

电 子 商 务 团 体 标 准

T/ZEA 004 —2020

区块链电子合同平台服务规范

Specifications of electronic contract service platform based on
blockchain

2020 - 5 - 8 发布

2020 - 5 - 8 实施

浙江省电子商务促进会 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 建设原则..... | 3 |
| 5 平台架构和功能框架..... | 3 |
| 6 功能基本要求..... | 4 |

前 言

本标准依据GB/T 1.1-2009给出的规则起草。

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

本标准由浙江省商务厅提出并归口。

本标准主要起草单位：浙江省电子商务促进中心，杭州趣链科技有限公司，浙江大学区块链研究中心，浙江省区块链技术研究院，浙江省标准化研究院，浙商银行股份有限公司，浙江之江企业征信服务有限公司，杭州天谷信息科技有限公司。

本标准主要起草人：蔡亮、沈霞俊、李伟、陈晓丰、郑佩玉、施珍、周莹、谢杨洁、张帅、施进、宋士正、杨国正、臧铖、周益群。

区块链电子合同平台服务规范

1 范围

本标准规定区块链电子合同平台建设原则，平台架构和功能框架，以及功能基本要求。

本标准适用于指导区块链服务供应商结合电子合同的业务流程，将区块链的优点和特性融入到传统电子合同平台中，开发和设计防篡改、全流程可追溯的区块链电子合同平台，同时为需要合同服务的企业提供选择原则和参考依据，为监管机构提供合同追踪和审计。

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 36298-2018 | 电子合同订立流程规范 |
| SB/T 11009-2013 | 电子合同在线订立流程规范 |
| GB/T 9387.2-1995 | 信息处理系统 开放系统互联 基本参考模型 |

3 术语和定义

以下术语和定义适用于本文件。

3.1

区块链 blockchain

一项新型的分布式技术，核心内容包括对等网络、共识机制、分布式存储、点对点传输等技术，具有去中心化、防篡改、可追溯的特性。

3.2

上链 on-chain

业务相关方向区块链系统发起一次请求，区块链节点将相关数据写入到区块链系统中。

3.3

哈希 hash

数据的“指纹”，数据经哈希算法的输出。通过哈希算法可将任意长度的输入计算成固定长度的输出，且输出具有工程意义上的唯一性和不可逆性。

3.4

校验 verify

通过对待校验的数据内容进行哈希计算，并将其与区块链系统中存储的哈希进行对比，确认数据是否与上链时一致。

电子合同 electronic contract

平等主体的自然人、法人、其他组织之间以数据电文为载体，并利用电子通信手段设立、变更、终止民事权利义务关系的协议。

[GB/T 36298-2018, 定义3.1]

3.5

要约 offer

希望和他人订立合同的意思表示。

[GB/T 36298-2018, 定义3.2]

3.6

受要约 accept offer

接受要约的意思表示。

[GB/T 36298-2018, 定义3.3]

3.7

电子合同要约人 electronic contract offeror

在订立电子合同的过程中，发出要约的一方当事人。

[GB/T 36298-2018, 定义3.4]

3.8

电子合同受要约人 electronic contract offeree

在订立电子合同的过程中，接受要约的一方当事人。

[GB/T 36298-2018, 定义3.5]

3.9

电子合同缔约人 electronic contract party

使用电子合同订立系统的合同当事人，简称合同缔约人在。

[SB/T 11009-2013, 定义3.4]

3.10

电子合同缔约相对人 electronic contract relative party

与电子合同缔约人共同签署合同的人，简称合同缔约相对人。

[SB/T 11009-2013, 定义3.5]

3.11

区块链电子合同平台 blockchain-based electronic contract platform

独立于合同缔约人，具备身份认证、谈判磋商、电子签名、合同存储与调用、信息上链、操作记录上链、区块链数据查询等功能，基于区块链技术能实现电子合同在线订立及处理的信息系统。

3.12

电子签名 electronic signature

数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

[GB/T 36298-2018, 定义3.9]

3.13

数字证书 digital certificate

附加在数据单元上的一些数据，或是对数据单元所作的密码变换，这种数据和变换允许数据单元接收者用以确认数据单元来源和数据单元的完整性，并保护数据，防止被人（例如接收者）进行伪造。

