ICS 号 03.060
中国标准文献分类号 A11

团 体 标 准

T/HBPFS 001. 6-2022

雄安新区区块链支付平台
第 6 部分：管理规范

The Standard of Xiong'An New Area Blockchain Payment Platform

Part 6：Management Specifications

2022-12-27 发布　　2022-12-27 实施

河北省金融学会　　发 布

目 次

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。区块链支付信息服务是以区块链与智能合约技术为核心，通过业务流程触发形成支付指令，并对接银行支付网关实现资金支付的一种创新性区块链应用。前期，为解决工程建设资金管理场景中从业主体多、业务流程复杂、资金流向监管难等问题，雄安新区已基于上述区块链支付信息服务模式研发应用了工程建设资金管理区块链平台，实现了工程建设资金从业主到总、分包单位的及时、准确与高效拨付，具备按需支付、可信支付、穿透支付和无损支付等特点。根据区块链支付信息服务模式与特点，我们认为该模式亦可在政府资金监管、多级供应链等多个复杂企业支付场景进行应用，具备较好复制与推广应用前景。

为促进雄安新区区块链+支付模式应用，便于政府、银行和企业各方接入区块链支付平台并规范相关接入规范与接口要求，特制定《雄安新区区块链支付平台》。本标准由以下 6 部分构成：

——第 1 部分：参考模型及流程规范，总体阐述区块链支付定义、业务参考模型、技术架构和主要功能介绍；

——第 2 部分：银行接入规范，重点阐述银行接入区块链支付平台的接入方法与接口规范；

——第 3 部分：场景开发与接入规范，重点阐述客户通过开放场景接入区块链支付平台的方法与接口规范；

——第 4 部分：安全与隐私规范，重点阐述区块链支付基础安全规范、数据安全与隐私规范等内容；

——第 5 部分：数据服务规范，重点阐述区块链支付平台提供数据服务的方式、内容；

——第 6 部分：管理规范，重点阐述区块链支付平台基础管理、银行与客户准入、交易安全与管理等基础管理规范。

本文件为该标准的第 6 部分

本文件负责起草单位：中国人民银行雄安新区营业管理部、雄安新区区块链实验室、中国工商银行股份有限公司河北雄安分行、中国农业银行股份有限公司河北雄安分行、中国银行股份有限公司河北雄安分行、中国建设银行股份有限公司河北雄安分行、中信银行股份有限公司河北雄安分行、中国农业银行总行研发中心金融科技创新中心

本文件主要起草人：孟宏伟、赵天奕、高远、焦欣欣、王蒙、左爵希、宋正罡、穆文涛、唐上淳、李亚科、王桐、楚会永、耿浩杰、康宁、胡园园、杨耀华、刘兰真、王婷婷

引　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。区块链支付信息服务是以区块链与智能合约技术为核心，通过业务流程触发形成支付指令，并对接银行支付网关实现资金支付的一种创新性区块链应用。前期，为解决工程建设资金管理场景中从业主体多、业务流程复杂、资金流向监管难等问题，雄安新区已基于上述区块链支付信息服务模式研发应用了工程建设资金管理区块链平台，实现了工程建设资金从业主到总、分包单位的及时、准确与高效拨付，具备按需支付、可信支付、穿透支付和无损支付等特点。根据区块链支付信息服务模式与特点，我们认为该模式亦可在政府资金监管、多级供应链等多个复杂企业支付场景进行应用，具备较好复制与推广应用前景。

为促进雄安新区区块链+支付模式应用，便于政府、银行和企业各方接入区块链支付平台并规范相关接入规范与接口要求，特制定《第 6 部分：管理规范》。

本文件规定了雄安区块链支付管理规范包含的基本要求，包括术语与定义、平台基础规范、平台银行准入与管理、平台客户与交易管理、平台数据安全与隐私管理等内容，主要面向使用区块链支付平台的企业管理人员、技术人员和接入银行的管理人员等。

雄安新区区块链支付平台
第 6 部分：管理规范

1 范围

本文件规定了雄安区块链支付管理规范包含的基本要求，包括术语与定义、平台基础规范、平台银行准入与管理、平台客户与交易管理、平台数据安全与隐私管理等内容，主要面向使用区块链支付平台的企业管理人员、技术人员和接入银行的管理人员等。

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。

JR/T 0184-2020 金融分布式账本技术安全规范

JR/T 0071 金融行业信息系统信息安全等级保护实施指引

JT/T 0068-2020 网上银行系统信息安全通用规范

3 术语和定义

3.1 区块链

区块链是一种不可篡改的分布式账本。

3.2 区块链支付

依托区块链技术，由业务流程触发的自动支付模式，是复杂场景下的有条件支付。满足对合规性、安全性、及时性、穿透性、协同性等有较高要求支付场景。

3.3 智能合约

一种旨在以信息化方式传播、验证或执行合同的计算机协议，其在分布式账本上体现为可自动执行的计算机程序。[JR/T 0184-2020，定义 3.20]

