中国区块链技术和产业发展论坛标准

CBD-Forum-001-2018

区块链 隐私保护规范

Blockchain—Privacy protection specification

2018-12-18 发布　　2018-12-18 实施

中国区块链技术和产业发展论坛　　发 布

目　　次

前　言

本标准按照 GB/T 1.1-2009 标准化工作导则 第 1 部分：标准的结构和编写给出的规则起草。

本标准由中国区块链技术和产业发展论坛提出。

本标准负责起草单位：深圳前海微众银行股份有限公司、中国电子技术标准化研究院、上海金丘信息科技股份有限公司、上海复星高科技（集团）有限公司、北京京东尚科信息技术有限公司、中国平安保险（集团）有限公司、上海万向区块链股份公司、永辉超市股份有限公司、浙江蚂蚁小微金融服务集团股份有限公司、普华永道中天会计师事务所（特殊普通合伙）、易见供应链管理股份有限公司、厦门安妮股份有限公司。

本标准主要起草人：徐磊、李斌、李鸣、洪蜀宁、韩峰、鞠鹏、张林、王招军、孙琳、齐宁宁、韩梅、王梦寒、张宝、张卫中、陈家乐、马光磊、李雷、孙曦、郭亦卓、华静娴、刘天成、郝汉、杨胜。

使用帮助信息：任何单位和个人在使用本标准的过程中，若存在疑问，或有对本标准的改进建议和意见，请与中国电子技术标准化研究院（中国区块链技术和产业发展论坛　秘书处）联系。

电话：010-64102801/2804

电子邮件：cbdforum@cesi.cn

通信地址：北京东城区安定门东大街 1 号（100007）

为了推动本标准的持续改进，使其内容更加贴近用户组织的实际需求，欢迎社会各方力量参加本标准的持续改进，本标准的更多信息欢迎关注中国区块链技术和产业发展论坛官方网站和公众号。

http://www.cbdforum.cn

区块链 隐私保护规范

1 范围

本标准规定了区块链隐私保护，包括如下内容：

a) 区块链隐私保护的原则；

b) 隐私保护的关注点；

c) 隐私保护的管理要求；

d) 隐私保护的监管和审计要求。

注：隐私保护策略与技术参见附录 A。

本标准适用于：

a) 为计划使用区块链系统的组织和机构选择和使用区块链服务提供隐私保护的参考；

b) 指导区块链系统提供方在区块链系统中建立区块链隐私保护机制；

c) 第三方评价区块链系统服务提供方的隐私保护能力。

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。凡是注明日期的引用文件，仅注明日期的版本适用于本文件。凡是不注明日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 5271.18-2008 信息技术 词汇

GB/T 11457-2006 信息技术软件 工程术语

GB/T 25069-2010 信息安全技术 术语

GB/T 32399-2015 信息技术 云计算

GB/T 35273-2017 信息安全技术 个人信息安全规范

JR/T 0167-2018 云计算技术金融应用规范 安全技术要求

ISO/IEC 27000 信息技术 安全技术信息安全管理体系 概述和词汇（Information technology-Security techniques-Information security management systems-Overview and vocabulary）

ISO/IEC 38505-1:2017 信息技术 IT 治理数据治理第 1 部分 :ISO/IEC 38500 在数据治理中的应用（Information technology-Governance of IT-Governance of data-Part 1: Application of ISO/IEC 38500 to the governance of data）

