

基于区块链数据价值分析指南

Blockchain based data value analysis guidelines

(点击此处添加与国际标准一致性程度的标识)

(征求意见稿)

联系单位：黑龙江省运通科技有限公司

联系人：吕翔宇

联系电话：13936673292

邮箱：sean.lv@foxmail.com

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

黑龙江省市场监督管理 发 布

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 基本原则 2

5 基础保障 2

6 数据价值 3

7 场景应用 4

附录 A（资料性） 涉及数据和区块链有关的术语和定义 7

参考文献 22

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。

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专利的责任。

本文件由××××提出。

本文件由××××归口。

本文件起草单位：

本文件主要起草人：

基于区块链数据价值分析指南

1 范围

本文件给出了基于区块链数据价值分析的术语和定义、基本原则、基础保障、数据价值、场景应用。
本文件适用于基于区块链的应用，分析和挖掘存在的数据价值。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

区块 block

一种区块链的基本组成单元，通常由一系列交易和一些关于区块的元信息组成。

[来源：ISO 22738:2020，3.2，有修改]

3.2

区块链 blockchain

一种将数据区块顺序相连，并通过共识协议、数字签名、杂凑函数等密码学方式保证的抗篡改和不可伪造的分布式账本。

[来源：ISO 22739：2020，3.6，有修改]

3.3

节点 node

具有特定功能的区块链组件，可独立运行的单元。

[来源：ISO 22739：2020，3.50，有修改]

3.4

地址 address

节点在区块链中的标识，具有唯一性。

3.5

交易 transaction

区块链双方或多方参与，并且会发生状态变更的一种基本区块组成单元。

[来源：ISO 22739：2020，3.77，有修改]

3.6

用户 user

参与产生区块链交易数据的个人、组织或进程。

[来源：ISO 22739：2020，3.2，有修改]

3.7

共识 consensus

在分布式节点间达成区块数据一致性的认可。

3.8

共识节点 consensus node

负责产生区块，并维护区块链数据的节点。节点保存着自己的一份或者部分账本，通过投票或者算力等方式来解决共识问题，在无信任或弱信任的方式下确保全体节点遵循的账本和自己的账本是一致的。

3.9

共识协议 consensus protocol

区块链中通过数学算法实现不同节点之间对记账内容达成一致的方法，是区块链确认世界状态，节点间建立信任、协同合作的基础。

4 基本原则

4.1 去中心化

区块链技术不依赖额外的第三方管理机构或硬件设施，没有中心管制，除自成一体的区块链本身，通过分布式核算和存储，各个节点负责产生区块共识节点，实现信息自我验证、传递和管理。

4.2 开放性

区块链基础技术是开源的，在共识协议的基础上，除了交易各方的私有信息被加密外，区块链的数据对所有人开放，任何人都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。

4.3 独立性

基于协商一致的规范和共识协议(如比特币采用的哈希算法等各种数学算法)，整个区块链系统不依赖其他第三方，所有节点能够在系统内自动安全地验证、交换数据，不需要任何人为的干预。

4.4 安全性

主观人为的数据变更者较难做到控制全部数据节点的51%以上，即无法肆意操控修改网络数据，确保区块链本身变得相对安全。

4.5 匿名性

除非有法律规范要求，单从技术上来讲，各区块节点的身份信息不需要公开或验证，信息传递可以匿名进行。

5 基础保障

5.1 制度建设

建立区块链信息服务提供者的信息安全管理责任制，制定和公开管理规则和平台公约，落实真实身份信息认证制度，规避区块链信息服务安全风险。

5.2 主体责任

树立区块链信息服务提供者的安全责任意识，建立信息安全管理主体责任制，配备与其服务相适应的技术条件。

5.3 技术保障

5.3.1 区块链系统宜采用的对称密码算法、非对称密码算法等，见 GB/T 32905、GB/T 32907 和 GB/T 32918 以及相应的国际标准的要求。

5.3.2 区块链框架见 GB/T 17901.1 的规定，运行环境见 GB/T 22239 三级及以上的要求。

5.3.3 技术密钥管理，包括但不限于：对称密钥、非对称密钥、群密钥以及密钥派生等见 GB/T 17901.3 的要求。

5.3.4 采用的密码模块见 GB/T 37092-2018 二级及以上的要求，密码模块安全检测要求见 GB/T 38625 的要求，公钥基础设施的标准符合性测评见 GB/T 30272。

5.3.5 区块链运维管理中的身份认证与权限管理、密钥管理等工作的安全运维见 GB/T 22239、GB/T 36626 和 ISO TR 23244-2020 的要求。

5.3.6 实体鉴别见 GB/T 15843 系列算法。

5.3.7 区块链中的可信时间源见 GB/T 20520 的要求。

5.3.8 随机数生成和敏感安全参数生成见 GB/T 37092 的要求，随机序列生成见 GB/T 32915 的要求。

6 数据价值

6.1 概述

区块链数据具有“不可伪造”“全程留痕”“可以追溯”“公开透明”“集体维护”等特征。区块链数据一旦在链上进行存储，即无法篡改，并支持在数据系统上进行查验和安全共享，提高系统参与方的协作效率。每个节点中都存有整个网络的所有数据，增加新的数据区块，需要经过这些节点的交叉验证，保障数据的真实性。

注：区块链和分布式分类帐技术系统中智能合约的概述和交互见 ISO TR 23455-2019 的规定，区块链数字资产保管人的安全管理见 ISO TR 23576-2020。