[GB/T 9387.2-1995, 定义3.3.26]

4 建设原则

4.1 完整性

区块链电子合同平台服务应覆盖包括电子合同订立、签署、履行、查询、校验等过程，针对每个过程的数据提供上链支持、区块链数据查询支持，且针对每个环节均有详细的功能支持。

4.2 安全性

区块链电子合同平台服务应提供覆盖电子合同数据存储、传输等过程中的安全机制，确保用户数据的隐私性与安全性。对已上链的数据，任何用户、任何机构无权通过任何方式篡改数据。

4.3 可用性

区块链电子合同平台服务应具备可用性，包括功能完整、流程科学、操作简便等。

4.4 易拓展性

区块链电子合同平台服务应具备易拓展性，包括功能模块易拓展性和区块链的易拓展性。

5 平台架构和功能框架

5.1 参考平台架构

平台利用电子签章实现合同有效签署，同时利用区块链不可篡改性的特性对合同进行有效存证，并将重要信息与重要操作记录上链，有效追溯合同信息，防止抵赖。平台架构如图1所示：

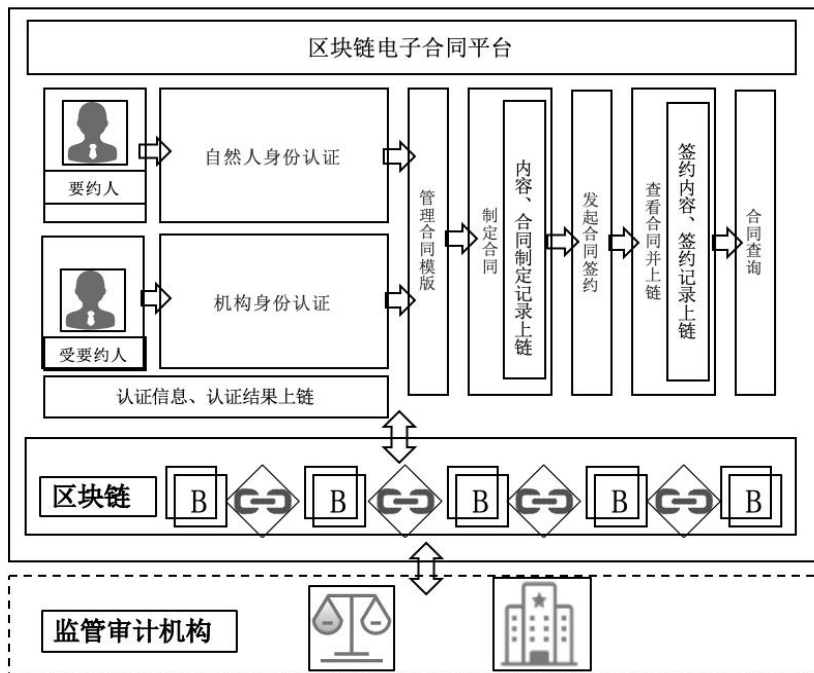


图 1 区块链电子合同参考平台架构

5.2 参考功能框架

区块链电子合同服务应提供覆盖电子合同及区块链相关的完整功能，包括区块链管理、用户身份管理、电子合同生命周期管理、电子合同管理、系统维护和监管审计。功能框架如图2所示：

