

MH

中华人民共和国民用航空行业标准

MH/T XXXX—XXXX

基于区块链的民航旅客行李全流程跟踪
技术要求

Technical requirements for blockchain-based full-process tracking of civil aviation
passenger baggage

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX-XX-XX 发布

XXXX-XX-XX 实施

中国民用航空局 发布

目 次

前言	II
引言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 一般要求	2
5.1 数据追溯性	2
5.2 数据有效性	2
5.3 数据隐私性	2
5.4 数据时效性	2
6 总体架构	2
7 数据感知层要求	3
7.1 行李识别要求	3
7.2 状态采集要求	4
7.3 事件记录要求	4
8 数据交互层要求	4
8.1 数据处理要求	4
8.2 数据上链与存证要求	4
8.3 数据查询与验证要求	5
9 区块链服务层要求	5
9.1 区块链节点服务要求	5
9.2 账本服务要求	5
9.3 共识服务要求	5
9.4 智能合约服务要求	6
10 业务应用层要求	6
10.1 状态查询要求	6
10.2 轨迹追溯要求	6
10.3 不正常行李处理要求	6
11 安全保障要求	6
11.1 身份认证要求	6
11.2 访问控制要求	7
11.3 行李全流程跟踪数据保护要求	7
11.4 隐私保护要求	7
11.5 安全审计要求	7
参考文献	8

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国民用航空局运输司提出。

本文件由中国民航科学技术研究院归口。

本文件起草单位：中国民航信息网络股份有限公司、上海民航华东凯亚系统集成有限公司、中国民航大学。

本文件主要起草人：孙召利、浦黎、智慧、耿思、刘增智、黄小东、孙琼巍、杨勃、潘乃槟、王刚、胡泽、何文博。

引 言

《民航行李全流程跟踪系统建设实施方案》明确提出按照“一标两端”的思路推进行李全流程跟踪系统建设。“机场端”主要负责采集、处理和传输机场内旅客托运行李相关环节的数据，以标准格式和固定制式向平台端上传行李数据，并从平台端获取行李全流程跟踪信息，实现行李查询、预警、不正常行李管理等功能。“平台端”主要负责汇集行李全流程跟踪信息，实现数据共享，向机场、航空公司等提供相关行李数据，为政府实施监督管理提供支持。

区块链已成为我国重点发展的数字经济产业之一，《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》在“加快数字发展，建设数字中国”篇章中明确提出推动智能合约、共识算法、加密算法、分布式系统等区块链关键技术创新，并以联盟链为重点发展区块链服务平台，拓展其在政务服务、供应链管理等领域的应用。同时，民航局在《智慧民航建设路线图》中提出，要推动大数据、人工智能、区块链等新一代信息技术与民航业务深度融合，推进数据资源赋能民航发展，深化基于区块链的核心业务场景应用。

当前行李全流程数据主要集中于各机场及相关系统内部，不同主体之间数据共享能力有限，尚难以实现高效、可信的数据协同。在引入区块链技术应用于行李全流程跟踪业务后，围绕行李数据提取、数据交换、异常行李处置、安全保护及全过程可追溯等关键环节，尚缺乏统一的业务规范和技术标准支撑，存在数据格式不统一、交换规则不明确、异常处置流程不规范以及敏感数据安全与责任追溯机制不完善等问题。因此，有必要针对行李全流程跟踪业务尽快制定基于区块链技术的统一规范标准，为区块链技术在民航行李领域的应用提供标准依据和技术支撑。

基于区块链的民航旅客行李全流程跟踪 技术要求

1 范围

本文件确立了基于区块链的民航旅客行李全流程跟踪的总体架构,规定了数据感知层、数据交互层、区块链服务层、业务应用层及安全保障的技术要求。

本文件适用于航空公司、民用机场、其它相关方系统开展基于区块链的民航旅客行李全流程跟踪相关业务过程中进行整体规划和技术架构设计与建设。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 42570—2023 信息安全技术 区块链技术安全架构

GB/T 42752—2023 区块链和分布式记账技术 参考架构

MH/T 1076.3 民航旅客行李全流程跟踪系统 第3部分:报文规范

3 术语和定义

GB/T 42570、MH/T 1076.3界定的以及下列术语和定义适用于本文件。

3.1

区块 block

一种由区块头和区块体组成的数据结构,用于记录区块元数据以及经确认的交易数据、业务数据或其摘要信息。

注:区块是组成区块链的基本结构单元。

[来源:GB/T 42752—2023, 3.6, 有修改]