6.2 无形要素

由经济责任、持续发展责任、法律责任和道德责任等构成的无形要素价值，包括但不限于：

- 社会责任，包括企业环境保护、安全生产、社会道德以及公共利益等方面的数据价值挖掘与分析；
- 知识产权，包括版权与邻接权、商标权、地理标志权、工业品外观设计权、专利权、集成电路布图设计权、未披露过的信息专有权的数据保护与价值分析；
- 品牌管理，包括品牌文化、品牌历史、品牌战略、品牌知名度、品牌忠诚度等；
- 商业秘密等。

6.3 质量要素

由基本概念、验证过程、验证工具、应用案例等保证数据的质量要素价值，包括但不限于：

- 质量管理，包括数据规范管理、信息分专业管理、数据核查管理、通知预警管理和质量统计分析等功能；
- 质量标准，包括数据的精度、准确性、关联性、及时性。

6.4 服务要素

区块链数据作为服务要素，具有无消耗性、增值性、依附性、全面性的特点，其价值运用，包括但不限于：

- 服务保障，包括用户数据安全性、隐私性、存储容量、存储设施、储存时效性等；
- 服务过程，包括管理人员、服务界面等；
- 服务结果，包括满意度、服务改进等。

6.5 创新要素

区块链数据作为重要的生产要素与资源，具备创新的动力，是企业核心的竞争力，运用数据作为可信的基础，包括但不限于：

- 研发管理，包括完善现有产品或开发新产品、新过程、新组织模式与新市场；
- 战略机制，包括目标定位、知识产权转换、标准制定固化成果等；
- 创新管理，包括企业管理、政府监管、社会管理等；
- 创新能力，包括基于区块链数据分析能力、市场拓展应用能力、创新投入能力等。

7 场景应用

7.1 物联网和物流领域

利用散状网络分层结构，将整个网络的信息通过结点连接，实现全面、准确、可检验的传递过程，价值优势包括但不限于：

- 通过区块链数据录入层、网络通信层、数据安全与隐私保护层、共识层、智能合约层、应用层等功能性层级达到全程留痕，使物品的生产和运送过程具有可追溯性，保证数据不可伪造，实现集体维护，降低物流成本，实现物联网交易便利化、智能化的数据要素价值；
- 通过大数据自动筛选过滤物联网交易，在区块链中建立信用资源模式，保证数据交易的安全性，实现应用智能物流模式节约时间成本的数据要素价值；
- 通过区块链节点在整个区块链体系中的独立性和非干扰性，实现智能物流分散用户对拓展和集体数据的共同维护；
- 通过支持核心信息与智能设备关联共同识别，设置预先定义的规则，对其进行编程后，实现无差错、防篡改执行的数据要素价值。

7.2 金融领域

区块链技术凭借其应用优势，包括但不限于：

- 通过共同协议直接连通付款方银行与接收方银行数据，绕过中转银行，减少中转费用支出，满足客户对金融服务及时性、便捷性的需求，实现数据要素价值；
- 实现全天候支付、实时到账、提现简便，消灭大量的隐性成本，降低跨境支付结算风险，实现数据要素价值；
- 通过将限定用户名册放到区块链上进行管理，限定用户用电子签名在区块链签订股权转让的电子合同，由区块链保证货银对付，实现数据流转价值；

- 在股权众筹型企业中，利用区块链技术，众筹投资者不仅可以在线上完成股权登记的所有电子合同，还能非常方便地进行股权的再次转让，为股权众筹提供良好的退出机制，实现便利的、真实传递的数据要素价值；
- 在进行员工持股激励方面，利用区块链技术，公司可以把股权、期权、限制性股权、分红权等各种权益在一个去中心化的区块链系统里管理起来，增加员工对自己权益的掌控权。

7.3 数据存证

区块链上数据被确权后，后续交易都会进行实时记录，实现数字版权全生命周期管理，包括但不限于：

- 通过区块链技术对作品进行鉴权，证明文字、视频、音频等作品的存在，保证权属的真实性、唯一性；
- 通过将合同、文档数据记录到区块链上，可向外证明在某个时间点，该合同、文档的存在性；
- 文件的数据记录置于区块链上，未来可以通过校验数据指纹判断这份文件是否被篡改过。

7.4 溯源、防伪与供应链

通过对每一次流转的登记，追踪记录有形商品或无形信息的流转链条，实现产地追溯、防伪鉴证，包括但不限于：

- 通过溯源信息系统安全平稳且高效率的运作，支持优化服务供应链目标的实现；
- 支持药品溯源、艺术品防伪、奢侈品防伪等，提供可靠的交易。

7.5 保险

区块链在保险领域的应用优势，包括但不限于：

- 区块链可实现信息的全程可追溯，信息不被调取时处于无标识状态，触发时能快速准确调取，高效的解决索赔，避免通过身份欺骗、数据抵赖导致的保险欺诈；
- 通过区块链的共识协议技术，保险公司可以自动触发理赔行为，而无需用户主动干预。