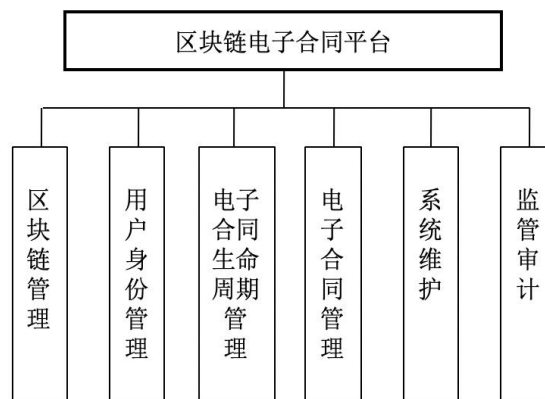


图 2 区块链电子合同平台参考功能框架

6 功能基本要求

6.1 区块链管理

区块链管理的功能设计应包括数据管理、节点管理、运行监控等。

6.1.1 数据管理

区块链电子合同平台应支持区块数据管理，支持用户查看区块链上区块信息、交易信息等。

6.1.2 节点管理

区块链电子合同平台应支持区块链节点管理。区块链节点管理功能应包括但不限于：

- a) 支持用户新增区块链节点；
- a) 支持用户删除区块链节点。

6.1.3 运行监控

区块链电子合同平台应支持区块链运行状态的监控。区块链运行监控功能应包括但不限于：

- a) 支持对于区块链各节点运行状态的监控，查看节点实时运行状态和所在服务器资源使用情况等；
- b) 支持对区块高度、区块交易信息的监控，使拥有权限的用户可通过图形化界面直观看到区块信息交易信息。

6.2 用户身份管理

用户身份管理的功能设计应包括登记、认证、变更与注销等。

6.2.1 登记

区块链电子合同平台支持对于用户（电子合同要约人和电子合同受要约人）的身份登记，并将身份信息上链。身份登记功能应包括但不限于：

- a) 支持对于用户（电子合同要约人和电子合同受要约人）所包含的自然人及其所属机构等的身份信息进行登记；
- b) 支持将用户（电子合同要约人和电子合同受要约人）身份信息通过私钥签名后上链，并反馈给用户此次存储所在的区块以及交易信息；
- c) 支持对于身份登记过程中所设计的相关证明文件进行上传，上传文件应采用如 JPG、JPEG、PNG、PDF 等较为通用的文件存储格式；
- d) 支持身份登记过程中上传的所有信息通过私钥签名后进行上链，并反馈给用户此次存储所在的区块以及交易信息；
- e) 支持用户查询已上链的身份信息；
- f) 在用户（电子合同要约人和电子合同受要约人）确认提交身份登记申请的情况下，提供对于身份登记信息的审核机制，对身份登记信息的完整性、合法性进行验证。并支持以系统通知或电子邮件等书面方式向用户（电子合同要约人和电子合同受要约人）发送身份登记结果的通知；

6.2.2 认证

区块链电子合同平台应支持通过身份登记并需要签署合同的用户（电子合同要约人和电子合同受要约人）进行身份认证，并将认证结果上链。身份认证功能应包括但不限于：

- a) 对于持有数字证书的用户（电子合同要约人和电子合同受要约人），支持对数字证书的状态、有效期等内容进行审核；
- b) 对于持有数字证书的用户（电子合同要约人和电子合同受要约人），支持将数字证书的状态、有效期等内容上链；

- c) 对于未持有数字证书的用户（电子合同要约人和电子合同受要约人），平台应提供合法、可靠的认证方式进行审核；
- d) 支持以系统通知或电子邮件等书面方式向用户（电子合同要约人和电子合同受要约人）发送身份认证结果的通知；
- e) 对身份认证结果通过私钥签名后上链，并反馈给用户此次存储所在的区块以及交易信息。并对认证通过的用户（电子合同要约人和电子合同受要约人）发放用户区块链私钥，用于调用区块链时的身份验证；
- f) 支持用户（电子合同要约人和电子合同受要约人）查询链上存储的身份认证结果；
- g) 支持用户（电子合同要约人和电子合同受要约人）下载用户区块链私钥，管理私钥。

6.2.3 变更与注销

区块链电子合同平台应支持对于通过身份登记及身份认证的用户（电子合同要约人、电子合同受要约人、电子合同缔约人、电子合同缔约相对人）进行身份信息变更与注销。身份信息变更与注销功能应包括但不限于：

- a) 提供对于提出变更或注销申请的用户（电子合同缔约人、电子合同缔约相对人）进行合同履行情况的审核；
- b) 支持对于用户（电子合同要约人、电子合同受要约人、电子合同缔约人、电子合同缔约相对人）的自然人以及所属机构等身份信息进行变更；
- c) 支持对于身份变更过程中所涉及的相关证明文件进行上传，上传文件应采用较为通用的文件存储格式；
- d) 支持以站内信或电子邮件等方式向用户（电子合同要约人和电子合同受要约人）发送身份认证结果的通知；
- e) 支持将变更申请记录、变更上传的证明文件、以及变更审核结果通过私钥签名后上链，并反馈给用户此次存储所在的区块以及交易信息；
- f) 支持用户（电子合同要约人、电子合同受要约人、电子合同缔约人、电子合同缔约相对人）查看区块链上的变更申请记录、变更上传的证明文件、以及变更审核结果。

