团　　体　　标　　准

T/GDFCA 037—2019

基于区块链技术食品追溯系统的信息安全性测试标准

Information security test standard for food tractability system based on blockchain technology

（征求意见稿）

2019-××-××发布　　2019-××-××实施

广东省食品流通协会发布

目　　次

前　言

本标准按照GB/T 1.1-2009《标准化工作导则-第一部分：标准的结构和编写》标准起草。

本指导性技术文件由广东省食品流通协会提出并归口。

本指导性技术文件起草单位：中山市仁达贸易发展有限公司、广州生命码科技有限公司、中科软件测评（广州）有限公司

本指导性技术文件主要起草人：

基于区块链技术食品追溯系统的信息安全性测试标准

1 范围

基于区块链技术食品追溯系统是一种基于物联网、云计算和区块链等先进技术构建的食品追溯系统，将传统追溯系统与区块链技术进行融合，实现对食品的种植、加工、仓储、运输、销售等全过程的追溯。通过区块链技术去中心化、不可篡改、开放的特性，确保食品源头可追溯、流向可跟踪、信息可查询、信息高可性，保障公众消费和食品安全。

本标准规定了基于区块链技术食品追溯系统的信息安全性测试的术语和定义、测试方法和过程、系统信息安全性测试规范。

本标准适用于基于区块链技术食品追溯系统的信息安全性测试。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB／T 25000.10 系统与软件工程 系统与软件质量要求和评价（SQuaRE）第10部分：系统与软件质量模型

GB／T 25000.51 系统与软件工程 系统与软件质量要求和评价（SQuaRE）第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则

3 术语和定义

下列术语和定义适用于本文件。

3.1

区块链 Blockchain

一种分布式分类账，由不可更改的数字化记录的数据组成，称为数据块。然后使用加密签名将每个块“链接”到下一个块。这允许块链像分类帐一样使用，可以由具有适当权限的任何人共享和访问。

3.2

行业区块链 Consortium block chains

由某个群体内部指定多个预选的节点为记账人，每个块的生成由所有的预选节点共同决定，其他接入节点可以参与交易，但不过问记账过程，其他任何人可以通过该区块链开放的API进行限定查询。

3.3

分布式账本 Distributed ledger

是分布在多个站点，国家或机构中的一种数据库。记录一个接一个地存储在连续分类账中。分布式账本数据可以通过“许可”或“不许可”来控制谁可以查看它。

3.4

非对称加密 Asymmetric encryption

非对称加密是一种密钥的保密方法，需要两个密钥：公开密钥（简称公钥）和私有密钥（简称私钥）。公钥与私钥是一对，如果用公钥对数据进行加密，只有用对应的私钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。

3.5

共识机制 Consensus mechanisms

共识机制是通过特殊节点的投票，在很短的时间内完成对交易的验证和确认；对一笔交易，如果利益不相干的若干个节点能够达成共识，我们就可以认为全网对此也能够达成共识。

3.6

食品追溯 Food tractability

通过记录和标识，追溯食品的历史、应用情况或所处位置的活动，连接生产、检验、监管和消费的各个环节。

3.7

信息编码 Information coding

是指为方便信息的存储、检索和使用，在进行信息处理时赋予信息元素以代码的过程。即用不同的代码与各种信息中的基本单位组成建立一一对应的关系。信息编码必须标准化、系统化。