7.6 医疗

区块链技术能为医疗机构解决大量敏感信息保存的问题，包括但不限于：

- 病史记录；
- 疾病的支付信息；
- 疾病的治疗过程；
- 安全和隐私的存储。

不仅为这些，而且它还能帮助降低医院和医疗服务者在管理病人和其他信息时的巨大成本。

7.7 预测市场

区块链预测市场应用的优点，包括但不限于：

- 无中心化服务器，难以被关闭；
- 用户可以创造自己的交易市场；
- 低成本运营，低费率；
- 众包型的结果判断；

——安全以及自动化的支付。

7.8 共服务领域

区块链在公共管理、能源、交通等与民众生产生活领域发挥社会责任的基础作用，包括但不限于：

- 通过网络中各个节点之间的点对点数据传输服务就能实现域名的查询和解析；
- 确保某个重要的基础设施的操作系统和固件没有被篡改；
- 可以监控软件的状态和完整性，发现不良的篡改；
- 确保传输的数据没用经过篡改。

7.9 公益领域

区块链存储数据捐赠项目、募集明细、资金流向、受助人反馈等公益流程，具有不可伪造、全程留痕、可以追溯、公开透明、集体维护的优势，包括但不限于：

- 可靠性高且不可篡改；
- 在社会公益场景中，可以有条件地进行透明公开公示，方便社会监督。

附录 A
(资料性)

涉及数据和区块链有关的术语和定义

表 A. 1 给出了涉及数据和区块链有关的术语和定义，并给出相关参考译文。

表 A. 1 涉及数据和区块链有关的术语和定义

中文	英文
过程 使用输入来交付预期结果的一组相互关联或相互活动的活动	process set of interrelated or interacting activities that use inputs to deliver an intended result
要求 明示的、暗示的或强制性的需要或期望	requirement need or expectation that is stated, generally implied or obligatory
质量 对象的一组固有特性满足要求的程度	quality degree to which a set of inherent characteristics of an object fulfils requirements
不一致 不满足要求	nonconformity non-fulfilment of a requirement
信息 关于对象的知识，如事实、事件、事物、过程，或在特定上下文中具有特定含义的概念	information knowledge concerning objects, such as facts, events, things, processes, or ideas, including concepts, that within a certain context has a particular meaning
数据 一种形式化的可再解释的信息表示方式，以适用于通信、解释或处理	data reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing
数据交换 数据的存储、访问、传输和归档	data exchange storing, accessing, transferring, and archiving of data
数据集 逻辑上有意义的数据分组	data set logically meaningful grouping of data
元数据 定义和描述其他数据的数据	metadata data defining and describing other data
客观证据 支持某事物存在或真实性的数据	objective evidence data supporting the existence or verity of something
标识符 由组织创建以引用数据集的字符串	identifier string of characters created by an organization to reference a data set

标识符解析 当应用于标识符时，返回相关数据集的过程	identifier resolution process that, when applied to an identifier, returns an associated data set
实体 所考虑领域中的具体或抽象事物	entity concrete or abstract thing in the domain under consideration
组织标识符 可以明确解析为组织的法定名称、位置和管理员的参考标识符	organization identifier reference that can be resolved unambiguously to the legal name, the location and the administrator of the organization
法人实体 由国家、州或社区的管理机构授予法律地位的自然人或法人	legal entity physical or juridical person granted legal status by the governing body of a nation, state or community
权威标识符 标识符由组织发布，该组织是已识别对象的发起者或法定机构	authoritative identifier identifier issued by an organization that is the originator of the object identified or that is a legal authority
权威法人标识 识别法人实体的标识符，由行政机构为有权授予法律地位的国家、州或社区的管理机构颁发	authoritative legal entity identifier ALEI identifier that identifies a legal entity and is issued by the administrative agency for a governing body of the nation, state, or community with the authority to grant legal status
代理标识符 由非标识对象发起者的组织发布的标识符	proxy identifier identifier issued by an organization that is not the originator of the object identified
代理法人实体标识符 识别法人实体的标识符，由非政府行政机构的组织颁发，因此无权授予法律地位	proxy legal entity identifier identifier that identifies a legal entity and is issued by an organization that is not the administrative agency for a government and, thus, has no authority to grant legal status
重要记录 政府授权保存的生活事件记录	vital record record of life events kept under governmental authority
免费解码 标识符解析，无需支付费用，即可返回关联的数据集	free decoding identifier resolution that, without the need to pay a fee, returns an associated data set
付费的解码 标识符解析，只有在支付费用后，才能返回相关的数据集	fee-based decoding identifier resolution that, only after paying a fee, returns an associated data set
免费编码 无需付费，使用术语和定义来发现概念标识符	free encoding without the need to pay a fee, using terms and definitions to discover concept identifiers