6.3 电子合同生命周期管理

电子合同生命周期处理的功能设计应包括创建、签署、变更、延续、终止等。

6.3.1 创建

电子合同生命周期管理的过程中，需将每一步的操作记录、操作数据上链。区块链的共识机制、加密机制保证了存储在区块链上的数据安全可靠，真正实现数据防篡改。

6.3.1.1 签署申请

在创建电子合同过程中，区块链电子合同平台应支持对于用户（电子合同要约人和电子合同受要约人）在平台中提出电子合同的签署申请的审核。签署申请环节的功能应包括但不限于：

- a) 受理用户（电子合同要约人和电子合同受要约人）所发出的签署申请，将签署申请信息通过私钥签名后上链，并以站内信或电子邮件等方式向用户发送受理通知；
- b) 对提交电子合同签署申请的用户（电子合同要约人和电子合同受要约人）的身份登记信息的审核；

- c) 支持将签署申请审核结果通过私钥签名后上链，并反馈给用户（电子合同要约人和电子合同受要约人）此次存储所在的区块以及交易信息；
- d) 支持用户（电子合同要约人和电子合同受要约人）查询到链上的审核结果。

6.3.1.2 合同起草

电子合同签署申请通过后，平台应支持用户（电子合同）调用电子合同起草功能模块，并将电子合同信息上链，其功能应包括但不限于：

- a) 支持各类型电子合同模板预览，用户（电子合同）可根据业务需求进行选择；
- b) 支持各类型电子合同模板通过私钥签名后上链，并可查询链上的电子合同模板信息；
- c) 根据用户（电子合同要约人）选择的合同模板，生成电子合同的起草页面，并允许用户（电子合同要约方）填写合同信息；
- d) 在电子合同的起草页面中，禁止用户（电子合同要约人）对无权修改的合同信息进行修改。同时，允许用户（电子合同要约人）对可修改的合同信息进行修改；
- e) 支持在电子合同起草页面中将电子合同要约人的地址、法定代表人、联系电话等必填信息向用户（电子合同要约人）发出提示；
- f) 支持用户（电子合同要约人）上传附件（包括文本、图片）；
- g) 完成创建电子合同并提交时，支持对合同信息的完整性、正确性以及上传附件的格式进行自动审核。如果通过审核，应向用户（电子合同要约人）进行告知。如果合同信息及上传附件存在缺失、错误等问题，应向用户（电子合同要约人）发出警报；
- h) 对电子合同信息上链与审核结果上链，并反馈给用户（电子合同要约人和电子合同受要约人）此次存储所在的区块以及交易信息；
- i) 支持用户（电子合同要约人和电子合同受要约人）查询链上的电子合同信息与审核结果；
- j) 支持用户（电子合同要约人和电子合同受要约人）对处于“协商中”状态的电子合同的信息进行修改，并重新提交；
- k) 支持电子合同修改信息通过私钥签名后上链，修改记录上链，并反馈给用户（电子合同要约人和电子合同受要约人）此次存储所在的区块以及交易信息；
- l) 支持用户（电子合同要约人和电子合同受要约人）查询链上的电子合同修改信息与修改记录。

6.3.2 签署

用户（电子合同要约人和电子合同受要约人）对合同信息达成一致，平台应支持用户（电子合同要约人和电子合同受要约人）调用签署合同功能模块，支持签署信息上链，其功能应包括但不限于：

- a) 提供电子数据安全机制，支持电子合同进行电子签名，以保证电子合同的安全性；
- b) 根据业务需求，支持添加时间戳，以保证电子合同的有效性；
- c) 在用户（电子合同要约人和电子合同受要约人）授权情况下，支持合同的委托代签；
- d) 签署完成的电子合同，平台应支持自动分配唯一编号，确定操作权限；
- e) 对签署完成的电子合同信息通过私钥签名后上链，签署记录通过私钥签名后上链，并反馈给用户（电子合同要约人和电子合同受要约人）此次存储所在的区块以及交易信息；
- f) 支持用户（电子合同要约人和电子合同受要约人）查询已上链的电子合同信息与签署记录；
- g) 根据电子合同类型，应按照监管部门的要求，将完成签署的电子合同数据通过合法途径获得，并向相关监管部门提交进行审查。