3.2

区块链 blockchain

将区块顺序相连,并通过共识机制、数字签名、杂凑函数等密码学方式保证数据难以篡改和不可伪造的分布式账本。

[来源:GB/T 42570—2023, 3.2, 有修改]

3.3

区块链节点 blockchain node

参与区块链网络运行,承担数据存储、交易验证、共识、查询或管理等功能的计算节点。

3.4

链上存证 on-chain evidence preservation

将行李全流程跟踪节点的数据、时间标识、数据来源、数字签名、业务事件标识等信息提交至区块链账本,用于证明相关数据在特定时间已经产生,并支持后续完整性和真实性验证的过程。

3.5

存证凭证 evidence preservation credential

区块链服务层在完成行李全流程跟踪数据存证后生成的,用于标识和验证链上存证结果的凭据信息。

3.6

数据摘要 data digest

通过密码杂凑算法对行李全流程跟踪数据或相关业务数据计算得到的固定长度数据值。

3.7

数字签名 **digital signature**

对行李全流程跟踪数据或数据摘要进行密码运算生成的值，用于验证数据来源和数据完整性，并支持操作行为的不可否认性。

3.8

智能合约 **smart contract**

部署在区块链系统中，能够按照预设规则自动执行行李全流程跟踪数据存证、状态更新、查询验证等操作的计算机程序。

4 缩略语

下列缩略语适用于本文件。

JSON: JavaScript对象表示法 (JavaScript Object Notation)

PKI: 公钥基础设施 (Public Key Infrastructure)

RBAC: 基于角色的访问控制 (Role-Based Access Control)

RFID: 射频识别 (Radio Frequency Identification)

SM2: SM2椭圆曲线公钥密码算法 (SM2 Elliptic Curve Public Key Cryptographic Algorithm)

SM3: SM3密码杂凑算法 (SM3 Cryptographic Hash Algorithm)

SM4: SM4分组密码算法 (SM4 Block Cipher Algorithm)

UTF-8: 8位统一码转换格式 (8-bit Unicode Transformation Format)

5 一般要求

5.1 数据追溯性

行李全流程跟踪数据应能够反映旅客托运行李在全流程处理过程中的关键事件，并支持按照行李编号、航班号、业务事件类型、事件发生时间、数据提供方等条件追溯相关活动主体、业务环节、处理过程和处理结果。

5.2 数据有效性

行李全流程跟踪数据在生成、采集、传输、处理、存储、上链存证和使用过程中，应保持真实、完整、准确和可验证，并支持数据来源确认、完整性核验和状态一致性检查。

5.3 数据隐私性

涉及敏感信息或其他不宜公开数据时，应采取隐私保护措施；涉及敏感信息的数据不宜以明文形式直接上链。

5.4 数据时效性

行李全流程跟踪数据应根据业务需要及时采集、传输和存证；对批量归档、审计留痕等非实时业务数据，可采用批量方式上传，且自相关行李运输任务结束后至数据完成上链存证的时间间隔不宜超过24h。

6 总体架构

基于区块链的民航旅客行李全流程跟踪技术架构用于支撑行李全流程跟踪数据的采集、处理、存证、查询、验证和应用。该架构以区块链服务层为可信支撑，通过数据感知层、数据交互层、业务应用层和安全保障的协同，实现行李全流程跟踪数据在多主体，例如航空公司、民用机场、其它相关方之间的可信共享、过程追溯和一致性验证。

基于区块链的民航旅客行李全流程跟踪技术架构由数据感知层、数据交互层、区块链服务层、业务应用层和安全保障组成，图1为示意图。



图1 民航旅客行李全流程跟踪技术架构

数据感知层应能获取旅客托运行李在托运、分拣、装载、中转、卸载、到达、提取以及不正常行李处理等环节产生的跟踪数据。数据感知层宜通过离港控制系统、值机系统、行李处理系统、行李再确认系统、不正常行李处理系统、RFID设备、条码扫描设备及其他相关业务系统或采集设备，完成行李识别、状态采集和事件记录，并为后续数据交互、链上存证、状态查询和过程追溯提供数据来源。