3.4 区块链支付平台/系统

是以区块链支付和智能合约技术为基础，通过连接第三方银行的账户与支付系统，根据客户在复杂场景的支付需求，由业务流程自动触发支付的平台或信息管理系统。

3.5 电子指令

指通过区块链信息系统平台发送的业务操作指令。

3.6 代付

指区块链支付平台接受客户的委托，根据客户提交的电子指令通过系统转出客户在区块链支付平台备案的金融机构账户内的资金。

3.7 代发

指区块链支付平台接受客户的委托，将客户向本单位职工或雇工等劳动者发放的工资、奖金等收入根据客户提交的电子指令通过系统存入上述主体在区块链支付平台备案的或金融机构存款账户内。

4 区块链支付平台基础管理规范

4.1 机构管理要求

1）岗位设置：

● 应建立与区块链支付平台规模相适应的信息安全保障与风险管理组织架构，明确相关负责机构或人员的职责及其对负责的安全保障与风险管理内容进行管理。

● 应设立区块链支付平台相关产品设计、系统研发、测试、运行维护等机构或团队，各机构或人员应明确本机构区块链支付平台的职责、安全保障与风险管理机制等基本情况。

2）授权与审批：

● 应针对区块链支付平台业务规划、技术架构、产品研发、系统变更、系统上线等重要事项建立授权与审批流程。

3）审核与检查：

● 应制定安全审核与安全检查制度，并按照制度要求进行安全审核与安全检查活动。

● 内部审计部门应至少每两年对区块链支付平台开展一次安全审计。

4.2 制度建设要求

1）应建立包括信息安全管理框架、系统开发、测试、运行、维护、应急处理、业务管理和客户信息与隐私保护在内的制度体系；

2）应做好区块链支付平台新产品设计与规划，开展产品合规性、安全性评审，平衡客户体验与安全性，防范潜在的信息系统安全风险。

3）应采取包括风险识别、评估、监测、控制、整改与优化在内的风险管理工作。

4.3 人员管理要求

1）应建立区块链支付平台员工培训机制，制定员工培训计划，对区块链支付平台的管理人员、和操作人员进行安全教育培训和岗位技能培训。

2）应对培训开展情况和效果进行监督，对培训情况和培训结果进行纪录和归档保存。

4.4 应急管理要求

1）应建立应急预案演练和应急处置机制，保证运维安全与数据安全。

2）应定期对本机构或行业类似信息安全风险事件进行分析、研判，评估现有措施脆弱性并及时优化。

4.5 等级保护要求

区块链支付平台系统应满足JR/T 0071“安全通用”中有关安全管理要求。区块链支付平台系统采用云计算技术的，应满足JR/T 0071“云计算安全扩展要求”中有关安全管理要求。区块链支付平台系统采用移动互联相关技术的，应满足JR/T 0071“移动互联安全扩展要求”中有关安全管理要求。

5 区块链支付平台银行准入与管理

5.1 银行申请与准入

1）应建立银行准入审批机制，规范申请银行在业务管理、技术、接口开发、测试等方面的要求，建立准入门槛或评分机制，满足相关准入门槛或评分要求的银行方可准入。
2）银行申请准入时，区块链支付平台应向银行提供相关支付、融资产品的接口文档。准入银行应按照接口文档要求，开展相关对接准备与实施工作。接口文档详见《区块链支付银行接入规范》。
3）申请接入银行，应按照区块链支付平台管理方要求，填写相关支付准入文件，并提供相关公司证明文件。
4）对于满足申请准入各项要求的银行，区块链支付平台银行准入银行签署相关银行准入协议，约定双方的各项权利、义务、保密责任、协议终止与变更、违约责任、免责条款、纠纷处理等。

5.2 银行上链与管理

1）银行与区块链支付平台进行对接，应确保区块链支付平台能够完成对银行客户账户的查询、转账、代发等功能实现。
2）银行应为客户办理适用于区块链支付平台系统的银行账户和相关配套业务。
3）银行应及时准确地处理客户在区块链支付平台系统上发送的电子指令，保证区块链支付平台系统查询、转账及代发等功能正常使用。
4）应对与银行相关支付交易的唯一性进行检查，防止重复支付：通过可靠的数字签名等机制保证交易信息的真实性、完整性。
5）在与银行合作时，应采取有效措施鉴别客户身份，取得客户授权，并保存记录，应采取有效的技术措施保证交易指令的安全性。

5.3 银行退出与动态管理

1）应建立准入银行动态管理与评价机制，持续督促准入银行按照要求配合做好业务管理，确保系统功能正常运行。
2）对于不满足区块链平台系统正常运营要求的准入银行，区块链支付平台应及时告知银行进行整改与优化。
3）对于不满足准入银行动态管理与持续运维要求的银行，区块链支付应根据业务合作协议要求，终止相关准入银行的接口服务，实现银行退出与动态管理。

