ICS 03.060
CCS A11

团 体 标 准

T/CBA 215—2023

银行函证服务平台
候选分布式账本技术节点接入要求

Banking confirmation service platform —

Requirements for a candidate of DLT node for participating in distributed ledger

2023－03－28 发布　　2023－03－28 实施

中国银行业协会　发布

目　　次

前　言

中国银行业协会(China Banking Association，CBA)成立于2000年5月，是经中国人民银行和民政部批准成立，并在民政部登记注册的全国性非营利社会团体，是中国银行业自律组织。2003年中国银监会成立后，中国银行业协会主管单位由中国人民银行变更为中国银监会。2018年3月，中国银行保险监督管理委员会成立后，中国银行业协会主管单位由中国银监会变更为中国银行保险监督管理委员会。凡经业务主管单位批准设立的、具有独立法人资格的银行业金融机构(含在华外资银行业金融机构)和经相关监管机构批准、具有独立法人资格、在民政部门登记注册的各省(自治区、直辖市、计划单列市)银行业协会以及相关监管机构批准设立，具有独立法人资格的依法与银行业金融机构开展相关业务合作的其他类型金融机构，以及银行业专业服务机构均能申请加入中国银行业协会成为会员单位。

中国银行业协会日常办事机构为秘书处。秘书处设秘书长1名，副秘书长若干名。根据工作需要，中国银行业协会设立32个专业委员会，其中银行业产品和服务标准化专业委员会旨在开展银行业产品和服务标准化工作，包括制定和发布银行业的产品和服务标准，积极参与制定国家标准、行业规划，参与制定有关政策和法律法规，不断提高银行业产品和服务质量。

本文件按照T/CBA 1—2021《中国银行业协会团体标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

T/CBA 215《银行函证服务平台 候选分布式账本节点接入要求》是按照财政部和银保监会的要求构建的银行函证服务平台的工作技术依据系列文件之一，本系列文件结构如下：

——T/CBA 210《银行函证服务平台 接入要求》；

——T/CBA 211《银行函证服务平台 加密体系》；

——T/CBA 212《银行函证服务平台 基础数据元》；

——T/CBA 213《银行函证服务平台 服务接口》；

——TR/CBA 214《银行函证服务平台 运营规则》；

——T/CBA 215《银行函证服务平台 候选分布式账本节点接入要求》。

本文件由中国银行业协会银行函证平台服务中心提出。

本文件由中国银行业协会银行业产品和服务标准化专业委员会归口。

本文件起草单位：中国银行业协会、工银科技股份有限公司、中国农业银行股份有限公司、中国邮政储蓄银行股份有限公司、中国光大银行股份有限公司、兴业银行股份有限公司、中央国债登记结算有限责任公司。

本文件主要起草人：邢炜、刘峰、高峰、李宽、李洪业、赵成刚、李朋乐、李海丽、仲峻锋、陈嘉、张纪峰、贾琳琳、崔梦枭、蒋启明、陆婷、杨扬、王琛、杨洋、涂晓枫。

地 址：北京市西城区金融街 20 号交通银行大厦 B 座
电 话：010-66553368 010-66291132
邮 编：100033
邮 箱：cba.china@china-cba.net
传 真：010-66553356

引　言

银行函证服务系统是实现银行函证业务数字化转型的重要技术手段，采用区块链技术，则可以有效提升系统的整体安全性和可信性。在分布式账本投入使用后，随着使用范围的扩大，必然会提出新加入节点的要求。如果没有统一的要求，则难以保证这一工作的有序开展。

为了提升对区块链和分布式账本的正确理解，本文件全面引入了ISO 22739:2020界定的术语；对环境的要求则在等级保护三级的基础上，提出了若干特定的要求，便于银行业金融机构和会计师事务所实现；通过给出对分户账记录的基本要求，为区块链分布式账本建立了基本规则；通过规定区块链分布式账本技术接入节点的基本功能要求和非功能要求，确保了整体银行函证系统区块链整体工作的稳定与可靠。

通过实施本文件，能够使得有意向申请加入银行函证服务系统分布式账本网络的银行业金融机构和会计师事务所能够有的放矢地进行准备，并对相关的开发测试工作量进行必要的评估；银行函证服务系统的管理部门则可以据此对相关准备就绪情况进行核验；其他没有加入银行函证服务系统分布式账本网络的成员单位，亦能通过本文件了解加入到银行函证服务系统分布式账本网络的技术要求，增强对整体银行函证系统稳定可靠工作的信心。

银行函证服务平台 候选分布式账本技术节点接入要求

1 范围

本文件规定了申请加入银行函证系统的DLT系统的候选DLT节点需要满足的环境要求、需遵循的分户账记录的基本要求以及基本功能要求和非功能要求。

本文件适用于对候选DLT节点申请加入银行函证系统的DLT系统以及加入后符合状况的判定。

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 7408—2005 数据元和交换格式 信息交换 日期和时间表示法

GB/T 22239—2019 信息安全技术网络安全等级保护基本要求

GB/T 32905—2016 信息安全技术 SM3密码杂凑算法

GB/T 32907—2016 信息安全技术 SM4分组密码算法

GB/T 32918（所有部分） 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 40473.1—2021 银行业应用系统 非功能需求 第1部分：描述框架

GB/T 40473.2—2021 银行业应用系统 非功能需求 第2部分：功能适宜性

GB/T 40473.3—2021 银行业应用系统 非功能需求 第3部分：性能效率

GB/T 40473.4—2021 银行业应用系统 非功能需求 第4部分：兼容性

GB/T 40473.5—2021 银行业应用系统 非功能需求 第5部分：易用性

GB/T 40473.6—2021 银行业应用系统 非功能需求 第6部分：可靠性

GB/T 40473.7—2021 银行业应用系统 非功能需求 第7部分：安全性

GB/T 40473.8—2021 银行业应用系统 非功能需求 第8部分：可维护性

GB/T 40473.9—2021 银行业应用系统 非功能需求 第9部分：可移植性

JR/T 0101—2013 银行业软件测试文档规范

ISO/IEC 10118-3:2018 IT安全技术 散列函数 第3部分：专用散列函数（IT Security techniques — Hash-functions — Part 3:Dedicated hash-functions）

ISO/IEC 18033-2:2006 信息技术 安全技术 加密算法 第2部分：非对称密码（Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers）

ISO/IEC 18033-3:2010 信息技术 安全技术 加密算法 第3部分：分组密码（Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers）

ISO 23257:2022 区块链和分布式账本技术 参考框架（Blockchain and distributed ledger technologies — Reference architecture）

3 术语、定义和缩略语

下列术语和定义适用于本文件。

3.1

银行函证业务　banking confirmation business

会计师事务所等在获取被审计单位授权后，直接向银行业金融机构发出询证函，银行业金融机构针对所收到的询证函，查询、核对相关信息并直接提供回函的过程。

术语条目注 1：询证函可能是能够进行数据元解析的，也可能仅是一个图像或不可更改格式的文件。

术语条目注 2：《关于进一步规范银行函证及回函工作的通知》（财会〔2020〕12 号）中，界定的相关概念为“银行函证及回函，是注册会计师在获取被审计单位授权后，直接向银行业金融机构发出询证函，银行业金融机构针对所收到的询证函，查询、核对相关信息并直接提供书面回函的过程”。因本文件面向的实施对象不是注册会计师个人，而是会计师事务所，故对定义进行了调整。

[来源：T/CBA 211—2021，3.1]

3.2

银行函证系统　banking confirmation business system

处理银行函证业务（3.1）的应用系统。

术语条目注 1：银行函证系统由银行函证服务平台、银行业金融机构、会计师事务所和相关机构构成，其框架和基本工作过程见 T/CBA 210—2021。

[来源：T/CBA 211—2021，3.2]

3.3

区块链　blockchain

由已确信区块(3.5)组成的分布式账本(3.4)，其按仅能追加使用密码链接(3.20)的顺序链方式组织

术语条目注 1：ISO 22739:2020 中 3.6 的原文为“distributed ledger with confirmed blocks organized in an append-only, sequential chain using cryptographic links”。

术语条目注 2：区块链被设计为抗篡改，并创建最终的、确定的和不可变更的(3.8)分户账记录(3.27)。该注释为 ISO 22739:2020 中 3.6 的术语条目注 1，其原文为“Blockchains are designed to be tamper resistant and to create final, definitive and immutable ledger records.”。

[来源：ISO 22739:2020，3.6，有修改——见术语条目注1～术语条目注2]

3.4

分布式账本　distributed ledger

由一组DLT节点(3.17)共享，并使用共识机制(3.15)在DLT节点之间同步的分户帐(3.26)

术语条目注 1：ISO 22739:2020 中 3.22 的原文为“ledger that is shared across a set of DLT nodes and synchronized between the DLT nodes using a consensus mechanism”。

术语条目注 2：分布式账本被设计为防篡改、仅追加和不可变更(3.8)，包含已确信的(3.6)和已确认的(3.7)交易(3.21)。该注释为 ISO 22739:2020 中 3.22 的术语条目注 1，其原文为“A distributed ledger is designed to be tamper resistant, append-only and immutable containing confirmed and validated transactions.”。

[来源：ISO 22739:2020，3.22，有修改——见术语条目注1～术语条目注2]

3.5

已确信区块　confirmed block

已确信的(3.6)区块(3.9)

术语条目注 1：ISO 22739:2020 中 3.9 的原文为“block that has been confirmed”。

[来源：ISO 22739:2020，3.9，有修改——见术语条目注1]

3.6

已确信的　confirmed

已通过共识(3.16)接受，可纳入分布式账本(3.4)

术语条目注 1：ISO 22739:2020 中 3.8 的原文为“accepted by consensus for inclusion in a distributed ledger”。

[来源：ISO 22739:2020，3.8，有修改——见术语条目注1]

3.7

已确认的 validated

当实体(3.20)所需的完整性条件已被检查后的状态

术语条目注 1：ISO 22739:2020 中 3.81 的原文为“status of an entity when its required integrity conditions have been checked”。

术语条目注 2：例如，在 DLT 系统(3.19)中，能确认交易(3.21)、分户账记录(3.27)或区块(3.9)。该注释为 ISO 22739:2020 中 3.81 的术语条目注 1，其原文为“For example, in a DLT system, a transaction, ledger record, or block can be validated.”。

[来源：ISO 22739:2020，3.81，有修改——见术语条目注1～术语条目注2]

3.8

不可变更性 immutability

一旦添加到分布式账本(3.4)中，分户帐记录(3.27)就不能修改或删除的属性

术语条目注 1：ISO 22739:2020 中 3.40 的原文为“property wherein ledger records cannot be modified or removed once added to a distributed ledger”。

术语条目注 2：在适当的情况下，不可变更性还假定保持分户帐记录(3.27)的顺序和分户帐记录之间的链接不变。该注释为 ISO 22739:2020 中 3.40 的术语条目注 1，其原文为“Where appropriate, immutability also presumes keeping intact the order of ledger records and the links between the ledger records”。

[来源：ISO 22739:2020，3.40，有修改——见术语条目注1～术语条目注2]

