# Guide

1	Usage	e of Achain wallets	2
	1.1	Achain wallets under Windows	2
	1.2	Achain wallet under Linux	2
	1.3	Docker wallet	2
	1.4	Wallet synchronization	3
	1.5	Create wallet	4
	1.6	Create accounts	4
2	Get transaction history		5
	2.1	block scanning step	5
	2.2	ori_trx_id and result_trx_id	6
3	ACT transaction		6
	3.1	Query ACT transaction	6
	3.2	Query ACT balance	8
	3.3	Withdraw ACT	9
4	Contract token transaction		9
	4.1	Query contract transaction	9
	4.2	Query contract token balance	11
	4.3	Withdraw of contract token	12
5	ASSET transaction		13
	5.1	Query ASSET ID	13
	5.2	Query ASSET transaction	14
	5.3	Query ASSET balance	16
	5.4	Withdraw ASSET	17

# 1 Usage of Achain wallets

## 1.1 Achain wallets under Windows

- 1. Official download address: <a href="https://www.achain.com/home.html">https://www.achain.com/home.html</a>
- 2. Start the wallet (2 kinds of startup method: QT and command line)
  - 1. QT method, double click the icon.
  - 2. Command line method: First go to the directory of the Achain wallet. Then start the wallet using command:

Achain-c.exe --rpcuser admin --rpcpassword 123456 --httpdendpoint 127.0.0.1:8299 --server --data-dir d:\config

## 1.2 Achain wallet under Linux

- 1. Official download address: https://github.com/Achain-Dev/Achain\_linux
- 2. The code need to be compiled. Compiling method refer to document:

  https://github.com/Achain-Dev/Achain\_linux/blob/master/linux\_installation\_guide
- 3. After compiling, start the wallet using command:

Achain --rpcuser admin --rpcpassword 123456 --httpdendpoint 127.0.0.1:8299 --server

## 1.3 Docker wallet

- 1. Official download address: <a href="https://github.com/Achain-Dev/Docker">https://github.com/Achain-Dev/Docker</a>
- 2. To start the wallet please refer to document:

https://github.com/Achain-Dev/Docker/blob/master/README.md

## Introduction of relevant Parameters:

- 1, rpcuser: username to start the rpc command;
- 2 rpcpassword :password to start the rpc command;
- 3. httpdentpoint :ip address of the http request. (Docker wallet don't need to set this parameter)
- 4. data-dir: storage path of the sync data.

## 1.4 Wallet synchronization

After starting the wallet, the wallet automatically connects the potential node and starts to update block information.

Do not use RPC command until the wallet synchronized to the newest block.

You can use info command to check the synchronization on.

Mainly concern three parameters:

The first is blockchain\_head\_block\_num, this is the current block number o

The second is blockchain\_head\_block\_age, this is the age of the current block. We generate new block every10 seconds. Therefore if this parameter is bigger than 10 seconds, the synchronization is not over yet.

The third is network\_num\_connection, this is the current connection number. If this equals 0, the synchronization won't start. This problem need to be solved in time.

Note: During synchronization, there will be delays or errors when calling RPC command.

Please call RPC command after synchronization.

For example:

```
(wallet closed) >>> info
 "blockchain_head_block_num": 1140371,
 "blockchain_head_block_age": "O second_o<del>ld"</del>
 "blockchain_head_block_timestamp": "2017-12-01T09:17:00",
 "blockchain_head_block_id": "f56bf37b0f76a16c46aef0ede5ad2f8d3239006c",
 "blockchain_average_delegate_participation": "100.00 %",
 "blockchain_confirmation_requirement": 1,
 "blockchain_share_supply": "1,005,701,855.00000 ACT",
 "blockchain_blocks_left_in_round": 10,
 "blockchain_next_round_time": "at least 2 minutes in the future",
 "blockchain_next_round_timestamp": "2017-12-01T09:18:40",
 "blockchain_random_seed": "75817d1800ba89e30d96f0b4f8e306a6d3a916ab",
 "client_data_dir": "d:/config",
 "client_version": "3.1.3",
 "network_num_connections": 15.
 "network_num_connections_max": 200,
 "network_chain_downloader_running": false,
 "network_chain_downloader_blocks_remaining": null,
 "ntp_time": "2017-12-01T09:17:00",
 "ntp_time_error": "-1.579765000000000010",
 "wallet_open": false,
 "wallet_unlocked": null,
 "wallet_unlocked_until": null,
 "wallet_unlocked_until_timestamp": null,
 "wallet_last_scanned_block_timestamp": null,
 "wallet_scan_progress": null,
 "wallet_block_production_enabled": null,
 "wallet_next_block_production_time": null,
 "wallet_next_block_production_timestamp": null
```

