

# Bitcoin and Altcoin Wallets 2.7.2 reference manual

dashed-slug info@dashed-slug.net

## Abstract

Integrating cryptocurrency wallets into your WordPress site, using the **Bitcoin and Altcoin Wallets** plugin, version **2.7.2**.

## At a glance

Turn your blog into a bank: Let your users deposit, withdraw, and transfer bitcoins and altcoins on your site.

Use **Bitcoin and Altcoin Wallets** to maintain cryptocurrency balances for the users of your WordPress site.

Install *coin adapters* to support more coins or *app extensions* to provide additional cryptocurrency functionalities, such as payment gateways for products and services.

## Pricing

The core wallets plugin is free.

The coin adapters require free signup to dashed-slug.net.

Access to premium app extensions, updates and support require a paid subscription of 10 USD per 3 months.

*If you choose to cancel your subscription you can continue using the plugins as long as you like, but you will lose access to updates and premium support.*

## Disclaimer

**By continuing to use the *Bitcoin and Altcoin Wallets* plugin, you indicate that you have understood and agreed to this disclaimer.**

You accept all responsibility for handling the account balances for all your users. Under no circumstances is dashed-slug.net or any of its affiliates responsible for any damages incurred by the use of this plugin.

Every effort has been made to harden the security of this plugin, but its safe operation depends on your site being secure overall.

You, the administrator, must take all necessary precautions to secure your WordPress installation before you connect it to any live wallets.

You are strongly advised to take the following actions (at a minimum):

- educate yourself about hardening WordPress security
- install a security plugin such as Wordfence
- enable **SSL/TLS** on your site if you have not already done so

## **Feature overview**

### **Crypto deposits**

Your users can now deposit and withdraw Bitcoins.

### **User transactions**

Users can transfer coins to other users.

### **Site fees**

You set the fees that your users pay to you when they transact or withdraw coins.

### **Altcoins integration**

Easily interface to other cryptocurrencies besides Bitcoin. Simply install the provided altcoin adapters for the currency you require.

### **Front-end UI**

Present a simple, knockout.js-enabled frontend UI using shortcodes. Or roll your own.

### **E-mail notifications and confirmations**

Users are notified by email whenever they perform transactions.

The admin can configure message strings via the admin interface, or bind to WordPress actions and code your own notification functions in PHP.

### **Capability-based access control**

Enable or disable user actions via WordPress capabilities.

### **DB storage**

All accounting data is stored safely and efficiently in your database.

## CSV Backups

Export accounting data to .CSV backup files with one click. Import again with ease.

## Pluggable

PHP and JSON APIs give access to the wallets from your theme or other plugins. Look out for more apps that build on this awesome APIs in the near future, or create your own! documentation

PDF Documentation explains the ins and outs of this plugin in detail. Full PHPdoc is included for the PHP API.

## Security

Protection against common plugin security vulnerabilities such as CSRF attacks and SQL injections.

You can extend the FREE Bitcoin and Altcoin Wallets plugin with:

- **coin adapter extensions** that connect to local nodes and other cloud wallets, and
- **app extensions**, such as payment gateways or user rewards.

Because these two concerns are decoupled, you can combine any of the existing app extensions with any of the coin adapters provided.

By mixing and matching plugins, you are in control of which currencies and services you provide.

## Frequently Asked Questions

### Which coins are currently available?

The list of wallets that you can connect to directly is constantly growing.

To check what's currently available go to <https://www.dashed-slug.net> and check the menu under *Wallets* → *Coin Adapter Extensions* and see the available RPC adapters.

Also, if you are OK with using a web wallet service, then you can install the CoinPayments adapter. You then automatically get all of the coins that platform supports.

### Is it secure?

The Bitcoin and Altcoin Wallets plugin is only as secure as your WordPress installation. Regardless of whether you choose to install this plugin, you should have already taken steps to secure your WordPress installation. At a minimum you should do the following:

- Install a security plugin such as Wordfence.
- Read the Codex resources on Hardening WordPress.
- If you are connecting to an RPC API on a different machine than that of your WordPress server over an untrusted network, make sure to tunnel your connection via `ssh` or `stunnel`. See [here](#).

### Do I really need to run a full node? bitcoind is too resource-hungry for my server.

Running a full node requires you to set up the daemon on a VPS or other machine that you own and administer. Normally the full blockchain needs to be downloaded, so you need to make sure that your server can handle the disk and network requirements.