3.9

区块 block

由区块数据(3.10)和区块头(3.11)组成的结构化数据

术语条目注 1：ISO 22739:2020 中 3.2 的原文为“structured data comprising block data and a block header”。

[来源：ISO 22739:2020，3.2，有修改——见术语条目注1]

3.10

区块数据 block data

包含零到多个交易记录(3.22)或交易记录引用的结构化数据

术语条目注 1：ISO 22739:2020 中 3.3 的原文为“structured data comprising zero or more transaction records or references to transaction records”。

[来源：ISO 22739:2020，3.3，有修改——见术语条目注1]

3.11

区块头 block header

包含到前一个区块(3.9)密码链接(3.23)的结构化数据，除非没有前一个区块

术语条目注 1：ISO 22739:2020 中 3.4 的原文为“structured data that includes a cryptographic link to the previous block unless there is no previous block”。

术语条目注 2：块头还可以包含时间戳(3.12)、一次性随机数(3.13)和其他 DLT 平台(3.18)特定的数据，包括对应交易记录(3.22)的哈希值(3.25)。该注释为 ISO 22739:2020 中 3.4 的术语条目注 1，其原文为“ A block header can also contain a timestamp, a nonce, and other DLT platform specific data, including a hash value of corresponding transaction records.”。

[来源：ISO 22739:2020，3.4，有修改——见术语条目注1～术语条目注2]

3.12

时间戳 timestamp

指出相对于公共时间基准时间点的时间变量参数

术语条目注 1： ISO 22739:2020 中 3.75 的原文为“time variant parameter which denotes a point in time with respect to a common time reference”。

[来源：ISO 22739:2020，3.75，有修改——见术语条目注1]

3.13

一次性随机数 nonce

在一套密码操作中仅用一次的数字或位字符串

术语条目注 1： ISO 22739:2020 中 3.51 的原文为“number or bit string used once in a set of cryptographic operations”。

术语条目注 2： 一次性随机数通常是随机数的或伪随机数。其通常用于防止重放攻击，而在重放攻击中，消息被恶意的参与者捕获并重新发送。在一些区块链系统(3.19)中，它用于在生成新区块(3.9)期间调节挖矿(3.14)，并存储在区块头(3.11)中。该注释为 ISO 22739:2020 中 3.51 的术语条目注 1，其原文为“A nonce is often random or pseudo-random. It is commonly used to guard against replay attacks, where a message is captured and re-sent by a malicious actor. In some blockchain systems it is used to modulate mining during the generation of a new block and is stored in the block header.”。

[来源：ISO 22739:2020，3.51，有修改——见术语条目注1～术语条目注2]

3.14

挖矿 mining

在某些共识机制(3.15)中，创建并确认区块(3.9)或确认分户账记录(3.27)的活动

术语条目注 1： ISO 22739:2020 中 3.49 的原文为“activity, in some consensus mechanisms, that creates and validates blocks or validates ledger records”。

术语条目注 2： 参与挖矿通常受到区块奖励和交易费用的激励。该注释为 ISO 22739:2020 中 3.49 的术语条目注 1，其原文为“Participation in mining is often incentivized by block rewards and transaction fees.”。

[来源：ISO 22739:2020，3.49，有修改——见术语条目注1～术语条目注2]

3.15

共识机制 consensus mechanism

达成共识(3.16)的规则和程序

术语条目注 1： ISO 22739:2020 中 3.12 的原文为“rules and procedures by which consensus is reached”。

[来源：ISO 22739:2020，3.12，有修改——见术语条目注1]

3.16

共识 consensus

DLT节点(3.17)之间的约定，一是一个交易(3.21)是已确认的(3.7)，二是分布式账本(3.4)包含已确认的(3.7)交易(3.21)排列的一致集合

术语条目注 1： ISO 22739:2020 中 3.11 的原文为“agreement among DLT nodes that 1) a transaction is validated and 2) that the distributed ledger contains a consistent set and ordering of validated transactions”。

术语条目注 2： 共识并不一定意味着所有 DLT 节点(3.17)都同意。该注释为 ISO 22739:2020 中 3.11 的术语条目注 1，其原文为“Consensus does not necessarily mean that all DLT nodes agree.”。

术语条目注 3： 有关共识的细节在 DLT 设计中有所不同，这是一种设计与另一种设计之间的区别特征。该注释为 ISO 22739:2020 中 3.11 的术语条目注 2，其原文为“The details regarding consensus differ among DLT designs and this is a distinguishing characteristic between one design and another.”。

[来源：ISO 22739:2020，3.11，有修改——见术语条目注1～术语条目注3]

3.17

DLT 节点　DLT node

分布式账本技术节点　distributed ledger technology node

节点　node

<分布式账本技术节点>参与网络并存储分户帐记录(3.27)的完整或部分副本的设备或过程

术语条目注 1：ISO 22739:2020 中 3.27 的原文为“<distributed ledger technology> device or process that participates in a network and stores a complete or partial replica of the ledger records”。

[来源：ISO 22739:2020，3.27，有修改——见术语条目注1]

3.18

DLT 平台　DLT platform

分布式账本技术平台 distributed ledger technology platform

一组处理、存储和通信的实体(3.20)，它们共同提供每个DLT节点(3.17)上DLT系统(3.19)的能力

术语条目注 1：ISO 22739:2020 中 3.29 的原文为“set of processing, storage and communication entities which together provide the capabilities of the DLT system on each DLT node”。

[来源：ISO 22739:2020，3.29，有修改——见术语条目注1]

3.19

DLT 系统　DLT system

分布式账本系统 distributed ledger system

分布式账本技术系统 distributed ledger technology system

实现分布式账本(3.4)的系统

术语条目注 1：ISO 22739:2020 中 3.30 的原文为“system that implements a distributed ledger”。

[来源：ISO 22739:2020，3.30，有修改——见术语条目注1]

3.20

实体　entity

在信息和通信技术系统内部或外部的项，如人、组织、设备、子系统，或能被清晰地识别出来的由多个项构成的项组

术语条目注 1：ISO 22739:2020 中 3.34 的原文为“item inside or outside an information and communication technology system, such as a person, an organization, a device, a subsystem, or a group of such items that has recognizably distinct existence”。

[来源：ISO 22739:2020，3.34，有修改——见术语条目注1]

3.21

交易　transaction

工作过程的最小单元，它是产生符合治理规则的结果所需的一个或多个活动序列

术语条目注 1：ISO 22739:2020 中 3.77 的原文为“smallest unit of a work process, which is one or more sequences of actions required to produce an outcome that complies with governing rules”。

术语条目注 2：在适当的情况下，作为与区块链(3.3)或分布式账本(3.4)交互相关的工作过程的最小单位，交易被理解得更狭隘。该注释为 ISO 22739:2020 中 3.77 的术语条目注 1，其原文为“Where appropriate, transaction is understood more narrowly, as the smallest unit of a work process related to interactions with blockchains or distributed ledgers.”。

[来源：ISO 22739:2020，3.77，有修改——见术语条目注1～术语条目注2]

3.22

交易记录　transaction record

记载任何类型的交易(3.21)的记录(3.29)

术语条目注 1： ISO 22739:2020 中 3.79 的原文为“record documenting a transaction of any type”。

术语条目注 2： 交易记录能够包含在分户账记录(3.27)中，亦可通过分户账记录引用。该注释为 ISO 22739:2020 中 3.79 的术语条目注 1，其原文为“Transaction records can be included in, or referred to, in a ledger record.”。

术语条目注 3： 交易记录能够包括交易(3.21)的结果。该注释为 ISO 22739:2020 中 3.79 的术语条目注 2，其原文为“Transaction records can include the result of a transaction.”。

[来源：ISO 22739:2020，3.79，有修改——见术语条目注1～术语条目注3]

3.23

密码链接　cryptographic link

使用密码哈希函数(3.24)技术构造的指向数据的引用

术语条目注 1： ISO 22739:2020 中 3.16 的原文为“reference, constructed using a cryptographic hash function technique, that points to data”。

术语条目注 2： 区块头(3.11)中使用了一个密码链接来引用前一个区块(3.9)，以创建仅追加的顺序链，形成一个区块链(3.3)。该注释为 ISO 22739:2020 中 3.16 的术语条目注 1，其原文为“A cryptographic link is used in the block header to reference the previous block in order to create the append-only, sequential chain that forms a blockchain.”。

[来源：ISO 22739:2020，3.16，有修改——见术语条目注1～术语条目注2]

3.24

密码哈希函数　cryptographic hash function

函数将任意长度的二进制字符串映射到固定长度的二进制字符串，这样在给定的输出中寻找一个映射到输出的输入在计算上成本很高，在给定的输入中寻找第二个映射到相同输出的输入在计算上不可行，且在计算上寻找任何两个不同的输入映射到相同的输出也不可行

术语条目注 1： ISO 22739:2020 中 3.15 的原文为“function mapping binary strings of arbitrary length to binary strings of fixed length, such that it is computationally costly to find for a given output an input that maps to the output, it is computationally infeasible to find for a given input a second input that maps to the same output, and it is computationally infeasible to find any two distinct inputs that map to the same output”。

术语条目注 2： 计算的可行性取决于具体的安全要求和环境。该注释为 ISO 22739:2020 中 3.15 的术语条目注 1，其原文为“Computational feasibility depends on the specific security requirements and environment.”。

[来源：ISO 22739:2020，3.15，有修改——见术语条目注1～术语条目注2]

3.25

哈希值　hash value

一个密码哈希函数(3.24)的输出位串

术语条目注 1： ISO 22739:2020 中 3.39 的原文为“string of bits which is the output of a cryptographic hash function”。

[来源：ISO 22739:2020，3.39，有修改——见术语条目注1]

3.26

分户账　ledger

保存最终的、确定的和不可变更(3.8)的交易(3.21)记录(3.28)的信息存储

术语条目注 1： ISO 22739:2020 中 3.43 的原文为“information store that keeps records of transactions that are intended to be final, definitive and immutable”。

[来源：ISO 22739:2020，3.43，有修改——见术语条目注1]

3.27

分户账记录　ledger record

包含交易记录(3.22)、交易记录的哈希值(3.25)或交易记录在分布式账本(3.4)上引用的记录(3.28)

术语条目注 1： ISO 22739:2020 中 3.44 的原文为“record containing transaction records, hash values of transaction records, or references to transaction records recorded on a distributed ledger”。

术语条目注 2： 引用可以实现为密码链接(3.23)。该注释为 ISO 22739:2020 中 3.44 的术语条目注 1，其原文为“A reference can be implemented as a cryptographic link (3.23).”。

[来源：ISO 22739:2020，3.44，有修改——见术语条目注1～术语条目注2]

3.28

记录　record

一个组织或个人在履行法律义务或在业务交易中(3.31)作为证据和资产(3.29)创建、接收和维护的信息

术语条目注 1： ISO 22739:2020 中 3.67 的原文为“information created, received and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of business”。

术语条目注 2： 本术语适用于任何媒介、形式或格式的信息。该注释为 ISO 22739:2020 中 3.67 的术语条目注 1，其原文为“This term applies to information in any medium, form or format.”。

[来源：ISO 22739:2020，3.67，有修改——见术语条目注1～术语条目注2]