## 1.5 Create wallet

Use command wallet\_create to create wallet. User accounts are saved in this wallet.

There are two parameters: first is the wallet name, second is the wallet password.

After the creation of the wallet, the wallet is unlock automatically.

For example:

```
(wallet closed> >>> wallet_create wallet wallet01
0K
```

#### 1.6 Create accounts.

Docking exchange management user mode:

Only create a main account. You can use sub\_address to separate user account by stitching 32bit sub\_address after the main account. (you can choose UUID by removing "-") Benefit:

When transferring ACT, the sub\_address will do bookkeeping work. You don't need to collect your funds.

The sub\_address method is recommended.

RPC command: wallet\_account\_create, the parameter is the account name.

This command return the address of the account. If the return value is none or error, the account name might be registered or invalid.

After doing the work we finish the preparation of the wallet.

wallet01 (unlocked) >>> wallet\_account\_create act01 ACTHE6bM2get3PkBCaG6kooA2xEXz4oEHQ6s

Subaddress for example :(the last 32 bits can be randomly generated by letters and Numbers themselves)

ACTM7pZQY7HU1wDNX2G2Wsw59s39VLBQRbw20f9c62a8385499b57304 f9d6b04eee0

# 2 Get transaction history

# 2.1 block scanning step

Get transaction history by block scanning, step follows:

1.call RPC method blockchain\_get\_block\_count to get the header block number.

2.call RPC method blockchain\_get\_block to query one block. The parameter is the block number.

3.call RPC method blockchain\_get\_transaction to judge the type of transaction(The logic of judgment is detailed in each section).

call RPC method blockchain\_get\_pretty\_contract\_transaction, for not contract transaction

call RPC method blockchain\_get\_pretty\_contract\_transaction, for contract transaction,

Note: The field "user\_transaction\_ids": []. If this field is empty, there is no transaction on this block. You can scan the next block If not empty, then do the transaction query job. user\_transaction\_ids records the trx\_id of transaction.

#### For example:

```
(wallet closed) >>> blockchain_get_block 1148371
(
    "previous": "a9652f371cf938671798f18f1eb7db424e364948",
    "block_num": 1148371.
    "block_num": 1148371.
    "inest_apm;" "2017-12-01109:17:00",
    "transaction_digest": "c8ef12fe3180ed981a58a8697a5222f1217de72d04529b4255627a4ad6164f8f8",
    "revt_seret_hash": "1328e82b218665f36441454430466b938a9a2d6",
    "previous_secret": "5442f8c1e384968b962d2333b56f1590170c2acd",
    "delegate_signature": "1f2195ef7582b5562b4b42327266b3e119b0daf11e4b3c4f82a6a2de0be21c03693132953a09ada312f3dc2441f291a5522fb18ad4320b2a48dd1b256a547de5dc",
    "user_transaction_ids": [1,
    "id": "f5bh37bh0f76af6d6aef0de6dead2f8d3239006c",
    "block_size": 166,
    "latency": 0,
    "signee_shares_issued": 0,
    "signee_shares_issued": 0,
    "signee_shares_issued": 0,
    "signee_fees_collected": 0,
    "processing_time": 0
```

Note: trx\_id is from the block fields user\_transaction\_ids

(Transaction id on achain browser: trx\_id for ACT transaction, ori\_trx\_id for contract calling)

## 2.2 ori\_trx\_id and result\_trx\_id

ori\_trx\_id and result\_trx\_id only occurs on contract calling. They are not occurred in ACT transaction.

ori\_trx\_id records the origin transaction, that is, the transaction relative to ACT. Therefore, when calling contract, ori\_trx\_id only records the costs of ACT, fee and call contract cost limit. As for the contract user are calling, the ori\_trx\_id only records the calling method and parameters. It won't record the result of the contract. So, the result of transaction called by RPC command is ori\_trx\_id.

result\_trx\_id records the complete transaction on the block. Except the ACT transaction we described above, the result\_trx\_id also records whether the calling contract is successful and the result of the calling contracts. The transaction id gotten by scanning block is result\_trx\_id.

