



链滴

Omni Layer 区块链 PHP 开发包【USDT 对接】

作者: [ciga2011](#)

原文链接: <https://ld246.com/article/1559830040215>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

OmniTool开发包适用于为PHP应用快速增加对Omni Layer/USDT数字资产的支持能力，即支持使用有Omni Layer节点的应用场景，也支持基于第三方API服务和离线裸交易的轻量级部署场景。下载地址：[omni/usdt php开发包](#)。

1、OmniTool开发包简介

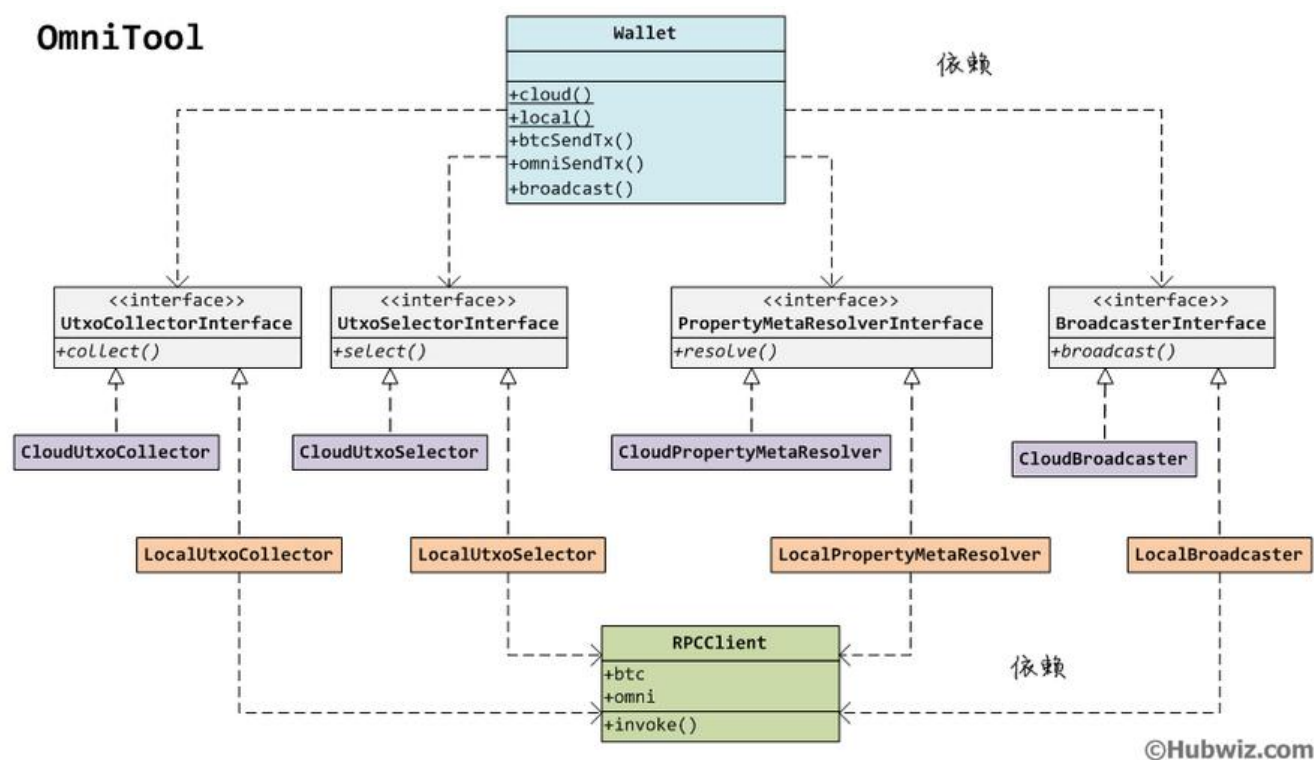
OmniTool开发包主要包含以下特性：

- 完善的Omni Layer节点RPC封装
- 支持利用自有节点或第三方服务获取指定地址的utxo集合
- 支持离线生成omni代币转账裸交易
- 支持利用自有节点或第三方服务广播裸交易

OmniTool支持本地部署的Omnicores节点，也支持blockchain.info、btc.com等提供的开放API，增加对其他第三方服务的支持也非常简单，只需要参考代码实现如下接口：