<p>测量</p> <p>确定或确定某物的大小或数量</p>	<p>measure</p> <p>ascertain or determine the magnitude or quantity of something</p>
<p>测量结果</p> <p>测量某物的结果</p>	<p>measurement</p> <p>result of measuring something</p>
<p>测量数据</p> <p>代表测量值的数据</p>	<p>measurement data</p> <p>data representing a measurement</p>
<p>测量要求</p> <p>对如何测量标准的文字描述，包括控制测试和要测试的一个或多个元素的任何必要的附加属性和规则，起到可靠测量算法的外部规范作用</p>	<p>measurement requirement</p> <p>textual description of how a criterion is measured, including any necessary additional attributes and rules to control the test and the element or elements to be tested, and which plays the role of an external specification for a reliable measuring algorithm</p>
<p>产品</p> <p>由自然或人工过程产生的东西或物质</p>	<p>product</p> <p>thing or substance produced by a natural or artificial process</p>
<p>产品数据</p> <p>以一种适合人类或计算机进行交流、解释或处理的正式方式表示有关产品的信息</p>	<p>product data</p> <p>representation of information about a product in a formal manner suitable for communication, interpretation, or processing by human beings or by computers</p>
<p>应用</p> <p>创建、使用产品数据的一个或多个过程</p>	<p>application</p> <p>one or more processes creating or using product data</p>
<p>应用协议</p> <p>指定了满足特定应用范围和信息要求的解释模型</p>	<p>application protocol</p> <p>AP</p> <p>specifies an application interpreted model satisfying the scope and information requirements for a specific application</p>
<p>应用参考模型</p> <p>描述应用程序协议或模块内应用程序的信息要求和约束的信息模型</p>	<p>application reference model</p> <p>ARM</p> <p>information model that describes the information requirements and constraints of an application within an application protocol or module</p>
<p>数据字典条目</p> <p>对至少包含明确标识符、术语和定义的实体类型的描述</p>	<p>data dictionary entry</p> <p>description of an entity type containing, at a minimum, an unambiguous identifier, a term and a definition</p>

数据字典 数据字典条目的集合，允许按实体标识符进行查找	data dictionary collection of data dictionary entries that allows lookup by entity identifier
数据规范 涵盖适合一个或多个特定目的的数据特征的一组要求	data specification set of requirements covering the characteristics of data being fit for one or more particular purposes
属性值 特定值的实例以及定义属性的数据字典条目的标识符	property value instance of a specific value together with an identifier for a data dictionary entry that defines a property
特征数据 实体所属的类和一组属性值对实体的描述	characteristic data description of an entity by the class to which it belongs and a set of property values
数据质量 数据的一组固有特征满足要求的程度	data quality degree to which a set of inherent characteristics of data fulfils requirements
数据质量管理 在数据质量方面指导和控制组织的协调活动	data quality management coordinated activities to direct and control an organization with regard to data quality
数据误差 不满足数据要求	data error non-fulfilment of a data requirement
数据来源记录 一条数据通过其不同的所有者或保管人的最终派生和传递的记录	data provenance record record of the ultimate derivation and passage of a piece of data through its various owners or custodians
确认 通过提供客观证据确认已满足特定要求	verification confirmation, through the provision of objective evidence, that specified requirements have been fulfilled
验证 通过提供客观证据确认已满足特定预期用途或应用的要求	validation confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled
权威数据源 创建数据的进程的所有者	authoritative data source owner of a process that creates data
可接受的参考值 作为商定的比较参考值	accepted reference value value that serves as an agreed-upon reference for comparison
真值 在考虑该特征时，该特征在存在的条件下被完美定义的值	true value value that characterizes a characteristic perfectly defined in the conditions that exist when the characteristic is considered

数据的准确性 数据的质量，表示值与相应的真实值在达到预期目的所必需的程度上一致	data accuracy quality of data in respect of the represented value agreeing with the corresponding true value to a degree necessary for an intended purpose
数据准确记录 所提供的关于某一特定数据集的数据准确性的信息记录	data accuracy record record of the information provided about the data accuracy of a specified data set
数据完整性 预期目的所必需的、与内容有关的数据集质量	data completeness quality of a data set in respect of the content being all that is necessary for an intended purpose
数据完整性记录 所提供的关于某一特定数据集数据完整性的信息记录	data completeness record record of the information provided about the data completeness of a specified data set
形式语法 使用形式语法规范形式语言的有效句子	formal syntax specification of the valid sentences of a formal language using a formal grammar
语义编码 用引用数据字典条目的标识符替换消息中的自然语言术语的技术	semantic encoding technique of replacing natural language terms in a message with identifiers that reference data dictionary entries
语义编码的数据规范 数据需求声明，使用数据字典中的条目的数据规范	semantically coded data specification data requirements statement data specification that uses entries from a data dictionary
商业交易 商业行为或行动过程的完成	business transaction completion of a business action or a course of action
交易数据 代表商业交易的数据	transaction data data representing a business transaction
主要数据 组织持有的数据，用于描述对该组织而言既独立又基本的实体，并被引用以执行其交易	master data data held by an organization to describe the entities that are both independent and fundamental for that organization, and referenced in order to perform its transactions
主数据信息 用于交换主数据的数据信息	master data message data message used to exchange master data

产品数据质量 产品数据的一致性、完整性和适用性	product data quality consistency, completeness, and suitability for the purpose of the product data
质量标准 评估产品数据质量的标准	quality criterion criterion for evaluating product data quality
产品形状数据 用几何和拓扑信息表示产品形状的数据	product shape data data representing product shape with geometric and topological information
阈值 通过数值试验评估形状数据质量的余量	threshold allowance used for the assessment of shape data quality by numerical test
检查 确定是否符合规定要求	inspection determination of conformity to specified requirements
检查结果 检查结果表明检查的产品形状数据中是否存在质量缺陷	inspection result result of inspection which indicates whether, or not, quality defects exist within the inspected product shape data
准确性 控制近似解精度的规范	accuracy specification to control precision of an approximate solution
生产项目 符合供应商定义的规格的商品或服务	item of production goods or service that conforms to a specification defined by a supplier
序列号 资产追踪号码 资产编号 用于识别生产项目的单个事件的编号	serial number asset tracking number asset number number used to identify an individual occurrence of an item of production
供应项目 满足买方定义的适合、形式或功能的可替代商品或服务类别	item of supply class of substitutable goods or services that fulfil a fit, form or function defined by a buyer
零件号 分配给制造系统中对象的唯一字母数字名称	part number unique alphanumeric designation assigned to an object in a manufacturing system
库存单位 一组产品特征的标识符，用于库存控制或采购	stockkeeping unit identifier of a set of product characteristics for the purpose of inventory control or procurement