# 3 ACT transaction

This step needs to be done on the basis of steps 1 and 2. Please note.

## 3.1 Query ACT transaction

Call RPC method blockchain\_get\_block\_count to get the header block number.

Call RPC method blockchain\_get\_block to query one block. The parameter is the block number.

1.Call RPC command blockchain\_get\_transaction. Parameter is trx\_id in field

user\_transaction\_ids (blockchain\_get\_block responsed).

2. If the alp\_inport\_asset field is asset\_id, which is 0 (the value must be judged), and the first type value in the operation field is withdraw\_op\_type or deposit\_op\_type, the transaction is ACT transaction.

Get if there is sub-address transaction. The field alp\_account is the deposit address. The figure is a transaction with sub-address. You can get sub-address from field alp\_account.

For example:

3.Call RPC method blockchain\_get\_pretty\_transaction to get the from and to account of this transaction, the parameter is trx\_id.

from\_account: withdraw address

 $to\_account: deposit\ address$ 

amount: 100,000 times of the transaction amount.

For example:

```
"is_virtual": false,
"is_confirmed": true,
"is_market": false,
"is_market_cancel": false,
"trx_id": "f7b58cecabc5a0a8cd8cc8244a6141f99feb29c5",
"block_num": 60435,
"block_position": 0,
"trx_type": 0,
"ledger_entries": [{
    "from_account": "ACTAGSsqKCRkyadVtqqeMZcPXot6dhTGbHGU",
    "from_account_name": "",
    "to_account": "ACTKwXoKGtYiby6fnohvsQpaCkm5Gd12wZ94",
    "to_account_name": "",
    "amount": {
        "amount": 1000000,
        "asset_id": 0
        },
        "memo": "",
        "running_balances": []
    }
}
```

# 3.2 Query ACT balance

Use RPC command: blockchain\_list\_address\_balances. The parameter is ACT address.

Return: Parse the result. Get all the values of the balance field with 0 asset\_id, and then sum, that is, the ACT balance on the address (10<sup>5</sup> times)..

```
>>> blockchain_list_address_balances ACT3AF1r1MuJMTk$RbKPLM1wkwPysyKJyfT0
"ACT9DXH9DUkxwgweWkUfqk25qekargGUCgqK",{
  'condition": {
    "asset_id": 1,
    "slate_id": 0,
    "type": "withdraw_signature_type",
    "balance_type": "withdraw_common_type",
    "data": {
      "owner": "ACT3AF1r1MuJMTkSRbKPLM1wkwPysyKJyfTQ"
  "balance": 400000,
 "deposit_date": "2018-03-01T08:17:19",
 "last_update": "2018-03-01T09:02:00",
  "meta_data": null
'ACTPDPXAUU2bfNJentAX2CriFpnhFDTAFnqE",{
  "condition": {
   "asset_id": 0,
"slate_id": 0,
"type": "withdraw_signature_type",
    "balance_type": "withdraw_common_type",
      "owner": "ACT3AF1r1MuJMTkSRbKPLM1_kwPysyKJyfTQ"
 "balance": "500010000000",
 "deposit_date": "2018-03-01T09:25:20",
"last_update": "2018-03-01T09:25:20",
  "meta_data": null
  (unlocked) >>>
```

## 3.3 Withdraw ACT

Call RPC method wallet\_transfer\_to\_address to withdraw ACT. Before calling this method, we should open and unlock wallet. This method need 4 parameters. The first is withdraw ACT amount. This is true transaction amount. The second is const string "ACT". The third is withdraw account name. The forth is the deposit ACT address. This method will return a transaction id, which is trx\_id.