3.29

资产　asset

任何对干系人有价值的东西

术语条目注 1： ISO 22739:2020 中 3.1 的原文为“anything that has value to a stakeholder”。

[来源：ISO 22739:2020，3.1，有修改——见术语条目注1]

3.30

智能合约　smart contract

存储在DLT系统(3.19)中的计算机程序，该程序的任何执行结果都被记录在分布式账本(3.4)上

术语条目注 1： ISO 22739:2020 中 3.72 的原文为“computer program stored in a DLT system wherein the outcome of any execution of the program is recorded on the distributed ledger”。

术语条目注 2： 智能合同可以在法律上代表合同中的条款，并在适用司法管辖区的立法下创建法律上可强制执行的义务。该注释为 ISO 22739:2020 中 3.72 的术语条目注 1，其原文为“A smart contract can represent terms in a contract in law and create a legally enforceable obligation under the legislation of an applicable jurisdiction.”。

[来源：ISO 22739:2020，3.72，有修改——见术语条目注1～术语条目注2]

3.31

候选 DLT 节点　candidate of DLT node

申请加入银行函证系统（3.2）的DLT节点（3.17）。

3.32

银行函证系统的 DLT 平台　DLT platform of banking confirmation business system

银行函证系统（3.2）中的DLT平台（3.18）。

注： 在非工程化的场合，银行函证区块链平台既可能指银行函证的DLT平台，也可能指整个银行函证系统。

3.33

大驼峰命名法　Upper CamelCase

由连在一起的单词（或汉语拼音）组成的字符串，其每个单词的第一个字符是大写的。如果字符串只包含一个单词，则只使用大写字符。

4　环境要求

4.1　硬件

候选DLT节点运行的硬件环境应符合如下要求。

a）　符合 GB/T 22239—2019 中三级及以上的物理和网络要求。

b）　主机可为物理主机或虚拟主机（包括云主机），具备如下加固能力：

1）　必要端口的关闭；

2）　进程限制；

3）　帐号关闭；

4）　连接网络控制；

5）　系统和软件版本指定。

c）　具备对节点运行状态与资源使用情况的监控能力，在异常情况下触发告警。

d）　在设备和存储介质重用、报废或更换时，对其承载的数据进行清除且不可恢复。

4.2　软件

候选DLT节点运行的软件环境应符合GB/T 22239—2019中三级以上的主机安全、应用安全、数据安全及备份恢复相关要求。

5　分户账记录要求

5.1　概述

候选 DLT 节点的分户账记录应描述下列属性：

a）　分户账记录英文名称；

b）　分户账记录内各字段英文名称；

c）　数据种类，按 A.2 给出；

d）　数据格式；

e）　呈现规则；

f）　备注。

5.2　分户账记录级

5.2.1　英文名称

分户账记录英文名称应符合如下要求：

a）　在银行函证系统中，分户账记录英文名称不重复；

b）　要能恰如其分地表达中文语义；

c）　采用大驼峰命名法。

5.2.2　呈现要求

分户账记录应按照A.4给出呈现要求。

5.3 分户账记录组分级

5.3.1 英文名称

分户账记录内各组分的英文名称：

a) 宜能恰如其分地表达中文语义；
b) 应采用大驼峰命名法。

5.3.2 数据种类

分户账记录内各组分的数据种类应为A.3.1所给出的数据种类之一。

5.3.3 数据格式

分户账记录内各组分，除组分为对象的情况外，均应按照附录A.3.2的要求给出数据格式。

5.3.4 呈现要求

分户账记录内各组分，均应按照附录A.4的要求给出呈现要求。

6 基本功能要求

6.1 角色与用户管理

6.1.1 角色管理

6.1.1.1 候选 DLT 节点应实现 6.1.1.2～6.1.1.10 的要求，并可在需要时按照 GB/T 40473.2—2021 中 5.1.8 进行更加广泛和深入的分析。

6.1.1.2 候选 DLT 节点应能支持如下角色：

a) 超级角色，拥有候选 DLT 节点所有操作权限；
b) 角色管理角色，拥有维护管理角色信息、给用户分配角色的权限；
c) 智能合约审计角色，拥有测试、审计智能合约功能的权限；
d) 智能合约部署角色，拥有部署、升级智能合约的权限；
e) 智能合约停止角色，拥有停止智能合约的权限；
f) 组织管理角色，拥有新建、删除组织的权限；
g) 用户管理角色，拥有新建、删除用户的权限；
h) 用户与节点绑定角色，拥有管理用户与节点绑定、解绑的操作权限；
i) 节点与组织绑定角色，拥有控制管理节点与组织绑定、解绑的操作权限；
j) 节点交易读写角色，拥有节点交易的读写权限；
k) 节点交易只读角色，拥有节点交易的只读权限；
l) 候选 DLT 节点审计角色，拥有节点日志只读审查权限；
m) 候选 DLT 节点运行状况角色，拥有节点运行状况展示审查权限。

6.1.1.3 候选 DLT 节点创建角色由角色管理角色操作，除超级角色和角色管理角色之外的角色均可由用户界面进行分配操作。

6.1.1.4 候选 DLT 节点在创建除超级角色和角色管理角色之外的角色时，应描述的角色基本属性包括：

a) 角色名称；

b) 角色描述；
c) 角色创建时间；
d) 角色有效期；
e) 角色对应的权限；
f) 角色状态；
g) 其他需要描述的信息。

6.1.1.5 候选 DLT 节点角色对应权限体现为通过菜单对系统的访问权限。

6.1.1.6 候选 DLT 节点删除角色的功能由角色管理角色进行操作。角色删除之后，该角色对应的所有用户将不再拥有该角色对应的所有权限，且系统中可查询到该角色状态为“删除”状态。

6.1.1.7 候选 DLT 节点支持提供由角色管理角色执行批量删除角色功能。

6.1.1.8 候选 DLT 修改角色的功能由角色管理角色进行操作，且：

a) 可进行修改的角色基本属性包括：
   1) 角色名称；
   2) 角色描述；
   3) 角色对应的权限。
b) 不可修改的角色基本属性包括：
   1) 角色 ID；
   2) 角色创建时间。

6.1.1.9 候选 DLT 查询角色的功能由角色管理角色进行操作，查询条件包括：

a) 角色 ID；
b) 角色名称；
c) 角色权限。

6.1.1.10 候选 DLT 节点角色互斥关系设置的功能由角色管理角色进行操作，具体角色互斥关系为：

a) 智能合约审计角色与智能合约部署、停止互斥；
b) 交易数据读取与只读权限互斥；
c) 角色管理角色、组织管理角色和用户管理角色与除超级角色外的其他角色互斥；
d) 其他根据业务需要进行的互斥。

6.1.2 用户管理

6.1.2.1 候选 DLT 节点实现 6.1.2.2～6.1.2.11 的要求，并可在需要时按照 GB/T 40473.2—2021 中 5.1.9 进行更加广泛和深入的分析。

6.1.2.2 候选 DLT 节点创建用户的功能由用户管理角色操作。

6.1.2.3 候选 DLT 节点创建用户时应描述的用户基本属性包括：

a) 用户 ID；
b) 用户名；
c) 用户别名；
d) 创建时间；
e) 用户所属机构；
f) 用户有效期；
g) 用户状态。

6.1.2.4 候选 DLT 节点标识用户的方法为用户 ID。

6.1.2.5 候选 DLT 节点删除用户功能由用户管理角色操作，用户被删除后：

a) 不能再登录系统；

b） 不再拥有系统任何权限；

c） 在系统中查询该用户状态为“删除”状态。

6.1.2.6 候选 DLT 节点可由用户管理角色实施批量删除用户功能。

6.1.2.7 候选 DLT 节点修改用户功能由用户管理角色操作：

a） 可进行修改的用户属性包括：

1） 用户名称；

2） 用户别名；

3） 所属机构；

4） 用户组别；

5） 联系方式；

6） 用户状态。

b） 不应修改的用户属性包括：

1） 用户 ID；

2） 用户创建时间。

6.1.2.8 候选 DLT 节点查询用户的功能由用户管理角色进行操作，查询条件包括：

a） 用户 ID；

b） 用户名；

c） 用户别名；

d） 用户所属机构。

6.1.2.9 候选 DLT 节点不提供用户分组管理功能。

6.1.2.10 候选 DLT 节点用户对应角色匹配功能：

a） 由角色管理角色操作；

b） 用户与角色之间的对应关系是一对多；

c） 用户不能同时分配具有互斥关系的多个角色；

d） 用户角色配置可具有永久有效期。

6.1.2.11 候选 DLT 节点有设置用户转授权功能，即允许用户将其所具有的部分或者全部权限转授给另一主体。

6.2 分布式账本

候选DLT节点应符合如下要求。

a） 候选 DLT 节点所用共识机制应符合 ISO 23257:2022 中 5.5 对共识的要求，与银行函证系统的 DLT 系统通过共识机制保持一致。

b） 候选 DLT 节点与银行函证系统的 DLT 系统所有参与共识的 DLT 节点得到的计算结果相同。

c） 当候选 DLT 节点在不超过共识最大容错数据量时发生故障，不影响银行函证系统的 DLT 系统正常工作。

d） 由于候选 DLT 节点离线导致数据差异量较大，导致 DLT 节点的分户账记录无法自动恢复时，应按 GB/T 40473.2—2021 中 5.1.5 的要求设立不同的运行状态，并按 GB/T 40473.2—2021 中 5.1.7 建立有人工干预的机制。