#### Cloud wallets

Instead, you can choose to install one of the available coin adapters that are backed by cloud wallet services. These currently are:

- The CoinPayments Adapter extension
- The block.io Cloud Wallet Adapter extension

Study the services and their terms of service including what fees they charge before choosing to use them.

#### bittiraha

From version 1.1.0 onward, this plugin is compatible with the bittiraha-walletd wallet. From the project's description on GitHub:

Lightweight Bitcoin RPC compatible HD wallet This project is meant as a drop-in replacement for bitcoind for use in lightweight servers.

This is a wallet based on bitcoinj and does not store the blockchain locally. You will have to install this on a VPS or other server via the shell.

A downside is that the walletnotify mechanism and the listtransactions command are not implemented. **This means that there is no easy way for the plugin to be notified of deposits.** Deposits will not be recorded in the transactions table. Users will not be emailed when they perform deposits and they will not be able to see their deposits in the [wallets\_transactions] UI. Deposits will correctly affect users' balances. You have been warned.

### Electrum

Alternatively, you can install and configure an Electrum wallet and the Electrum Bitcoin RPC Adapter extension. **Don't forget to disable the built-in Bitcoin core adapter.**

### Can you install/configure the plugin for me? / I am having trouble with the bitcoin.conf file

I am available to answer any specific questions if you attempt to install the plugin and you face some problem. Unfortunately I do not undertake installation and configuration of the plugin.

Keep in mind that no software is set-and-forget. Once you install software, it then needs to be maintained. If you find that you are having trouble installing the plugin or connecting it to a wallet, even with help, this is a good indication that you should not be running a wallet with people's money on it.

Remember that you have two options: stand-alone wallets or web wallets. Running a web wallet is considerably easier than a stand-alone wallet, as it does not require system administration skills. As a general rule, if you have trouble using Linux from the command line, you will be better off installing a web wallet.

### I cannot connect to a wallet running on my home computer

Unless your home internet connection has a static IP and you have opened the correct ports on your router/firewall you will not be able to use your home computer as a wallet backend. In fact, this is not a very good idea. Ideally you need a dedicated server to run a wallet with the availability required by a site that serves multiple users. Virtual private servers (VPSs) should be OK as the wallets do not max-out CPU usage under normal operation, after the blockchain finishes syncing. Shared/managed hosting plans are not appropriate for running wallet daemons. If you have a shared/managed hosting plan (i.e. no ssh access), you are stuck with using web wallets.

Check with your hosting plan for disk space and memory requirements against the requirements of the wallet you wish to run. For Bitcoin core, [click here](#).

## How can I integrate the plugin with my site?

Just insert the shortcodes anywhere to create forms to let a logged in user:

- **deposit funds:** [wallets\_deposit]
- **withdraw funds:** [wallets\_withdraw]
- **transfer funds to other users:** [wallets\_move]
- **view their balance:** [wallets\_balance]
- **view past transactions:** [wallets\_transactions]

These shortcodes render knockout.js-enabled forms. Read the shortcodes documentation for more details.

You can enter the same UI elements into your theme's widget area. Simply go to *Appearance* → *Widgets* and use the provided front-end widgets.

You can also use a special menu item to display the user balances as part of a nav menu:

1. Go to *Appearance* → *Menus*.
2. At the top right side of the screen, click *Screen Options*.
3. Under *Boxes*, make sure that *Bitcoin and Altcoin Wallets balances* is selected.
4. Now you are free to enter the balances menu item into your menus.

## I don't like the built-in forms. Can I provide my own?

First of all, the forms can be styled with CSS. They have convenient HTML classes that you can use.

If you wish to create forms with completely different markup, you can provide your own views for these shortcodes. Use the `wallets_views_dir` filter to override the directory where the views are stored (the default is `wallets/includes/views`). Most people will not need to do this.

Read the shortcodes documentation for more details.

## I want to do transactions from JavaScript. I don't want to use the provided shortcodes and their associated forms.

The provided built-in forms talk to a JSON API that is available to logged in users. If you choose to build your own front-end UI, you can do your AJAX calls directly to the JSON API.

Refer to the JSON API documentation for details.

## I want to do transactions from the PHP code of my theme or plugin.

You can use the PHP API directly.

Refer to the PHP API documentation for details.

### **I want to replace an adapter with another one.**

You can only have one coin adapter enabled per each coin. The plugin will warn you about this.