6 区块链支付平台客户与交易管理

6.1 业务申请与开通

1） 应制定严格的企业客户申请与开通流程，验证企业客户身份，并要求客户提交相关身份证明材料，包括但不限于加盖公章的申请书、企业营业执照、法定代表人身份证明材料、申请客户个人身份证明材料等，并审查其申请材料的真实性、完整性和合规性。
2） 对于满足申请与开通要求的企业客户，区块链支付平台应与企业客户签订相关协议，约定双方的各项权利、义务、保密责任、协议终止与变更、违约责任、免责条款、纠纷处理等。
3） 客户申请智能密码钥匙（以下简称Ukey）作为数字证书载体或其他安全设备时，应持提交相关身份证明材料,包括但不限于加盖公章的申请书、企业营业执照、法定代表人身份证明材料、申请客户个人身份证明材料等。
4） 客户下载客户数字证书时，应对客户身份进行认证，并采取相关技术手段保证客户数字证书只能被下载一次，身份认证信息应设置有效期，超出有效期而未下载证书，应重新办理。
5） 客户Ukey在暂停、终止、挂失或注销后，如需要恢复、解除挂失需客户本人持有效身份证件材料办理。
6） 应提示客户妥善保管其Ukey、登录密码，并对通过Ukey及密码进行的业务操作负责。

6.2 身份认证管理

1） 并应组合选用下列三类要素对交易进行验证：一是客户知悉的要素，例如，静态密码等；二是仅客户本人持有并特有的，不可复制或者不可重复利用的要素，如经过安全认证的数字证书、电子签名，以及通过安全渠道生成和传输的一次性密码等；三是客户本人生物特征要素，如指纹、人脸等。
2） 区块链支付平台采用智能密码钥匙、动态令牌、短信验证码及生物特征认证的，应符合JT/T 0068-2020 6.2.2中关于专用安全机制的要求。
3） 对于区块链支付系统设置的初始登录密码，应强制客户首次登录时修改初始密码。
4） 应采取有效措施引导客户设置差异化的区块链支付平台登录、交易密码，并避免设置易猜解的简单密码（例如，连续或相同字母数字、键盘顺序、常见单词短语等）。
5） 客户登录区块链支付平台时，若身份认证连续失败超过一定次数（不超过10次）,应在短时间内锁定该客户登录权限或交易账户使用权限。

6.3 交易流程与交易监控

1） 客户使用区块链支付平台进行支付时，应根据区块链支付平台要求，按照相关业务与项目背景提交相关支付审核与证明材料、包括但不限于相关付款申请书、项目结算申请单、项目竣工申请书、工资确认单等文件，作为使用区块链支付平台支付的付款要件。
2） 客户通过区块链支付平台发起的扣款指令应明确款项事由、扣款账户名称及账号、收款账号名称及账号、扣款时间、扣款金额等内容。
3） 应对客户发送的电子指令及相关文件资料进行审查，并采取必要措施要求客户确保提交的相关文件资料合法、真实、完整和有效。
4） 应保障系统的安全、日常运营和维护工作，确保按照客户开户行协商确定的接口规范、数据格式等技术标准建立与客户开户行支付系统的连接。
5） 应定期对系统进行升级、改造，期间造成服务与业务终止服务的，应提前24小时通知客户。
6） 应采取措施监控客户相关系统交易与行为，对于客户未按有关业务规定或恶意操作以及利用系统从事违反国家法律法规活动的，应终止相关客户系统服务。
7） 应根据客户提交录入的电子指令及付款证明文件，通过系统对客户的账户资金进行代付和代发。

8）应妥善保管客户提供的申请资料和其他信息，并不得向第三方泄露，法律法规及人行、银保监局等监管单位另有规定的除外。

9）应根据自身业务特点，建立系统异常交易监控机制，识别并及时处理异常交易，交易监测范围至少包括客户登录、查询、委托、授权等交易。

7 区块链支付平台客户教育与隐私保护

7.1 客户培训与教育

1）应切实加强客户培训和风险提示，向客户详细解释本机构业务流程和安全控制措施。

2）应建立相关客户投诉、纠纷处理及舆情应对机制，严格按照行业、机构的相关规定和要求对外发布信息。

3）应通过多种渠道及时公告相关的服务内容、协议、资费标准等重大调整，可能影响服务的系统重要升级或变更等重大事项。

7.2 客户隐私保护

1）本标准中所涉及的隐私信息是指在区块链支付平台系统中，单独或者与其他信息相结合能识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括但不限于系统中各方的账户信息、鉴别信息、交易信息、个人身份信息、支付审批附件及其他反映特定自然人活动的各种信息。

2）应将隐私信息按照敏感程度进行分级，并设置对应的隐私保护策略。

3）应从认证授权、访问控制、保密、完整性、审计、监控、策略等方面，采取相应的技术手段保证隐私信息各环节不被未授权的第三方获取，并保护交易方的身份不被识别和冒用。

4）隐私保护技术和方法包括认证授权、局部广播、摘要存储、变更标识、混淆技术以及零知识证明、群签名、环签名、同态加密等算法组合，可根据业务场景组合解决方案，实现信息保密性和隐私保护的目的。