数据交互层应实现数据感知层、业务应用层与区块链服务层之间的数据交换。数据交互层应对数据感知层提供的行李全流程跟踪及相关业务数据进行处理，使其满足区块链服务层数据上链、上链状态查询和数据验证的要求，并将区块链服务层返回的交易标识、存证凭证、上链状态、查询结果或验证结果反馈至相关业务系统或业务应用层。

区块链服务层应为民航旅客行李全流程跟踪数据提供节点管理、账本管理、共识确认和智能合约等基础能力。区块链服务层应接收数据交互层提交的行李全流程跟踪数据、数据摘要或存证请求，并向数据交互层返回交易标识、存证凭证、上链状态、查询结果或验证结果。

业务应用层面向航空公司、民用机场及其他相关方的业务系统，应提供基于区块链可信数据的行李状态查询、轨迹追溯、不正常行李处理、行李全流程跟踪数据验证和监管审计等应用服务。业务应用层应具有通过数据交互层调用区块链服务层提供的上链状态查询、存证凭证查询和数据验证能力，并按照授权规则展示或使用相关数据。

安全保障应贯穿数据感知层、数据交互层、区块链服务层和业务应用层，覆盖行李全流程跟踪数据采集、处理、传输、上链、查询、验证和展示全过程。应采用SM2数字签名、SM3摘要校验、SM4加密保护、RBAC访问控制和审计日志防篡改等技术措施，保障行李全流程跟踪数据来源可信、传输安全、内容完整、访问可控和操作可追溯。

7 数据感知层要求

7.1 行李识别要求

7.1.1 数据感知层应支持对民航旅客行李全流程跟踪过程中的旅客托运行李进行识别，并将行李对象与旅客行程、航班、始发机场、到达机场、中转机场等相关业务信息进行关联。

7.1.2 应采集能够唯一标识或辅助识别行李对象的信息，如行李编号、行李牌号、行李条码、RFID标识等，并与行李运输过程中相关信息进行关联，如航班号、始发机场等。

7.1.3 应保证同一件行李在全流程跟踪中的识别结果一致、连续和可追溯。

7.1.4 对行李识别结果不一致、缺失或异常的情况，应记录异常信息，并为后续数据校验、状态核验和业务处理提供依据。

7.2 状态采集要求

- 7.2.1 数据感知层应支持采集旅客托运行李在托运、分拣、装载、中转、卸载、到达、提取以及不正常行李处理等环节产生的状态数据。
- 7.2.2 应覆盖行李托运、安检、存储、分拣、装载、中转、卸载、到达、提取以及不正常行李处理等业务环节。
- 7.2.3 状态数据应能够反映行李所处业务环节、状态变化、事件发生时间、事件发生地点、数据来源和处理结果等信息。
- 7.2.4 状态数据应根据业务需要及时采集和传输，并保证关键状态变化能够被记录。
- 7.2.5 同一件行李在不同业务环节、不同业务系统和不同采集设备中形成的状态数据应能够关联一致。
- 7.2.6 对状态缺失、状态冲突、时间异常或处理结果异常的情况，应记录异常信息，并为后续数据校验、状态核验和业务处理提供依据。

7.3 事件记录要求

- 7.3.1 数据感知层应将旅客托运行李全流程处理过程中的状态变化、操作行为和处理结果记录为行李全流程跟踪事件。行李全流程跟踪事件应能够反映行李处理过程中的关键节点和状态变化。
- 7.3.2 应以行李在各业务环节产生的状态事件、操作事件和异常处理事件作为记录对象。
- 7.3.3 事件记录宜包括事件标识、行李标识、事件类型、事件发生时间、事件发生地点、数据提供方、数据来源系统、操作主体和处理结果等信息。
- 7.3.4 同一件行李的不同事件记录之间应能够按照时间顺序、业务环节或状态变化关系进行关联，形成连续的行李全流程跟踪记录。
- 7.3.5 对补录、修正、撤销或异常处理形成的事件记录，应保留原始记录、处理记录和关联关系。
- 7.3.6 事件记录应能够支撑后续数据处理、上链存证、状态查询、轨迹追溯。

