区块链 可装配系统 模块编程接口规范

1 范围

本文件主要内容包括：

a ）规定了可装配区块链各模块的最小接口集合；

b）规定了可装配区块链各模块的各个接口的具体功能。

本文件适用于：

a ）指导区块链服务提供方进行各模块的具体开发工作；

b）指导对可装配区块链各模块具体实现进行评估。

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。

T/CESA 6001-2016 区块链参考架构

T/CESA xxxx 区块链可装配系统装配规范

T/CESA xxxx 区块链可装配系统流程规范

3 术语和定义

T/CESA 6001-2016，T/CESA xxxx和T/CESA xxxx界定的术语和定义适用于本文件。

3.1 区块 block

区块链中存储交易和交易相关的数据的单元，通常由区块头和区块体组成。

3.2 区块头 block head

应包含当前区块的属性信息和链接信息。属性信息通常包括时间戳、区块版本等。链接信息通常包括能唯一标识前一个区块特征的哈希值和能唯一标识区块体特征的哈希值。

3.3 区块体 block body

区块中存储交易和交易相关的数据的主要部分。

3.4 交易 transaction

也称为事务，区块链上的一次原子性账本数据状态变更及其过程和结果记录,。

3.5 读写集 read-write set

区块链上的一条交易执行过程中，被读取和被修改或写入的状态数据的集合。

3.6 交易快照 transaction snapshot

记录区块链某一高度的状态数据集合。

4 接口描述

4.1 交易缓存模块接口

4.1.1 数据类型定义

组件类型 Transaction为复合类型，描述一条交易。其包括：

contractId 合约ID字段

method 调用合约的方法

parameters 交易参数

refTxType，交易类型

其余内容可依据区块链场景或应用需求进行定义。

组件类型 TxSource为枚举类型，描述交易来源。可取值为：

RPC 服务接收端口

P2P P2P广播

INTERNAL 内部

4.1.2 交易缓存接口

继承：无

属性：无

方法：

any AddTx(in Transaction tx, in TxSource source)

说明：增加一条交易。

参数：tx为需加入缓存的交易，source为交易来源。

返回：错误对象。

sequence<*Transaction> FetchTxBatch(in short blockHeight) ;

说明：获取供打包的一批交易。

参数：blockHeight为区块高度。

返回：一批交易。

any RemoveTxs(sequence <*Transaction >removeTxs) ;

说明：移除已打包过的一批交易。

参数：removeTxs为要移除的交易集合。

返回：错误对象。

4.2 区块提议模块接口

4.2.1 数据类型定义

组件类型 TxPoolSignal为复合类型，描述交换缓存提议信号结构。其包含：
signalType 信号类型

chainTag 链标识

4.2.2 区块提议接口

继承：无

属性：无

方法：

TxPoolSignal(in *TxPoolSignal proposeSignal)；

说明：响应来自交易缓存模块的区块提议信号，进行打包规则验证，通过后执行打包操作。
参数：proposeSignal为从交易缓存模块接收到的区块提议信号。

返回：无。

ProposeStatusChange(in boolean proposeStatus)；

说明：处理来自共识算法模块的区块提议状态通知。

参数：proposeStatus为是否进入区块提议状态。

返回：无。

4.3 交易调度模块接口

4.3.1 数据类型定义

组件类型 Block为复合类型，描述区块结构，其包括：

header 区块头

Transactions 交易集

组件类型 Snapshot为复合类型，区块链交易快照保存只读的世界状态数据，其包括：
status 世界状态数据。

4.3.2 交易调度接口

继承：无

属性：无

方法：

any Schedule(in *Block b, in sequence<*Transaction> txBatch, in Snapshot snapshot)；
说明：调度交易的执行，并修改候选区块，由区块提议模块调用。