Suppose you wish to replace the internal *Bitcoin core adapter* with the *block.io BTC adapter*. You would have to:

1. Wait for pending deposits and withdrawals to execute. They should be in 'done' state.
2. Disable your original coin adapter.
3. Delete the deposit addresses from your database with:

```
DELETE FROM wp_wallets_adds WHERE symbol = 'BTC';
```

4. Activate and configure the new adapter.

### **Can you add XYZ coin for me?**

Yes and no. I have received a large amount of requests from small coins and cannot cater for them all. I do try to implement some of the requests I receive.

If your coin's wallet has a standard RPC API that is a direct fork of Bitcoin core, then you should be able to modify the Litecoin adapter to suite your needs. Feel free to republish it after modifying the code. There are some instructions on how to do this [here](#).

If your coin is an ERC-20 token then there is no support for that at the moment. Ideally this is something that will be implemented in the future.

### **Are you available for custom development work?**

Unfortunately I do not undertake custom projects. If you have an idea about a cool extension then please let me know about it. If it is a good fit for the project, it will be added to the backlog. When implemented, It will be available either to all users for free, or for dashed-slug premium members.

### **Can you add fiat currency deposits?**

I do not have plans to add fiat currency deposits. That is not to say that someone cannot develop an extension to do this.



### **Can you build an exchange on top of the plugin?**

Yes this is in the future plans.

### **I want to pay for premium membership but cannot or do not want to pay via PayPal.**

I am currently in the process of building a plugin extension that will allow you to pay for membership via cryptocurrencies. In the meantime, you may contact me directly at [info@dashed-slug.net](mailto:info@dashed-slug.net) if you wish to send a Bitcoin payment and I will activate your membership manually.

### **How can I get support or submit feedback?**

Please use the support forum on [WordPress.org](https://wordpress.org/support/plugin/dashed-slug) for all issues and inquiries regarding the plugin.

To get support on the provided extensions, subscribe to dashed-slug and go to the support forums.

For all other communication, please contact [info@dashed-slug.net](mailto:info@dashed-slug.net).

## Available extensions

**Bitcoin and Altcoin Wallets** *Turn your blog into a bank: Let your users deposit, withdraw, and transfer bitcoins and altcoins on your site.* Support forum

- This plugin is always available at the dashed-slug download area and at wordpress.org.
- The extensions can be downloaded at the dashed-slug download area.

## App extensions

**Bitcoin and Altcoin Wallets: Author Payroll extension** *Pay your article authors with cryptocurrencies based on Google Analytics metrics.* Support forum

**Bitcoin and Altcoin Wallets: Events Manager Cryptocurrency Payment Gateway** *Let logged in users pay for tickets in Events Manager Pro from their cryptocurrency wallet.* Support forum

**Bitcoin and Altcoin Wallets: Faucet Extension** *Reward your users for solving CAPTCHAs.* Support forum

**Bitcoin and Altcoin Wallets: Tip the Author** *Allows users with cryptocurrency wallets to tip content authors.* Support forum

**Bitcoin and Altcoin Wallets: WooCommerce Cryptocurrency Payment Gateway** *Let logged in users pay at WooCommerce checkout from their cryptocurrency wallet.* Support forum

## Wallet Coin adapters

**Bitcoin and Altcoin Wallets: BlockIO Cloud Wallet Adapter** *Allows your Bitcoin and Altcoin Wallets WordPress plugin to interface with your block.io cloud wallet account.* Support forum

**Bitcoin and Altcoin Wallets: CoinPayments Adapter** *Allows your Bitcoin and Altcoin Wallets WordPress plugin to interface with your CoinPayments.net cloud wallet account.* Support forum

## Local wallet adapters

**Bitcoin and Altcoin Wallets: Dogecoin RPC Adapter** *Allows your Wallets plugin to interface with the Dogecoin daemon (dogecoind).* Support forum

**Bitcoin and Altcoin Wallets: Electrum Bitcoin RPC Adapter** *Allows your Wallets plugin to interface with the Bitcoin Electrum Bitcoin wallet.* Support forum

**Bitcoin and Altcoin Wallets: eMark RPC Adapter** *Allows your Wallets plugin to interface with the Deutsche eMark wallet.* Support forum

**Bitcoin and Altcoin Wallets: Feathercoin RPC Adapter** Allows your Wallets plugin to interface with the Feathercoin daemon (*feathercoind*). Support forum