- UtxoCollectorInterface：utxo收集器
- UtxoSelectorInterface：utxo筛选器
- BroadcasterInterface：裸交易广播器
- ExplorerInterface：数据查询接口

OmniTool软件包运行在**Php 7.1+**环境下，当前版本1.0.0，主要类/接口及关系如下图所示：



OmniTool的主要代码文件清单如下：

```
<table class="table table-striped">
<thead>
<tr><th>代码文件</th><th>说明</th></tr>
```

```

</thead>
<tbody>
  <tr><td>omni.php/src/RpcClient.php</td><td>Omni Layer的RPC协议封装类</td></tr>
  <tr><td>omni.php/src/RpcModule.php</td><td>Omni Layer的RPC协议分模块访问语法糖</td></tr>
  <tr><td>omni.php/src/protocol-spec.json</td><td>Omni Layer协议描述元信息</td></tr>
  <tr><td>omni.php/src/SerializeBuffer.php</td><td>Omni Layer协议序列化缓冲区</td></tr>
  <tr><td>omni.php/src/PayloadFactory.php</td><td>Omni Layer协议载荷工厂类</td></tr>
  <tr><td>omni.php/src/Utxo.php</td><td>未消费交易输出类</td></tr>
  <tr><td>omni.php/src/UtxoBag.php</td><td>Utxo集合类</td></tr>
  <tr><td>omni.php/src/UtxoCollectorInterface.php</td><td>Utxo收集器接口</td></tr>
  <tr><td>omni.php/src/LocalUtxoCollector.php</td><td>基于OmniCore节点的Utxo收集实现</td></tr>
  <tr><td>omni.php/src/CloudUtxoCollector.php</td><td>基于第三方服务的Utxo收集器实现</td></tr>
  <tr><td>omni.php/src/UtxoSelectorInterface.php</td><td>Utxo筛选器接口</td></tr>
  <tr><td>omni.php/src/DefaultUtxoSelector.php</td><td>默认的Utxo筛选器实现</td></tr>
  <tr><td>omni.php/src/BroadcasterInterface.php</td><td>裸交易广播器接口</td></tr>
  <tr><td>omni.php/src/LocalBroadcaster.php</td><td>基于OmniCore节点的裸交易广播器实现</td></tr>
  <tr><td>omni.php/src/CloudBroadcaster.php</td><td>基于第三方服务的裸交易广播器实现</td></tr>
  <tr><td>omni.php/src/ExplorerInterface.php</td><td>数据查询接口</td></tr>
  <tr><td>omni.php/src/CloudExplorer.php</td><td>基于第三方服务的数据查询接口实现</td></tr>
  <tr><td>omni.php/src/LocalExplorer.php</td><td>基于OmniCore节点的数据查询接口实现</td></tr>
  <tr><td>omni.php/src/Utils.php</td><td>常用辅助函数</td></tr>
  <tr><td>omni.php/src/Wallet.php</td><td>离线钱包类</td></tr>
  <tr><td>demo/rpc-demo.php</td><td>RpcClient使用示例，完整实现OMNI代币的发行与账</td></tr>
  <tr><td>demo/omni-tx-cloud.php</td><td>创建并广播Omni代币转账裸交易，使用第三方服务API</td></tr>
  <tr><td>demo/omni-tx-local.php</td><td>创建并广播Omni代币转账裸交易，使用自有节点</td></tr>
  <tr><td>demo/btc-tx-cloud.php</td><td>创建并广播比特币转账裸交易，使用第三方云服务PI</td></tr>
  <tr><td>demo/btc-tx-local.php</td><td>创建并广播比特币转账裸交易，使用自有节点</td></tr>
  <tr><td>demo/explorer-cloud.php</td><td>查询指定的地址比特币余额/Omni代币余额，用第三方云服务API</td></tr>
  <tr><td>demo/explorer-local.php</td><td>查询指定地址的比特币余额/Omni代币余额，使用自有节点</td></tr>
  <tr><td>demo/wallet-init.php</td><td>本地钱包初始化</td></tr>
  <tr><td>demo/wallet-demo.php</td><td>钱包载入、裸交易构造和广播</td></tr>
  <tr><td>vendor</td><td>第三方依赖包目录</td></tr>
  <tr><td>composer.json</td><td>composer配置文件</td></tr>
</tbody>
</table>