3 术语和定义

GB/T 35273-2017 界定的以及下列术语和定义适用于本文件。

3.1

个人标识信息 personally identifiable information

能够单独或者与其他信息组合以识别、追踪到特定自然人身份或反映特定自然人活动情况的信息。

3.2

隐私 privacy

与公共利益无关，除了只能公开于有保密义务的一方之外，当事人不愿第三方知道的个人信息及当事人不愿第三方侵入的个人领域。

注：隐私的三条要素包括：

——隐私的主体是自然人；

——隐私的客体是自然人的个人信息和个人领域；

——隐私的内容指特定个人对其信息或领域秘而不宣、不愿他人探知或干涉的事实或行为。

3.3

隐私数据 privacy data

特定自然人的个人标识信息及其在区块链系统的活动信息。

3.4

隐私主体 privacy principal

个人标识信息所标识的特定自然人。

3.5

隐私控制者 privacy controller

可决定隐私数据处理目的、方式等的组织或个人，并承担处理数据的责任。

3.6

隐私处理者 privacy processor

根据隐私控制者指示，对隐私数据进行处理的组织或个人。

3.7

隐私利益相关方 privacy stakeholder

隐私数据在被处理的过程中所影响到的自然人、法人或任何组织。

3.8

隐私披露 privacy disclose

将隐私主体的隐私数据发布给社会或不特定人群的行为。

3.9

隐私侵犯 privacy breach

在违反隐私保护准则的情况下处理或泄露隐私数据的行为。

3.10

隐私保护 privacy protection

致力于隐私数据受到妥善的保护，避免不必要的泄露。

3.11

隐私保护技术 privacy enhancing technology

在保持信息系统正常运作的同时，用以减少或消除隐私数据泄露、避免隐私数据被非正当处理利用的信息技术手段、产品或服务。

注：隐私保护技术包括但不局限于将隐私数据匿名化、去标识化、伪装化的工具。

3.12

隐私偏好 privacy preference

隐私主体关于如何处理其隐私数据的特定选择。

3.13

隐私策略 privacy policy

隐私控制者在关于处理隐私数据时所正式表达的一系列原则、意图、方式或承诺。

4 缩略语

下列缩略语适用于本文件

API：应用程序接口（Application Programming Interface）

5 原则

5.1 个人信息安全基本原则

区块链隐私保护应遵循 GB/T 35273-2017 中第 4 章“个人信息安全基本原则”。

5.2 最小授权原则

最小授权原则是指授权对象最小、授权数据内容最小、授权权限最小和授权时间最小原则。具体内容如下：

a) 授权对象最小是指仅将隐私数据授权给职责范围内或应用场景涉及的相关方；
b) 授权数据内容最小是指仅将涉及的数据内容授权给相关方；
c) 授权权限最小是指仅将职责范围内或应用场景需要的数据操作权限授权给相关方；
d) 授权时间最小是指仅在必要的时间范围内将隐私数据授权给相关方。

5.3 明示同意原则

明示同意原则是指处理隐私数据时，应获得隐私主体的明确授权，具体内容如下：

a) 隐私数据被侵犯时，隐私控制者应及时通知隐私主体；
b) 隐私控制者应依据所声明的处理目的和隐私主体的授权，保留和更新必要的隐私数据，处理目的达成或授权时效过期后应及时删除相关隐私数据；
c) 隐私主体应有权审核和修改其隐私数据；