**Bitcoin and Altcoin Wallets: Goldcoin RPC Adapter** Allows your Wallets plugin to interface with the Goldcoin daemon (*goldcoind*). Support forum

**Bitcoin and Altcoin Wallets: Goshencoin RPC Adapter** Allows your Wallets plugin to interface with the Goshencoin wallet. Support forum

**Bitcoin and Altcoin Wallets: Gridcoin RPC Adapter** Allows your Wallets plugin to interface with the Gridcoin daemon (*gridcoinresearch*). Support forum

**Bitcoin and Altcoin Wallets: Litecoin RPC Adapter** Allows your Wallets plugin to interface with the Litecoin daemon (*litecoind*). Support forum

## Transactions

Users can perform three types of transactions:

- *Deposits*, by sending funds from a blockchain to a deposit address.
- *Withdrawals*, by requesting to send funds to an external address on the blockchain.
- *Internal transfers* (aka *moves*) to other users.

Also, feature plugin extensions can perform such operations on behalf of the users with the `do_move()` and `do_withdraw()` functions. See the PHP API section for more.

## Admin panel

As of release 2.3.0, administrators with the `manage_wallets` capability can view all transactions on the system, via the admin panel titled *Transactions*.

## Confirmations

As of release 2.3.0, administrators with the `manage_wallets` capability can choose what kind of confirmation, if any, move and withdraw transactions need before they can change from unconfirmed to pending. This is set via the admin panel titled *Confirms*.

There are two possible types of confirmation that may be required for a withdraw or move transaction.

- *admin confirmation* This is given via the admin transactions table. For unconfirmed and pending transactions, there are actions to confirm and unconfirm a transaction in the column titled *Accepted by admin*.
- *user confirmation* The user that originates the transaction request receives an email containing a nonce and an ID that uniquely identifies the transaction request. If the user clicks on the link, the transaction is considered to be confirmed by the user. The body

of the email is configurable. Administrators can also modify the *Verified by user* column via the *Transactions* admin panel.

## **Lifecycle (states)**

As of release 2.3.0, transactions can have one of the following states:

- **unconfirmed** This is the initial state for all transactions.
- **pending** For moves and withdrawals, this is the state that a transaction gets when it has been confirmed by a user and/or admin. You can choose which types of confirmation is required in the admin panel, under “Confirms”.
- **done** Transactions that have been executed and affect a user’s balance are in this state. Also, deposits that have reached the required number of network confirmations. The required confirmation count is set at the coin adapter settings for each coin separately.
- **failed** Transactions that could not be executed are marked as failed. They do not affect user balances.

## Shortcodes

Wallet shortcodes display UI forms to the front-end that let the user do basic operations with their cryptocurrency accounts.

All the operations accessible via shortcodes are only relevant to logged in users. The shortcodes will only display if:

1. the user is logged in,
2. there is at least one wallet online, and
3. the user has the necessary capabilities, including `has_wallets`.

### Shortcode reference

#### Deposit funds

**Required capabilities:** `has_wallets`

A screenshot of a web form for depositing funds. It features a label 'Coin:' followed by a dropdown menu showing 'Bitcoin' with a downward arrow. Below this is a label 'Deposit address:' followed by a text input field containing the address '1DaShEDyeAwEc4snWq14hz5EBQXeHrVBxy'.

Use the `[wallets_deposit]` shortcode to display a form that will let the user know which address they can send coins to if they wish to make a deposit.

#### Withdraw funds

**Required capabilities:** `has_wallets`, `withdraw_funds_from_wallets`

Coin:

Bitcoin

Withdraw to address:

Amount:

Fee:

฿0.00005000

Transaction comment:

Address label:

SEND

RESET FORM

Use the `[wallets_withdraw]` shortcode to display a form that will let the user withdraw funds. The user will be notified by email when the withdrawal succeeds.

#### Transfer funds to other users

**Required capabilities:** `has_wallets`, `send_funds_to_user`

Coin:

Bitcoin

Recipient user:

luser

Amount:

Transfer comment:

Fee:

฿0.00000100

SEND

RESET FORM

Use the `[wallets_move]` shortcode to display a form that lets the user transfer coins to other users on your site. Both users will be notified by email when the transaction succeeds.

#### Display user balance(s)

**Required capabilities:** `has_wallets`

Coin:

Bitcoin

Balance: ฿0.00079295

Use the `[wallets_balance]` shortcode to show the current user's balances.