3.8

信息采集 Information collection

是指根据特定的目标和要求，将分散在不同时空域的有关信息，通过特定的手段和措施采集的过程。采集溯源单位生产企业的基本信息，产品的基本信息、产品质量安全信息。

3.9

信息交换 Information exchange

指数据在不同的信息实体之间进行交互的过程，其目标是在异构环境中实现数据的共享，从而有效的利用资源，加快数据流通，实现数据的集成和共享。

3.10

信息发布 Information release

指信息提供给企业、监管部门和消费者，不同使用者对信息要求不同，信息发布的内容、方式应满足信息使用者的需求。

3.11

信息安全性测试 Information security testing

指通过不同的测试方法，发现系统安全性的问题。不仅适用于存储在系统中的数据，也适用于传输中的数据。

3.12

保密性 Confidentiality

指产品或系统确保数据只有在被授权时才能被访问。

3.13

完整性 Integrity

指系统、产品或组件防止未授权访问、篡改计算机程序或数据的程度。

3.14

抗抵赖性 Anti-denial

指活动或时间发生后可以被证实且不可否认的程度。

3.15

可核查性 Verification

指实体的活动可以被唯一地追溯到该实体的程度。

3.16

真实性 Authenticity

指对象或资源的身份标识能够被证实符合其声明的程度。

3.17

依从性 Compliance

指产品或系统遵循与信息安全性相关的标准、约定或法规以及类似规定的程度。

4 测试范围

基于区块链技术食品追溯系统信息标准应包括追溯信息编码、信息采集、信息交换、信息发布四大部分，系统中的关键追溯信息记录在区块链的分布式账本节点。分布式账本节点在政府监管部门、行业协会、检测机构和利益相关企业部署。基于区块链技术食品追溯系统组成架构图见图4.1，测试范围涵盖下图方框的子系统的软件部分。