注：候选DLT节点如遇到网络故障等情况与银行函证系统的区块链断开连接，可能会出现与银行函证系统的DLT系统中其他DLT节点分户账记录不一致的情况。一般情况下，在恢复连接后，通过与银行函证系统的DLT系统中其他DLT节点交互等干预方法，候选DLT节点分户账记录将恢复保持与正常DLT节点间分户账记录的一致。

e） 支持候选 DLT 节点提供查询区块数、区块内容等的接口说明，包括：

1） 功能；

2） 格式；
3） 方法；
4） 参数；
5） 返回值；
6） 使用方式；
7） 其他需要说明的内容。

6.3 智能合约

候选DLT节点应符合如下要求。

a） 候选 DLT 节点智能合约如下方面符合 ISO 23257:2022 中 5.12 中智能合约规定的具体要求：
1） 版本控制；
2） 访问控制；
3） 复杂度限制；
4） 一致性；
5） 安全审计；
6） 攻击防范；
7） 安全验证。

b） 候选 DLT 节点针对智能合约约定的条件和事项，按照规则强制执行。

c） 候选 DLT 节点的智能合约模块具备合约执行引擎，支持三种以上的主流编程语言；WASM 智能合约引擎所支持的语言示例如图 1 所示。

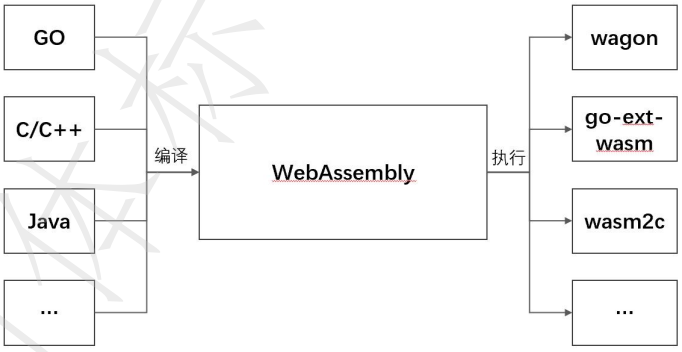

图 1 WASM 智能合约引擎支持示意图

d） 候选 DLT 节点的智能合约对所有区块链节点公开。

e） 通过升级智能合约实现漏洞修复、满足业务变更，升级智能合约应保证原智能合约中的数据不被破坏，且在需要且可行时能够被新合约使用。

6.4 部署要求

候选DLT节点加入银行函证系统DLT系统部署要求如下。

a） 部署候选 DLT 节点以与银行函证系统的 DLT 系统组网并提供服务的方式包括：
1） 应以公有云方式部署候选 DLT 节点；
2） 宜支持私有云方式部署候选 DLT 节点；
3） 宜支持自建数据中心部署候选 DLT 节点；
4） 可支持混合云方式部署候选 DLT 节点。

b） 应由候选 DLT 节点按照银行函证系统 DLT 系统要求开通如下端口：

1） 候选 DLT 节点与银行函证系统组网端口；
2） 候选 DLT 的文件传输端口；
3） HTTPS 协议端口。

c） 候选 DLT 节点版本应通过参数配置与生产环境一致的投产上线测试，提供符合 JR/T 0101-2013 要求的测试报告，其中应说明是否有针对如下内容的测试用例和测试规程：
1） 候选 DLT 节点加入银行函证系统 DLT 系统后，银行函证系统功能与接入前一致；
2） 候选节点设置了 6.1.1 所要求的角色，并按 6.1.2 设置了最小数量的用户；
3） 候选节点能够部署符合 6.3 的智能合约；
4） 候选节点符合 6.2 中 a)项对共识的要求；
5） 候选 DLT 节点能够通过智能合约完成交易，并返回正确的交易信息；
6） 候选 DLT 节点具有银行函证系统的分布式账本的分户账记录数量与内容一致的能力。

6.5 运行监控

6.5.1 联机监控分析

6.5.1.1 候选 DLT 节点实现 6.5.1.2～6.5.1.6 的要求，并可在需要时按照 GB/T 40473.2—2021 中 5.1.3 进行更加广泛和深入的分析。

6.5.1.2 候选 DLT 节点在运行时，对如下内容进行监控，包括：

a） 内存；
b） 通信带宽；
c） 无交易持续时间；
d） 连续失败笔数；
e） 单笔交易时长；
f） 累计失败笔数；
g） 交易成功率；
h） 交易量变化率；
i） 应用使用的网络端口可用性状态；
j） 服务端口可用性状态；
k） 智能合约可用性状态；
l） 分户账记录数量。

6.5.1.3 候选 DLT 节点在运行时，其联机监控要求如下。

a） 所有监测均可由工具软件实现，其误差由该工具软件的限制所决定，本文件的使用者应评估该误差是否足以满足监测需求。
b） 监测结果可使用工具软件展示，在建设有集中监控平台时，宜集成到集中监控平台中。
c） 在监测到异常值后，应由候选 DLT 节点的系统管理相关人员和业务人员联合采用手动措施（包括使用操作系统提供的工具和第三方工具）进行控制，包括在需要时对中断的交易进行处理以保证交易的完整性。

示例：Prometheus(普罗米修斯）即为一种可能实现上述监控功能的软件。Prometheus 是由 SoundCloud 公司开发的开源软件。给出这一信息是为了方便本文件使用者，并不表示对这一产品的认可。

6.5.1.4 候选 DLT 节点运行时，6.5.1.2 列出的各指标按可能造成的危害程度、紧急程度和发展态势，分为如下告警级别。

a） 提示告警（I 级）：
1） 内存，剩余 30%时需提供提示告警；

2) 通信带宽，占用带宽 70%时需提示告警；
3) 无交易持续时间，在 8:00 到 20:00 时间段区间内，持续无交易时间为 30 分钟提示告警；
4) 连续失败笔数，3 笔提示告警；
5) 累计失败笔数，10 笔提示告警；
6) 单笔交易时长，30 秒提示告警；
7) 交易成功率，99%时提示告警；
8) 交易量变化率，30%时提示告警。

b) 警告告警（II 级）：
1) 内存，剩余 20%需提示警告告警；
2) 通信带宽，占用 80%需警告告警；
3) 无交易持续时间，在 8:00 到 20:00 时间段区间内，持续无交易时间为 60 分钟警告告警；
4) 连续失败笔数，5 笔警告告警；
5) 累计失败笔数，20 笔警告告警；
6) 单笔交易时长，40 秒警告告警；
7) 交易成功率，97%时警告告警；
8) 交易量变化率，20%时警告告警。

c) 次要告警（III 级）：
1) 内存，剩余 15%需提示次要告警；
2) 通信带宽，占用 85%需次要告警；
3) 无交易持续时间，在 8:00 到 20:00 时间段区间内，持续无交易时间为 90 分钟次要告警；
4) 连续失败笔数，10 笔次要告警；
5) 累计失败笔数，30 笔次要告警；
6) 单笔交易时长，60 秒次要告警；
7) 交易成功率，94%时次要告警；
8) 交易量变化率，10%时次要告警。

d) 主要告警（IV 级）：
1) 内存，剩余 10%需提示主要告警；
2) 通信带宽，占用 90%需主要告警；
3) 无交易持续时间，在 8:00 到 20:00 时间段区间内，持续无交易时间为 120 分钟主要告警；
4) 连续失败笔数，15 笔主要告警；
5) 累计失败笔数，40 笔主要告警；
6) 单笔交易时长，75 秒主要告警；
7) 交易成功率，92%时主要告警。
8) 交易量变化率，5%时次要告警。

e) 严重告警（V 级）：
1) 内存，剩余 5%需提示严重告警；
2) 通信带宽，占用 95%需提示严重告警；
3) 无交易持续时间，在 8:00 到 20:00 时间段区间内，持续无交易时间为 150 分钟严重告警；
4) 连续失败笔数，20 笔严重告警；
5) 累计失败笔数，45 笔严重告警；
6) 单笔交易时长，90 秒严重告警；
7) 交易成功率，90%时严重告警；
8) 应用使用的网络端口可用性状态，端口不可用时提示严重告警；

9） 服务端口可用性状态，端口不可用时提示严重告警；

10）智能合约可用性状态，智能合约不可用时提示严重告警；

11）分户账记录数量，与银行函证系统分户账记录数量不一致时提示严重告警。

注：当某一告警级别严重/缓解后，改为对应的更为严重/较为缓解的告警。

6.5.1.5 对监测阈值按如下三种方式确定。

a） 直接对状态进行判定，包括：

1） 应用使用的网络端口可用性状态；

2） 服务端口可用性状态；

3） 智能合约可用性状态；

4） 分户账记录数量。

b） 按不同业务时段，采用动态基线确定阈值指标，包括：

1） 内存；

2） 通信带宽；

3） 无交易持续时间；

4） 连续失败笔数；

5） 单笔交易时长。

c） 按不同业务日期，采用动态基线确定阈值指标，包括：

1） 累计失败笔数；

2） 交易成功率；

3） 交易量变化率。

6.5.1.6 对 6.5.1.2 指标内容达到阈值时，采用的报警方式如下：

a） 短信；

b） 微信；

c） 自动拨打电话；

d） 专用 APP 信息推送；

e） 在建设有统一监控平台时，发送报文到监控平台。

6.5.2 批量监控分析

6.5.2.1 候选 DLT 节点实现 6.5.2.2～6.5.2.6 的要求，并可在需要时按照 GB/T 40473.2—2021 中 5.1.4 进行更加广泛和深入的分析。

6.5.2.2 候选 DLT 系统提供以下的批量监控内容：

a） 运行中作业；

b） 完成的作业；

c） 任务；

d） 节点；

e） 系统整体的标识；

f） 名称；

g） 状态；

h） 系统整体的运行开始时间；

i） 系统结束时间；

j） 运行开始时间；

k） 运行完成时间；

l） 记录总笔数；

m） 已经处理记录笔数；
n） 处理成功笔数；
o） 处理失败笔数；
p） 处理位置指针；
q） 处理记录总笔数；
r） 先导任务；
s） 后继任务。

注：必要时，通过计算提供运行时长、秒均处理笔数、成功笔数占比和失败笔数占比。

6.5.2.3 候选 DLT 节点在运行时，其批量监控要求如下。

a） 所有监测均可由工具软件实现，其误差由该工具软件的限制所决定，本文件的使用者应评估该误差是否足以满足监测需求。
b） 监测结果可使用工具软件展示，在建设有集中监控平台时，宜集成到集中监控平台中。
c） 在监测到异常值后，应由候选 DLT 节点的系统管理相关人员和业务人员联合采用手动措施（包括使用操作系统提供的工具和第三方工具）进行控制，包括在需要时对中断的交易进行处理以保证交易的完整性。

示例：Prometheus(普罗米修斯）即为一种可能实现上述监控功能的软件。Prometheus 是由 SoundCloud 公司开发的开源软件。给出这一信息是为了方便本文件使用者，并不表示对这一产品的认可。

6.6 节点日志

6.6.1.1 候选 DLT 节点实现 6.6.1.2～6.6.1.5 的要求，并可在需要时按照 GB/T 40473.2—2021 中 5.1.10 进行更加广泛和深入的分析。

6.6.1.2 运行日志记录各系统节点的运行情况，分为调试（debug）、信息（info）、警告（warning）、出错（error）四个级别，优先级依次递增，可由日志级别来控制日志的输出。

6.6.1.3 节点日志存储方案，可采用文本文件、数据库或其他存储方式；无论哪种模式，均应满足 7.6.5 规定的可核查性要求。

6.6.1.4 节点日志的保存策略，应满足银行函证系统对日志管理的要求的时限；在超出时限后，宜进行日志归档，归档后的联线日志可按银行函证系统要求的存储天数进行周期滚动式存储。

6.6.1.5 节点日志在人工删除前验证应对日志归档状况进行确认。

6.7 运行状况分析

6.7.1.1 候选 DLT 节点实现 6.7.1.2～6.7.1.3 的要求，并可在需要时按照 GB/T 40473.2—2021 中 5.1.6 进行更加广泛和深入的分析。

6.7.1.2 候选 DLT 节点可由自身或通过集中监控系统对运行状况提供数据和图形方式的展示。

6.7.1.3 候选 DLT 节点应按照每周、每月或需要的时间间隔，对如下指标的同比、环比、增减量信息进行展示，展示的指标包括：

a） 分户账记录数量；
b） 交易量数据；
c） 单笔交易时长；
d） 使用的网络共识算法；
e） 列于 6.5.1.2 和 6.5.2.2 的相关指标。

6.8 异常处理

6.8.1.1　候选 DLT 节点实现 6.7.1.2～6.7.1.3 的要求，并可在需要时按照 GB/T 40473.2—2021 中 7.1 进行更加广泛和深入的分析。