参数：b为候选区块（已含部分字段），txBatch为待调度执行的一批交易，snapshot为交易快照。

返回：结果读写集，错误对象。

any SimulateWithDag(in *Block b, in Snapshot snapshot)；

说明：参照候选区块里的DAG，按序验证执行其中的交易，由区块验证模块调用。
参数：b为候选区块，snapshot为交易快照。

返回：结果读写集，错误对象。

any GetRWSet(in *Block b)；

说明：返回读写集。

参数：b为区块。

返回：读写集，错误对象。

4.4 智能合约模块接口

4.4.1 数据类型定义

组件类型 ContractId为复合类型，合约标识结构，其包括：

name 合约名称

version 合约版本

openv 合约运行环境

组件类型 TxSimContext为any类型。交易执行上下文，用于缓存交易读写集。
组件类型 TxType为枚举类型，描述交易类型，取值可为：

USERINVOKE 用户合约调用

USERQUERY 用户合约查询

组件类型 ContractResult为复合类型，描述合约执行结果，其包括：

responseCode 结果返回码

message 返回消息

result 结果数据

resource 资源消耗

4.4.2 智能合约接口

继承：无

属性：无

方法：

*ContractResult RunContract(in *ContractId cid, in string method, in sequence<octet> byteCode, in map<string,string> parameters, in TxSimContext txContext, in long gasUsed, in TxType refTxType)

说明：运行合约以执行交易验证。

参数：cid为合约ID，method为调用的合约方法，byteCode为合约字节码，parameters为交易参数，txContext为上下文，gasUsed为资源消耗量，refTxType为交易类型。其中，cid、method、parameters和refTxType来自一条交易，byteCode和txContext来自链上，gasUsed来自字节码命令集的计算。

返回：交易验证结果。

4.5 共识算法模块接口

4.5.1 数据类型定义

组件类型NetMsg为复合类型，描述网络消息结构，其包括：

messageType 消息类型

message 交易消息体

targetNodeID 目标节点标识

4.5.2 共识算法接口

继承：无

属性：无

方法：

OnProposedBlock(in *Block b)；

说明：响应来自区块提议模块的通知，对候选区块进行共识。共识时须验证提议节点和候选区块的合法性，并在共识节点间执行共识算法。

参数：b为候选区块。

返回：无。

ConsensusMsg(in *NetMsg nmsg)；

说明：处理对等网络模块发来的消息。

参数：nmsg为共识消息。

返回：无。

4.6 对等网络模块接口

4.6.1 数据类型定义

消息类型 NetMsg_MsgType为枚举类型，取值可为：

TRANSACTION_MESSAGE 交易消息

BLOCK_MESSAGE 区块消息

CONSENSUS_MESSAGE 共识消息

4.6.2 对等网络接口

继承：无。

属性：无。

方法：

error BroadcastMsg(in sequence<octet> msg, in NetMsg_MsgType msgType)
说明：将消息（交易）广播到网络中所有节点。

参数：msg为要广播的消息字节数组，msgType为消息类型。

返回：错误对象。

error ConsensusBroadcastMsg(in sequence<octet> msg, in NetMsg_MsgType msgType)
说明：将消息（区块）广播给共识节点。

参数：msg为要广播的消息字节数组，msgType为消息类型。

返回：错误对象。

error OnReceiveNetMsg(in string from, in *NetMsg nmsg, in NetMsg_MsgType msgType)
说明：接收来自共识算法模块或对等网络模块的消息。

参数：from为消息来源，nmsg为消息内容，msgType为消息类型。

返回：错误对象。

4.7 区块验证模块接口

4.7.1 数据类型定义

候选区块验证类型 VerifyMode为枚举类型，取值可为：

CONSENSUS_VERIFY_MODE 共识验证模式

SYNC_VERIFY_MODE 同步验证模式

4.7.2 区块验证接口

继承：无。

属性：无。

方法：

error VerifyBlock(in *Blockb b, in VerifyMode mode)

说明：候选区块合法性验证。

参数：b为要验证的候选区块，mode为验证模式。

返回：错误对象。

4.8 区块执行模块接口

4.8.1 区块执行接口

继承：无。

属性：无。

方法：

error AddBlock(in *Blockb b)

