**DAEX**

**数字资产钱包**

**技术对接**

|  |  |
| --- | --- |
| 版本号 | V1.0 |
| 修订日期 | 2019/09/05 |
| 修订人 | 李文萌 |

**ATOM资产钱包对接文档**

修订记录

|  |  |  |  |
| --- | --- | --- | --- |
| **版本号** | **修订内容** | **修订日期** | **修订人** |
| V1.0.0 | 制定文档 | 2019/9/05 | 李文萌 |

# 钱包对接文档

## 主链简介

### 项目背景

COSMOS是一个由多条平行区块链组成的去中心化网络，每条平行区块链均采用BFT公式算法（Tendermint）。COSMOS HUB是COSMOS的主链，也是链接其他区块链的中心，ATOM流行在HUB并用来锁定权益。

COSMOS官方网址：https://cosmos.network/

* + 1. **COSMOS项目共识**

COSMOS采用自主开发的Tendermint共识算法。体制内两种节点，负责达成状态一致的负责达成状态一致的节点称为“验证者”。任何愿意协助整个网络达成共识的参与节点都能成为验证者；作为回报，验证者会获得交易手续费和区块奖励。Tendermint 整合这些验证者的投票结果，确定下一个区块的正确状态；节点可以是轻节点或是全节点，而不是验证者，这类节点也被称为 “非验证者节点”。验证者及非验证者节点都要肩负传递数据的责任（例如提案数据、区块数据和投票数据），以确保所有节点都能收到系统正在产生的信息和交易。

1. 区块产生时间：7s
2. 交易确认时间：即时确认
   * 1. **COSMOS性能**

COSMOS主网当前性能：（理论200+）

* + 1. **COSMOS项目团队**
    2. **交易费**

**fees = ceil(gas \* gasPrices)**

**1atom = 1,000,000uatom**

**推荐价格：0.025uatom**

### 技术架构

### Github

https://github.com/cosmos

## 主链节点部署

<https://cosmos.network/docs/cosmos-hub/join-mainnet.html>

## 钱包及节点功能

**ATOM官方RPC文档地址**：

[https://tendermint.com/rpc/#/Info/blockchain](https://tendermint.com/rpc/" \l "/Info/blockchain)

### 接口：

本节主要介绍充值确认逻辑所需相关功能以及与其相关接口调用规则，根据相关主链的需求选择对应的功能和接口，以及介绍为满足钱包功能需求所需节点API的调用规则；

### 创建账户

**ATOM账户：**

1. ATOM账户格式一般满足如下要求：

地址是一个带有人类可读前缀的公共字符串(例如cosmos10snjt8dmpr5my0h76xj48ty80uzwhraqalu4eg)，用于标识帐户。账户创建的方式：使用助记词通过BIP32生成，操作时使用gaiacli命令生成（如gaiacli keys add <yourAccountName> --ledger）

### 一对一转账功能

1. 将交易信息由交易信息进行本地签名

### 查询交易功能

根据交易Hash查询交易信息

接口：https://stargate.cosmos.network/txs/{hash}

示例API：https://stargate.cosmos.network/txs/FF2CA1C6F28DBD4B172571A79F390AF635FA946CF60134CB50B78385C685C0FF

输入参数(Input)：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名称 | 数据类型 | 数据字节数 | 参数说明 |
| Hash | string | —— | 交易hash |