8 数据交互层要求

8.1 数据处理要求

- 8.1.1 数据交互层应接收数据感知层采集的行李全流程跟踪及相关业务数据，并对其进行格式转换、标准化处理和数据校验，使其满足数据上链、上链状态查询、数据验证及相关业务交互要求。
- 8.1.2 应将接收的数据转换为统一的数据结构、字段定义、编码方式和时间格式；数据交换格式宜采用 JSON，字符编码宜采用 UTF-8。
- 8.1.3 应在格式转换和标准化处理后进行数据校验，校验内容包括必填项校验、格式校验、逻辑有效性校验、重复性校验和业务状态一致性校验。
- 8.1.4 经处理后的行李全流程跟踪数据应符合 MH/T 1076.3 第五条的相关要求。

8.2 数据上链与存证要求

8.2.1 基本要求

数据交互层应根据行李全流程跟踪业务需要，将经处理的行李全流程跟踪数据提交至区块链服务层，并接收区块链服务层返回的交易标识、存证凭证、上链状态。

数据上链方式可采用事件驱动上传和批量上传。

8.2.2 事件驱动上传要求

- 8.2.2.1 对行李状态查询、异常预警、不正常行李处理等实时性要求较高的业务数据，以及行李托运、分拣、装载、中转、卸载、到达、提取等环节产生的关键状态变化或处理结果，数据交互层宜采用事件驱动方式及时提交上链。
- 8.2.2.2 数据感知层或相关业务系统触发行李全流程跟踪事件后，数据交互层应接收对应的行李全流程跟踪事件数据。
- 8.2.2.3 应将经处理的数据、数据摘要或存证请求提交至区块链服务层进行存证。

8.2.2.4 应接收区块链服务层返回的交易标识、存证凭证、上链状态或异常信息，并反馈至相关业务系统或业务应用层。

8.2.2.5 对提交失败、重复提交、数据校验失败或上链状态异常的情况，应记录异常信息，并支持重新提交、补传。

8.2.3 批量上传要求

8.2.3.1 对实时性要求较低、数据量较大，或因网络中断、系统异常等原因需要补传的数据，可采用批量上传方式提交上链。

8.2.3.2 批量上传前，数据交互层应对待上传数据进行完整性校验、格式校验和重复性校验。

8.2.3.3 批量上传时，宜对批量数据生成数据摘要、摘要集合或 Merkle 树根哈希，并提交至区块链服务层进行存证。

8.2.3.4 采用数据摘要、摘要集合或 Merkle 树根哈希上链时，链下应保存对应的原始数据、明细数据及其关联关系，保证后续可进行完整性验证。

8.2.3.5 对批量归档、审计留痕等非实时业务数据，自相关行李运输任务结束后至数据完成上链存证的时间间隔不宜超过 24 h。

8.2.3.6 批量上传完成后，数据交互层应接收并记录区块链服务层返回的交易标识、存证凭证、上链状态或异常信息。

8.2.3.7 对批量上传失败、部分失败或重复上传的数据，应支持异常记录、重新提交或补传处理。

8.3 数据查询与验证要求

数据交互层应支持业务应用层、相关业务系统或经授权的数据使用方对交易标识、存证凭证、上链时间、上链状态和异常信息等内容进行查询，并支持对已上链数据的数据摘要一致性、数字签名有效性、数据来源可信性和存证时间有效性等进行验证。

9 区块链服务层要求

9.1 区块链节点服务要求

9.1.1 区块链服务层应支持对参与民航旅客行李全流程跟踪业务的区块链网络节点进行管理，保障区块链节点运行状态可见、节点变更可记录、节点异常可处理。

9.1.2 应支持节点接入、节点退出、节点角色和节点运行状态管理。

9.1.3 应支持对航空公司、机场、地面服务代理人、平台运营方、监管部门等不同参与方节点进行分类管理。

9.1.4 应根据节点角色和服务能力，区分数据提交、存证、查询、验证、监管审计等功能。

9.1.5 节点接入、退出、状态变更和异常处理过程应形成记录，并支持后续追溯。

9.2 账本服务要求

9.2.1 区块链服务层应提供账本记录、账本查询和存证验证能力，支撑行李全流程跟踪数据的可信保存、查询核验和过程追溯。

9.2.2 应支持对经共识确认的行李全流程跟踪数据、数据摘要、交易标识、存证凭证、时间信息和相关操作记录进行保存、查询和核验。

9.2.3 应保证链上记录的完整性、连续性和可追溯性。

9.2.4 应支持对已上链数据的存证状态和完整性进行验证。

9.2.5 验证内容宜包括交易标识、存证凭证、数据摘要、数字签名、存证时间、数据来源等信息。

9.2.6 应为行李状态查询、轨迹追溯、数据验证和监管审计提供链上依据。

9.3 共识服务要求

9.3.1 区块链服务层应提供共识服务，对数据交互层提交的行李全流程跟踪数据、数据摘要或存证请求进行确认，并支持相关节点对交易有效性、交易顺序和账本状态形成一致结果。