### View past transactions

Required capabilities: has\_wallets, list\_wallet\_transactions

Coin:

Bitcoin

Rows per page:

10

Page:

1

Latest transactions

| Type     | Time                           | Amount<br>(+fee) | Fee         | From                               | To                                 | Comment              | Confirmations |
|----------|--------------------------------|------------------|-------------|------------------------------------|------------------------------------|----------------------|---------------|
| deposit  | 17/12/2016,<br>5:17:38<br>μ.μ. | ฿0.00001000      | ฿0.00000000 | 1rXEs8Kbj7mcMU1ZAq84Kdm85Vdd2Xg2b2 | me                                 |                      | 3791          |
| move     | 27/12/2016,<br>6:47:19<br>μ.μ. | ฿-0.00001334     | ฿0.00000100 | me                                 | luser                              | unique test          | -             |
| withdraw | 30/12/2016,<br>1:44:37<br>μ.μ. | ฿-0.00006000     | ฿0.00005000 | me                                 | 3i1B4pkLQ2VmLZwhuEGto3NAJdeh4xjr1W | withdrawing bitcoins | 541           |

Use the [wallets\_transactions] shortcode to display an interactive table that shows past deposits, withdrawals and transfers that affect the user's account. The table is paginated and data is loaded dynamically.



## Modifying front-end UIs (for developers)

### Capturing events on the front-side

Withdraw and move forms use JavaScript to emit bubbling DOM events to denote that a withdrawal or a transfer to another user has succeeded.

The event names are:

- wallets\_do\_withdraw, and
- wallets\_do\_move.

The default behavior is to display informative message boxes using the browser's `alert()` function.

You can bind handlers to these DOM events to override, or to add to, this behavior.

The event handlers have access to the response of the JSON API, and to the form values entered by the user. Here's some example JavaScript code:

#### Observing transfers between users:

```
jQuery('body').on( 'wallets_do_move', function( event, response, symbol, amount, toaccount, coin ) {
    if ( typeof(response.result) == 'string' ) {
        if ( response.result == 'success' ) {
            alert( 'Successfully sent ' + amount + ' ' + symbol );
        } else {
            alert( "Move failed: \n" + response.message );
        }
    } else {
        alert( "Move failed!" );
    }
    event.preventDefault();
});
```

#### Observing withdrawals:

```
jQuery('body').on( 'wallets_do_withdraw', function( event, response, symbol, amount, address, coin ) {
    if ( typeof(response.result) == 'string' ) {
        if ( response.result == 'success' ) {
            alert( 'Successfully withdrew ' + amount + ' ' + symbol + ' to ' + address );
        } else {
            alert( "Move failed: \n" + response.message );
        }
    } else {
        alert( "Move failed!" );
    }
    event.preventDefault();
});
```

```
});
```

The above examples override the default handlers. If you wish to add to the default behavior, simply delete the `event.preventDefault()` statements and let the events bubble up.

## Overriding the default UI

### Using CSS

All the UI elements have the `dashed-slug-wallets` class to help you with CSS styling:

```
.dashed-slug-wallets.move { }  
.dashed-slug-wallets.withdraw { }  
.dashed-slug-wallets.balance { }  
.dashed-slug-wallets.deposit { }  
.dashed-slug-wallets.transactions { }
```

### Using HTML and PHP and JavaScript and CSS and stuff!

If you are a developer, you can override the default forms provided to do much more than just change the styling.

All the UI elements are implemented as knockout.js forms that talk to the provided JSON API.

These forms live in the `wp-content/plugins/wallets/includes/views` directory of your WordPress installation:

```
wp-content/plugins/wallets/includes/views/balance.php  
wp-content/plugins/wallets/includes/views/move.php  
wp-content/plugins/wallets/includes/views/deposit.php  
wp-content/plugins/wallets/includes/views/withdraw.php  
wp-content/plugins/wallets/includes/views/transactions.php
```

You can copy these files to another directory of your choosing. Make sure to override the views directory using the `wallets_views_dir` filter, to let the plugin know where to look for the templates. Here's sample code for how to do this:

```
function my_wallets_views_dir_override( $dir ) {  
    return '/path/to/the/directory/where/the/new/templates/are/copied';  
}  
add_filter( 'wallets_views_dir', 'my_wallets_views_dir_override' );
```

## Capabilities

WordPress does access control using the concept of Roles and Capabilities. You can read about it in the WordPress Codex.

