可能性，需要结合区块链和多重签名机制来补足安全性，而区块链的数据存储形式不易于实现快速查询，所以，需要将二者结合起来。结合方式如下：

存入区块链

传统ERP系统

传统数据

共识过程和结果存入区块链

多重签名共识管理

存入带区块编号和共识编号的传统数据库

图7 区块链+传统数据库的结合流程图

由上图可见，在区块链节点上建立带区块编号和共识编号的传统数据库，对于从传统ERP系统传来的传统数据：先存入区块链，然后一边做多重签名共识管理，一边存入带区块编号和共识编号的传统数据库，并将共识过程和结果也均随后存入区块链，保证共识过程的可信性。

建立带区块编号和共识编号的传统数据库，即梳理从外部ERP系统可能传来的接口数据，提取质量安全关键信息，建立如上节所述的传统数据结构，但在每张数据表中新添“区块ID”和“共识ID”字段。

每当外部ERP系统传来数据，首先实时存入区块链，获得区块编号，然后为其建立初始共识需求，获得共识ID，将数据存入区块链，所建立的共识需求也存入区块链。关于共识需求和初始建立和解析，多重签名的管理过程，以及为此建立的数据，见图8：

1

区块编号

生成

传统数据

数据表名

签名组ID

1

区块编号

1

初始共识需求

多重签名组

1

m

数据表名

共识ID

区块编号

解析

分组

已签名用户ID

区块编号

1

n

签名

多重签名需求

共识ID

用户

区块编号

ERP系统用户ID

签名组ID

区块链用户公钥

已签名用户集合

未签名用户集合

图8 多重签名和共识过程实体-关系图（ER图）

在上图中，首先建立区块链上的用户与外部ERP系统上的用户关系，顺序存入区块链和传统数据库，传统数据库上的相应数据表包括区块编号、ERP系统用户ID、区块链上的用户公钥。

其次，建立多重签名组，顺序存入区块链和每个组只对一张特定数据表（数据表名所指）有权限共识确认其中的数据，具有签名组ID和数据表名两个常规字段，以及一个区块编号字段用于存储其在区块链中的区块号码。

接着，建立用户和多重签名组之间的多对多关联，将关联表也顺序存入区块链和传统数据库。

当传统ERP系统的数据来到时，首先整理其中所含的质量安全关键信息和输入数据的人员，确定数据表名，先存入区块链，得到区块ID，然后生成一个初始的共识需求，得到共识ID，再将数据存入区块链，接着把输入数据的人员ID作为“已签名用户ID”（第一个签名的人员），将填补完整的初始共识需求也顺序存入区块链和传统数据库。

然后，使用多重签名组相关信息对初始共识需求进行解析，搜索既包含已签名用户又对该数据表有权限的多重签名组（只支持唯一），建立一条多重签名需求记录，包含共识ID、签名组ID、已签名用户集合和未签名用户集合，顺序存入区块链和传统数据库。其中，已签名用户集合是一个数组，包含每个已签名用户的区块链公钥和签名时间，以json字符串格式保存；未签名用户集合类似，只是不包含签名时间。

当多重签名需求记录通过区块链上的P2P网络同步到各个节点时，未签名用户集合中的用户检查信息发现需要自己的签名，于是提交给用户签名。每个用户签名完成后，均生成一条新的多重签名需求记录，更新其中的已签名用户集合和未签名用户集合，顺序存入区块链和传统数据库。这样，每个用户均可知道多重签名共识的进行过程，然后进行数字安全签名。

最后，当出现未签名用户集合为空的多重签名需求记录时，该需求即告满足，该数据共识完成，且共识过程中的关键信息也已完整记录在区块链上。

**2.2.1.3 区块链+传统数据库结合的优势**

区块链+传统数据结合的优势如下表：

|  |  |  |
| --- | --- | --- |
| 种类 | 安全性 | 查询效率 |
| 传统数据库 | 低 | 高 |
| 区块链 | 高 | 低 |
| 区块链+传统数据库 | 高 | 高 |