<p>数据技术员</p> <p>根据数据质量管理指南创建、读取、修改和删除数据，测量数据质量并纠正因测量数据质量而发现的数据错误的人员</p>	<p>data technician</p> <p>person who creates, reads, modifies, and deletes data in accordance with the guidelines for data quality management, and measures data quality and corrects data errors found as a result of measuring data quality</p>
<p>数据管理员</p> <p>通过定义维护数据质量所需的标准、设计数据模式以及分析错误原因以防止错误再次发生来控制 and 协调数据技术人员工作的人</p>	<p>data administrator</p> <p>person who controls and coordinates the work of data technicians by defining criteria needed to maintain data quality, by designing data schemata, and by analysing the causes of errors to prevent their recurrence</p>
<p>数据管理器</p> <p>为组织中的数据质量改进制定计划的人员，授予数据管理员在信息系统或组织中跟踪和纠正数据的权限，并通过整个组织范围的数据体系结构在各个信息系统中维护数据一致性</p>	<p>data manager</p> <p>person who establishes plans for data quality improvement in an organization, grants data administrators the authority to trace and correct data over the information systems or organization, and maintains data consistency in individual information systems through the organization-wide data architecture</p>
<p>数据管家</p> <p>被委派负责管理一组特定数据资源的个人或组织</p>	<p>data steward</p> <p>person or organization delegated the responsibility for managing a specific set of data resources</p>
<p>过程评估模型</p> <p>适用于评估特定过程质量特性的模型，基于一个或多个过程参考模型</p>	<p>process assessment model</p> <p>model suitable for the purpose of assessing a specified process quality characteristic, based on one or more process reference models</p>
<p>过程维度</p> <p>过程评估模型中与相关过程参考模型中定义的过程明确相关的一组元素</p>	<p>process dimension</p> <p>set of elements in a process assessment model explicitly related to the processes defined in the relevant process reference model(s)</p>
<p>成熟度模型</p> <p>从一个或多个指定的过程评估模型派生的模型，该模型确定了在组织过程成熟度的指定规模中与级别相关的过程集</p>	<p>maturity model</p> <p>model derived from one or more specified process assessment models that identify the process sets associated with the levels in a specified scale of organizational process maturity</p>
<p>组织单位</p> <p>组织中已确定的部署一个或多个过程的部分，这些过程在一组一致的业务目标中运行，并构成评估范围的基础</p>	<p>organizational unit</p> <p>identified part of an organization that deploys one or more processes that operate within a coherent set of business goals and which forms the basis for the scope of an assessment</p>
<p>成熟度级别</p> <p>在组织过程成熟度的有序尺度上的点，表征在成</p>	<p>maturity level</p> <p>point on an ordinal scale of organizational process</p>

<p>熟度模型的范围内评估的组织单元的成熟度</p>	<p>maturity that characterises the maturity of the organizational unit assessed in the scope of the maturity model used</p>
<p>过程评估</p> <p>根据过程评估模型对组织单位的过程进行有纪律的评估</p>	<p>process assessment</p> <p>disciplined evaluation of an organizational unit's processes against a process assessment model</p>
<p>评估输入</p> <p>开始过程评估之前所需的信息</p>	<p>assessment input</p> <p>information required before a process assessment can commence</p>
<p>评估输出</p> <p>过程评估的所有有形结果</p>	<p>assessment output</p> <p>all of the tangible results from a process assessment</p>
<p>评估小组</p> <p>一个或多个共同执行过程评估的个人</p>	<p>assessment team</p> <p>one or more individuals who jointly perform a process assessment</p>
<p>过程属性</p> <p>过程质量属性</p> <p>过程质量特性的可测量属性</p>	<p>process attribute</p> <p>process quality attribute</p> <p>measurable property of a process quality characteristic</p>
<p>过程属性等级</p> <p>判断被评估过程的过程属性的实现程度</p>	<p>process attribute rating</p> <p>judgement of the degree of achievement of the process attribute for the assessed process</p>
<p>过程配置文件</p> <p>被评估的过程属性评级集</p>	<p>process profile</p> <p>set of process attribute ratings for an assessed process</p>
<p>评估记录</p> <p>对与过程评估有关的信息进行有序的文档化收集，并增加对由评估生成的过程概要的理解和验证</p>	<p>assessment record</p> <p>orderly documented collection of the information which is pertinent to a process assessment and adds to the understanding and verification of the process profiles generated by the assessment</p>
<p>评估指标</p> <p>用于支持评估人员对评定过程属性的判断的客观证据来源</p>	<p>assessment indicator</p> <p>sources of objective evidence used to support the assessor's judgement in rating process attributes</p>
<p>过程能力</p> <p>描述过程满足当前或预期业务目标的能力</p>	<p>process capability</p> <p>characterization of the ability of a process to meet current or projected business goals</p>
<p>过程能力水平</p> <p>在过程能力的顺序度量尺度上描述过程的特性</p>	<p>process capability level</p> <p>characterization of a process on an o</p>
<p>过程的结果</p> <p>成功实现过程目的的可观察结果</p>	<p>process outcome</p> <p>observable result of the successful achievement of process purpose</p>
<p>数据治理</p>	<p>data governance</p>