```

2、RpcClient类使用说明

RpcClient类封装了Omni Layer的RPC接口协议。创建RpcClient对象时，需要传入包含有效身份信息的节点RPC URL。例如，假设安装在本机的omnicored节点软件配置如下：

- rpcuser: user
- rpcpassword: 123456
- rpcport: 8332

那么可以使用如下的代码来实例化RpcClient：

```
use \OmniTool\RpcClient;

$client = new RpcClient(
    'http://user:123456@localhost:8332' /*节点RPC接口的URL*/
);
```

Omni Core节点在Bitcoin原有的RPC接口之外，扩充了额外的接口用来操作Omni层的数据，这些扩充的RPC接口采用omni_前缀以区别于Bitcoin的原有RPC接口。为了便于区隔这两层的RPC调用，RpcClient引入了协议子模块的概念，将Bitcoin的原始RPC接口和Omni的扩展RPC接口分别挂接到btc子模块和omni子模块。

例如，获取某个地址的USDT代币余额需要使用Omni层的omni_getbalance调用，这个RPC调用对于RpcClient实例的omni子模块的getBalance()方法。下面的代码获取地址1EXoDusjGwvnjZUyKkxZUHEf77z6A5S4P的USDT（资产ID:31）余额：

```
$ret = $client->omni->getBalance(
    '1EXoDusjGwvnjZUyKkxZ4UHEf77z6A5S4P', /*地址*/
    31 /*资产ID: USDT*/
);
```

类似的，可以使用omni_send调用来执行简单的USDT转账，这个调用对应于RpcClient实例的omni模块的send()方法。下面的代码从地址3M9qvHKtgARhqcMtM5cRT9VaiDJ5PSfQGY向地址37FaKpnF7zqoMLUjEiko25pDiuVH5YLEa

转入100.0个USDT代币：

```
$ret = $client->omni->send(
    '3M9qvHKtgARhqcMtM5cRT9VaiDJ5PSfQGY', /*代币转出地址*/
    '37FaKpnF7zqoMLUjEiko25pDiuVH5YLEa', /*代币转入地址*/
    31, /*代币ID: USDT*/
    "100.00" /*转移的代币数量*/
);
```

原有的bitcoin层的RPC接口则可以通过RpcClient的btc子模块来访问。例如，使用listunspent调用来取本地节点中指定地址的utxo：

```
$ret = $client->btc->listUnspent(
    6, /*最小确认数*/
    999999, /*最大确认数*/
    ['mgnucj8nYqdrPFh2JfZSB1NmUThUGnmsqe'] /*地址清单*/
);
```

开发包中的demo/rpc-demo.php示例代码使用RpcClient类完整演示了在Omni层的代币发行与转账

能，如果你计划搭建自己的Omni Core节点，相信这个示例会有很大帮助。

3、Wallet类使用说明

如果不愿意搭建自己的Omni Core节点，而是希望基于第三方API为自己的PHP应用增加对Omni Layer/USDT的支持，那么最简单的方法是使用离线交易的入口类**Wallet**。

Wallet类的主要作用是根据创建并广播Omni代币转账裸交易或比特币转账裸交易，它的基本使用步骤如下：

- 使用 `Wallet::cloud()`静态方法创建一个支持云端API服务的Wallet实例
- 使用 `addKey()`方法将必要的私钥加入该Wallet实例，例如转出地址的私钥，因为Wallet需要利用私钥对裸交易进行签名
- 使用 `omniSendTx()`方法生成Omni代币转账裸交易，或者使用**`btcSendTx()`**方法比特币转账裸交易
- 使用 `broadcast()`方法广播裸交易

3.1 Omni代币转账

使用Wallet实现的Omni代币转账示例代码如下，说明见注释：

```
<?php
require('../vendor/autoload.php');

use OmniTool\Wallet;                                /*引入开发包*/

$wallet = Wallet::cloud(
    './demo.wallet',                                /*钱包文件地址，自动创建*/
    'testnet'                                        /*网络ID*/
);
$privKey = '4aec8e45106....00d5c5af494a4e05b';    /*私钥：16进制字符串*/
$wallet->addKey($privKey);                          /*将私钥加入钱包，只需加入一次*/

$addressList = $wallet->getAddressList();           /*返回钱包管理的所有地址，数组*/

$rawtx = $wallet->omniSendTx(
    $addressList[0],                                /*发送方地址，私钥必须已经加入钱包*/
    'mgYPLmNuZymK...e2XUNF6VFtT',                /*接收方地址*/
    2,                                              /*转账OMNI代币ID，2：TOMN*/
    '0.000001'                                     /*转账OMNI代币数量*/
);

$ret = $wallet->broadcast($rawtx);                  /*广播OMNI裸交易*/
var_dump($ret);
```

