

团体标准

T/HBPFS 001.1-2022

雄安新区区块链支付平台

第1部分：参考模型及流程规范

The Standard of Xiong'An New Area Blockchain Payment Platform

Part 1: Reference Model and Process Specifications

2022-12-27 发布

2022-12-27 实施

河北省金融学会 发布

全国团体标准信息平台

目次

前 言	III
引 言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
3.1 区块链	1
3.2 智能合约	1
3.3 共识机制	1
3.4 区块	1
3.5 分布式账本	1
3.6 摘要算法	2
3.7 数字签名	2
3.8 银行支付网关	2
4 区块链支付信息服务概述	2
4.1 内涵	2
4.2 适用范围	2
4.3 技术特征	2
5 参考模型	3
6 应用系统架构	3
7 区块链支付信息服务功能及流程图	4
7.1 支付	4
7.2 审批支付	7
7.3 自动支付	8
7.4 受托支付	9

全国团体标准信息平台

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 1 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 1 部分：参考模型及流程规范》。

区块链技术是密码算法、共识机制、点对点通讯协议、分布式存储等多种核心技术体系高度融合形成的一种分布式基础架构与计算范式。根据雄安新区实际情况，制定区块链支付平台相关建设规范的团体标准，用于指导各参与方使用和建设区块链支付平台，为区块链技术大规模应用提供技术支持，快速服务于雄安建设。

本文档主要介绍参考模型及流程规范。

雄安新区区块链支付平台

第1部分：参考模型及流程规范

1 范围

本文件规定了雄安区块链支付平台的支付标准及包含的基本要求，包括术语与定义、区块链支付信息服务、参考模型、应用系统架构、区块链支付信息服务功能及流程图等内容，主要面向使用区块链支付平台的政府、银行、企业技术人员、管理人员等，参考本文档可顺利完成区块链支付平台的接入、使用、管理等工作。

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

3 术语和定义

下列术语和定义适用于本文件。

3.1 区块链

使用密码技术链接将共识确认过的区块按顺序追加形成的分布式账本。

3.2 智能合约

是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。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。

3.3 共识机制

在分布式节点间达成区块数据一致性的规则和程序。

3.4 区块

一种包含区块头和区块数据的数据结构，其中区块头包含前一个区块的摘要信息。

3.5 分布式账本

在分布式节点间使用共识机制实现具备最终一致性的账本，包括区块和事务数据的集合。

3.6 摘要算法

通常通过将任意长度的信息输入变成固定长度的短信息输出来保障数据的完整性。

3.7 数字签名

附加在数据单元上的数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人（例如接收者）伪造或抵赖。

3.8 银行支付网关

指银行金融网络系统和区块链支付平台之间的接口，是由银行操作的将区块链支付平台上传的数据转换为金融机构内部数据的一组服务器设备。

4 区块链支付信息服务概述

4.1 内涵

区块链支付信息服务是依托区块链技术实现的支持复杂场景支付新模式，连通政府、企业、银行多个参与方，通过业务流程触发形成支付指令，通过银行支付网关驱动资金流，具备按需支付、可信支付、穿透支付和无损支付等特点，可满足对合规性、安全性、及时性、穿透性、协同性等较高要求的复杂支付场景。

4.2 适用范围

区块链支付信息服务适用于政府资金监管和多级供应链等企业复杂支付场景。传统企业支付方式在资金的合规支付、安全支付、及时支付和穿透支付等方面无法有效满足，在诸如工程建设资金、征拆迁资金管理、房屋预售资金管理等场景中，存在从业主体多、业务流程复杂、资金流向监管难等问题，区块链支付信息服务将传统的层级结构转变为扁平的区块链结构，消除信息不对称，用智能合约将事前业务数据、事中划拨资金、事后审查监督等核心数据自动关联，形成项目全周期资金管理闭环，提升资金支付管理的智能化、数字化水平，从根本上改变了传统项目的支付模式。

参与方包括银行和企业，其中，银行负责构建并维护区块链支付信息服务基础设施，提供应用场景的接入，根据区块链支付信息服务指令进行资金的划转；参与企业构建应用场景，使用区块链支付信息服务开展复杂场景支付业务。