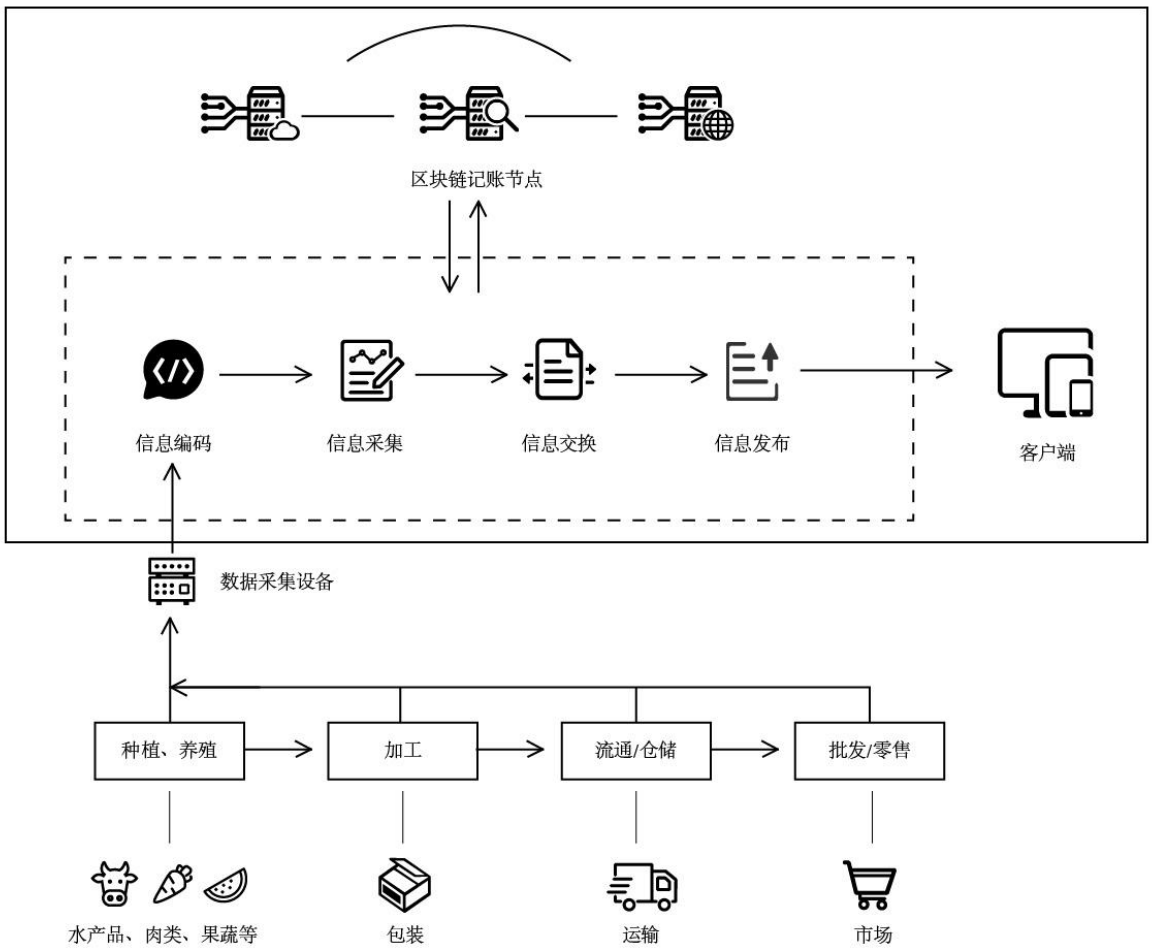

图4.1基于区块链技术食品追溯系统组成架构图

信息采集：是指未出版的生产在信息资源方面做准备的工作，包括对信息的收集和处理。

信息交换：是指数据在不同的信息实体之间进行交互的过程，其目标是在异构环境中实现数据的共享，从而有效地利用资源，提高整个信息系统的性能，加快信息系统之间的数据流通，实现数据的集成和共享。

信息发布：是系统面向用户终端的主要信息发送方式，是用户获取位置及相关信息的重要途径。

数据采集设备：所有的数据采集是从设备采集的。设备有多种，有些通过传感器来采集，有些设备属于智能设备，本身就是一台小型计算机，能够自己采集，不管是传感器，还是智能设备本身，采集方式一般包含两种，一种是报文方式，所谓报文就是根据你设置的采集频率进行数据传输，一般放到消息队列中。还有一种采集是以文件的方式采集，在做数据分析的时候，工业设备的数据希望是连续不断的，我们可以理解为毫秒级采集，就是设备不停的发送数据，然后形成一个文件或者多个文件。

区块链记账节点：是区块链分布式系统中的网络节点，是通过网络连接的服务器、计算机等，针对不同性质的区块链，成为节点的方式也会有所不同。

客户端：或称为用户端，是指与服务器相对应，为客户提供本地服务的程序。

5 测试方法

根据被测系统的特点，采用功能验证、漏洞扫描、模拟攻击等方法，采用安全渗透测试（如SQL注入漏洞，跨站脚本漏洞，文件上传漏洞，越权漏洞，敏感信息泄漏漏洞，失效的身份认证和会话管理漏洞，安全配置错误漏洞，未验证的重定向和转发漏洞等），验证身份认证、传输安全、安全审计、资源控制、数据安全等，是否存在潜在的安全性缺陷。从保密性、完整性、抗抵赖性、可核查性、真实性、信息安全性的依从性等方面对系统的信息安全性进行质量测试，并将信息安全性测试结果与信息安全性要求比较，评价系统的信息安全性的符合性。