注意：

- Wallet实例利用钱包中的私钥生成地址列表，并利用这些地址从第三方服务获取utxo信息。因此要钱包中的私钥对应地址在链上有utxo存在，Wallet对象才能够成功构造裸交易。
- 转账目标地址应当与创建Wallet对象时指定的链ID一致，例如mainnet的p2pkh地址，前缀应当为1

3.2 指定Omni交易的手续费支付地址

在Omni协议层不需要支付交易手续费，但是Omni交易所嵌入的比特币交易依然需要支付手续费。默认情况下`omniSendTx()`方法使用发送方地址支付比特币交易手续费，但可以传入额外的参数来指定其地址支付交易手续费，当你的PHP应用需要实现多账户归集功能时，使用统一的手续费支付地址会更容易管理一些。

例如，下面的代码使用地址`mnRo8JyTHDd5NxRb3UvGbAhCBPQTQ4UZ8W`支付omni交易的手续：

```
$rawtx = $wallet->omniSendTx(  
    $addressList[0],          /*发送方地址，私钥必须已经加入钱包*/  
    'mgYPLmNuZymK...e2XUNF6VFnT', /*接收方地址*/  
    2,                        /*转账OMNI代币ID， 2: TOMN*/  
    '0.000001',              /*转账OMNI代币数量*/  
    'mnRo8JyTHDd5...CBPQTQ4UZ8W' /*交易手续费支付地址*/  
);
```

注意：

- 即使指定了余额充足的手续费支付地址，Omni交易的发送方依然必须有微量的比特币 余额（546 ATOSHI），因为Omni协议需要交易发送方至少有一个可用UTXO。
- 手续费支付地址同时也是找零地址，多余的比特币将返回至该地址

3.3 指定Omni交易的比特币转账数量

由于Omni交易要求发送方必须有可用的UTXO，因此为了便于接收Omni代币的地址可以继续流通所有的Omni代币，`omniSendTx()`方法在默认情况下将向接收方地址转入微量的比特币（546 SATOSH），可以在调用该方法时修改这个默认数值。

例如，下面的代码转入接收方1000个SATOSHI：

```
$rawtx = $wallet->omniSendTx(  
    $addressList[0],          /*发送方地址，私钥必须已经加入钱包*/  
    'mgYPLmNuZymK...e2XUNF6VFnT', /*接收方地址*/  
    2,                        /*转账OMNI代币ID， 2: TOMN*/  
    '0.000001',              /*转账OMNI代币数量*/  
    'mnRo8JyTHDd5...CBPQTQ4UZ8W', /*交易手续费支付地址*/  
    1000                      /*转账比特币数量，单位：SATOSHI*/  
);
```

3.4 比特币转账

OmniTool也支持比特币转账裸交易的生成与广播。

例如，下面的代码从钱包的第一个地址向指定接受地址转入1000个SATOSHI：

```
<?php  
require('../vendor/autoload.php');  
  
use OmniTool\Wallet;  
  
$wallet = Wallet::cloud('../demo.wallet','testnet');  
$addressList = $wallet->getAddressList();
```

```

$rawtx = $wallet->btcSendTx(
    $addressList[0],          /*发送方地址*/
    'moneyqMan7u...8qVrc9ikLP', /*接收方地址*/
    1000,                     /*转账比特币数量, 单位: SATOSHI*/
    500,                      /*手续费, 单位: SATOSHI*/
);
echo 'btc rawtx => ' . $rawtx . PHP_EOL;

$ret = $wallet->broadcast($rawtx);          /*广播裸交易*/

```

默认情况下, `btcSendTx()` 使用发送方地址作为找零地址, 也可以在调用时指定其他地址作为找零地, 例如, 下面的代码创建一个新地址接收找零:

```

$changeAddress = $wallet->getNewAddress(); /*创建新地址*/
$rawtx = $wallet->btcSendTx(
    $addressList[0],          /*发送方地址*/
    'moneyqMan7u...8qVrc9ikLP', /*接收方地址*/
    1000,                     /*转账比特币数量, 单位: SATOSHI*/
    500,                      /*手续费, 单位: SATOSHI*/
    $changeAddress            /*找零地址*/
);