制定和执行与数据管理相关的政策	development and enforcement of policies related to the management of data
资产 所有对利益相关者有价值的东西	asset anything that has value to a stakeholder
区块 包含块数据和块头的结构化数据	block structured data comprising block data and a block header
块数据 包含零个或多个交易记录的结构化数据或交易记录的参考	block data structured data comprising zero or more transaction records or references to transaction records
区块头 包含前一块加密链接的结构化数据，除非没有前块	block header structured data that includes a cryptographic link to the previous block unless there is no previous block
区块奖励 在区块链系统中确认区块后给予矿工或验证者的奖励	block reward reward given to miners or validators after a block is confirmed in a blockchain system
区块链 带有确认块的分布式账本，使用加密链接组织在只加的顺序链中	blockchain distributed ledger with confirmed blocks organized in an append-only, sequential chain using cryptographic links
区块链系统 使区块链生效的系统	blockchain system system that implements a blockchain
确认 经协商一致同意纳入分布式分类账	confirmed accepted by consensus for inclusion in a distributed ledger
确认区块 已确认的块	confirmed block block that has been confirmed
确认交易 已确认的交易	confirmed transaction transaction that has been confirmed
共识 DLT 节点之间的协议，在该协议中，交易已被验证且分布式账本包含已验证交易的一致集合和顺序	consensus 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
共识机制 达成共识的规则和程序	consensus mechanism rules and procedures by which consensus is reached
加密资产 使用加密技术实现的数字资产	crypto-asset digital asset implemented using cryptographic techniques
加密货币 旨在作为价值交换媒介的加密资产	cryptocurrency crypto-asset designed to work as a medium of value exchange
加密哈希函数 将任意长度的二进制字符串映射到固定长度的	cryptographic hash function function mapping binary strings of arbitrary length to

二进制字符串的函数，因此对于给定的输出查找映射到输出的输入在计算上是昂贵的，对于给定的输入查找映射到的第二个输入在计算上是不可行的 相同的输出，并且要找到映射到相同输出的任何两个不同的输入在计算上是不可行的	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
加密链接 使用加密哈希函数技术构造并指向数据的参考标识	cryptographic link reference, constructed using a cryptographic hash function technique, that points to data
密码学 数据转换的原则、手段和方法的规程，以隐藏其语义内容、防止其未经授权的使用或防止其未被发现的修改	cryptography discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification
去中心应用 在去中心系统上运行的应用程序	decentralized application DApp application that runs on a decentralized system
去中心系统 控制分布在参与系统操作的个人或组织之间的分布式系统	decentralized system distributed system wherein control is distributed among the persons or organizations participating in the operation of the system
数据集 逻辑上有意义的数据分组	digital asset asset that exists only in digital form or which is the digital representation of another asset
电子签名 当附加到数字对象时，使数字对象的用户能够验证其来源和完整性的数据	digital signature data which, when appended to a digital object, enable the user of the digital object to authenticate its origin and integrity
分布式账本 在一组 DLT 节点之间共享并使用共识机制在 DLT 节点之间同步的分类账本	distributed ledger ledger that is shared across a set of DLT nodes and synchronized between the DLT nodes using a consensus mechanism
DLT 分布式账本技术； 能够运行和使用分布式账本的技术	DLT distributed ledger technology; technology that enables the operation and use of distributed ledgers
DLT 账户 分布式账本技术账户； 代表参与交易的实体	DLT account distributed ledger technology account; representation of an entity participating in a transaction
DLT 地址 分布式账本技术地址； 标识参与交易的 DLT 账户的值	DLT address distributed ledger technology address; value that identifies a DLT account participating in a

	transaction
DLT 网络 分布式账本技术网络； 构成 DLT 系统的 DLT 节点网络	DLT network distributed ledger technology network; network of DLT nodes which make up a DLT system
DLT 节点 分布式账本技术节点	DLT node distributed ledger technology node
DLT 预报 分布式账本技术预报	DLT oracle distributed ledger technology oracle
DLT 平台 一组处理、存储和通信实体； 它们共同在每个 DLT 节点上提供 DLT 系统的功能	DLT platform distributed ledger technology platform; set of processing, storage and communication entities which together provide the capabilities of the DLT system on each DLT node
DLT 系统 分布式账本系统； 分布式账本技术系统； 实现分布式账本的系统	DLT system distributed ledger system; distributed ledger technology system system that implements a distributed ledger
DLT 用户 分布式账本技术用户； DLT 系统提供服务的实体	DLT user distributed ledger technology user; entity that uses services provided by a DLT system
分布式系统 位于联网计算机上的组件通过相互交互进行通信和协调其动作的系统	distributed system system in which components located on networked computers communicate and coordinate their actions by interacting with each other
双重支付 代币或加密资产的控制权被多次错误转移的 DLT 平台故障	double spending failure of a DLT platform where the control of a token or crypto-asset is incorrectly transferred more than once
实体 信息和通信技术系统内部或外部的项目，例如一个人、一个组织、一个设备、一个子系统，或具有可识别的不同存在的一组此类项目	entity 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
故障 丧失执行要求的能力	failure loss of ability to perform as required
容错 功能单元在出现故障或错误的情况下继续执行所需功能的能力	fault tolerance ability of a functional unit to continue to perform a required function in the presence of faults or errors
创世区块 区块链中的第一个区块	genesis block first block in a blockchain