9.3.2 经共识确认的数据方可写入账本。

- 9.3.3 应支持多主体参与场景下的数据提交一致性确认。
- 9.3.4 应支持对数据提交结果和交易顺序进行确认，避免未经确认、重复提交或顺序异常的数据写入账本。
- 9.3.5 共识算法的选择应满足民航旅客行李全流程跟踪业务对可靠性、处理效率、可扩展性和容错能力的要求。
- 9.3.6 在部分节点异常的情况下，应支持维持系统可用性和账本一致性。

9.4 智能合约服务要求

- 9.4.1 区块链服务层应支持智能合约服务，用于固化行李全流程跟踪数据存证、状态更新和查询验证等业务规则。
- 9.4.2 应支持行李全流程跟踪数据存证、存证状态更新和数据验证等规则的配置与执行。
- 9.4.3 应支持对数据提交、状态更新、查询验证等操作进行规则化处理。
- 9.4.4 智能合约或等效规则的部署、升级和停用应进行管理，相关操作记录应纳入安全审计。

10 业务应用层要求

10.1 状态查询要求

- 10.1.1.1 业务应用层应支持对旅客托运行李当前状态和关键状态信息进行查询。
- 10.1.1.2 应支持按照行李标识、航班号、业务环节、事件时间等条件查询行李状态。
- 10.1.1.3 查询结果应能够反映行李当前业务环节、状态变化、事件发生时间、事件发生地点和处理结果等信息。
- 10.1.1.4 查询结果应能够关联展示交易标识、存证凭证、上链状态等链上存证信息。
- 10.1.1.5 查询结果应按照访问主体的授权范围进行展示，涉及旅客个人信息、商业敏感信息和运行管理敏感信息的，应按照访问控制和隐私保护要求进行处理。

10.2 轨迹追溯要求

- 10.2.1 业务应用层应支持基于行李全流程跟踪事件记录，对旅客托运行李全流程处理过程进行追溯。
- 10.2.2 应支持按照行李标识、航班号、事件类型、业务环节、事件发生时间、数据提供方等条件查询相关事件记录。
- 10.2.3 追溯结果应能够反映行李在托运、安检、存储、分拣、装载、中转、卸载、到达、提取以及不正常行李处理等环节的关键节点、状态变化、时间顺序和处理结果。
- 10.2.4 应支持对链上存证信息与链下业务数据的一致性进行核验。
- 10.2.5 追溯结果应能够为行李状态查询、不正常行李处理、责任核验和争议处理提供依据。

10.3 不正常行李处理要求

- 10.3.1 业务应用层应支持行李延误、错运、丢失、破损、补运、赔付、旅客投诉等不正常行李处理相关应用。
- 10.3.2 应支持不正常行李案件与行李全流程跟踪事件的关联，反映行李异常发生前后的状态变化和处理过程。
- 10.3.3 不正常行李处理过程中的关键操作、处理结果和状态变化应形成可追溯记录，并支撑后续查询、验证、监管审计和争议处理。

11 安全保障要求

11.1 身份认证要求

- 11.1.1 应对接入的区块链节点、业务系统、接口服务、采集设备和操作用户进行身份认证，保证接入主体身份真实、唯一、可核验。
- 11.1.2 区块链节点、数据交互接口和相关业务系统之间通信应使用基于 PKI 的数字证书进行双向身份认证。

- 11.1.3 数据提交、存证请求、查询验证请求和关键管理操作应进行 SM2 数字签名校验。
- 11.1.4 对系统管理员、节点管理人员、权限配置人员和监管审计人员等高权限用户，应采用数字证书与口令、动态验证码或其他认证因子相结合的加强认证方式。
- 11.1.5 身份认证失败、证书失效或签名校验不通过的请求不应继续处理，并应记录异常信息。