6.8.1.2　候选 DLT 节点能够及时有效给出系统技术错误信息，并给出用户后继处理活动建议。

6.8.1.3　候选 DLT 节点能够对表 1 给出的异常按照规定的返回码反馈。

表 1　DLT 系统业务异常返回码及异常描述

返回码	异常描述
100000	区块链用户未登录
100001	区块链用户不合法
100002	该用户无操作智能合约权限
100003	智能合约部署失败
100004	智能合约调用失败
100005	智能合约查询失败
100006	智能合约终止失败
100007	传入参数的格式不正确
100008	智能合约更新失败
100009	智能合约不存在
100010	智能合约状态不正常
100011	调用方法不存在
100012	返回结果已存在
100013	入参校验失败，存在不合法参数
100014	区块链内容通讯错误
100015	节点资源释放失败
100016	账本查询失败
100017	无法找到配置文件
100018	数据库未启动，不允许查询数据
100019	获取数据库连接失败
100020	初始化数据库连接管理对象失败
100021	请求超过限流次数，稍后再试

7　基本非功能要求

7.1　概述

按照GB/T 40473.1—2021，非功能需求涉及到性能效率、兼容性、易用性、可靠性、安全性、维护性和可移植性七类，由于候选DLT节点的特点，某些涉及到非功能性要求或其某个方面可能已经在第6章提及。

7.2　性能效率

7.2.1　时间特性

7.2.1.1　候选 DLT 节点实现 7.2.1.2～7.2.1.5 的要求，并可在需要时按照 GB/T 40473.3—2021 中第 5 章进行更加广泛和深入的分析。

7.2.1.2 候选 DLT 节点应支持每秒 1000 笔以上的 TPS。

7.2.1.3 候选 DLT 节点与银行函证系统内其他各 DLT 节点之间进行共识计算时，候选 DLT 节点应在 100ms 内给出结果。

7.2.1.4 候选 DLT 节点与银行函证系统内其他各 DLT 节点之间的时间戳误差，应在共识协议允许的范围内。

7.2.1.5 候选 DLT 节点可使用经过认证的中心化时间源与银行函证系统内其他各 DLT 节点，进行节点间的时间同步。

7.2.2 资源利用

7.2.2.1 资源控制

7.2.2.1.1 候选 DLT 节点的直接用户在退出客户端时，当前会话结束，且对服务器端和客户端相关资源占用内存进行释放。

7.2.2.1.2 对采用长连接的候选 DLT 节点，当与候选 DLT 节点通信的另一方在 30 秒内没有信息交换时，候选 DLT 节点结束会话。

7.2.2.1.3 对于候选 DLT 节点采用会话方式时，允许单个用户多重并发会话。

7.2.2.1.4 候选 DLT 节点对以下所需系统资源监控使用状况，并动态确定可用上限。

a) CPU。
b) 内存。
c) 硬盘。
d) 带宽。

7.2.2.1.5 候选 DLT 节点的文件系统清理策略为以下策略，清理方式为定期脚本或程序清理。

a) 定期清理。
b) 根据文件使用空间清理。
c) 根据文件保留期限清理。
d) 根据文件产生时间清理。

7.2.2.1.6 候选 DLT 节点的数据库系统清理策略为以下策略，清理方式为定期脚本或程序清理。

a) 定期清理。
b) 根据数据库表记录数清理。
c) 根据数据库表所占空间进行清理。
d) 根据数据记录日期期限进行清理。

7.2.2.1.7 在候选 DLT 节点实际交易量超过业务设计容量时，应用系统可选择如下策略之一：

a) 流量控制，阈值设定方式为人工可调整；
b) 拒绝；
c) 排队。

7.2.2.2 负荷分配

候选DLT节点对所承担负荷的分配可为如下方式：

a) 单机；
b) 服务器集群；
c) PaaS；
d) 负载均衡；
e) 应用级负荷分布。

7.2.2.3 数据库使用

候选DLT节点关系数据库事务的隔离级别是序列化。

注：关于数据库事务的隔离级别的进一步信息参见GB/T 40473.3—2021的附录B。

7.2.3 容量

7.2.3.1 候选 DLT 节点实现 7.2.3.2～7.2.3.5 的要求，并可在需要时按照 GB/T 40473.3—2021 中第 6 章进行更加广泛和深入的分析。

7.2.3.2 用户数量

候选DLT节点能够支持如下用户数量：

a) 注册直接用户数为 4000；
b) 在线直接用户数为 1000；
c) 同期交易直接用户数为 200。

7.2.3.3 交易量

7.2.3.3.1 候选 DLT 节点支持的并发交易量为：

a) 峰值每秒 2000 笔；
b) 平均每秒 1000 笔。

7.2.3.3.2 候选 DLT 节点按峰值并发量且持续时间为 10 分钟，交易成功率为 100%。

7.2.3.3.3 在使用数据库的情况下，候选 DLT 节点一个事务内支持宜达到：

a) 50 个交易；
b) 3 张数据库表；
c) 150 条数据库记录；
d) 单表 3 个索引。

7.2.3.4 网络资源

7.2.3.4.1 从网络管理的视角看，候选 DLT 节点处理的业务属于第三方接入。

7.2.3.4.2 从网络管理的视角看，候选 DLT 节点所需的链路类型为多点连接链路、上下行的链路速度至少为 50M、端口类型为 100 兆、接口类型为光口、工作模式为全双工。

7.3 兼容性

7.3.1 总体要求

候选DLT节点实现7.3.1～7.3.3的要求，并可在需要时按照GB/T 40473.4—2021中第5章进行更加广泛和深入的分析。

7.3.2 操作系统兼容性

候选DLT节点能够运行的64bit服务器操作系统包括：

a) 应兼容 Linux，Centos 7.3 及以上版本，Ubuntu 16.04 LTS 及以上版本；
b) 应兼容 Windows，Windows Server 2016 及以上版本；
c) 可兼容 MacOS，MacOS Sierra 10.12.6 及以上版本。

注：Windows 是微软公司研发的服务器操作系统；Linux，全称GNU/Linux，是一种免费使用和自由传播的类UNIX操作系统；MacOS是一套由苹果开发的运行于Macintosh系列电脑上的操作系统。Windows、Linux、MacOS即为当

前主流的服务器操作系统。给出这一信息是为了方便本文件使用者，并不表示对这一产品的认可。

7.3.3 数据库兼容性

候选DLT节点应在64位关系数据库、非关系数据库的支撑下运行。

a) 关系数据库典型包括：
   1) Mysql，支持版本为 5.7 及以上版本；
   2) Oracle，支持 12C 及以上版本。

注 1：Mysql 是由瑞典 MySQL AB 公司开发关系型数据库管理系统;Oracle 是甲骨文公司的一款关系数据库管理系统。Mysql、Oracle 均为当前主流的关系型数据库。给出这一信息是为了方便本文件使用者，并不表示对这一产品的认可。

b) 非关系数据库典型包括：
   1) Leveldb，支持 1.2 版本及以上版本；
   2) Couchdb，支持 4.1 及以上版本。

注 2：Leveldb 是用 C/C++编程语言编写的，是一个 GOOGLE 公司实现的 kv 数据库；Couchdb 用 Erlang 编程语言编写的，是一个开源的面向文档的数据库管理系统。Leveldb、Couchdb 均为区块链常用的非关系型数据库。给出这一信息是为了方便本文件使用者，并不表示对这一产品的认可。

7.3.4 浏览器兼容性

当用户使用PC通过Web访问候选DLT节点时，宜支持如下浏览器以及相关版本之一：

a) Edge 浏览器，102.0 及以上版本；
b) 火狐浏览器，Firefox52 及以上版本；
c) IE 浏览器，IE9 及以上版本；
d) 谷歌浏览器，Chrome44 及以上版本。

注：Edge浏览器一般指Microsoft Edge。 Microsoft Edge是由微软开发的基于 Chromium 开源项目及其他开源软件的网页浏览器；火狐浏览器一般指Mozilla Firefox。 Mozilla Firefox，中文俗称“火狐”（正式缩写为Fx或fx），是一个由Mozilla开发的自由及开放源代码的网页浏览器；IE浏览器一般指Internet Explorer。Internet Explorer（简称：IE）是微软公司推出的一款网页浏览器；谷歌浏览器一般指Google Chrome。 Google Chrome是一款由Google公司开发的网页浏览器。Edge浏览器、火狐浏览器、IE浏览器、谷歌浏览器均为当前主流的浏览器。给出这一信息是为了方便本文件使用者，并不表示对这一产品的认可。

7.3.5 节点功能兼容

候选DLT节点应兼容旧版本的候选DLT节点的既有功能，或提供能涵盖既有功能的新功能。

7.4 易用性

7.4.1 总体要求

候选DLT节点实现7.4.2～7.4.4的要求，并可在需要时按照GB/T 40473.5—2021进行更加广泛和深入的分析。

7.4.2 易学性要求

7.4.2.1 在线帮助

7.4.2.1.1 候选 DLT 节点宜通过当前页面展示、弹出窗口提示来提供在线帮助；

7.4.2.1.2 在用户进入候选 DLT 节点后，在操作前和操作过程中，候选 DLT 节点宜提供如下的在线帮助：

a) 在线教程；
b) 视频演示；
c) 联机帮助；
d) 用户反馈。

7.4.2.1.3 当候选 DLT 节点提供在线帮助时，宜能访问提供帮助信息的内容服务器。

7.4.2.2 对话易学性

7.4.2.2.1 候选 DLT 节点宜能以与日常办公类软件相似的方式提供对话。

7.4.2.2.2 针对不常见的使用情况，候选 DLT 节点应提供用户可寻求支持的线索。

7.4.2.2.3 候选 DLT 节点的反馈信息或进度解释应能有助于用户对整个交互系统形成概念性的认识。

7.4.2.2.4 候选 DLT 节点与用户的交互产生的中间结果和最终结果的信息，宜能提供用户从使用候选 DLT 节点过程中进一步掌握候选 DLT 节点的足够信息。

7.4.3 易操作性要求

7.4.3.1 使用手册

7.4.3.1.1 候选 DLT 节点应提供数字方式的使用手册；并在用户需要时，提供纸质使用手册。在同时提供数字方式使用手册和纸质使用手册时，应通过有效的版本管理，说明手册内容的对应关系。

7.4.3.1.2 对于用户手册，宜能提供按照不同用户视角按该用户工作场景组织的手册，在每个场景中描述涉及到的相关角色、需要执行的操作和需要处理的数据。

7.4.3.1.3 为运维人员提供的手册应包括如下内容：

a) 软件发布管理；
b) 应用验证；
c) 应用启停；
d) 开关联机；
e) 补丁管理；
f) 在线升级；
g) 批量处理；
h) 数据备份与恢复；
i) 数据清理；
j) 应急方案。