6.3.3 变更

用户（电子合同要约人和电子合同受要约人）对正在履行的电子合同的相关内容信息进行变更，其功能应包括但不限于：

- a) 支持对提出申请的用户（电子合同缔约人或电子合同缔约相对人）的身份进行验证，若身份验证不合格，应不受理申请，并向用户（电子合同缔约人或电子合同缔约相对人）发出警报；
- b) 支持对于电子合同状态不符合要求的情况（如：电子合同已终止），应不受理申请，并向用户（电子合同缔约人或电子合同缔约相对人）发出警报；
- c) 支持将变更申请记录通过私钥签名后上链，并反馈给用户（电子合同要约人和电子合同受要约人）此次存储所在的区块以及交易信息；
- d) 支持对电子合同的内容进行编辑，即：变更申请通过，允许提出变更申请的一方对电子合同中允许用户修改的部分进行变更。修改完成，应通知对方，若对方同意变更内容，则提交合同进行审核；
- e) 支持将变更信息与变更审核记录通过私钥签名后上链，并反馈给用户（电子合同要约人和电子合同受要约人）此次存储所在的区块以及交易信息；
- f) 支持用户（电子合同要约人和电子合同受要约人）查询链上的变更申请记录、变更信息、变更审核记录；
- g) 如果缔约双方所签署的合同内容不同于正在履行的合同，系统应提示其重新创建合同，并在新电子合同完成签署后，将原电子合同终止。

6.3.4 延续

用户（电子合同要约人和电子合同受要约人）对正在履行的合同申请延续，其功能应包括但不限于：

- a) 支持对提出申请的用户（电子合同缔约人或电子合同缔约相对人）的身份进行验证，若身份验证不合格，应不受理申请，并向用户（电子合同缔约人或电子合同缔约相对人）发出警报；
- b) 支持对于电子合同状态不符合要求的情况（如：电子合同已终止），应不受理申请，并向用户（电子合同缔约人或电子合同缔约相对人）发出警报；
- c) 支持对电子合同的内容进行编辑，即：变更申请通过，允许提出变更申请的一方对电子合同中允许用户修改的部分进行变更。修改完成，应通知对方，若对方同意变更内容，则提交合同进行审核；
- d) 支持将变更申请信息与变更记录通过私钥签名后上链，并反馈给用户（电子合同缔约人或电子合同缔约相对人）此次存储所在的区块以及交易信息；
- e) 支持用户（电子合同缔约人或电子合同缔约相对人）查询链上的变更申请信息与变更记录；
- f) 如果缔约双方所签署的合同内容不同于正在履行的合同，系统应提示其重新创建合同，并在新电子合同完成签署后，将原电子合同终止。且将此次签署记录通过私钥签名后上链，并可查询链上的此次签署记录。

6.3.5 终止

用户（电子合同缔约人或电子合同缔约相对人）对正在履行的合同提出终止申请，其功能应包括但不限于：

- a) 支持对提出申请的用户（电子合同缔约人或电子合同缔约相对人）的身份进行验证，若身份验证不合格，应不受理申请，并发出警报；
- b) 支持对于合同状态不符合要求的情况（如：合同已终止），应不受理申请，并向用户（电子合同缔约人或电子合同缔约相对人）发出警报；
- c) 支持提出申请的用户（电子合同缔约人或电子合同缔约相对人）进行终止原因的填写；

- d) 支持将终止申请信息与终止申请记录上通过私钥签名后链，并可查询链上对应的终止申请信息与终止申请记录；
- e) 支持缔约双方对终止合同的操作进行确认；
- f) 支持将终止申请确认结果与确认记录通过私钥签名后上链，并反馈给用户（电子合同缔约人或电子合同缔约相对人）此次存储所在的区块以及交易信息；
- g) 支持用户（电子合同缔约人或电子合同缔约相对人）查询链上对应的终止申请确认结果与确认记录。

6.4 电子合同管理

电子合同管理应包括电子合同验证、谈判、归档、阅览、查询、统计等。

6.4.1 验证

为确保电子合同的真实性、有效性以及完整性, 应提供离线或在线两种方式对于电子合同中的电子签名、数字证书、电子合同内容、电子合同要约人信息、电子合同受要约人信息等进行验证, 且支持验证结果及验证记录上链, 并可查看对应的验证结果及验证记录。