4.3 技术特征

区块链支付信息服务具备合同约定、条件触发、流程驱动、多方协同、全程监管等技术特征。

合同约定：支付框架基于支付主体间的合同、或政府的监管规则等实际业务场景设定。

条件触发：支付指令按照履约进度、支付要件、时间等条件触发。

流程驱动：支付行为符合企业或政府支付管理流程，流程审批后发生。

多方协同：支付对象涉及政府、多个企业参与方和多家银行。

全程监管：支付过程满足企业内控、政府监管、银行服务要求。

5 参考模型



图1 参考模型

区块链支付信息服务参考模型如图 1 所示，包括：应用场景、区块链支付平台和资金支付层三个层次。

其中，应用场景利用区块链支付信息服务通道提供的支付服务接口，构建满足具体业务需求的应用场景系统，如工程建设资金管理系统、住房预售资金监管系统、供应链金融系统等；区块链支付平台基于区块链底层系统构建（如雄安链），实现与资金支付层接入，通过智能合约提供主动支付、审批支付、自动支付和受托支付等基础功能，以及数据服务、用户管理等管理功能，并构建开放开发平台，支持与应用场景系统对接；资金支付层负责与区块链支付平台连接，通过区块链支付平台接收来自用户的支付指令，执行资金划转并返回执行的结果。

6 应用系统架构

区块链支付信息服务的应用系统架构如图 2 所示：

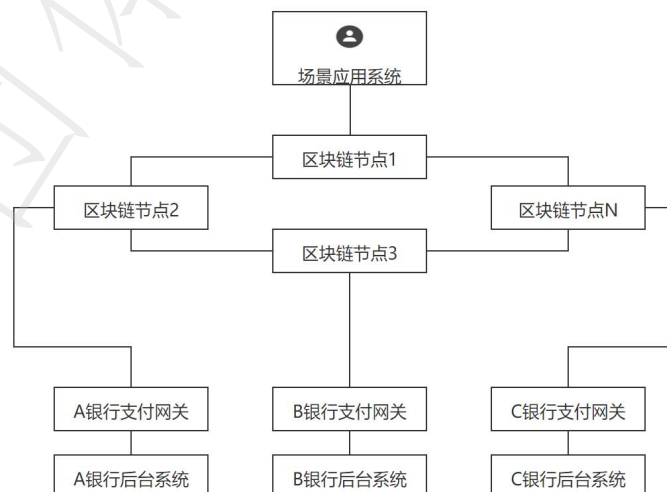


图2 应用系统架构

区块链节点之间相互连接构成区块链支付信息服务网络，提供区块链支付信息服务能力，区块链节点分布式部署，根据业务管理规则动态加入和退出。区块链节点与银行支付网关连接，实

现支付指令向银行后台系统的可信传递，完成实际资金支付。各银行可独立部署区块链节点或支付网关，加入区块链支付信息服务网络。

复杂场景应用系统（如工程建设资金管理系统、住房预售资金监管系统、供应链金融系统等）与区块链节点连接，接入区块链支付信息服务网络，使用区块链支付信息服务网络提供的区块链支付信息服务功能，完成特定应用场景的支付需求。