7.4.3.2 与用户期望一致

7.4.3.2.1 候选 DLT 节点宜基于用户的已有知识，使用用户熟悉的词汇。

7.4.3.2.2 候选 DLT 节点应在执行到每一个能够产生输出的步骤时，给出含义明确的输出。

7.4.3.2.3 对执行时间超过 3 秒的任务，候选 DLT 节点宜提示如下内容：

a) 已经消耗的时间；
b) 预计的剩余时间；
c) 已经完成的百分比。

7.4.3.2.4 候选 DLT 节点宜能使得候选 DLT 的直接用户明确知道下一步应采取的操作和对应的业务动作。

7.4.3.2.5　候选 DLT 节点的快捷键和对输入信息的确认键宜可以通过配置定义。

7.4.3.3　对话可控

7.4.3.3.1　在候选 DLT 节点与用户对话过程中，在变更信息提交前，用户应能中断对话。
7.4.3.3.2　候选 DLT 节点应提供对中断正常操作进行确认。
7.4.3.3.3　在候选 DLT 节点与用户对话过程中，如果对话中断，用户宜能从对话中断之处重新开始，已经输入的信息不需要重新输入。
7.4.3.3.4　候选 DLT 节点宜在能回退时提供回退功能。

7.4.3.4　参数配置

7.4.3.4.1　候选 DLT 节点配置参数应加密存储于操作系统文件。
7.4.3.4.2　候选 DLT 节点在变更配置参数后，需重新启动操作系统后生效。

7.4.4　用户差错防御

7.4.4.1　输入数据检查与控制

7.4.4.1.1　候选 DLT 节点能够通过以下验证方式对用户输入数据进行合法性检查与安全性控制：

a)　显式验证；
b)　隐式验证。

7.4.4.1.2　候选 DLT 节点能够对输入的数额巨大的数字、不符的数据类型提供确认机制。

7.4.4.2　容错响应

当用户在操作过程中发生涉及到增删改数据的交易超时后，候选DLT节点内部提供自动发起冲正的机制。

7.5　可靠性

7.5.1　总体要求

候选DLT节点实现7.5.2～7.5.5的要求，并可在需要时按照GB/T 40473.6—2021进行更加广泛和深入的分析。

7.5.2　成熟性

7.5.2.1　候选 DLT 节点分月度、季度进行投产。
7.5.2.2　候选 DLT 节点的月度期投产时：

a)　涉及到的直接用户仅可包括内部所有业务的用户；
b)　一旦发生应用系统的故障，宜能提供可能采用变通的方式办理业务，变通后不涉及应用系统的批处理结果的变更。

7.5.2.3　候选 DLT 节点的季度期投产时：

a)　涉及到的直接用户可包括外部和内部所有业务的用户；
b)　一旦发生应用系统的故障，应能提供可能采用变通的方式办理业务，变通后不涉及应用系统的批处理结果的变更。

7.5.3　可用性

7.5.3.1　功能可用性

7.5.3.1.1　候选 DLT 节点应整体工作下 7×24 模式下。

7.5.3.1.2　候选 DLT 节点在交易量不超过 7.2.3.3 规定的情况下，候选 DLT 节点与银行函证系统组网进入稳定运行状态的时间不超过 1 分钟。

7.5.3.2　数据可用性

候选DLT节点数据宜能处理5.3.2所规定的数据种类，至少应包括如下数据种类：

a)　流水类数据；

b)　时点类数据；

c)　日志类数据；

d)　业务配置类数据。

7.5.3.3　运行平台可用性

7.5.3.3.1　部署在公有云的候选 DLT 节点，其运行支撑环境应至少有冷备且状态同步周期不长于 1 周，宜有主从式热备。

7.5.3.3.2　部署在公有云的候选 DLT 节点运行所依赖的基础软件，采用如下方法：

a)　操作系统应采用云部署；

b)　数据库宜采用主从同步方案。

7.5.3.4　网络可用性

7.5.3.4.1　候选 DLT 节点宜支持链路负载均衡服务，如下内容及其变更应在投产前 7 天提供：

a)　源地址组；

b)　目标地址组；

c)　链路阈值。

7.5.3.4.2　候选 DLT 节点能支持服务器负载均衡服务，如下内容及其变更应在投产前 7 天提供：

a)　服务器地址列表；

b)　映射 VIP 地址。

7.5.3.4.3　候选 DLT 节点网络设备宜为热备冗余。

7.5.3.4.4　候选 DLT 节点通讯链路可为专线冗余或 VPN 冗余。

7.5.4　容错性

7.5.4.1　功能容错

7.5.4.1.1　当候选 DLT 节点网络出现障碍时，6.1 所述的角色与用户管理功能和 6.7 所述的运行状况分析应能继续工作；在与银行函证系统的联网恢复后，应能自动恢复正常的候选 DLT 节点的所有功能。

7.5.4.1.2　对通过区块链传递过来的分户账记录，应进行数据有效性检验。

7.5.4.2　角色容错

7.5.4.2.1　候选 DLT 节点中超级角色与角色管理角色应一直能正常使用，其他角色在网络故障等情况下准许不能正常工作。

7.5.4.2.2　候选 DLT 节点准许不能正常工作的角色，在网络等故障回复后，宜能自动恢复；可人工干涉后恢复使用。

7.5.4.3　外部系统容错

7.5.4.3.1　银行函证系统故障可能影响候选 DLT 节点功能时，候选 DLT 节点应能自动检测出外部系统故障并主动隔离规避影响。

7.5.4.3.2　在银行函证系统故障恢复后，候选 DLT 节点的功能宜自动恢复；如银行函证系统的分户账记录数量与候选 DLT 分户账记录数量不一致时，宜能自动恢复，可在人工干预后恢复。

7.5.5　易恢复性

7.5.5.1　业务影响范围

7.5.5.1.1　候选 DLT 节点异常中断导致候选 DLT 节点的业务影响时间范围宜在 30 分钟内，不应超过 120 分钟。

7.5.5.1.2　候选 DLT 节点异常中断，准许影响候选 DLT 节点所在参与方的银行函证业务功能。

7.5.5.2　数据备份

7.5.5.2.1　候选 DLT 节点的数据备份策略应为：

a)　每 7 天执行一次全量备份；

b)　每天执行一次增量备份。

7.5.5.2.2　候选 DLT 节点的数据备份文件的存储方式为：

a)　宜采用加密文件；

b)　可采用备份为文本文件后加密存储的方式。

7.5.5.3　数据丢失处理

在灾难恢复阶段，候选DLT节点所需的数据调整手段如下：

a)　宜通过区块同步机制自动将丢失的数据重新记录到候选 DLT 节点的分户账记录中；

b)　可人工将银行函证系统的的分户账记录同步到候选 DLT 节点的分户账记录中。

7.5.5.4　恢复时间目标

7.5.5.4.1　候选 DLT 节点灾备恢复前提条件为：

a)　银行函证系统正常运行；

b)　候选 DLT 节点网络与银行函证系统网络联通。

7.5.5.4.2　候选 DLT 节点 RTO 为 1 小时。

7.5.5.5　恢复点目标

候选DLT节点RPO为0。

7.5.5.6　恢复数据源

在灾难发生后，可能用于候选DLT节点的数据调整的数据源为：

a)相关配置文件为备份文件；

b)分户账记录为当前其他工作正常的 DLT 节点的数据。

7.6　安全性

7.6.1　总体要求

候选DLT节点实现7.6.2～7.6.5的要求，并可在需要时按照GB/T 40473.7—2021进行更加广泛和深入的分析。

7.6.2 保密性

7.6.2.1 使用算法要求

7.6.2.1.1 候选 DLT 节点支持的对称密钥算法应包括 GB/T 32907—2016 规定的 SM4 算法，宜包括 ISO/IEC 18033-3:2010 规定的 AES 算法；

7.6.2.1.2 候选 DLT 节点支持的非对称密钥算法应包括 GB/T 32918 规定的 SM2 算法，宜包括 ISO/IEC 18033-2:2006 规定的 RSA 算法；

7.6.2.1.3 候选 DLT 节点支持的摘要算法应包括 GB/T 32905—2016 规定的 SM3 算法，可包括 ISO/IEC 10118-3 规定的 SHA 系列算法。

7.6.2.1.4 候选 DLT 节点拟使用其他对称密钥算法、非对称密钥算法和/或摘要算法时，应与银行函证系统的 DLT 系统协商一致，并按照银行函证系统的 DLT 系统的要求进行部署。

7.6.2.2 访问控制

7.6.2.2.1 应根据 6.1 规定管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。

7.6.2.2.2 应控制对操作系统的超级用户和 6.1 规定的超级角色分配具体用户，必要时通过管理措施，要求超级角色用户的操作双人在场。

7.6.2.2.3 应及时删除多余的、过期的帐户，避免共享帐户的存在。

7.6.2.2.4 应能够检测虚拟机对宿主机资源的异常访问，并进行告警。

7.6.2.3 数据保密

候选DLT节点应采用点对点的数据加解密网络，应实现采集、传输、使用、存储过程中的如下数据的加密：

a) 候选 DLT 节点管理数据；
b) 候选 DLT 节点鉴别信息；
c) 重要业务数据。

7.6.2.4 处理保密

7.6.2.4.1 候选 DLT 节点应能对存储、传输、处理的信息区分如下特征：

a) 可披露信息：不经授权即可被披露，其披露不会带来负面影响的数据；
b) 保密信息：未授权不能获知内容的数据。

7.6.2.4.2 候选 DLT 节点可采取如下的处理加密措施：

a) 介质级加密；
b) 嵌入式加密；
c) 文件级加密；
d) 数据库加密。

7.6.2.5 存储保密

7.6.2.5.1 候选 DLT 节点的宜具有安全机制：

a) 数据库访问具有身份认证；
b) 通信加密与完整性保护；
c) 数据库加密设置；
d) 多级密钥管理；

e） 安全备份的安全机制。

7.6.2.5.2 候选 DLT 节点的数据库宜具有如下加密机制：

a） 数据库用户数据；

b） 数据库应用数据；

c） 配置文件中的数据库连接参数。

7.6.2.5.3 候选 DLT 节点的操作系统中的文件宜具有加密存储机制。

7.6.2.5.4 候选 DLT 节点存放在内存和硬盘中的用户鉴别信息，在存储空间被释放或再分配给其他应用使用前，应能得到完全清除。

7.6.2.5.5 候选 DLT 节点的系统文件、系统目录、数据库记录等资源所在的存储空间，被释放或再分配给其他应用使用前，应能得到完全清除。

7.6.2.6 通信保密

7.6.2.6.1 候选 DLT 节点在与银行函证系统之间的通信，以及候选 DL 节点与其他 DLT 节点之间的通讯宜采用如下通信协议：

a） 安全套接层协议 SSL；

b） 安全传输层协议 TLS；

c） 安全超文本传输协议 HTTPS。

7.6.2.6.2 从消息的来源来考虑，候选 DLT 节点采用的 7.6.2.6.1 通信协议，应具有防止协议轮内攻击的报文重放攻击的机制。

7.6.2.6.3 从消息的去向来考虑，候选 DLT 节点采用的 7.6.2.6.1 通信协议，应具有防止直接攻击的报文重放攻击的机制。

7.6.2.6.4 候选 DLT 节点采用的 7.6.2.6.1 通信协议，需要防止以下的攻击：

a） 防 SQL 注入攻击；

b） 防跨站脚本攻击；

c） 防敏感信息泄露的攻击。

7.6.2.7 运行环境保密

7.6.2.7.1 候选 DLT 节点的运行环境应具有病毒防范、跟踪 cookies 防范、恶意的移动代码防范的措施。

7.6.2.7.2 候选 DLT 节点的运行环境应具有以下安全监测内容。并在发生严重入侵事件时，应能提供报警功能。

a） 端口扫描；

b） 强力攻击；

c） 木马后门攻击；

d） 拒绝服务攻击；

e） 缓冲区溢出攻击注人式攻击；

f） IP 碎片攻击；

g） 网络蠕虫攻击的措施。

7.6.2.7.3 在环境监测到 7.6.2.7.2 中每种攻击时，能够记录以下信息：

a） 攻击源 IP；

b） 攻击类类型；

c） 攻击目的；

d） 攻击时间。

7.6.2.7.4 候选 DLT 节点的运行环境能定期对恶意代码防护设备进行代码库升级和系统更新。
7.6.2.7.5 候选 DLT 节点的主机系统对与之相连的服务器，终端设备进行身份标识和鉴别。
7.6.2.7.6 候选 DLT 节点的客户端宜建立以下内容：