6.4.2 谈判

电子合同管理系统宜提供在线谈判服务, 其功能可包括但不限于:

- a) 支持链上谈判双方身份信息查看;
- b) 支持链上谈判内容的实时记录, 并对谈判内容进行保密;
- c) 支持链上查询谈判内容。

6.4.3 归档

电子合同缔约双方完成合同签署后, 系统应支持对电子合同进行归档操作, 并支持将归档的电子合同上链, 其功能应包括但不限于:

- a) 按照已配置的分类方案可对电子合同进行自动分类, 无法进行自动分类的合同系统应支持手动分类;
- b) 自动审核待归档电子合同等信息的完整性, 如有缺失, 应支持手动补充;
- c) 对自动分类的电子合同与手动分类的电子合同通过私钥签名后上链, 并可查询链上的电子合同归档信息。

6.4.4 阅览

系统应支持对于合同信息进行阅览, 并提供打印服务, 其功能应包括但不限于:

- a) 支持在线阅读和离线阅读两种模式;
- b) 允许对在线阅读所运用的嵌入式组件的外观进行设置, 以保证组件与系统应用环境的协调性;
- c) 支持在线阅读功能运行状态的实时监控;
- d) 支持对电子合同的在线打印;
- e) 支持对于电子合同文本的下载。

6.4.5 查询

系统应提供电子合同查询、查询结果浏览以及管理等服务, 其功能应包括但不限于:

- a) 支持全文查询、条件查询等模式;
- b) 支持签署时间、电子合同缔约人、电子合同缔约相对人、电子合同状态等字段的检索;

- c) 提供查询进度的提示;
- d) 支持对查询结果导出,并设置导出文件的格式。

6.4.6 统计

系统应提供电子合同文件数据统计以及报表生成等服务,其功能应包括但不限于:

- a) 提供按签署时间、合同类型、合同状态等方面进行的统计;
- b) 支持统计结果形成报表;
- c) 支持统计报表的查看、打印和下载。

6.5 系统维护功能

系统维护的功能设计应包括用户管理、权限管理、日志管理、分类方案管理、模板管理、接口管理、安全管理等。

6.5.1 用户管理

应对使用系统的用户进行统一管理,其功能应包括但不限于:

- a) 提供机构、部门、人员表的维护和管理;
- b) 支持对机构、部门、人员信息的创建、修改、删除、查询;
- c) 支持对机构、部门、人员信息的创建记录、修改记录、删除记录上链。

6.5.2 权限管理

为实现用户使用系统功能的访问控制,保证有效用户正常使用的同时,防止非法用户和无权限用户对系统功能的使用及用户数据的访问,其功能应包括但不限于:

- a) 支持对用户的权限进行新增、修改、删除和查询等操作;
- b) 支持设置不同用户的访问和操作权限。

6.5.3 合同模板管理

为保证电子合同签署的便捷化、规范化,系统提供合同模板的管理服务,其功能应包括但不限于:

- a) 支持新增电子合同模板,可对模板名称、类型、适用对象、正文等内容进行编辑;
- b) 支持电子合同模板的预览;
- c) 支持对电子合同模板的修改、删除;
- d) 提供电子合同模板状态管理,包括草稿、启用等。

6.5.4 接口管理

为完善服务功能、提升安全性,系统应提供各类功能接口,应包括但不限于:

- a) 电子合同第三方存储服务商接口;
- b) 电子邮箱接口;
- c) 时间戳接口;
- d) 电子合同验证接口;
- e) 校验数据和链上的数据是否一致的接口。

6.5.5 安全管理

区块链电子合同平台的安全管理应遵循《信息安全等级保护管理办法》的所应用行业的相关规定,建立完善的数据安全防护机制,在保障可用性的基础上为业务数据提供完整性和保密性。

6.6 监管审计

区块链电子合同平台应支持监管审计，监管部门在职权范围内可以调阅存储在区块链上的各种信息，包括合同信息、签署记录、合同变更记录等。

监管部门如互联网法院、公证处等具有监督、公证职能的政府部门。