11.2 访问控制要求

- 11.2.1 应采用 RBAC 访问控制机制，对数据访问、功能调用和管理操作进行权限控制。
- 11.2.2 应按照航空公司、机场、地面服务代理人、平台运营方、监管部门、旅客服务系统和系统运维管理人员等角色配置访问权限。
- 11.2.3 应对数据提交、数据查询、数据验证、数据导出、业务应用展示、链上数据提交、链上记录查询、智能合约调用、节点管理和系统配置等操作进行权限控制。
- 11.2.4 涉及旅客个人信息、商业敏感信息和运行管理敏感信息的数据，应采用最小权限原则和字段级访问控制机制。
- 11.2.5 未经授权的主体不应查询、导出、共享或使用超出授权范围的数据。
- 11.2.6 权限配置、权限变更、权限撤销和高权限操作应形成记录，并支持后续追溯。

11.3 行李全流程跟踪数据保护要求

- 11.3.1 应对行李全流程跟踪数据在传输、处理、存储、上链和验证过程中的安全进行保护，防止数据被窃取、篡改、替换或重放。
- 11.3.2 数据传输应采用安全传输协议，并使用 SM2、SM4 或等效密码算法保障传输安全。
- 11.3.3 接口调用和数据提交报文应包含时间戳、随机数或请求序列号，并结合数字签名进行完整性校验和防重放校验。
- 11.3.4 数据交互层提交上链前，应采用 SM3 或等效密码杂凑算法生成数据摘要。
- 11.3.5 采用摘要上链方式时，链下原始数据或明细数据应能够通过重新计算摘要与链上摘要进行一致性验证。
- 11.3.6 密钥、证书私钥等敏感安全材料应与业务数据分离保存，并进行访问限制和使用记录。

11.4 隐私保护要求

- 11.4.1 处理敏感信息时，应采取隐私保护措施，防止相关数据被非授权访问、使用、泄露或篡改。
- 11.4.2 涉及敏感信息的数据，不应以明文形式直接公开上链。
- 11.4.3 确需用于存证验证的敏感数据，应采用 SM3 摘要上链、链下加密保存和授权查询相结合的方式处理。
- 11.4.4 业务应用层展示行李状态查询、轨迹追溯、不正常行李处理和监管审计结果时，应根据访问主体角色和授权范围，对敏感字段进行隐藏、脱敏或限制返回。
- 11.4.5 个人信息的采集、使用、共享和查询应遵循最小必要原则。
- 11.4.6 个人信息访问和使用行为应保留记录，并支持审计追溯。

11.5 安全审计要求

- 11.5.1 应对关键操作和异常行为进行安全审计，保证操作行为可记录、可核验、可追溯。
- 11.5.2 应对身份认证、接口调用、数据提交、数据上链、数据查询、数据验证、数据导出、权限变更、节点接入退出、智能合约调用和系统配置变更等关键操作生成安全审计记录。
- 11.5.3 安全审计记录应至少包括操作主体、操作时间、操作对象、操作类型、操作结果和异常信息。
- 11.5.4 安全审计记录应能够与交易标识、存证凭证、节点标识或业务事件标识进行关联；
- 11.5.5 安全审计日志应采用 SM3 摘要校验、摘要上链或等效防篡改技术进行完整性保护，防止未经授权的修改、删除或覆盖。
- 11.5.6 系统应对证书失效、签名校验失败、摘要不一致、越权访问、批量异常查询、重复提交、上链失败、节点异常和链上链下数据不一致等情况进行异常记录和告警。
- 11.5.7 异常处置结果应形成记录，并支持后续追溯。

参 考 文 献

- [1] GB/T 42752-2023 区块链和分布式记账技术参考架构
 - [2] GB/T 43572-2023 区块链和分布式记账技术术语
 - [3] GB/T 32905 信息安全技术 SM3 密码杂凑算法
 - [4] GB/T 32907 信息安全技术 SM4 分组密码算法
 - [5] GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法
 - [6] GB/T 43579-2023 区块链和分布式记账技术智能合约生命周期管理技术规范
 - [7] GB/T 43582-2023 区块链和分布式记账技术应用程序接口中间件技术指南
 - [8] MH/T 1076.1 民航旅客行李全流程跟踪系统 第1部分：机场端建设规范
 - [9] T/CATAGS 63.3 不正常行李交互规范第3部分：流程数据
-