### Bitcoin and Altcoin Wallets capabilities

You can assign capabilities to roles using the admin interface. Just navigate to *Wallets* → *Capabilities* and check capabilities in the matrix, then hit *Save changes*.

Capabilities control which shortcodes and JSON API endpoints are available to a user.

By default, the PHP API overrides capabilities checks. You can enforce checking with the new argument, `$override_capabilities`.

As of 2.2.4 you cannot modify the capabilities of the administrator role using this interface. This is to prevent admin accounts from locking themselves out of the `manage_wallets` capability.

#### **manage\_wallets**

- Enables admin interface. For administrators only.

#### **has\_wallets**

- Needed for all shortcodes.
- Needed for the `get_transactions`, `do_withdraw` and `do_move` JSON APIs.
- Needed for the `do_move()`, `do_withdraw()`, `get_coin_adapters()`, `get_balance()`, `get_new_address()`, `get_account_id_for_address()` and `get_transactions()` PHP APIs. Only checked when `$override_capabilities` is true.

#### **list\_wallet\_transactions**

- Need for the `wallets_transactions` shortcode.
- Needed for the `get_transactions` JSON API.
- Needed for the `get_transactions()` PHP API. Only checked when `$override_capabilities` is true.

#### **send\_funds\_to\_user**

- Need for the `wallets_move` shortcode.
- Needed for the `get_users_info` JSON API.

- Needed for the `do_move()` PHP API. Only checked when `$override_capabilities` is `true`.

#### **withdraw\_funds\_from\_wallet**

- Needed for the `wallets_withdraw` shortcode.
- Needed for the `do_withdraw` JSON API.
- Needed for the `do_withdraw()` PHP API. Only checked when `$override_capabilities` is `true`.

## E-mail notification settings

Users are notified by e-mail when they perform deposits or withdrawals and when they send or receive funds. In the admin interface navigate to *Wallets* → *E-mail settings*.

- You can control which notifications are sent.
- You can edit the subject line templates.
- You can edit the text body templates.

You can use the following variable substitutions in your templates:

- **###ACCOUNT###** — Account username
- **###OTHER\_ACCOUNT###** — Username of other account (for fund transfers between users)
- **###TXID###** — Transaction ID. ( This is normally the same as the txid on the blockchain. Internal transactions are also assigned a unique ID. )
- **###AMOUNT###** — The amount transacted.
- **###FEE###** — For withdrawals and transfers, the fees paid to the site.
- **###SYMBOL###** — The coin symbol for this transaction (e.g. “BTC” for Bitcoin)
- **###CREATED\_TIME###** — The date and time of the transaction in ISO-8601 notation. YYYY-MM-DDThh:mm:ssZZZZ
- **###COMMENT###** — For internal fund transfers, the comment attached to the transaction.
- **###ADDRESS###** — For deposits and withdrawals, the external address.

## Cold Storage

There is a cold storage section in the admin panel of the Bitcoin and Altcoin Wallets free WordPress plugin.

### What is Cold Storage

When users hold cryptocurrencies on your site, these funds are stored on your back-end wallets. The plugin uses these wallets to communicate with the blockchains.

If a malicious hacker were to somehow gain access to your WordPress, they could steal your users' money. This is why you must:

- keep your site secure, and
- plan for the possibility that your site can be breached. No system is 100% safe.

One very popular security measure is to keep part of the funds in *cold storage*. This is an offline wallet, to which your site's code does not have access to.

The concept is not much unlike that of fractional reserve banking: You do not keep all of the deposited funds on the live wallet. Instead you keep a fraction of those funds online, and the rest you keep on another wallet. Preferably a wallet that is not even connected to the internet. Paper wallets and hardware wallets are good for this, but you could also use a computer that you keep offline at all times.

This release features an admin page that makes it easy to split funds into a live and cold wallet: For every currency you have installed, the page will tell you

- how many coins you have in your online wallet,
- how much is the total of all your users' balances, and
- how much you need to deposit or withdraw to reach your target level.

### Using Cold Storage to secure your site

You can now target to keep a **fixed percentage of the total balances** online at all times. Send the rest of the coins to cold storage and keep them safe. At a later time you can deposit them again into your site as needed.