<p>硬分叉</p> <p>更改为 DLT 平台，其中 DLT 节点使用新版本的 DLT 平台创建的新分类帐记录或块不被使用旧版本 DLT 平台的 DLT 节点接受</p>	<p>hard fork</p> <p>change to a DLT platform in which new ledger records or blocks created by the DLT nodes using the new version of the DLT platform are not accepted as valid by DLT nodes using old versions of the DLT platform</p>
<p>哈希值</p> <p>密码散列函数输出的位串</p>	<p>hash value</p> <p>string of bits which is the output of a cryptographic hash function</p>
<p>不变性</p> <p>一旦添加到分布式分类帐中，分类帐记录就无法修改或删除的属性</p>	<p>immutability</p> <p>property wherein ledger records cannot be modified or removed once added to a distributed ledger</p>
<p>互操作性</p> <p>两个或多个系统或应用程序交换信息和相互使用已交换信息的能力</p>	<p>interoperability</p> <p>ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged</p>
<p>叶节点</p> <p>没有子节点的节点</p>	<p>leaf node</p> <p>node that has no child nodes</p>
<p>分类账本</p> <p>保存最终、确定和不可变交易记录的信息存储</p>	<p>ledger</p> <p>information store that keeps records of transactions that are intended to be final, definitive and immutable</p>
<p>分类账本记录</p> <p>包含交易记录的记录，交易记录的哈希值，或对记录在分布式账本上的交易记录的引用</p>	<p>ledger record</p> <p>record containing transaction records, hash values of transaction records, or references to transaction records recorded on a distributed ledger</p>
<p>分类账拆分</p> <p>分叉；</p> <p>创建两个或多个不同版本的分布式账本，来源于具有单一历史的共同起点</p>	<p>ledger split</p> <p>fork;</p> <p>creation of two or more different versions of a distributed ledger originating from a common starting point with a single history</p>
<p>Merkle 根</p> <p>Merkle 树的根节点</p>	<p>Merkle root</p> <p>root node of a Merkle tree</p>
<p>Merkle 树</p> <p>树数据结构，其中每个叶节点都用数据元素的哈希值标记，每个非叶节点都用其子节点标签的哈希值标记</p>	<p>Merkle tree</p> <p>tree data structure in which every leaf node is labelled with the hash value of a data element and every non-leaf node is labelled with the hash value of the labels of its child nodes</p>
<p>矿工</p> <p>从事挖矿的 DLT 节点</p>	<p>miner</p> <p>DLT node which engages in mining</p>
<p>挖矿</p> <p>在某些共识机制中，创建和验证区块或验证账本记录的活动</p>	<p>mining</p> <p>activity, in some consensus mechanisms, that creates and validates blocks or validates ledger record</p>

节点 构建数据结构的基本组件	node elementary component from which a data structure is built
随机数 在一组密码操作中使用一次的数字或位串	nonce number or bit string used once in a set of cryptographic operations
链外 与区块链系统相关，但位于、执行或运行在该区块链系统之外	off-chain related to a blockchain system, but located, performed, or run outside that blockchain system
账外 与 DLT 系统相关，但位于、执行或运行在该 DLT 系统之外	off-ledger related to a DLT system, but located, performed, or run outside that DLT system
链上 在区块链系统内定位、执行或运行	on-chain located, performed, or run inside a blockchain system
账上 在 DLT 系统内定位、执行或运行	on-ledger located, performed, or run inside a DLT system
对等网络 关联、使用或成为平等对等网络，直接相互共享信息和资源，而不依赖于中央实体	peer-to-peer relating to, using, or being a network of equal peers that share information and resources with each other directly without relying on a central entity
许可 需要授权执行特定活动	permissioned requiring authorization to perform a particular activity or activities
免许可 DLT 系统 免许可分布式账本系统； 免许可分布式账本技术系统； 免许可分布式账本系统	permissioned DLT system permissioned distributed ledger system permissioned distributed ledger technology system DLT system in which permissions are required
私有 DLT 系统 私有分布式账本系统； 私有分布式账本技术系统； DLT 系统仅供有限的 DLT 用户使用	private DLT system private distributed ledger system; private distributed ledger technology system; DLT system that is accessible for use only to a limited group of DLT users
私钥 实体的非对称密钥对的密钥，该密钥是保密的，只能由该实体使用	private key key of an entity's asymmetric key pair that is kept secret and which should only be used by that entity
修剪 通过删除所有满足指定标准的交易记录，同时确保在需要时可以完整地恢复这些交易，从而生成分布式账本的较小副本	prune produce a smaller replica of a distributed ledger by removing all transaction records meeting specified criteria while ensuring that those transactions can be restored with integrity if needed
公共 DLT 系统	public DLT system