## 4 Contract token transaction

This step needs to be done on the basis of steps 1 and 2. Please note.

## 4.1 Query contract transaction

Call RPC method blockchain\_get\_block\_count to get the header block number.

Call RPC method blockchain\_get\_block to query one block. The parameter is the block number. Then perform the following steps:

- 1.Call RPC command: blockchain\_get\_transaction to get the from and to account of this transaction. Parameter is trx\_id in field user\_transaction\_ids (blockchain\_get\_block responsed).
- 2.In field operation, if the value of field type is transaction\_op\_type, this is contract transaction.

```
vallet (locked) >>> blockchain_get_transaction fd88fb7d1b3aac1fe617f8332fdcb62db047117e
 "fd88fb7d1b3aac1fe617f8332fdcb62db047117e",{
    "trx": {
      "expiration": "2017-12-05T10:01:49",
"alp_account": "",
      "alp_inport_asset": {
    "amount": 0,
        "asset_id": 0
      "operations": [{
          "type": "transaction_op_type",
          "data": {
             "trx": {
               "expiration": "2017-12-05T10:01:49",
               "alp_account": ""
               'alp_inport_asset": {
    "amount": 0,
                 "asset_id": 0
               'operations'': [{
                   "type": "call_contract_op_type",
                   "data": {
                      "caller": "ACT7UZfdCJoNGzeAiEuK7dxzdtQzzhXWu5F2UmZ9fcNc2JKQLRzWk",
                     "balances": [[
                         "ACT9Ek1tYy4KUNMKx49Wvcm5uUJjYnSfJnY",
                     "contract": "ACT92cJUVM6qS9qp1ihnJB5DJrf1pP9F2fSB",
                     "costlimit": {
                       "amount": 1000,
                       "asset_id": 0
                      "transaction_fee": {
                        "amount": 1000,
                       "asset_id": 0
```

3.Call RPC command blockchain\_get\_pretty\_contract\_transaction, the parameter is trx\_id. Parse the response, we first check the field to\_account whether it is the right token contract id. If not, just pass it.The from\_account: withdraw address.Then we check field reserved. First parameter is the method the contract called. If the value is transfer\_to, this is a contract transaction. If not, skip it. The second parameter is the parameter of method transfer\_to, using to separate different parameters. The first is deposit address, the second is transaction amount. To monitor whether your address has received the contract token, you can check if this address is your own address.

```
lwallet (locked) >>> blockchain_get_pretty_contract_transaction
ransaction_id_prefix: fd88fb7d1b3aac1fe617f8332fdcb62db047117e
 "result_trx_id": "fd88fb7d1b3aac1fe617f8332fdcb62db047117e",
 "orig_trx_id": "31c7e13f79ba1b9952aae7b104020ddc89603a81",
 "block_num": 1174841,
 "block_position": 0,
 "trx_type": 14,
 "is_completed": false,
 "to_contract_ledger_entry": {
   "from_account": "ACT7bWPwBBHUFoCkmHitJ318FZ6Pn1E9gFPx",
   "from_account_name": "coinfix",
   "to_account": "CON92cJUUM6qS9qp1ihnJB5DJrf1pP9F2fSB",
   "to_account_name".
                       "USD COIN".
   "amount": {
     "amount": 0,
     "asset_id": 0
   "fee": {
     "amount": 1660,
     "asset_id": 0
   "memo": ""
 "from_contract_ledger_entries": [],
 "timestamp": "2017-12-05T09:02:00",
 "expiration_timestamp": "2017-12-05T10:01:49",
 "reserved": [
   "transfer_to",
   "ACTLM5zptEYL6kqDfJG5AJUuucyu2DD75EW93df22f5790062ed839ed4f0bb395f00d;999.9900000"
```

# 4.2 Query contract token balance

Use RPC command blockchain\_get\_events, the parameter is the block number and result\_trx\_id.

To get event\_type and event\_param.

event\_type indicate whether the transaction succeed. If the result is transfer\_to\_success, the transaction succeed. If not, the transaction failed.

event\_param have 4 parameters, separate by ",". First is withdraw address and balance, separate by ":". Second is deposit address and balance. Third is the version (increment). Forth is timestamp.