7 区块链支付信息服务功能及流程图

7.1 支付

7.1.1 点对点支付

点对点支付是指用户 A 通过区块链支付平台生成并发出支付指令，完成向用户 B 转账的过程。

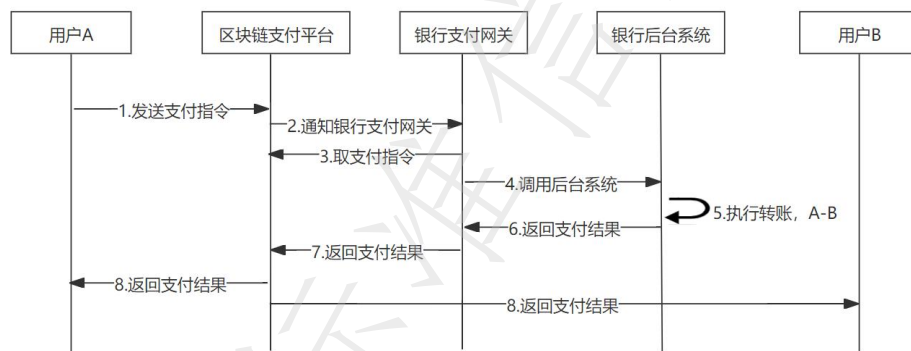


图3 点对点支付流程图

- 步骤 1: 用户 A 发送支付指令至区块链支付平台;
- 步骤 2: 区块链支付平台将支付指令通知发送到银行支付网关;
- 步骤 3: 银行支付网关从区块链支付平台取支付指令信息;
- 步骤 4: 银行支付网关将支付指令信息传送至银行后台系统;
- 步骤 5: 银行后台系统执行支付指令，完成 A 向 B 的资金转账;
- 步骤 6: 银行后台系统将支付结果返回银行支付网关;
- 步骤 7: 银行支付网关将支付结果返回至区块链支付平台;
- 步骤 8: 区块链支付平台通知用户 A、B 支付结果。

7.1.2 点对多点支付

点对多点支付是指用户 A 通过区块链支付平台生成并发出支付指令，完成向多个用户转账的过程。

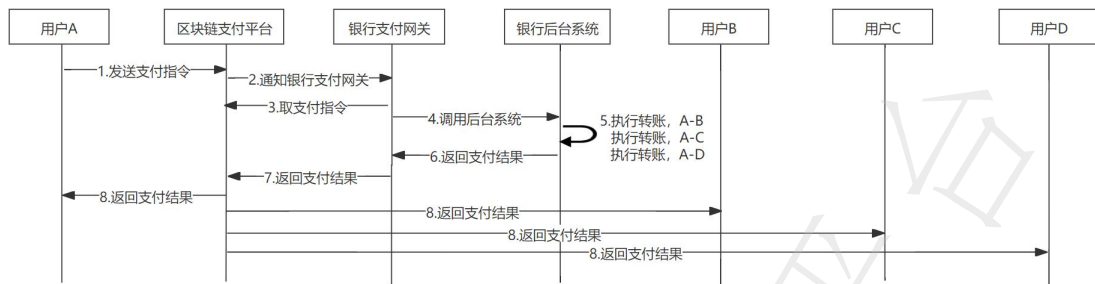


图 4 点对多点支付流程图

- 步骤 1：用户 A 发送支付指令至区块链支付平台；
- 步骤 2：区块链支付平台将支付指令通知发送到银行支付网关；
- 步骤 3：银行支付网关从区块链支付平台获取支付指令信息；
- 步骤 4：银行支付网关将支付信息传送至银行后台系统；
- 步骤 5：银行后台系统执行支付指令，完成 A 向 B、C、D 的资金转账；
- 步骤 6：银行后台系统将支付结果返回银行支付网关；
- 步骤 7：银行支付网关将支付结果返回至区块链支付平台；
- 步骤 8：区块链支付平台通知用户 A、B、C、D 支付结果。