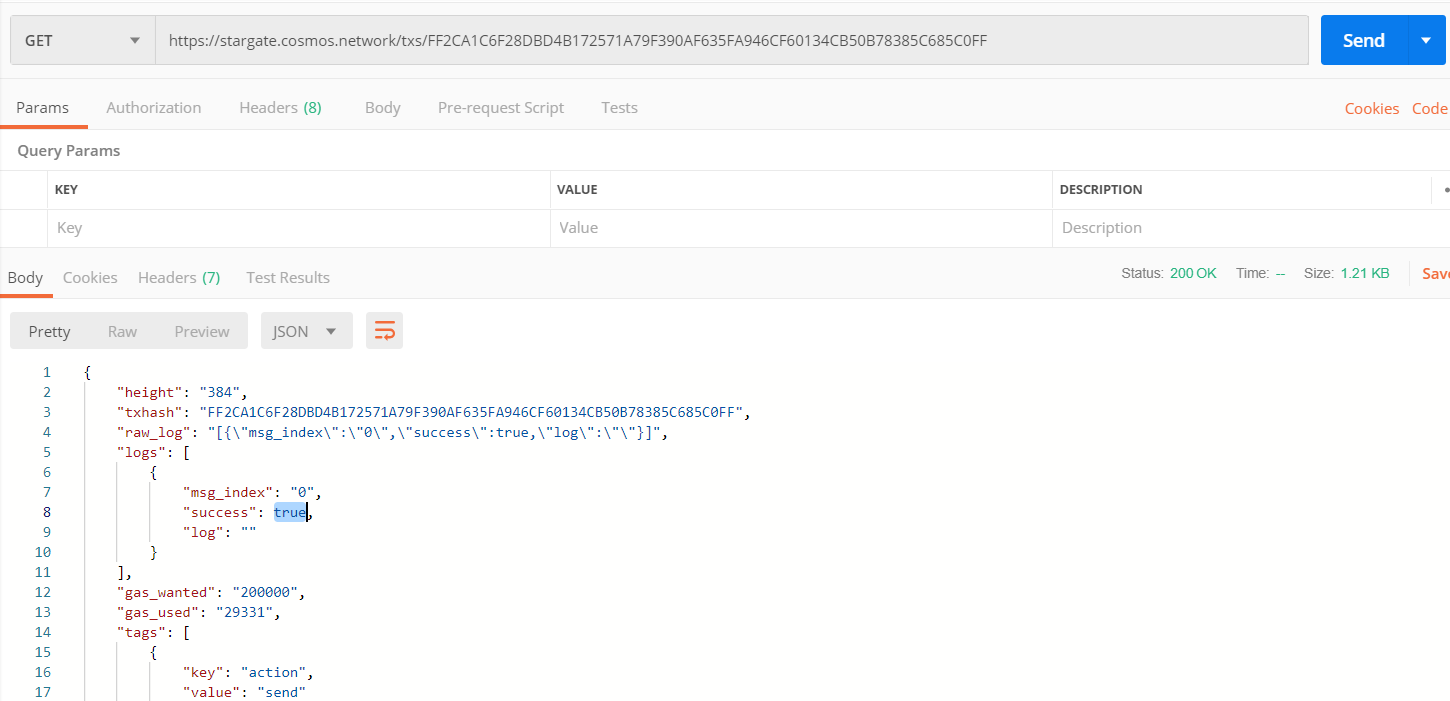
输出参数(Output)：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名称 | 数据类型 | 数据字节数 | 参数说明 |
| Hight | Int | —— | 区块高度 |
| Logs/success | String | —— | 交易状态 |
| Tx/value/msg/value | Object | —— | 交易地址和数量 |
| Tx/value/msg/fee | Object | —— | 交易手续费 |
| Memo | String | —— | 附加信息 |
| Timestamp | String | —— | 时间戳 |
| Tags | Array | —— | 交易属性 |

Tags字段

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名称 | 数据类型 | 数据字节数 | 参数说明 |
| Key：value | string | —— | 三对键值对，分别代表交易类型from和to |

**调用实例**



### 根据账户信息查询交易信息

API：<https://stargate.cosmos.network/bank/balances/cosmos14hncmchnakqwgsfla866kztd2qmd6puarp3r5y>