a) 防键盘窃听；
b) 防恶意程序盗取敏感信息；
c) 防屏幕录像技术机制。

7.6.2.8 运行网络保密

7.6.2.8.1 候选 DLT 节点的运行网络能对非授权设备私自联到内部网络的行为进行检查，能准确定出位置，能对其进行有效阻断。
7.6.2.8.2 候选 DLT 节点的运行网络能对内部网络用户私自联到外部网络的行为进行检查，能准确定出位置，能对其进行有效阻断。
7.6.2.8.3 候选 DLT 节点的运行网络能控制数据带宽通用协议。
7.6.2.8.4 候选 DLT 节点的运行网络能控制带有敏感标记的数据。
7.6.2.8.5 候选 DLT 节点应在以下网路中实现网络隔离，需要进行远程访问时需由被访问单位开启远程访问服务。不定期进行安全问题评估并提供评估报告：

a) 测试网；
b) 准生产网；
c) 生产网。

7.6.2.8.6 候选 DLT 节点的运行网络有对网络设备系统自带的服务端口的控制机制，该控制机制应采用白名单进行管理。

7.6.3 完整性

7.6.3.1 网络协议完整性

7.6.3.1.1 候选 DLT 节点与如下方通信的协议，具有防止信息被未经授权变更的机制：

a) 其他 LDT 节点；
b) 银行函证系统。

注：变更包括增加、修改、删除。

7.6.3.1.2 候选 DLT 节点具有防止未经授权变更能力的协议包括在通信过程对全部数据加密、通信双方建立连接前利用密码技术进行会话初始化验证。

注：使用的常见的通信协议包括SSH、HTTPS等网络协议，以及路由协议、工业控制协议等专用通信协议。

7.6.3.2 本地数据完整性

7.6.3.2.1 候选 DLT 节点检测到数据在采集、传输、使用和存储过程中出现完整性错误时，应进行恢复：

a) 候选 DLT 节点管理数据；
b) 候选 DLT 节点鉴别信息；
c) 重要业务数据。

7.6.3.2.2 候选 DLT 节点应防止存储在本地的信息被未经授权变更。
7.6.3.2.3 候选 DLT 节点应防止以未被授权重新擦写方式来清除数据的存储空间。

7.6.4 抗抵赖性

7.6.4.1 原发和接收证据

7.6.4.1.1 候选 DLT 节点作为数据的发送者或接受者，应能提供不可否认的证据。

7.6.4.1.2 候选 DLT 节点具有在请求的情况下为数据原发者或接收者提供数据原发/接收证据的能力。原发/接收证据包括：

a) 操作时间；
b) 操作人员；
c) 操作类型；
d) 操作内容；
e) 业务流水号；
f) 账户名；
g) IP 地址；
h) 交易指令。

7.6.4.2 支持数字签名

候选DLT节点应在与其他DLT节点通信时对请求数据/返回数据进行数字签名。

7.6.5 可核查性

7.6.5.1 候选 DLT 节点审计

7.6.5.1.1 候选 DLT 节点记录日志的审计功能不应被单独中断;该审计功能记录的日志不应被未经授权的查看。

7.6.5.1.2 候选 DLT 节点记录的日志不应被未经授权的变更。

7.6.5.1.3 候选 DLT 节点按 6.1.1.2 中角色要求设定节点审计角色；

7.6.5.1.4 候选 DLT 节点的安全审计功能应能记录如下的系统重要安全事件：

a) 用户管理相关操作；
b) 用户在系统中的关键业务操作；
c) 应用系统关键数据更新；
d) 应用系统警告与错误信息。

7.6.5.1.5 候选 DLT 节点应对 7.6.5.1.4 中规定事件的记录日志，包括：

a) 事件的日期时间；
b) 操作者信息；
c) 类型；
d) 描述；
e) 结果。

7.6.5.1.6 候选 DLT 节点审计记录、保存和备份清理期限均应与银行函证系统要求一致。

7.6.5.1.7 候选 DLT 节点审计日志的访问应记录在审计日志中。

7.6.5.1.8 当从互联网登录候选 DLT 节点的监控页面时，应能提供用户上一次成功登录的如下内容：

a) 日期；
b) 时间；
c) 登录用户；
d) 登录位置。

7.6.5.2 运行环境审计

7.6.5.2.1 候选 DLT 节点的运行环境应有审计机制，能根据记录数据进行分析并生成审计报表。

7.6.5.2.2 候选 DLT 节点审计范围为服务器的每个操作系统用户和每个数据库用户；

7.6.5.2.3 候选 DLT 节点审计内容包括以下内容的启动与关闭：

a) 重要用户行为；
b) 系统资源异常使用；
c) 重要系统命令使用；
d) 账号分配；
e) 创建与变更；
f) 审计策略调整；
g) 审计系统功能。

7.6.5.2.4 候选 DLT 节点审计记录包括以下内容的定期备份，保存时间不少于 6 个月：

a) 事件的日期；
b) 事件时间；
c) 事件类型；
d) 主体标识；
e) 客体标识；
f) 结果。

7.6.5.3 网络审计

7.6.5.3.1 候选 DLT 节点的运行网络应有审计机制，能根据记录数据进行分析，并生成审计报表。

7.6.5.3.2 候选 DLT 节点的运行网络审计机制应对运行网络中的以下内容进行记录：

a) 网络设备运行状况，记录事件的日期和时间、用户、事件类型、事件是否成功；
b) 网络流量，记录事件的日期和时间、用户、事件类型、事件是否成功；
c) 用户行为进行日志记录，记录事件的日期和时间、用户、事件类型、事件是否成功。

7.6.5.3.3 候选 DLT 节点的运行网络审计机制能够保护审计记录，避免受到未预期的删除、修改、覆盖。

7.6.5.3.4 候选 DLT 节点的运行网络审计机制能定义审计跟踪阈值，当存储空间接近极限时时能采取有效措施，防止审计数据丢失。

7.6.6 真实性

7.6.6.1 用户划分与身份鉴别

7.6.6.1.1 对用户进行身份标识和鉴别，身份标识应具有唯一性。

注：口令、共享密钥、数字证书或生物特征均为常见的身份标识和鉴别机制。

7.6.6.1.2 使用口令鉴别方式时，支持如下内容：

a) 应支持首次登录设备时强制修改默认口令或设置口令；
b) 宜支持随机的初始口令；
c) 应支持设置口令生存周期；
d) 应支持口令复杂度检查功能；用户输入口令时，应仅在用户要求时明文回显口令；
e) 宜支持口令复杂度检查功能，口令复杂度检查包括口令长度检查、口令字符类型检查、口令与账号无关性检查。

注：不同类型口令复杂度要求和实现方式不同。通常，口令长度要求为长度不小于8位；口令字符类型包含数字、小写字母、大写字母、标点符号、特殊符号中的至少两类；口令中不包含账号信息。

7.6.6.1.3 应支持启用安全策略或具备安全功能，以防范用户鉴别信息猜解攻击。

注：常见的防范用户鉴别信息猜解攻击的安全策略或安全功能包括默认开启口令复杂度检查功能；限制连续的非法登录尝试次数或支持限制管理访问连接的数量；双因素鉴别(例如口令+证书、口令+生物鉴别等)等措施出现鉴别失败时，设备提供无差别反馈。避免提示“用户名错误”“口令错误”等类型的具体信息。

7.6.6.1.4 应支持启用安全策略或具备安全功能，以防止用户登录后会话空闲时间过长。

注：常见的防止用户登录后会话空闲时间过长的安全策略或安全功能之一为登录用户空闲超时后自动退出。

7.6.6.2 登录保护

7.6.6.2.1 候选 DLT 节点用户口令输入方式，应支持如下输入方式：

a) 实体键盘输入方式；

b) 软建盘输入方式。

7.6.6.2.2 候选 DLT 节点使用软键方式输入口令时，应对整体键盘布局进行随机干扰。

7.6.6.2.3 候选 DLT 节点用户口令密码登录机制宜具有密码存储介质和/或密码的更新机制，防范暴力破解静态密码的保护措施。

7.6.6.2.4 候选 DLT 节点监控页面用户登录失败时结束会话，返回登录的界面，提示用户名/密码错，限制非法登录次数。

7.6.6.2.5 候选 DLT 节点用户登录功后，提供上一次成功登录的日期、时间、登录用户、登录位置信息。

7.6.6.3 系统连接

候选DLT节点与其他DLT节点连接时，应采用另外的用户鉴别机制，用户名与口令的密文存放于候选DLT节点的配置文件中。

7.7 维护性

7.7.1 总体要求

候选DLT节点实现7.7.2～7.7.6的要求，并可在需要时按照GB/T 40473.8—20211进行更加广泛和深入的分析。

7.7.2 模块性

7.7.2.1 入口检查

候选DLT节点的模块入口应按照5.2与5.3中要求对以下内容进行检查：

a) 数据类型；

b) 数据格式。

7.7.2.2 信息交换方式

7.7.2.2.1 候选 DLT 节点的模块间，可通过如下技术手段进行数据交换：

a) 函数；

b) 类；

c) 共享内存；

d) 共享数据库表；

e) 共享文件；

f) TCP；

g） 管道。

7.7.2.2.2 候选 DLT 节点与其他 DLT 节点间，可通过如下技术手段进行数据交换：

a） 类；
b） 共享数据库表；
c） 共享文件；
d） TCP；
e） 管道。

7.7.2.3 总控模块

7.7.2.3.1 候选 DLT 节点使用自身总控模块进行应用逻辑的控制。

7.7.2.3.2 候选 DLT 节点内确定所处理的信息唯一性的标识，应由总控模块产生。

注：分户账记录同步和节点联网可能会导致候选DLT节点的总控模块完全停止工作。

7.7.2.4 候选 DLT 架构

7.7.2.4.1 候选 DLT 节点部署架构为 B/S 且不需控件和插件。

7.7.2.4.2 候选 DLT 节点的数据存储在本 DLT 节点的数据库和文件中。

7.7.3 易分析性

7.7.3.1 错误信息

7.7.3.1.1 候选 DLT 节点在执行中遇到错误时，应返回包括如下内容的信息，并宜通过返回信息定位到出错信息：

a） 错误码；
b） 错误模块标识；
c） 错误语句标识；
d） 导致错误的变量；
e） 错误相关参数。

7.7.3.1.2 候选 DLT 节点的错误码应在候选 DLT 节点的内部唯一。

7.7.3.1.3 候选 DLT 节点在运行中发生错误时，应将以下内容向直接用户报错，报错宜可直接辨别，每一种错误引起的原因都宜有明确文档描述，且文档的版本与程序版本一致：