7.1.3 穿透支付

穿透支付指资金经中间各收付环节到各收款方账户的过程，如用户 A 发起经过 B 转账给 C。在实际的项目中穿透支付可能存在多级穿透，二级穿透示例如下图所示。

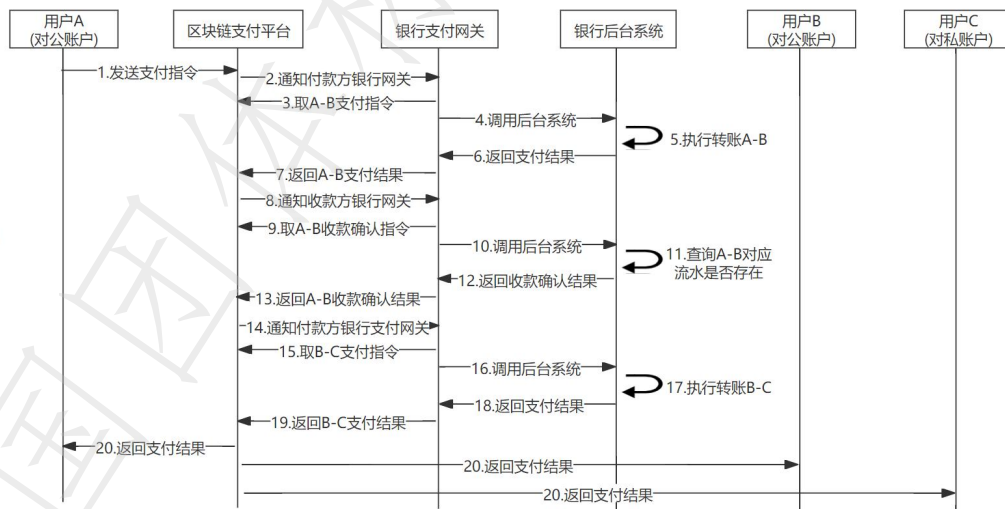


图 5.1 穿透支付流程图（ABC 均使用同一家银行账户）

- 步骤 1：用户 A 发送支付指令至区块链支付平台；
- 步骤 2：区块链支付平台将支付指令通知发送到银行支付网关；
- 步骤 3：银行支付网关从区块链支付平台获取支付指令信息；
- 步骤 4：银行支付网关将支付信息传送至银行后台系统；
- 步骤 5：银行后台系统执行支付指令，完成 A 向 B 的资金转账；

- 步骤 6: 银行后台系统将支付结果返回银行支付网关;
 步骤 7: 银行支付网关将支付结果返回区块链支付平台;
 步骤 8: 通知收款方银行网关;
 步骤 9: 收款方银行网关去区块链平台去收款确认指令;
 步骤 10: 银行支付网关调用后台系统;
 步骤 11: 查询 A-B 对应流水是否存在;
 步骤 12: 返回收款确认结果至银行支付网关;
 步骤 13: 返回 A-B 收款确认结果至区块链平台;
 步骤 14: 通知付款方银行支付网关;
 步骤 15: 银行支付网关取 B-C 支付指令;
 步骤 16: 银行支付网关调用银行后台系统;
 步骤 17: 执行转账 B-C;
 步骤 18: 返回支付结果至银行支付网关;
 步骤 19: 返回 B-C 支付结果;
 步骤 20: 返回支付结果;