Note: balance is the balance after this transaction.

## 4.3 Withdraw of contract token

The transfer function of contract token is realized by contract calling.

Therefore we should use RPC command call\_contract to transfer contract token.

call\_contract method needs 6 parameters:

First is contract\_id, start with "CON".

Second is user account who calls contract, that is, withdraw account.

Third is calling method. Here we use method transfer\_to.

Forth is parameter that calling method used. The format is to\_address|amount. The parameters are separate by "|".

Fifth parameter is const string "ACT".

Sixth parameter is the cost limit of contract call. This can be set to any number bigger than 0.01.

Note: Transfer amount up to 5 decimal places. If decimal more than 5, the last will be ignored.

After call\_contract, the block will return the specific information of the transaction. Here we get field entry\_id, that is ori\_trx\_id we described before.

Call RPC method blockchain\_get\_contract\_result, use entry\_id as parameter. There are two parameters in the result. The first is the block number that the transaction occurred. The second is result\_trx\_id. Then use these two parameter to call RPC method blockchain\_get\_events.

Then we will get event\_type and event\_param.

Among these parameters, event\_type indicate whether the transaction succeed. If the result is transfer\_to\_success, the transaction succeed. If not, the transaction failed.

There are 4 parameters in field event\_param, separate by ",". First is withdraw address and balance, separate by ":". Second is deposit address and balance. Third is the version (increment). Forth is timestamp.

Note: after call\_contract, the transaction is not record in the block immediately. Therefore when querying transaction information, we should wait until the new block generates or the query result may be empty. We generate new block every10 seconds

```
lwallet01 (unlocked) >>> blockchain_get_contract_result 743585dae0a3bdd93c7b1ab0
4a6b55f10ef2f18f
{
"block_num": 79078,
"trx_id": "d2ad6d51dfe1d503c602512f662b31b1b1f7c6dd"
}
```

## 5 ASSET transaction

This step needs to be done on the basis of steps 1 and 2. Please note.

# 5.1 Query ASSET ID

Each ASSET has a corresponding asset symbol (asset\_symbol), as well as the corresponding asset ID(asset\_id), which is used to distinguish between different assets.

Call blockchain\_list\_assets to query the asset ID command, for example::

## 5.2 Query ASSET transaction

Call RPC method blockchain\_get\_block\_count to get the header block number.

Call RPC method blockchain\_get\_block to query one block. The parameter is the block number.

- 1.Call RPC command blockchain\_get\_transaction. Parameter is trx\_id in field user\_transaction\_ids (blockchain\_get\_block responsed).
- 2. Transactions are divided into transfer to the subaddress and transfer to the main address, which need to be judged separately

#### Transfer to subaddress:

If alp\_inport\_asset field, asset\_id is the corresponding asset ID (must be judged), and the first type value in operation field is withdraw\_op\_type or deposit\_op\_type, then this transaction is assets transaction.

Get if there is sub-address transaction. The field alp\_account is the deposit address. The figure is a transaction with sub-address. You can get sub-address from field alp\_account.

For example:

```
allet (unlocked) >>> blockchain_get_transaction 697a6687d9aac3f983d20c49c12037501e0e0285
"697a6687d9aac3f983d20c49c12037501e0e0285", {
    "expiration": "2018-03-01T10:02:01",
     alp_account": "ACT3AF1r1MuJMTkSRbKPLM1wkwPysyKJyfTQ12345678901234567890123456789012",
     alp_inport_asset":
      "amount": 100000,
      "asset_id": 1
     'operations": [{
        "type": "withdraw_op_type",
        "data": {
          "balance_id": "ACTCxeMRR5F4cEmipJuRQqCN9jesE882Qdx5",
          "amount": 100000,
          "claim_input_data": ""
        "type": "withdraw_op_type",
"data": {
          "balance_id": "ACT5szmFP1grYpvU89ypk3cNXzZv1SbkvhDD",
          "amount": 1000,
          "claim_input_data": ""
```

Transfer to the main address:

If the first type value in the operation field is withdraw\_op\_type or deposit\_op\_type, and the asset\_id in the deposit\_op\_type is the corresponding asset ID(must be judged)), then this transaction is assets transaction.