根据系统安全指标不同测试策略也不同，信息安全性测试包括程序、网络、数据库等安全性测试。

1）用户认证安全的测试要考虑问题：

a）明确区分系统中不同用户权限。

b）系统中会不会出现用户冲突。

c）系统会不会因用户的权限的改变造成混乱。

d）用户登陆密码是否是可见、可复制。

e）是否可以通过绝对途径登陆系统（拷贝用户登陆后的链接直接进入系统）。

f）用户退出系统后是否删除了所有鉴权标记，是否可以使用后退键而不通过输口令进入系统。

2）系统网络安全的测试要考虑问题：

a）测试采取的防护措施是否正确装配好，有关系统的补丁是否打上。

b）模拟非授权攻击，看防护系统是否坚固。

c）采用成熟的网络漏洞检查工具检查系统相关漏洞（即用最专业的黑客攻击工具攻击试一下，现在最常用的是 NBSI 系列和 IPhacker IP ）。

d）采用各种木马检查工具检查系统木马情况。

e）采用各种防外挂工具检查系统各组程序的外挂漏洞。

3）数据库安全考虑问题：

a）系统数据是否机密（比如对银行系统，这一点就特别重要，一般的网站就没有太高要求）。

b）系统数据的完整性。

c）系统数据可管理性。

d）系统数据的独立性。

e）系统数据可备份和恢复能力（数据备份是否完整，可否恢复，恢复是否可以完整）。

4）系统安全考虑问题：

a）验证系统的安全等级和识别潜在安全性缺陷。查找系统程序设计中存在的安全隐患，并检查系统对非法侵入的防范能力，根据安全指标不同测试策略也不同。

注意：安全性测试并不最终证明应用程序是安全的，而是用于验证所设立策略的有效性，这些对策是基于威胁分析阶段所做的假设而选择的。例如，测试应用系统在防止非授权的内部或外部用户的访问或故意破坏等情况时的运作。

b）测试系统保护信息和数据的能力，以使未授权的人员或系统不能阅读或修改这些信息和数据，而不拒绝授权人员或系统对它们的访问。

c）测试系统配置项防止非法操作的模式，包括防止非授权的创建、删除或修改程序或信息，必要时做强化异常操作的测试，测试系统测试配置项防止数据被讹误和被破坏的能力，测试系统测试项目的加密和解密功能。

d）测试系统是否具有当前使用系统的用户列表、历史日志。

e）测试对系统访问的控制程度如何。采用非授权人创建、删除或修改信息，观察系统的响应。

f）检验系统防止数据丢失的能力。

g）检查系统是否具有有效的数据备份和恢复策略。测试系统的数据备份、数据恢复功能是否可用。

5）对于web应用，需使用测试工具明鉴Web应用弱点扫描器，对web应用进行弱点扫描。使用明鉴网站恶意代码检查工具对源文件进行扫描。

6 测试过程

系统测试通常要经历测试需求分析、测试计划制定，测试用例设计、测试数据准备、测试环境搭建、测试用例执行、测试缺陷跟踪、测试结果分析、测试报告编写等环节。

7 测试规范

基于区块链技术食品追溯系统信息安全性测试应从系统的保密性、完整性、抗抵赖性，可核查性，真实性，依从性以及系统遵循与信息安全性相关的标准、约定或法规以及类似规定等方面进行测试。

7.1 保密性

基于区块链技术食品追溯系统信息保密性测试一般需进行：

1）验证系统是否具有对系统正常访问的控制能力，依据安全策略和用户角色设置访问控制矩阵，用户权限应遵循“最小权限原则”，例如管理员不应具备业务操作权限，不同账号之间形成相互制约关系，例如系统审计人员不应具有系统管理权限，保证得到授权的人或系统能正常访问相关的信息和数据测试系统是否符合系统说明所引用的任何需求文档中的全部要求。