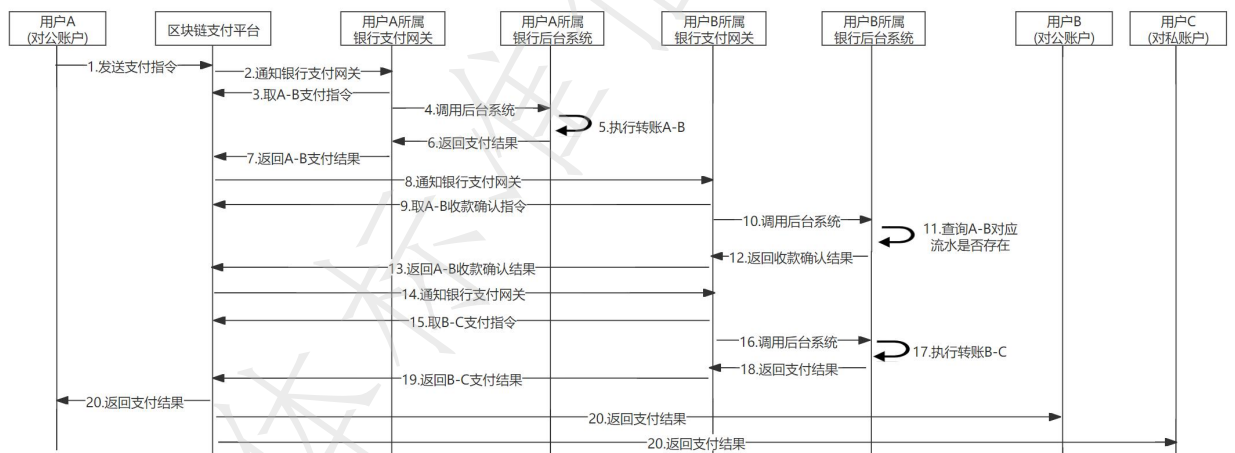


图 5.2 穿透支付流程图（ABC 均使用不同银行账户）

- 步骤 1: 用户 A 发送支付指令至区块链支付平台;
 步骤 2: 区块链支付平台将支付指令通知发送到 A 银行支付网关;
 步骤 3: A 银行支付网关从区块链支付平台获取支付指令信息;
 步骤 4: A 银行支付网关将支付信息传送到 A 银行后台系统;
 步骤 5: A 银行后台系统通知 B 银行支付网关, 完成 A 向 B 的资金转账;
 步骤 6: A 银行后台系统将支付结果返回 A 银行支付网关;
 步骤 7: A 银行支付网关将支付结果返回区块链支付平台;
 步骤 8: 区块链支付平台通知 B 银行支付网关有 A-B 收款确认指令;
 步骤 9: B 银行支付网关取 A-B 收款确认指令;
 步骤 10: B 银行支付网关调用 B 银行后台系统;
 步骤 11: B 银行后台系统查询 A-B 对应流水是否存在;
 步骤 12: B 银行后台系统返回收款确认结果至 B 银行支付网关;
 步骤 13: B 银行支付网关返回收款确认结果至区块链支付平台;

- 步骤 14: 区块链支付平台通知 B 银行支付网关有支付指令;
 步骤 15: B 银行支付网关去区块链支付平台取 B-C 支付指令;
 步骤 16: B 银行支付网关调用 B 银行后台系统;
 步骤 17: B 银行后台系统执行转账 B-C;
 步骤 18: 返回 B-C 支付结果至 B 银行支付网关;
 步骤 19: 返回 B-C 支付结果至区块链支付平台;
 步骤 20: 区块链支付平台通知用户 A、B、C 支付结果。

7.2 审批支付

7.2.1 一般审批支付

一般审批支付指不带附件的审批支付，在实际应用中，可能存在多层审批环节。

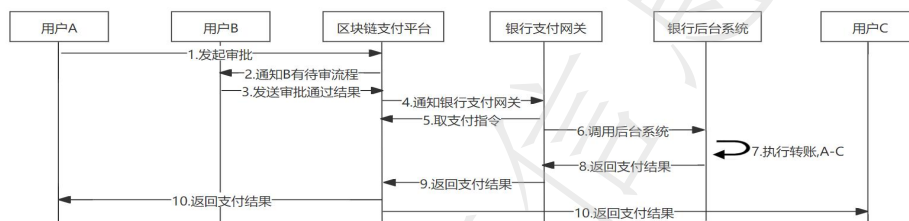


图6 一般审批支付流程图

- 步骤 1: 用户 A 发起支付请求审批流程至区块链支付平台;
 步骤 2: 区块链支付平台通知用户 B 有待审批流程;
 步骤 3: 用户 B 审批通过，发送审批通过结果至区块链支付平台;
 步骤 4: 区块链支付平台将支付指令通知发送到银行支付网关;
 步骤 5: 银行支付网关从区块链支付平台取支付指令信息;
 步骤 6: 银行支付网关将支付信息传送至银行后台系统;
 步骤 7: 银行后台系统执行支付指令，完成 A 向 C 的资金转账;
 步骤 8: 银行后台系统将支付结果返回银行支付网关;
 步骤 9: 银行支付网关将支付结果返回区块链支付平台;
 步骤 10: 区块链支付平台通知用户 A、C 支付结果。

7.2.2 带附件的审批支付

带附件的审批支付指用户 A 需要添加审批附件通过审批流程进而发起支付的过程。在实际应用中，可能存在添加多个附件、多层审批环节。

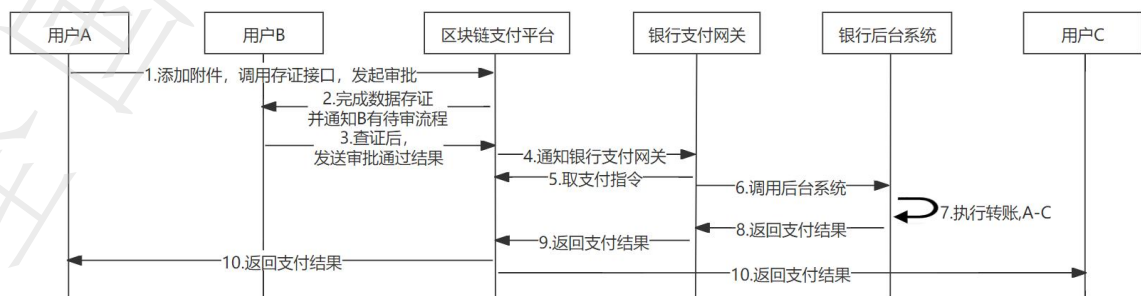


图7 带附件审批支付流程图

- 步骤 1: 用户 A 添加附件、调用存证接口、发起支付审批流程至区块链支付平台;

- 步骤 2: 区块链支付平台完成数据存证并通知 B 有待审批流程;
 步骤 3: 查证后, 用户 B 发送审批通过结果至区块链支付平台;
 步骤 4: 区块链支付平台将支付指令通知发送到银行支付网关;
 步骤 5: 银行支付网关去区块链支付平台取支付指令信息;
 步骤 6: 银行支付网关将支付信息传送至银行后台系统;
 步骤 7: 银行后台系统执行支付执行, 完成 A 向 C 的资金转账;
 步骤 8: 银行后台系统将支付结果返回银行支付网关;
 步骤 9: 银行支付网关将支付结果返回区块链支付平台;
 步骤 10: 区块链支付平台通知用户 A、C 支付结果。

7.2.3 请款支付

请款支付指收款方 B 向付款方 A 发起请款流程, 付款方 A 同意后发送支付指令完成向用户 B 支付的过程。

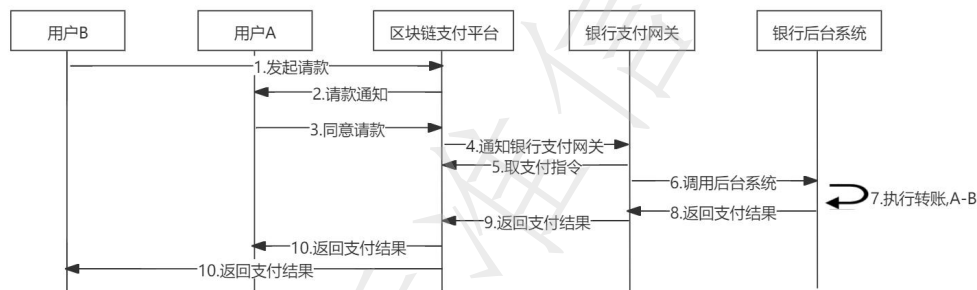


图8 请款支付流程图

- 步骤 1: 用户 B 发起请款流程至区块链支付平台;
 步骤 2: 区块链支付平台通知用户 A 有请款通知;
 步骤 3: 用户 A 同意请款;
 步骤 4: 区块链支付平台将支付指令通知发送到银行支付网关;
 步骤 5: 银行支付网关去区块链支付平台取支付指令信息;
 步骤 6: 银行支付网关将支付信息传送至银行后台系统;
 步骤 7: 银行后台系统执行支付指令, 完成 A 向 B 的资金转账;
 步骤 8: 银行后台系统将支付结果返回银行支付网关;
 步骤 9: 银行支付网关将支付结果返回区块链支付平台;
 步骤 10: 区块链支付平台通知用户 A、B 支付结果。

7.3 自动支付

自动支付指通过规则和条件设定, 程序自动触发的支付过程, 不需要人工干预。

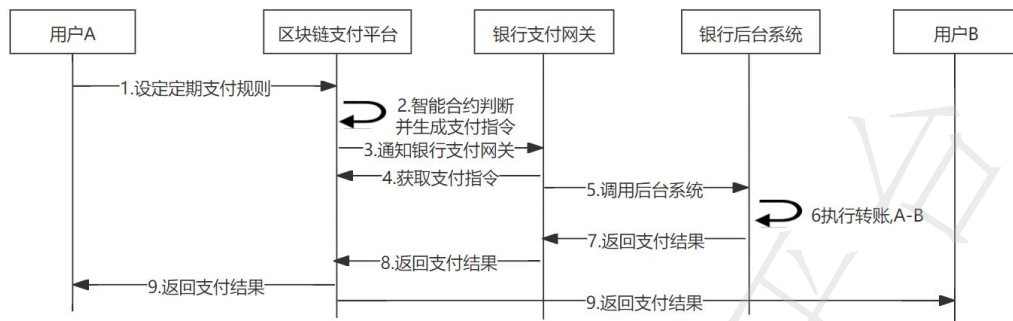


图9 自动支付流程图

- 步骤 1: 用户 A 设定定期支付规则;
 步骤 2: 智能合约判断并生成支付指令;
 步骤 3: 区块链支付平台将支付指令通知发送到银行支付网关;
 步骤 4: 银行支付网关去区块链支付平台取支付指令信息;
 步骤 5: 银行支付网关将支付信息传送至银行后台系统;
 步骤 6: 银行后台系统执行支付指令, 完成 A 向 B 的资金转账;
 步骤 7: 银行后台系统将支付结果返回银行支付网关;
 步骤 8: 银行支付网关将支付结果返回区块链支付平台;
 步骤 9: 区块链支付平台通知用户 A、B 支付结果。

7.4 受托支付

受托支付是指贷款银行 B 根据借款人 A 的提款申请和支付要件, 发送支付指令将资金支付给合同约定用途的用户 C 的过程。

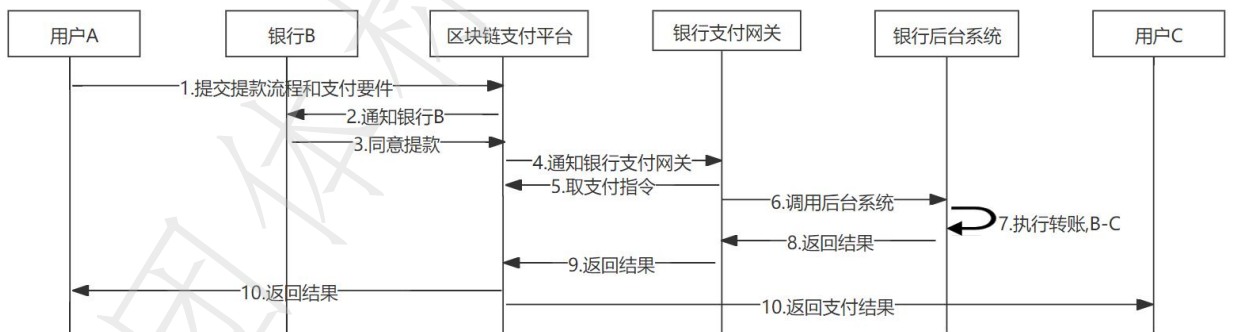


图10 受托支付流程图

- 步骤 1: 用户 A 提交提款流程和支付要件至区块链支付平台;
 步骤 2: 区块链支付平台通知银行 B 有待审流程;
 步骤 3: 银行 B 同意用户 A 的提款流程;
 步骤 4: 区块链支付平台将支付指令通知发送到银行支付网关;
 步骤 5: 银行支付网关去区块链支付平台取支付指令信息;
 步骤 6: 银行支付网关将支付信息传送至银行后台系统;
 步骤 7: 银行后台系统执行支付指令, 完成银行 B 向用户 C 的资金转账;
 步骤 8: 银行后台系统将支付结果返回银行支付网关;
 步骤 9: 银行支付网关将支付结果返回区块链支付平台;
 步骤 10: 区块链支付平台通知用户 A、C 支付结果。