```

4、UTXO收集器

OmniTool使用接口 `UtxoCollectorInterface` 来约定UTXO的收集功能。该接口的实现需要支持获取地址的候选UTXO集合, 可指定多个地址。

接口方法:

- `collect($addressList)`: 提取并返回候选UTXO集合

参数 `$addressList` 用来声明要收集UTXO的地址清单, 类型为数组。

当前实现类:

- `CloudUtxoCollector`: 基于blockchain.com的开放API实现的Utxo收集器
- `LocalUtxoCollector`: 基于omnicored节点RPC API实现的Utxo收集器

例如, 下面的代码使用 `CloudUtxoCollector` 获取地址 `mi8BvbK73nDQfaN3acpaFGYQKhfQ5ysKRn` UTXO:

```

use OmniTool\CloudUtxoCollector;

$collector = new CloudUtxoCollector(
    'testnet'          /*测试网*/
);
$candidateBag = $collector->collect(
    ['mi8BvbK73nDQ...KhfQ5ysKRn'] /*地址清单*/
);

```

5、UTXO筛选器

OmniTool使用 `UtxoSelectorInterface` 来约定UTXO筛选功能。该接口的实现需要根据目标金额从候

UTXO中选择可用UTXO，并返回新的UtxoBag实例。

接口方法：

- select(**target**,candidates): 选择可消费UTXO，返回UtxoBag对象

参数**\$target**声明要达成的最低金额目标，单位：wei。

参数**\$candidates**是候选的utxo集合，通常是UtxoCollectorInterface实现对象的collect()调用返回的txoBag对象。

当前实现类：

- DefaultUtxoSelector

例如下面的代码使用DefaultUtxoSelector实例从候选UTXO中删选出至少100000 wei 的UTXO：

```
use OmniTool\DefaultUtxoSelector;

$selector = new DefaultUtxoSelector();
$selectedBag = $selector->select(
    100000,           /*最低目标金额*/
    $candidateBag     /*候选UTXO集合*/
);
```

考虑到UTXO的不可分割性，筛选出的若干UTXO的总和，有可能超过目标金额。可以使用UtxoBag例的**getTotal()**方法查看集合中的UTXO总额：

```
echo 'total wei in bag => ' . $selectedBag->getTotal() . PHP_EOL;
```

6、裸交易广播器

OmniTool使用**BroadcasterInterface**来约定裸交易广播的功能。该接口的实现应当将裸交易广播到Omni网络中。

接口方法：

- broadcast(\$rawtx): 广播裸交易

参数**\$rawtx**用来声明要广播的裸交易，类型为16进制字符串。

当前实现类：

- CloudBroadcaster
- LocalBroadcaster

例如，下面的代码使用CloudBroadcaster将裸交易码流广播到Omni网络中：

```
use OmniTool\CloudBroadcaster;

$broadcaster = new CloudBroadcaster(
    'testnet'           /*测试网*/
);
$ret = $broadcaster->broadcast(
```

```
'01000000011da9283b4...59f58488ac00000000' /*裸交易*/  
);
```

7、数据查询接口

OmniTool使用`ExplorerInterface`来约定Omni数据查询功能。

接口方法：

- `getBtcBalance($address)`: 查询指定地址的比特币余额
- `getOmniBalance( address,propertyId)`: 查询指定地址的Omni代币余额

当前实现类：

- `CloudBroadcaster`
- `LocalBroadcaster`

例如，下面的代码使用`CloudExplorer`查询地址`1Jekm8ZswQmDhLFMp9cuYb1Kcq26riFp6m`的比特币余额与USDT代币余额：

```
use OmniTool\CloudExplorer;  
  
$explorer = new CloudExplorer('mainnet');  
  
$address = '1Jekm8ZswQmDhLFMp9cuYb1Kcq26riFp6m';  
  
$balance = $explorer->getBtcBalance($address);  
echo 'btc balance => ' . PHP_EOL;  
  
$balance = $explorer->getOmniBalance($address,31);  
echo 'usdt balance => ' . $balance['balance']. PHP_EOL;
```

OmniTool下载地址：<http://sina.lt/gbpd>