2）测试系统是否进行用户身份鉴别，并在每次用户登录系统时进行鉴别。

3）测试系统鉴别信息是否为不可见，且具有相应的抗攻击能力，并在存储或传输时用加密方法/具有相同安全强度的其他方法进行安全保护。

4）验证数据在传输过程中不被窃听，对整个通信过程中的整个报文或会话过程进行加密处理。

5）明确区分系统中不同用户权限，系统不会因用户的权限的改变造成混乱。

6）合适的身份认证方式，用户登陆密码是否是可见、可复制，密码的存储和传输安全，密码策略保证密码安全。

7）测试系统是否对不成功的鉴别尝试的值（包括尝试次数和时间的阀值）进行预先定义，并明确

规定达到该值时是否采取了具有规范性和安全性的措施来实现鉴别失败的处理。

8）系统应能防止对程序和数据的未授权访问（不管是无意的还是故意的）。

7.2 完整性

基于区块链技术食品追溯系统信息安全完整性测试一般需进行：

1）验证系统是否具有对未授权用户非法访问的控制能力。

2）采用专业测试工具，开展“渗透测试”、“漏洞扫描”等手段，在模拟非法入侵攻击事件的条件下，验证系统是否有控制和处理能力。

3）验证系统对非授权人创建、删除或修改信息是否有控制处理能力。

4）系统应能识别出对结构数据库或文件完整性产生损害的事件，且能阻止该事件，并通报给授权。

5）系统数据的完整性、可管理性、可备份和恢复能力，数据传输、数据使用、数据存储的完整性。

7.3 抗抵赖性

基于区块链技术食品追溯系统信息安全抗抵赖性测试一般需进行：

1）测试系统是否具有在请求的情况下为数据原发者提供数据原发证据的功能。

2）测试系统是否具有在请求的情况下为数据接收者提供数据接收证据的功能。

3）测试系统是否使用数字证书等方式保证用户的身份认证，在收到请求的情况下为数据原发者或接受者提供数据原发和接收的证据。

4）测试系统是否具备完整且无法篡改的审计记录，确保用户操作可经过审计及追踪。系统操作日志/审计、异常日志、告警日志，审计/日志的完整性、保密性。

5）验证审计日志的管理，日志不能被任何人修改和删除，能够形成完整的证据链。

7.4 可核查性

基于区块链技术食品追溯系统信息安全可核查性测试一般需进行：

1）测试系统是否将用户进程与所有者用户相关联，使用户进程行为可以追溯到进程所有者用户。

2）测试系统是否将将系统进程动态地与当前服务要求者用户相关联，使系统进程的行为可以追溯到当前服务要求者用户。

3）测试系统的审计模块，检查模块是否具有完善的安全审计功能。考察启用安全审计功能后，覆盖用户的多少和安全事件的程度，覆盖到每个用户活动，日志记录内容至少应包括事件日期、事件、发起者信息、类型、描述和结果等，审计跟踪设置是否定义了审计跟踪极限的阀值，当存储空间被耗尽时，能否采取必要的保护措施。

4）账户管理，包括账户唯一性、登录机制、密码管理策略。

5）会话管理，设计登录成功使用新的会话；设计会话数据的存储安全；设计会话数据的传输安全；设计会话的安全终止；设计合理的会话存活时间；设计避免跨站请求伪造。

7.5 真实性

基于区块链技术食品追溯系统信息安全真实性测试一般需进行：

1）验证系统是否具有当前使用系统的用户列表和配置表。

2）验证系统在系统的访问历史数据库中记录的访问登录记录是否完整。

3）检查系统是否具有用户使用系统的历史日志及日志管理功能。

4）在模拟攻击事件的入侵的情况下，验证系统的日志内容是否有相关记录。

5）检查系统中的"用户访问系统和数据"的记录内是否包括防止病毒的"病毒检测记录"。

7.6 依从性

基于区块链技术食品追溯系统信息安全依从性测试要求：

1）系统遵循与信息安全性相关的标准、约定或法规以及类似规定的程度；

2）检查系统的信息安全性是否遵循了所实施法规、标准和约定。

附 录 A

表A.1 信息安全危害等级表

漏洞等级	说明
紧急	可以直接被利用的漏洞，且利用难度较低。被攻击之后可能对网站或服务器的正常运行造成严重影响，或对用户财产及个人信息造成重大损失
高危	被利用之后，造成的影响较大，但直接利用难度较高的漏洞。或本身无法直接攻击，但能为进一步攻击造成极大便利的漏洞
中危	利用难度极高，或满足严格条件才能实现攻击的漏洞。或漏洞本身无法被直接攻击，但能为进一步攻击起较大帮助作用的漏洞
低危	无法直接实现攻击，但提供的信息可能让攻击者更容易找到其他安全漏洞
信息	本身对网站安全没有直接影响，提供的信息可能为攻击者提供少量帮助，或可用于其他手段的攻击，如社工等。