d) 数据使用方应仅按照明确声明和授权的用途使用隐私数据。

6 主要关注点

区块链隐私保护的关注点包括隐私相关数据收集、数据存储、数据迁移、数据备份与恢复、数据应用、数据披露和数据处置。各关注点间的关系如图 1 所示。

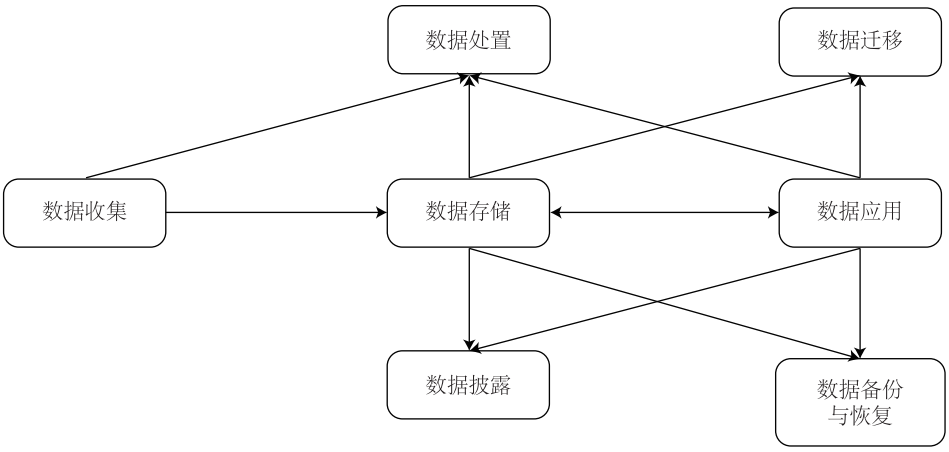

图 1 七个隐私保护关注点的关系

6.1 概述

数据收集的数据经处理后进行存储。存储的数据可提供给应用系统进行处理，也可向社会或不特定人群直接或通过应用系统进行披露。应用系统处理后产生的数据可根据需要记录到区块链上。数据收集、数据存储和数据应用中所产生的隐私数据，可根据隐私主体的要求进行数据处置等操作。

本标准重点关注数据收集、数据存储、数据应用、数据披露和数据处置的隐私保护。

6.2 数据收集

数据收集是隐私控制者获取隐私主体的隐私数据，并发布给其他节点的过程。该过程应符合 GB/T 35273-2017 中第 5 章“个人信息的收集”的要求，同时，隐私控制者应符合以下要求：

a) 收集隐私数据前，获得隐私主体的授权同意，并明确告知以下内容：
   1) 产品或服务功能收集的隐私数据类型，以及收集、使用隐私数据的规则，如收集和使用隐私数据的目的、收集方式和频率、存储地域和期限、对外共享、转让、公开披露的有关情况等；
   2) 其他节点的隐私数据共享形式和约束，如智能合约内容、隐私政策、区块链加密机制等；
   3) 隐私控制者可能获取隐私主体未授权信息和因区块链的特殊性而产生的隐私风险等；
   4) 明确告知区块链的基本情况，如区块链类型、区块链选取机制，智能合约内容等。
b) 收集隐私数据后：
   1) 通过密钥对隐私数据进行加密处理；
   2) 将加密后的隐私数据与密钥分开存储；
   3) 密钥发送至隐私主体后，明确告知其妥善保管密钥。

6.3 数据存储

数据存储是指将隐私数据保存在节点中的过程，包括但不限于打包生成区块、广播区块至其他节点、获取密钥解密隐私数据等。

区块链隐私数据存储时，应符合 GB/T 35273-2017 中第 6.3 节“个人敏感信息的传输和存储”的要求，隐私控制者应符合以下要求：

a) 打包的隐私数据解密前获得隐私主体的授权同意，并明确告知解密的隐私数据类型及用途；
b) 停止运营其产品或服务时，及时停止继续收集隐私数据的活动，并通知隐私主体。对所持有的隐私数据进行处置，并向其他节点发布已停止运营和处置隐私数据的消息；
c) 以适当方式处置解密后的隐私数据，并向其他节点发布已处置该数据的消息。

6.4 数据应用

数据应用是指对解密后的隐私数据进行使用、修改、更新和处置等操作的过程。

区块链隐私数据应用应符合 GB/T 35273-2017 中第 7 章“个人信息的使用”的要求，同时应符合以下要求：

a) 默认采用密文展示隐私数据，除该客户端或应用系统已获取隐私数据的授权。非密文展示应对隐私数据采取去标识化措施；
b) 使用隐私数据时，明确记录使用者、使用数据内容以及使用频率等信息；
c) 访问隐私数据时，明确记录访问者、访问数据内容以及访问时间等信息。