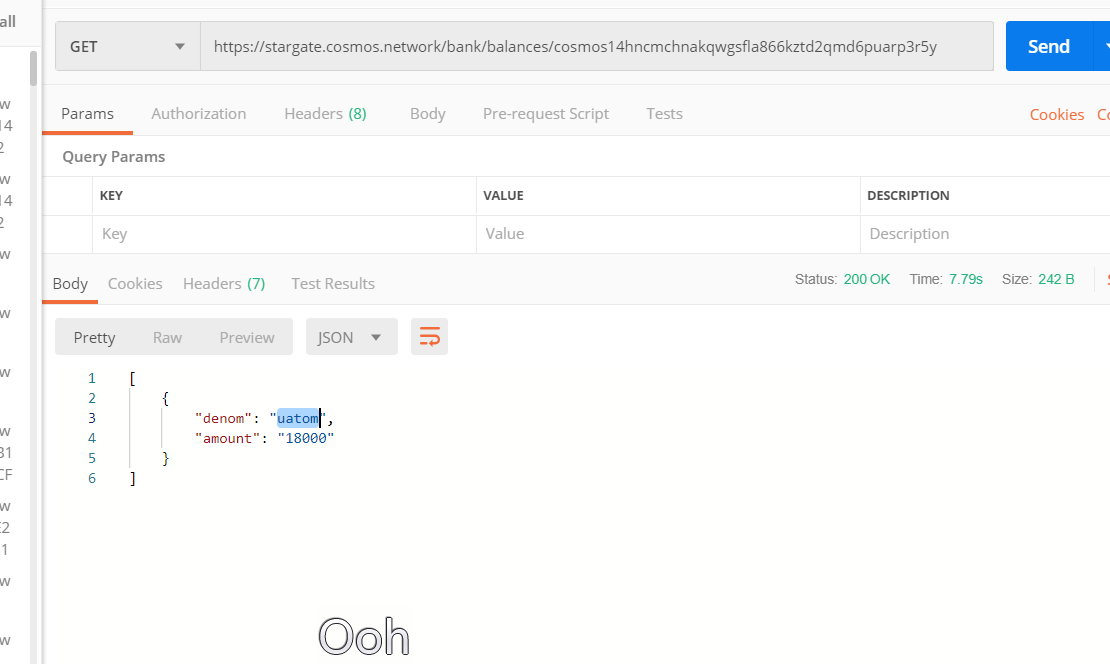
输入参数(Input)：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名称 | 数据类型 | 数据字节数 | 参数说明 |
| Address | string | —— | 地址 |

输出参数(Output)：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名称 | 数据类型 | 数据字节数 | 参数说明 |
| Denom | String | —— | 币种 |
| Amount | Int | —— | 数量 |

调用实例：



### 获取区块高度

获取当前区块的最新验证高度，API参考：curl -X GET https://stargate.cosmos.network:26657/block?