For example:

```
(wallet closed> >>> blockchain_get_transaction 296c9159d8f403b1df8ff689a23dad052f3429fc
  "296c9159d8f403b1df8ff689a23dad052f3429fc",{
      "expiration": "2018-08-02T12:02:59",
"alp_account": "",
      "alp_inport_asset": {
         "amount": 0,
         "asset_id": 0
       "operations": [{
"type": "withdraw_op_type",
           "data": {
             "balance_id": "ACTKFmEA5vdsqMF1rxeqE8ZG32g8CKzuDFnp",
"amount": 190,
             "claim_input_data": ""
            "type": "withdraw_op_type",
           "data": {

"balance_id": "ACTG6ijouLEaRAaJpScgoueXSWAcQW9sKfEt",

"amount": 1000,
            "type": "deposit_op_type",
              "amount": 100,
              "condition":
                "asset_id": 3,
                "slate_1d": v,
"type": "withdraw_signature_type",
"balance_type": "withdraw_common_type",
                "data": {
                   "owner": "ACTNcLHUnbmAvEgKFPTsvVU2hGhDCVHieQcQ"
```

3. Call RPC command blockchain\_get\_pretty\_transaction to get the from and to account of this transaction, the parameter is trx\_id.

from\_account: withdraw address

to\_account : deposit address

amount: 100,000 times of the transaction amount.

For example:

```
"is_virtual": false,
"is_confirmed": true,
"is_market": false,
"is_market_cancel": false,
"trx_id": "75bebaf014591b7aaaec9f50f03b9de93d62c6c9",
"block_num": 1277,
"block_position": 0,
"trx_type": 0,
"ledger_entries": [{
    "from_account": "ACT9hRWWWeo8hQ6MeYT5EgunHK8eaXN5z9z5",
    "from_account_name": "zxlasset",
    "to_account": "ACT3AF1r1MuJMTkSRbKPLM1wkwPysyKJyfTQ",
    "to_account_name": "",
    "amount": {
      "amount": 100000,
      "asset_id": 1
    "memo": "",
    "running_balances": []
"fee": {
  "amount": 1000,
  "asset_id": 0
```

# 5.3 Query ASSET balance

Use RPC command: blockchain\_list\_address\_balances. The parameter is ACT address.

Return: Parse the result to get the balance field value corresponding to the asset\_id value.

```
(unlocked) >>> blockchain_list_address_balances ACT3AF1r1MuJMTkSRbKPLM1wkwPysyKJyfTQ
  "ACT9DXH9DUkxwgweWkUfqk25qekargGUCgqK",{
    "condition": {
      "asset_id": 1,
      "slate_id": 0,
      "type": "withdraw_signature_type",
      "balance_type": "withdraw_common_type",
      "data": {
        "owner": "ACT3AF1r1MuJMTkSRbKPLM1wkwPysyKJyfTQ"
    "balance": 400000,
    "deposit_date": "2018-03-01T08:17:19",
    "last_update": "2018-03-01T09:02:00",
    "meta_data": null
1,[
  "ACTPDPXAUU2bfNJentAX2CriFpnhFDTAFnqE",{
    "condition": {
      "asset_id": 0,
"slate_id": 0,
"type": "withdraw_signature_type",
      "balance_type": "withdraw_common_type",
        "owner": "ACT3AF1r1MuJMTkSRbKPLM1_kwPysyKJyfTQ"
    "balance": "500010000000",
    "deposit_date": "2018-03-01T09:25:20",
"last_update": "2018-03-01T09:25:20",
    "meta_data": null
     (unlocked) >>>
```

## 5.4 Withdraw ASSET

Call RPC method wallet\_transfer\_to\_address to withdraw ASSET. Before calling this method, we should open and unlock wallet. This method need 4 parameters.

The first is withdraw ASSET amount. This is true transaction amount.

The second is const string of asset\_symbol.

The third is withdraw account name.

The forth is the deposit ACT address.

This method will return a transaction id, which is trx id.

For example,

wallet transfer to address 10 AAA zxlasset ACT3AF1r1MuJMTkSRbKPLM1wkwPysyKJyfTQ