BSN-DDC 基础网络

OPB 跨链应用合约说明书

V1.0

北京红枣科技有限公司

2023 年 4 月

修改记录

日期	版本	修改说明	修改者
2023.4.3	v1.0	版本初始化	

目录

1. 编写目的

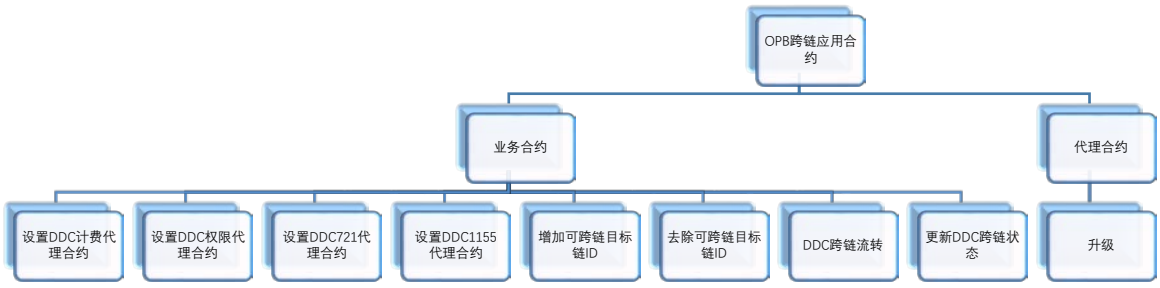
为了让项目组成员以及各开放链盟链框架方对 BSN-DDC OPB 跨链应用合约的整体设计有一个全面详细的了解，同时为项目的开发、测试、验证、交付等环节提供原始依据以及开发指导，特此整理 BSN-DDC OPB 跨链应用合约整体设计规范方案说明文档。

2. 文档概述

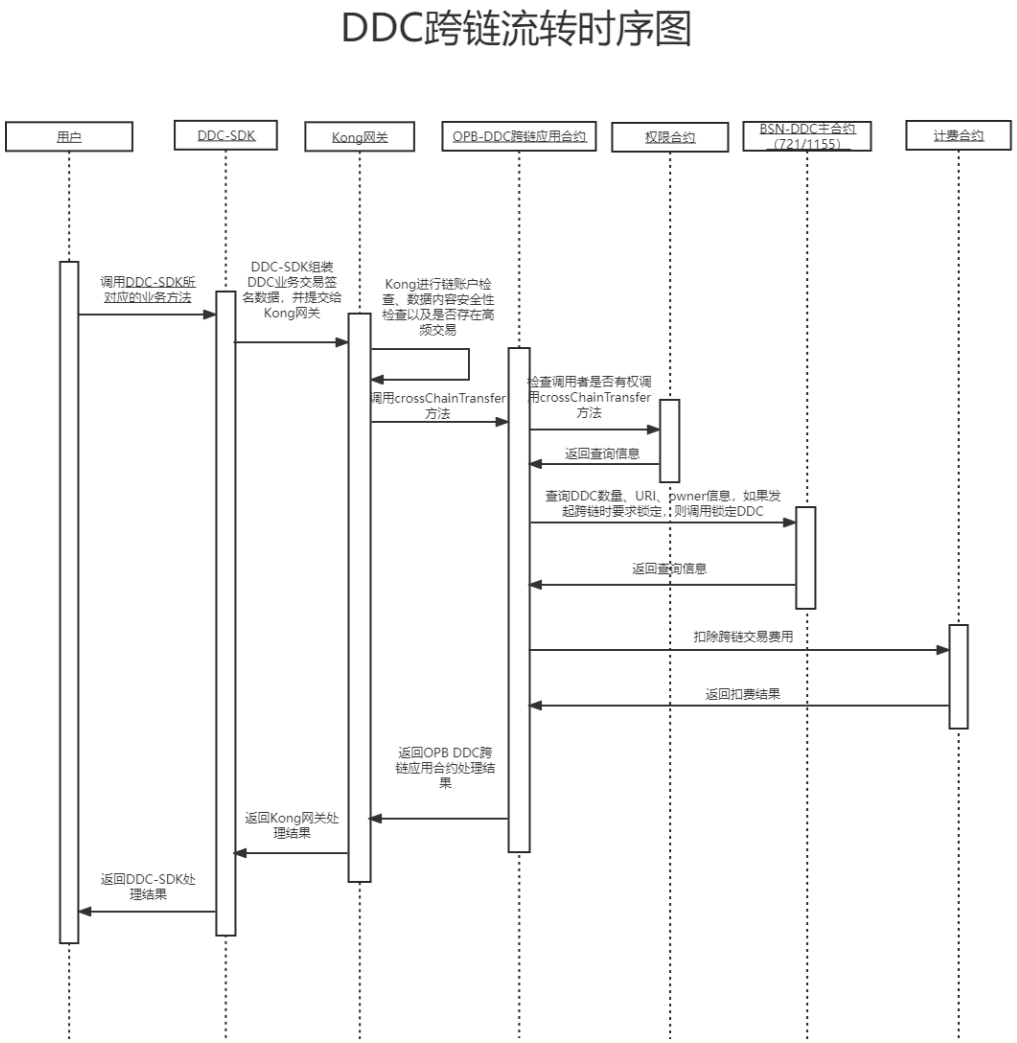
DDC 除了在 OPB 链内交易的业务场景外，也有跨 OPB 交易的需求，本文档是中心化跨链机制中在起始链上的 OPB 跨链应用合约的说明。

3. 整体设计

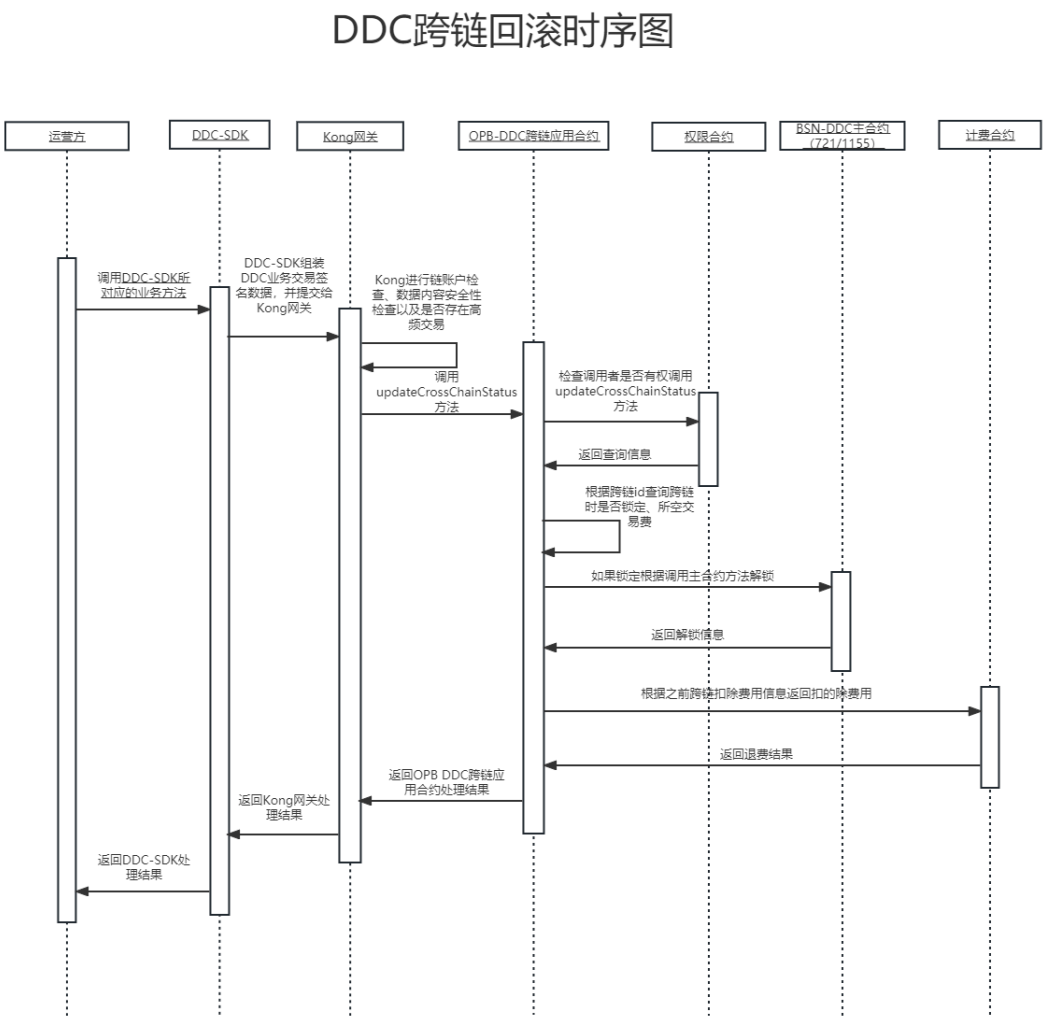
3.1 合约整体结构



3.2 DDC 跨链流转时序图



3.3 DDC 跨链回滚时序图



3.4 安全性设计说明

OPB DDC 跨链合约的整体设计目前采用 2 层设计模式，分别是代理合约和业务合约，业务合约只允许与之对应的代理合约进行调用。

注：业务合约都需要定义相应的接口，业务处理在业务合约中进行实现。

3.5 合约更新设计说明

OPB DDC 跨链合约通过 UUPS（EIP-1822: Universal Upgradeable Proxy Standard）模式实现其业务合约的可升级。OPB DDC 跨链合约有一个代理合约。

- 业务合约的修改如下：

1. 继承 UUPSUpgradeable。该类库实现了 UUPS 代理设计的可升级机制。
2. 添加初始化方法 initialize()。用于代理合约部署时调用以进行合约的初始化操作。

- 业务合约的部署过程如下：

1. 部署业务合约。
2. 部署代理合约。部署时构造传参写入业务合约地址、initialize 的方法签名，实现其与业务合约的映射以及初始化操作。

- 业务合约的升级过程如下：

1. 部署新版本的业务合约。
2. 调用当前代理合约中的 upgradeTo 方法。执行时传入新的业务合约地址，实现其与新版本业务合约的映射，达到升级的目的。

4. 合约设计

4.1 BSN-DDC-跨链应用合约

4.1.1 功能介绍

OPB 跨链应用合约用于在 OPB 链之间发起跨链，和跨链失败后由运营方发起回退跨链。

4.1.2 数据结构

- 可跨链目标链 ID 数据

编号	字段名	字段	类型	备注
1.	可跨目标链 ID 数组	_chainId	uint64[]	目标链的 ID 数组

- 跨链信息数据

编号	字段名	字段	类型	备注
2.	目标链 ID	toChainId	uint256	目标链的 ID
3.	DDC 类型	ddcType	uint8	用于区分 DDC 跨链所对应的 DDC 类型: 0.721 业务主合约 1.1155 业务主合约
4.	目标链接收者账户	toAddress	address	
5.	DDC 资源标识符	ddcURI	bytes	
6.	数量	amount	uint256	
7.	附加数据	data	bytes	
8.	起始链上 DDC 唯一标识	fromDDCId	uint256	
9.	起始链上 DDC owner	fromAddress	address	
10.	跨链唯一标识	crossChainId	uint256	
11.	是否锁定	lock	bool	true 为锁定，false 为未锁定
12.	跨链费用	crossChainFee	uint256	

4.1.3 API 定义

4.1.3.1 设置 DDC 计费代理合约

本合约需要调用官方 DDC 计费合约方法，所以需要设置官方 DDC 计费合约地址，用以做调用。

方法：function setChargeProxyAddress (address chargeProxyAddress)

入参：官方 DDC 计费合约代理合约地址

出参：N/A

事件：N/A

核心逻辑:

- 检查调用者是否为合约拥有者，不是则返回提示信息；
- 检查该地址是否是合约地址，不是则返回提示信息；

4.1.3.2 设置 DDC 权限代理合约

本合约需要调用官方 DDC 权限合约方法，所以需要设置官方 DDC 权限合约地址，用以做调用。

方法：function setAuthorityProxyAddress(address authorityProxyAddress)

入参：官方 DDC 权限合约代理合约地址

出参：N/A

事件：N/A

核心逻辑：

- 检查调用者是否为合约拥有者，不是则返回提示信息；
- 检查该地址是否是合约地址，不是则返回提示信息；

4.1.3.3 设置 DDC721 代理合约

本合约需要调用官方 DDC721 合约方法，所以需要设置官方 DDC721 合约地址，用以做调用。

方法：function setDDC721Proxy(address ddc721ProxyAddress)

入参：官方 DDC721 合约代理合约地址

出参：N/A

事件：N/A

核心逻辑：

- 检查调用者是否为合约拥有者，不是则返回提示信息；
- 检查该地址是否是合约地址，不是则返回提示信息；

4.1.3.4 设置 DDC1155 代理合约

本合约需要调用官方 DDC1155 合约方法，所以需要设置官方 DDC1155

合约地址，用以做调用。

方法：function setDDC1155Proxy(address ddc1155ProxyAddress)

入参：官方 DDC1155 合约代理合约地址

出参：N/A

事件：N/A

核心逻辑:

- 检查调用者是否为合约拥有者，不是则返回提示信息;
- 检查该地址是否是合约地址，不是则返回提示信息;

4.1.3.5 增加可跨链目标链 ID

DDC 跨链流转时，不能任何目标链 ID 都可流转，需先在这里增加目标链 ID 后，才需要向这个目标链跨链。

方法：function addTargetChainId (uint64 chainId)

入参：目标链 id

出参：N/A

事件：N/A

核心逻辑:

- 检查调用者是否为合约拥有者，不是则返回提示信息;
- 检查将目标链 ID 存入合约;

4.1.3.6 去除可跨链目标链 ID

DDC 跨链流转时，一些之前已允许跨往的目标链 ID，现在需要禁止，使用此方法移除这个目标链 ID。

方法：function deleteTargetChainId(uint64 chainId)

入参：目标链 id

出参：N/A

事件：N/A

核心逻辑:

- 检查调用者是否为合约拥有者，不是则返回提示信息；
- 检查将目标链 ID 移除合约；

4.1.3.7 DDC 跨链流转

DDC 拥有者或 DDC 授权者通过调用该 API 进行 DDC 的跨链流转。

- 输入参数：DDC 类型，DDC 唯一标识，是否锁定，目标链链 ID，目标链接收者账户，附加数据；
- 输出参数：
- 方法命名：crossChainTransfer;
- 方法举例：crossChainTransfer(DDCType ddcType, uint256 ddcId, bool isLock, uint64 toChainID, address to, bytes memory data);
- 事件：CrossChain(toChainId, ddcType, toAddress, ddcURI, amount, data, fromDDCId, fromAddress, crossChainId, lock, crossChainFee);
- 核心逻辑：
  - 检查调用者账户状态是否可用，不可用则返回提示信息；
  - 检查调用者账户是否有权限，没有则返回提示信息；
  - 检查目标链链 ID 是否允许的链 ID，不是则返回提示信息；
  - 检查 DDC 类型是否为 721 或 1155，不是则返回提示信息；
  - 所有检查通过后则根据 DDC 类型调用不同的业务主合约对 DDC 查询 owner、URI、数量，再检查现在的调用者是否有权调用此 ddcid 跨链，如果入参 isLock 为 true，则调用业务主合约锁定；
  - 判断 ddcURI 的长度是大于 0 的，不是则返回提示信息；
  - 调用计费合约支付 DDC 跨链业务费；
  - 跨链 ID 自增 1；
  - 将跨链 ID、跨链类型、跨链发起者、ddc 的 owner、ddcId、是否锁定、目标链 Id、本次跨链的业务费、跨链状态存入；
  - 最后触发 CrossChain 事件；

4.1.3.8 更新 DDC 跨链状态

运营方通过调用 API 接口对 DDC 进行回滚。

- 输入参数：跨链 ID，跨链状态，备注；
- 输出参数：
- 方法命名：updateCrossChainStatus;
- 方法举例：updateCrossChainStatus(uint256 crossChainID, State state, string memory remark);
- 事件：UpdateCrossChainStatus(operator, ddcId, state, remark);
- 核心逻辑：
  - 检查调用者账户状态是否可用，不可用则返回提示信息；
  - 检查调用者账户是否有权限，没有则返回提示信息；
  - 检查调用者是否是运营方，不是则返回提示信息；
  - 根据跨链 ID 查询跨链信息，如果信息为空，则返回提示信息；
  - 如果跨链状态为成功，则更新跨链 ID 对应信息为成功；
  - 如果跨链状态为失败，如果之前的跨链是锁定 DDC 的，则根据 DDC 类型在 DDC721 或 DDC1155 合约上解锁；再根据之前跨链所扣费用，给原账户返回；
  - 最后触发 UpdateCrossChainStatus 事件;