说明：将已共识区块写入数据存储模块，并清理交易缓存模块中对应的交易集。
参数：b为已共识的区块。

返回：错误对象。

4.9 数据存储模块接口

4.9.1 数据存储接口

继承：无。

属性：无。

方法：

error PutBlock(in *Block b, in sequence<*TxRWSet> txRWSets)

说明：保存区块和对应读写集，并保证事务原子性。

参数：b为要保存的区块，txRWSets为一组交易读写集。

返回：错误对象。

any GetBlock(in long blockHeight)

说明：读取区块。

参数：blockHeight为区块高度。

返回：读到的区块对象，错误对象。

any GetTx(in string txId)

说明：读取交易。

参数：txId为交易标识。

返回：读到的交易对象，错误对象。

any ReadObject(in string contractName, in sequence<octet> key)

说明：读取账本上指定合约数据项的最新世界状态。

参数：contractName为合约名称，key为数据项关键字。

返回：世界状态数据，错误对象。

4.10 数据快照模块接口

4.10.1 数据快照接口

继承：无。

属性：无。

方法：

any GetKey(in long txExecSeq, in string contractName, in sequence<octet> key)

说明：读取快照。

参数：txExecSeq为交易执行序号，constractName为合约名称，key为关键字。

返回：快照数据，错误对象。

4.11 加密组件库接口

4.11.1 数据类型定义

组件类型 KeyType为枚举类型，密钥类型，可取值为：

SM4、AES、SM2、RSA1024、RSA2048、ECC_Secp256k1、ECC_Ed25519、ECC_NISTP256等
组件类型 PrivateKey为any类型，私钥

组件类型 HashType为枚举类型，哈希算法类型，可取值为：

SM3、SHA256、SHA3_256等

4.11.2 加密组件库接口

继承：无。

属性：无。

方法：

any Sign(in sequence<octet> data)

说明：私钥签名。

参数：data为待签数据。

返回：签名，错误对象。

any Verify(in sequence<octet> data, in sequence<octet> sig)

说明：签名验证。

参数：data为待验数据，sig为签名。

返回：是否通过验签，错误对象。

any GenerateKeyPair(in KeyType ktype)

说明：生成非对称密钥。

参数：kType为密钥类型。

返回：私钥，错误对象。

any Hash(in sequence<octet> data, in HashType htype)

说明：生成哈希。

参数：data为原始数据,hType为哈希类别。

返回：哈希数据，错误对象。

4.12 身份和权限管理模块接口

4.12.1 数据类型定义

组件类型 EndorsementEntry为复合类型，描述背书信息，其包括：

signerIdentity 签名者标识

message 签名信息

4.12.2 身份和权限管理接口

继承：无。

属性：无。

方法：

any CreatePrincipal(in string resourceName, in sequence<EndorsementEntry *> endorsements, in sequence<octet> message)

说明：为一次性授权创建规则。

参数：resourceName为资源名称，endorsements为背书列表，message为消息。
返回：新建规则，错误对象。

any VerifyPrincipal(in Principal prin)

说明：验证规则是否匹配资源的使用策略。

参数：prin为规则。

返回：是否匹配，错误对象。

4.13 调参模块接口

4.13.1 数据类型定义

组件类型 ChainConfig为any类型，描述链配置参数

4.13.2 调参接口

继承：无。

属性：无。

方法：

ChainConfig * ChainConfig()

说明：获取链的最新配置。

参数：无。

返回：最新配置。

error CompleteBlock(Block * b)

说明：区块插入数据库后的回调函数，更新链的配置。

参数：b为区块。

返回：错误对象。

4.14 跨链模块接口

4.14.1 数据类型定义

组件类型 srcChain为字符串类型，表示源链标识

组件类型 srcTxId为字符串类型，表示原链交易编号

组件类型 srcTxData为字节数组类型，表示原链交易信息

组件类型 dstChain为字符串类型，表示目标链标识

组件类型 dstTxId为字符串类型，表示目标链交易编号

组件类型 dstTxData为字节数组类型，表示目标链交易信息