a） 操作系统；
b） 数据库；
c） 其他支撑软件；
d） 候选 DLT 节点应用自身。

7.7.3.2 现场保护

候选DLT节点在执行中遇到错误时，宜能保存如下现场信息：

a） 输入信息；
b） 变量值；
c） 试图操作；
d） 错误原始信息；
e） 全局变量值；
f） 环境变量值。

7.7.4 易修改性

7.7.4.1 系统调试

系统调试信息按如下方式处理：

a) 对编译型语言，在生成生产版本时应通过编译开关屏蔽调试信息；在后继应用程序发现问题需要跟踪程序时，通过变更编译开关重新编译应用系统进行跟踪；

b) 对解释型语言，应设有控制调试信息的参数，在正常运行时设置为不产生/显示调试信息；在后继应用程序发现问题需要跟踪程序时，通过设置开关重新执行应用进行跟踪。

7.7.4.2 应用版本变更

候选DLT节点自身进行变更时的规则如下。

a) 宜支持如下变更模式：
   1) 自动变更平台；
   2) 变更执行脚本；
   3) 手工输入命令。

b) 在变更处于如下状态时，宜支持回退：
   1) 过程中；
   2) 完成后。

注：本条描述的变更不包括智能合约的变更。

7.7.5 易测试性

7.7.5.1 测试依据

7.7.5.1.1 候选 DLT 节点的测试依据应能在测试执行前明确，并可根据测试过程升级版本。

7.7.5.1.2 候选 DLT 节点的测试依据应体现在测试文档中。

7.7.5.2 测试文档

7.7.5.2.1 候选 DLT 节点宜按照 JR/T 0101—2013 选择适用的测试文档规范度和联动度，并按照所选择测试文档规范度和联动度，在规定的时间阶段编制、评审相关测试文档。

7.7.5.2.2 候选 DLT 节点测试工具和文档及数据宜能够执行回归测试。

7.8 移植性

7.8.1 总体要求

候选DLT节点实现7.8.2～7.8.3的要求，并可在需要时按照GB/T 40473.9—2021进行更加广泛和深入的分析。

7.8.2 易安装性

7.8.2.1.1 候选 DLT 节点安装程序在发现运行目标环境中缺少运行所需的支撑软件时，宜在安装包中带有适宜的软件或提供获取的路径，先行安装后再安装候选 DLT 节点。

7.8.2.1.2 候选 DLT 节点有多种功能而使用者可能不会用到全部的功能时，提供典型安装和全部安装的选项。

7.8.2.1.3 候选 DLT 节点的安装过程宜有详细安装步骤说明。

7.8.2.1.4 候选 DLT 节点安装过程中失败时，应报错并指出错误产生的原因后退出，报错并回滚到未安装的状态。

7.8.2.1.5 候选 DLT 节点安装后，应通过功能性验证确保安装正确性。

7.8.2.1.6 候选 DLT 节点安装后，系统参数的配置方式为提供参数配置界面，提供配置执行脚本。

7.8.2.1.7 候选 DLT 节点安装后，配置系统参数时，操作系统、数据库等支撑软件的用户名、密码来源于人工输入。

7.8.2.1.8 候选 DLT 节点在卸载时，应删除如下内容：

a) 删除所有原始安装文件；
b) 删除所有升级安装的文件；
c) 删除所有运行产生的临时文件；
d) 提示用户选择删除或保留所有的配置文件。

7.8.2.1.9 候选 DLT 节点卸载后，对原来进行了文件关联的能够恢复原来的文件关联。

7.8.2.1.10 候选 DLT 节点卸载后，对某些临时文件和配置文件不能卸载的给出未能卸载的文件清单。

7.8.3 易替换性

注：候选DLT节点的易替换性仅体现为版本升级。

7.8.3.1 候选 DLT 节点升级宜能妥善处理以下内容：

a) 可能涉及到的智能合约的代码结构；
b) 可能涉及到的分户账记录数据结构；
c) 可能涉及到的用户调用分户账记录的 SDK。

7.8.3.2 候选 DLT 节点在升级后，对原来配置参数可用的，宜保留原来的参数配置；对需变更和新增加的配置参数，应提供明确的说明。

7.8.3.3 在候选 DLT 节点升级过程中，尤其是在应用部署在多台设备的情况下，允许升级和未升级的软件同时工作。

附 录 A
（规范性）
分户账记录描述约定

A.1 概述

本附录给出了在描述分户账记录时，对相关属性的取值范围、描述方法以及呈现标记的约定。

A.2 分户账记录字段数据种类

分户账记录中各字段分为如下种类：

a) 对象，以多键多值的方式表述，其组分可为对象、数组和字段；

b) 数组，以一键多值的方式表述；

c) 字段，以键值对的方式表述。

A.3 分户账记录中组分描述

注：本条的内容与JR/T 0105—2014中附录B的规定保持了技术一致，并根据需要做了表述上的修改。

A.3.1 数据种类

A.3.1.1 编码类

编码是与数字、非数字或抽象实体字符相关的紧凑字符序列。即用少量、简单的基本符号，选用一定的组合规则，表示大量复杂多样的信息。

示例：客户编码、机构编码、产品编码。

注：编码的概念来自GB/T 40474-2021中的3.3。

A.3.1.2 代码类

代码是将第一组元素映射到第二组元素的规则集合。即一个预先定义的符号集合，用来描述一个有限集合的事物或事物的属性。

示例：国家和地区代码、押品类型代码。

注：代码的概念来自GB/T 40474-2021中的3.2。

A.3.1.3 布尔类

表示“是/否”意义的标志。

示例：是否组合产品标志、是否采用区块链标志。

A.3.1.4 文本类

需要以文本的形式对与业务活动密切相关的事宜进行描述的数据。

示例：备注。

注：文本在语义上可能是进一步结构化组织的，即分为若干组分且每个组分有自己的表达规则；也可能是没有进一步结构化组织的，即不再做组分的划分。

A.3.1.5 金额类

金额类指以货币金额的形式体现的数据项。金额类数据应说明度量单位（元、万元等）。在可能涉及到多币种时，还应说明币种。

示例：贷款余额、资产总额。

A.3.1.6 比率类

比率类指以比率的形式体现的数据项。

示例：利息税率、利率浮动幅度。

A.3.1.7 数值类

数值类指除金额类及比率类外的以整数或小数的形式体现的数据项，适用于各类以数量反映的信息。数值类在必要时应带有度量单位。

示例：营业场所办公面积、流通股数。

A.3.1.8 日期类

日期类指以日期的形式体现的数据项。

示例：客户出生日期、客户开户日期。

A.3.1.9 时间类

时间类指以时间的形式体现的数据项。

示例：登陆时间、取款时间。

A.3.1.10 日期时间类

日期时间类指以日期和当日时间的组合形式体现的数据项。

示例：账户开户日期时间、账户销户日期时间。

A.3.1.11 对象类

对象类是由A.3.1.1～A.3.1.10描述的数据类型，以及由对象类本身为组分构成的复合类。

注：对象类中各组分均是对象类不可分割的部分，对象类中的组分继承了对象类的呈现特征。

A.3.2 数据格式

分户账记录的数据格式如表A.1。

表 A.1 分户账记录格式

格式标识	格式含义
a	字母字符
n	数字字符
an	字母数字字符
anc	字母数字汉字字符
M!a	M 位字母字符，定长
M!n	M 位数字字符，定长
M!an	M 位字母数字字符，定长
M!anc	M 位字母数字汉字字符，定长

a..M	最多为 M 位字母字符
n..M	最多为 M 位数字字符
an..M	最多为 M 位字母数字字符
anc..M	最多为 M 位字母数字汉字字符
aM..N	最少为 M 位最多为 N 位字母字符
anM..N	最少为 M 位最多为 N 位字母数字字符
ancM..N	最少为 M 位最多为 N 位字母数字汉字字符
M(N)	M 位数字字符，其中包括小数点和 N 个小数位（M>N+1）
YYYY-MM-DD[a]	日期格式，表示年月日。Y 表示时间元素“年”所使用的数字，M 表示时间元素“月”所使用的数字，D 表示时间元素“日”所使用的数字
hh:mm:ss[b]	时间格式（24 小时制），表示时分秒。h 表示时间元素“小时”所使用的数字，m 表示时间元素“分钟”所使用的数字，s 表示时间元素“秒”所使用的数字
YYYY-MM-DDThh:mm:ss[c]	日期时间格式，表示某年某月某日某时某分某秒。T 为时间标识符，在日期和日的时间组合表达式中，用以标识该日的时间表示法的开始
注：本表的内容与JR/T 0105—2014中附录C的规定保持了技术一致，并根据需要做了表述上的修改。 **示例 1：**7!an 表示定长 7 个字母数字字符。 **示例 2：**anc3..8 表示最小长度为 3，最大长度为 8 的不定长字母数字汉字字符。	
[a] 日期格式与 GB/T 7408—2005 中 5.2.1.1 规定的扩展格式一致。 [b] 时间格式与 GB/T 7408—2005 中 5.3.1.1 规定的扩展格式一致。 [c] 日期时间格式与 GB/T 7408—2005 中 5.4.1 规定的扩展格式一致。	

A.4 呈现标记

分户账记录和分户账记录字段的呈现要求标记如下。

a) 应有，标记为M(Mandatory)，表示一定要出现。

b) 可选，标记为O(Optional)，在不填写时，处理时视作空值。

c) 条件，标记为C(Conditional)，在满足给出的条件时等同于应有，在不满足给出的条件时等同于可选。

参 考 文 献

[1] GB/T 5271.18—2008 信息技术 词汇 第18部分：分布式数据处理

[2] GB/T 22239—2019 网络安全等级保护基本要求

[3] GB/T 25069—2010 信息安全技术 术语

[4] GB/T 35273—2020 信息安全技术 个人信息安全规范

[5] GB/T 40474—2021 银行业应用系统 代码与编码处置指南

[6] JR/T 0105—2014 银行数据标准定义规范

[7] JR/T 0184—2020 金融分布式账本技术安全规范

[8] JR/T 0197—2020 金融数据安全 数据安全分级指南

[9] JR/T 0223—2021 金融数据安全 数据生命周期安全规范

[10] ISO/IEC 9804:1998 Information technology — Open systems interconnection — Service definition for the commitment, concurrency and recovery service element

[11] ISO/IEC 16350:2015 Information technology — Systems and software engineering — Application management

[12] ISO 22739:2020 Blockchain and distributed ledger technologies — Vocabulary

[13] ISO/TR 23455:2019 Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems