BSN-DDC 基础网络

Solidity 跨链应用合约详细设计

北京红枣科技有限公司

2022 年 8 月

目 录

1. 编写目的

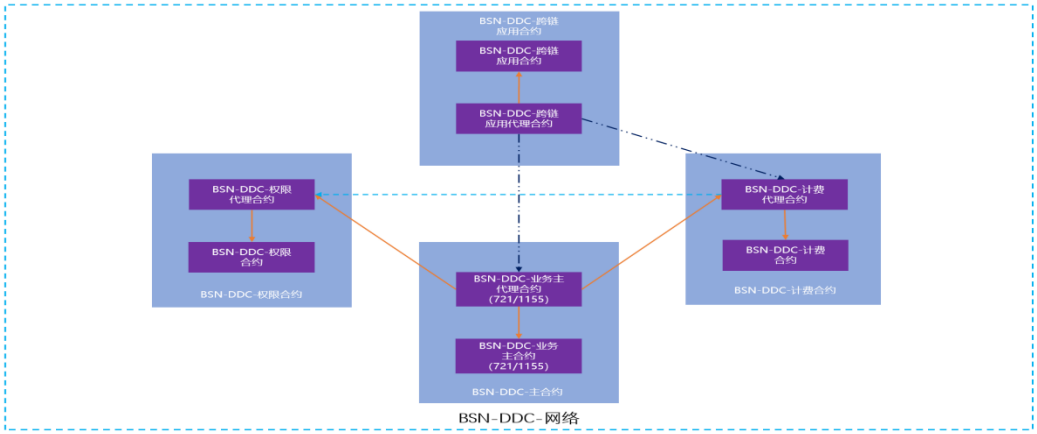
为了让项目组成员以及各开放链盟链框架方对 BSN-DDC 跨链应用合约的整体设计有一个全面详细的了解，同时为项目的开发、测试、验证、交付等环节提供原始依据以及开发指导，特此整理 BSN-DDC 跨链应用合约整体设计规范方案说明文档。

2. 需求文档

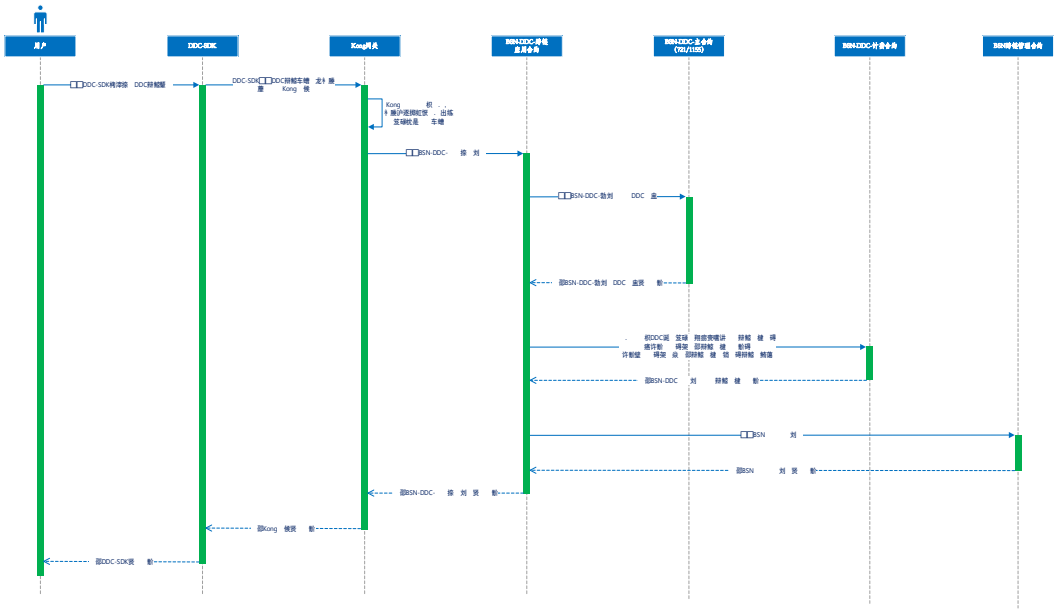
需求文档引用 BSN-DDC Solidity 合约详细设计-V1.6.docx

3. 整体设计

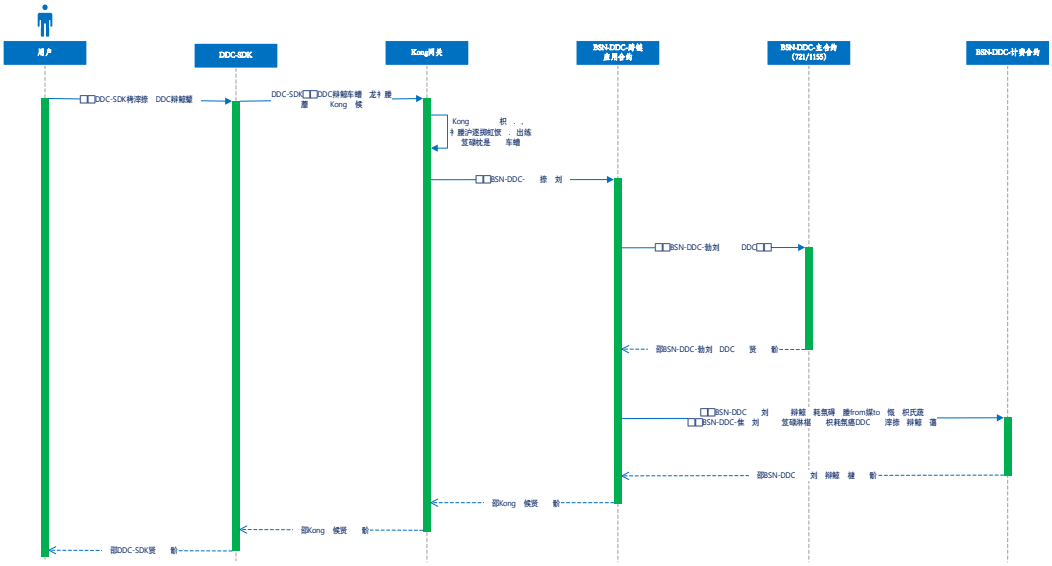
3.1 合约整体结构



3.2 DDC 跨链流转时序图



3.3 DDC 跨链回滚时序图



4. 合约设计

4.1 BSN-DDC-跨链应用合约

4.1.1 功能介绍

跨链应用合约用于对 DDC 跨链进行统一管理，其中包括官方 DDC 向公链进行 DDC 跨链流转以及官方 DDC 之间的跨链流转。

4.1.2 数据结构

- 基础数据

编号	字段名	字段	类型	备注
1.	跨链管理合约地址	eccmpAddress	address	跨链管理合约地址
2.	原链链 ID	chainId	uint64	原链链 ID
3.	最新跨链 ID	lastCrossChainID	uint256	
4.	DDC 跨链原链记录	tagCrossChainList	mapping(uint256=>CrossChainInfo)	Key：跨链 ID Value：原链数据
CrossChainInfo				
1.	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
2.	调用者	sender	address	发起 DDC 跨链流转时所对应的调用者
3.	拥有者	owner	address	发起 DDC 跨链流转时所对应的 DDC 拥有者
4.	DDC 唯一标识	ddcId	uint256	
5.	DDC 跨链业务费	fee	uint256	
6.	状态	state	uint8	0：跨链中； 1：跨链成功； 2：跨链失败；

7.	备注	remark	string	

- 跨链传递数据

编号	字段名	字段	类型	备注
1.	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
2.	目标链签名者账户	signer	bytes	目标链签名者账户
3.	目标链接收者账户	to	bytes	
4.	DDC 唯一标识	ddcId	uint256	
5.	DDC 资源标识符	ddcURI	bytes	
6.	附加数据	data	bytes	
7.	数量	amount	uint256	如果 DDC 类型为 1155，则此字段必填

4.1.3 API 定义

4.1.3.1 基础数据设置

跨链应用合约拥有者通过调用该 API 接口对合约相关数据进行设置，包括跨链管理合约地址以及原链链 ID（链 ID 用于对应中继链所对应的链 ID），后续进行 DDC 跨链调用时无需传递跨链管理合约所对应的合约地址以及链 ID 信息。

- 输入参数：跨链管理代理合约地址，原链链 ID；
- 输出参数：
- 方法命名：setBaseData;
- 方法举例：setBaseData(address eccmpAddress,uint64 fromChainID);
- 事件：SetBaseData(operator,eccmpAddress,fromChainID)；
- 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；
- 检查跨链管理代理合约地址是否为 0 地址，是则返回提示信息；
- 检查原链链 ID 是否大于 0，不是则返回提示信息；
- 所有检查通过后则保存跨链管理代理合约地址以及原链链 ID 信息数据，最后触发事件。

4.1.3.2 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，目标链签名者账户，目标链接收者账户，DDC 唯一标识，附加数据，目标链链 ID，目标链应用合约地址，目标链应用合约方法；
- 输出参数：
- 方法命名：crossChainTransfer;
- 方法举例：crossChainTransfer(DDCType ddcType,address signer,address to,uint256 ddcId,bytes memory data,uint64 toChainID,address toCCAddr,string memory funcName);
- 事件：CrossChainTransfer(address indexed operator, uint256 crossChainId,DDCType ddcType, address signer,address to,uint256 ddcId,string ddcURI,uint256 amount,uint64 fromChainID,uint64 toChainID,string fromCCAddr,string toCCAddr,uint256 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；
  - 检查目标链签名者账户地址是否为 0 地址，是则返回提示信息；
  - 检查目标链接收者账户地址是否为 0 地址，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 进行锁定（具体逻辑参考 BSN-DDC 业务主合约的锁定方法），再调用计费合约支付 DDC 跨链业务费，并保存 DDC 跨链原链记录。

- 最后组装跨链业务数据（跨链数据由 DDC 类型、目标链签名者账户、目标链接收者账户、DDC 唯一标识、DDC 资源标识符、附加数据以及数量组成）调用跨链管理代理合约，并触发事件；

4.1.3.3 DDC 跨链通知

运营方通过调用 API 接口对 DDC 跨链状态进行更新。

- 输入参数：跨链 ID，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(address indexed operator,uint256 crossChainID,State state,string 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；
  - 检查跨链 ID 是否大于 0，不是则返回提示信息；
  - 检查跨链 ID 对应的 DDC 跨链原链记录是否存在，不存在则返回提示信息；
  - 所有检查通过后，则所传的状态参数进行判断：
    1. 如果状态成功，则根据跨链 ID 更新 DDC 跨链原链记录状态；
    2. 如果状态不成功，则根据跨链 ID 获取 DDC 跨链原链记录，根据查询的 DDC 跨链原链记录所对应的 DDC 类型调用不同的业务主合约对 DDC 进行解锁（具体逻辑参考 BSN-DDC 业务主合约的解锁方法），并根据 DDC 跨链原链记录中所对应的跨链业务费和调用者账户，调用计费合约将跨链业务费充值给调用者账户，DDC 解锁和跨链业务费退回成功后，则根据跨链 ID 更新 DDC 跨链原链记录状态；
    3. 最后触发事件；

4.1.3.4 DDC 跨链生成

平台方或终端用户通过调用该 API 进行 DDC 的跨链生成。

- 输入参数：跨链数据，原链合约，原链链 ID；
- 输出参数：
- 方法命名：crossChainMint;
- 方法举例：crossChainMint(bytes memory ccData,bytes memory fromCCAddr,uint64 fromChainID);
- 事件：CrossChainTransfer(address indexed operator, uint256 crossChainId,DDCType ddcType, address signer,address to,uint256 ddcId,string ddcURI,uint256 amount,uint64 fromChainID,uint64 toChainID,string fromCCAddr,string toCCAddr)
- 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；
  - 解析跨链数据(由 DDC 类型、目标链签名者账户、目标链接收者账户、DDC 唯一标识、DDC 资源标识符、附加数据以及数量组成)；
  - 根据解析出的跨链数据，检查接收者账户地址是否为 0 地址，是则返回提示信息；
  - 根据解析出的跨链数据，检查不同的 DDC 类型，根据不同的 DDC 类型以及 DDC 唯一标识是否大于 0 再调用不同的业务主合约（721 或 1155 的安全生成方法），调完业务主合约后最后触发事件（跨链 ID 传 0）。