6.5 数据披露

隐私数据披露应符合 GB/T35273-2017 中第 8 章“个人信息的委托处理、共享、转让、公开披露”的要求，同时应符合以下要求：

a) 在区块链平台以密文格式存储敏感的个人标识信息；
b) 在多方数据共享的场景下，以密文格式共享个人标识信息。

6.6 数据处置

数据处置是指隐私主体授意或隐私控制者因业务需要将隐私数据设置为不可用的过程。对于存储在区块链节点的隐私数据，可通过删除密钥等技术手段确保隐私数据不可用。

7 隐私保护管理要求

7.1 日常管理要求

区块链隐私保护的日常管理要求如下：

a) 隐私控制者应完善组织管理制度，加强隐私保护管理，应符合 GB/T35273-2017 中第 10 章“组织的管理要求”，或 JR/T0167-2018 中第 10 章“安全管理功能”的要求；
b) 隐私控制者应确定隐私保护管理部门，明确相应的主体责任，建立完善的隐私保护策略，符合监管方的要求，定期审查隐私保护策略的合理性及适用性。

7.2 应急处理要求

区块链隐私保护的应急处理应符合 GB/T35273-2017 中第 9 章“个人信息安全事件处置”的要求，隐私控制者收到隐私侵犯事件报告时应：

a) 核实涉及的信息是否存在于系统中；
b) 根据可适用的法律、法规及管理规定，明确该信息是否属于隐私信息，是否需要保护；
c) 判定该隐私数据的暴露范围，以及该暴露范围是否符合系统设计规范及相关监管规定，同时评估该事件的严重程度及影响程度；
d) 启动应急预案和整改措施，并及时向隐私主体及监管部门汇报。

8 监管和审计

8.1 监管要求

区块链隐私保护的监管要求包括：

a) 区块链系统在结构设置上，应满足以下要求：
   1) 提供具有特定功能的监管节点和角色；
   2) 提供监管类智能合约的运行环境和接口；
   3) 提供用户实名认证功能。
b) 区块链隐私保护的监管内容包括但不限于：
   1) 数据内容、格式、流程、算法和相关授权方；
   2) 使用的数字证书颁发机构和类型；
   3) 存储隐私数据的节点的开放接口和权限、地理位置。

8.2 审计要求

隐私审计为隐私保护过程提供控制措施，在审计过程中应：

a) 审阅隐私保护策略，发现内部控制薄弱环节；
b) 检查控制执行的支持性文档，确认按照既定设计文档有效地执行隐私保护策略。

附 录 A
（资料性附录）
隐私保护策略与技术

A.1 隐私保护策略

在设计和实现区块链系统时，应考虑提供适当的隐私保护策略，包括但不限于如下内容：

A.1.1 差异化策略

区块链系统的隐私保护，应针对链上和链下数据、不同链上数据、不同安全等级数据，制定差异化的隐私保护策略。

A.1.2 访问控制

在设计和实现区块链系统时，应采取技术措施控制隐私数据的访问权限，并验证数据访问者的身份。

A.1.3 加密策略

根据隐私数据对象的需求设计加密保护方案，确保在区块链系统中传输或存储时，不被未授权用户获取明文信息。

A.1.4 物理分割策略

将隐私数据碎片化，并存储在不同的物理存储上。

A.2 数据存储过程中的保护技术

A.2.1 链外存储

链外存储是将要保护的隐私数据存到非区块链系统中，可以公开的数据记录在链上。通常将原文存到非区块链系统中，对应的摘要信息存到区块链系统中。

A.2.2 账本隔离

账本隔离是将具有不同隐私需求的账本，分别存放到不同的分布式账本上。

A.2.3 加密保护

加密保护是利用密码学算法对账本数据进行加密，使授权的相关方能够解密查看。对应的加密算法包括对称加密、非对称加密、同态加密、模糊的基于身份的加密（Fuzzy Identity-Based Encryption）等。

A.2.4 部分明文

部分明文是将分布式账本数据分为敏感部分与非敏感部分，对敏感部分进行隐私保护。

A.2.5 经许可方式

构建许可（permissioned）账本将区块链的参与者限制在已知的节点范围内，设置节点查看链上数据的权限。

A.3 数据传输过程中的保护技术

在区块链网络中，数据传输的隐私威胁主要来自恶意节点接入网络后可以轻易获得重要数据信息，如节点的 IP 地址、节点间的拓扑关系和传输消息等。隐私保护的重点在于增加攻击者搜集信息的难度。数据传输过程中的常用区块链隐私保护技术如下：

A.3.1 路径混淆

借助可信第三方或某种协议机制，对交易来源和交易去向进行模糊混淆，使攻击者无法通过阅读交易信息获得交易双方的真实信息。

A.3.2 安全信道

利用认证密钥交换协议，如 SSL/TLS 协议，建立节点间的安全通信信道，使用密码算法生成共享会话密钥，然后使用会话密钥对传输消息进行对称加密，来保证消息的机密性和完整性，使攻击者无法窃听到传输内容，并且篡改内容将会被消息接收者发现。

A.3.3 节点检测

使用恶意节点检测方法，快速定位恶意节点，将恶意节点加入黑名单，阻止其搜集敏感信息。

A.4 身份隐私保护技术

身份隐私保护是隐匿区块链系统中用户的身份的过程。

A.4.1 环签名

签名者利用自己的私钥和环中其他人的公钥，独自完成对目标消息的签名，使验签者无法判断签名者的确切身份。

A.4.2 数据混淆

将区块链运行在具有隐私保护特性的网络上，将数据进行多层加密后再传输，防止攻击者获得真实 IP 地址和溯源消息。

A.4.3 隐藏地址

发送者使用接收者的公钥并选取随机数对地址进行加密，密文作为新地址信息，使攻击者无法发现新地址和接收者之间的关系，无法获得接收者相同的多次交易间的关联性，并掩盖接收者身份信息。

A.4.4 零知识证明

证明者向验证者提供关于交易发送者、接收者身份和交易细节的证明，证明内容不透露交易双方身份和交易细节等相关信息。

A.5 隐私保护内容比较

隐私保护技术的保护内容可以是数据发送者或接收者的身份信息，也可以是数据信息机密的本身，

各种技术路线的保护内容比较如表 A.1 所示。

表 A.1　隐私保护技术路线的保护内容比较

技术关注点	技术路线	发送者	接收者	数据信息
数据存储过程	链外存储	×	×	√
	账本隔离	×	×	√
	加密保护	×	×	√
	部分明文	×	×	Λ
	经许可方式	×	×	Λ
数据传输过程	数据混淆	√	×	√
	安全信道	×	×	√
	节点检测	×	×	Λ
身份隐私保护	环签名	Λ	×	×
	路径混淆	√	√	×
	零知识证明	√	√	×
	隐藏地址	×	√	×

注：“√”：能够提供隐私保护；“×”：不能提供隐私保护；“Λ”：能够提供受限的隐私保护

参 考 文 献

[1] GB/T 5271.18-2008 信息技术 词汇

[2] GB/T 11457-2006 信息技术软件 工程术语

[3] GB/T 25069-2010 信息安全技术 术语

[4] GB/T 32399-2015 信息技术 云计算

[5] GB/T 35273-2017 信息安全技术 个人信息安全规范

[6] JR/T 0167-2018 云计算技术金融应用规范 安全技术要求

[7] ISO/IEC 27000 信息技术 安全技术信息安全管理体系 概述和词汇（Information technology-Security techniques-Information security management systems-Overview and vocabulary）

[8] ISO/IEC 38505-1:2017 信息技术 IT 治理数据治理第 1 部分 :ISO/IEC 38500 在数据治理中的应用（Information technology-Governance of IT-Governance of data-Part 1:Application of ISO/IEC 38500 to the governance of data）

CBD-Forum-001-2018

电话：010-64102801/2804
电子邮件：cbdforum@cesi.cn
网址：http://www.cbdforum.cn