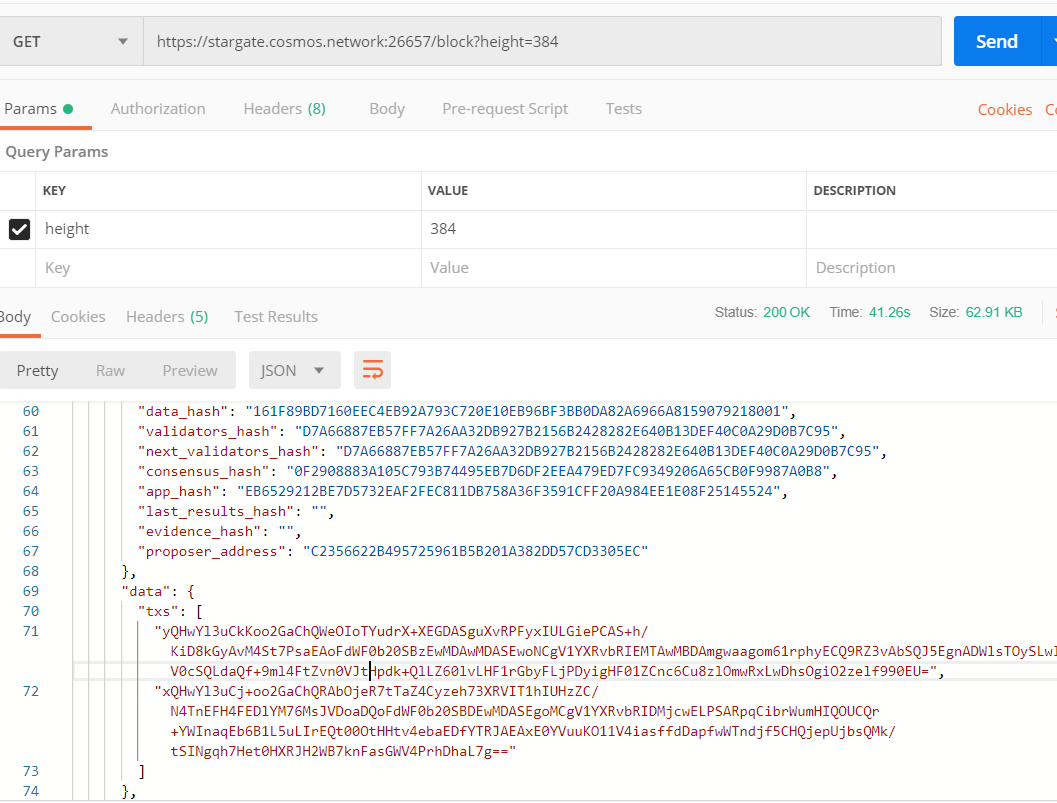
**输入参数**（Input）

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名称 | 数据类型 | 数据字节数 | 参数说明 |
| Height | Int | —— | 区块高度，为空则默认为零即为最新区块 |

**输出参数（Output）**

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名称 | 数据类型 | 数据字节数 | 参数说明 |
| Height | Int | —— | 区块高度，为空则默认为零即为最新区块 |
| Block/data/txs | Array | —— | 交易数组 |
| Time | String | —— | 时间戳 |
| Last\_black\_id/hash | String | —— | 上个区块hash |

**调用方式**



### 获取某高度区块

API参考：<https://stargate.cosmos.network:26657/block?height=1002>

即获取区块高度API，修改指定其Index即可，增加height参数 。

### 充值确认逻辑

#### 原生币ATOM充值确认逻辑

**ATOM充值确认逻辑：**

1. 交易所采用block获取ATOM主链接点的最近验证区块高度，记为H1；
2. 交易所获取当前ATOM主链的扫描区块高度，记为：H2；
3. 当H1-H2H，当前扫描的ATOM区块已经达到安全高度，利用GET/block获取H2+1的区块信息;
4. 读取区块信息，获取hight、time、last\_black\_id字段用于记录区块信息，读取txs字段获取交易数据集合，循环读取每条交易记录，获得hash值后调用交易查询接口根据获取交易数据中，tags中的键值对字段用于记录交易信息，判断**logs中值为true&** **tags字段中action对应值为send &**

**Tx中to\_address字段为交易所充值地址&**

**Ledger\_index<Transactions.LastLedgerSequence&**

**Tx.value.msg.value.amount.denom字段为uatom(币种)&Tx.value.msg.value.amount.amount实际充值金额&**

**memo或SourceTag字段为附加信息标记来源**，则对充值交易信息进行入账操作；否则不做处理（官方判断方式）；

1. 交易所内部转账操作只设计账户余额的变化，暂无上链操作；

### 3.5提现逻辑

交易所采用1对1发起交易从交易所ATOM地址发送ATOM到用户地址

## 可视化工具区块链浏览器

### 区块链浏览器

1. 地址：https://www.mintscan.io/
2. 地址：https://hubble.figment.network/chains/cosmoshub-1
3. 地址：https://cosmos.bigdipper.live/

问题：由于使用接口查询出来的区块包含的tx信息都是经过编码的，cosmos的amino编码机制网址：<https://github.com/tendermint/go-amino/blob/master/binary-decode.go>

目前不清楚解码之后是hash值还是完整的交易信息