公共分布式账本系统； 公共分布式账本技术系统； 可供公众使用的分布式账本技术系统	public distributed ledger system; public distributed ledger technology system; DLT system which is accessible to the public for use
公钥 可以公开的、实体的对称密钥对	public key key of an entity's asymmetric key pair which can be made public
公钥密码学 公钥和相应的私钥分别用于加密和解密，或分别用于数字签名和验证数字签名的密码学	public-key cryptography cryptography in which a public key and a corresponding private key are used for encryption and decryption, or are used for verifying digital signatures and digitally signing, respectively
记录 组织或个人为履行法律义务或在业务交易中作为证据和资产创建、接收和维护的信息	record 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
奖励制度和激励机制 为与 DLT 系统运行有关的某些活动提供奖励的方法	reward system and incentive mechanism method of offering reward for some activities concerned with the operation of a DLT system
根节点 没有父节点的节点	root node node that has no parent node
共享账本 分布式账本记录的内容可由多个实体访问	shared ledger distributed ledger in which the content of ledger records is accessible by multiple entities
侧链 区块链系统与单独的关联区块链系统互操作，以执行与关联区块链系统相关的特定功能	sidechain blockchain system that interoperates with a separate associated blockchain system to perform a specific function in relation to the associated blockchain system
智能合约 存储在 DLT 系统中的计算机程序，其中任何程序执行的结果都记录在分布式账本上	smart contract computer program stored in a DLT system wherein the outcome of any execution of the program is recorded on the distributed ledger
软分叉 更改为不是硬分叉的 DLT 平台，其中 DLT 节点使用旧版本 DLT 平台创建的某些记录或块不被使用新版本 DLT 平台的 DLT 节点接受	soft fork change to a DLT platform that is not a hard fork and in which some records or blocks created by the DLT nodes using the old version of the DLT platform are not accepted as valid by DLT nodes using new versions of the DLT platform
子链 逻辑上独立的链，可以构成区块链系统的一部分	subchain logically separate chain that can form part of a blockchain system
时间戳 时变参数，表示与公共时间参考有关的时间点	timestamp time variant parameter which denotes a point in time with

	respect to a common time reference
代币 代表权利集合的数字资产	token digital asset that represents a collection of entitlements
交易 工作过程的最小单元，是产生符合管理规则的结果所需的一个或多个行动序列	transaction smallest unit of a work process, which is one or more sequences of actions required to produce an outcome that complies with governing rules
交易费 向矿工或验证者支付的将交易纳入分布式分类账的费用	transaction fee fee paid to miners or validators for inclusion of a transaction in a distributed ledger
交易记录 所有交易类型的记录	transaction record record documenting a transaction of any type
信任 用户或其他利益相关者对产品或系统按照预期运行的信心程度	trust degree to which a user or other stakeholder has confidence that a product or system will behave as expected by that user or other stakeholder
已验证 一个实体在其所需的完整性条件已被检查时的状态	validated status of an entity when its required integrity conditions have been checked
验证 验证交易、分类账记录或区块的功能	validation function by which a transaction, ledger record, or block is validated
验证器 DLT 系统中参与验证的实体	validator entity in a DLT system that participates in validation
钱包 用于生成、管理、存储或使用私钥和公钥的应用程序	wallet application used to generate, manage, store or use private and public keys

参 考 文 献

[1] GB/T 15843.1-2017 信息技术 安全技术 实体鉴别 第1部分：总则

[2] GB/T 15843.2-2017 信息技术 安全技术 实体鉴别 第2部分：采用对称加密算法的机制

[3] GB/T 15843.3-2016 信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制

[4] GB/T 15843.4-2008 信息技术 安全技术 实体鉴别 第4部分：采用密码校验函数的机制

[5] GB/T 15843.5-2005 信息技术 安全技术 实体鉴别 第5部分：使用零知识技术的机制

[6] GB/T 15843.6-2018 信息技术 安全技术 实体鉴别 第6部分：采用人工数据传递的机制

[7] GB/T 17901.1-2020 信息技术 安全技术 密钥管理 第1部分：框架

[8] GB/T 17901.3-2021 信息技术 安全技术 密钥管理 第3部分：采用非对称技术的机制

[9] GB/T 20520-2006 信息安全技术 公钥基础设施 时间戳规范

[10] GB/T 30272-2021 信息安全技术 公钥基础设施 标准符合性测评

[11] GB/T 32905-2016 信息安全技术 SM3 密码杂凑算法

[12] GB/T 32907-2016 信息安全技术 SM4 分组密码算法

[13] GB/T 32915-2016 信息安全技术 二元序列随机性检测方法

[14] GB/T 32918.1-2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第1部分：总则

[15] GB/T 32918.2-2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第2部分：数字签名算法

[16] GB/T 32918.3-2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第3部分：密钥交换协议

[17] GB/T 32918.4-2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第4部分：公钥加密算法

[18] GB/T 32918.5-2017 信息安全技术 SM2 椭圆曲线公钥密码算法 第5部分：参数定义

[19] GB/T 36626-2018 信息安全技术 信息系统安全运维管理指南

[20] GB/T 37092-2018 信息安全技术 密码模块安全要求

[21] GB/T 38625-2020 信息安全技术 密码模块安全检测要求

[22] YD/T 3747-2020 区块链技术架构安全要求

[23] ISO 22738-2020 Intelligent transport systems — Localized communications — Optical camera communication - First Edition

[24] ISO 8000-2:2020 Data quality — Part 2: Vocabulary 2020-06-09

[25] ISO/TS 8000-311:2012 Data quality — Part 311: Guidance for the application of product data quality for shape

[26] ISO TR 23244-2020 Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations - First edition

[27] ISO TR 23455-2019 Blockchain and distributed ledger technologies - Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems - First edition

[28] ISO TR 23576-2020 Blockchain and distributed ledger technologies — Security management of digital asset custodians - First edition

[29] 《中华人民共和国网络安全法》

- [30] 《中华人民共和国密码法》
 - [31] 《区块链信息服务管理规定》
-