The admin page will let you **deposit** and **withdraw** funds to and from an external cold storage wallet. These transactions are not recorded in your transactions table. They do not affect any user balances. They only affect the online wallet balance. In the event of a security breach, all of the offline coins are safe and your risk is minimized.

You will want to **keep online more money than you expect your users to withdraw** all at once. If there are not enough funds online, user-requested withdrawals will fail.

On the other hand, you could decide that all withdrawals require **confirmation by an admin**. Then you can keep all of the funds in cold storage and only put them back online before you manually approve user withdrawals.

Any administrator with the `manage_wallets` capability has access to that page. Keep in mind that you need to wait for transactions to confirm before they affect your balance. If you are using the CoinPayments adapter, withdrawals might take a few minutes to execute.

## Hardware wallets

Consider getting a hardware wallet to use for cold storage. A Trezor or Ledger Wallet will do nicely.

## APIs, APIs everywhere!

The modular philosophy of the Bitcoin and Altcoin Wallets plugin is about **providing programmatic** access to an **abstraction layer** that can then talk to a **bitcoin** wallet or to other cryptocurrencies.

In simple English: You and others can build and use applications that do financial transactions, without worrying about the implementation details of each coin, or about UI issues, accounting, etc.

### For site administrators

- Install wallet daemons
- Install this plugin and configure it to use your wallets.
- Insert the simple shortcodes into your site's content.

### For developers

If you're a developer, by now you will probably be asking:

Can I see the software stack diagram?

OK, here it is:

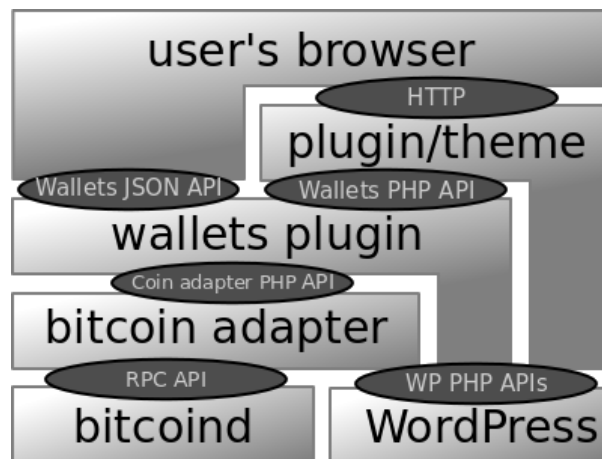


Figure 1: software stack



## JSON API

The Bitcoin and Altcoin Wallets WordPress plugin exposes two JSON APIs:

1. The transaction API enables logged in users to perform and view transactions from the frontend.
2. The notification API lets the wallet daemons notify the system of incoming transactions. (For bitcoind, this maps to `-walletnotify` and `-blocknotify`).

### Transaction API

You can control which parts of the API are available by setting capabilities in the admin screens.

#### Get users info

Retrieves usernames and user IDs of all users on the site.

Used by the `[wallets_move]` shortcode UI to display a drop-down selection of users to send coins to.

**URI path:** `/wallets/get_users_info`

**Parameters:** none

**Required capabilities:** `has_wallets`, `send_funds_to_user`

**Example response:**

```
{
  "users": [
    {
      "id": 2,
      "name": "luser"
    }
  ],
  "result": "success"
}
```

#### Get coins info

Retrieves information relevant to all the coins enabled on the site.

Used by all shortcode front-ends to display a drop-down selection of available coins.

**URI path:** `/wallets/get_coins_info`

**Parameters:** none

**Required capabilities:** `has_wallets`

**Example response:**

```

{
  "coins":{
    "LTC":{
      "name":"Litecoin",
      "symbol":"LTC",
      "icon_url":"http://www.turbox.lan:81/wp-content/plugins/wallets-litecoin/assets",
      "sprintf":"\u0141%01.8f",
      "balance":0.00659988,
      "balance_string":"\u01410.00659988",
      "unconfirmed_balance":0.00659988,
      "unconfirmed_balance_string":"\u01410.00659988",
      "deposit_address":"LPsj8nDiuBjbvRFR8CDoYhSbd4nDekbBQV",
      "deposit_address_qrcode_uri":"litecoin:LPsj8nDiuBjbvRFR8CDoYhSbd4nDekbBQV"
    },
    "BTC":{
      "name":"Bitcoin",
      "symbol":"BTC",
      "icon_url":"http://www.turbox.lan:81/wp-content/plugins/wallets/includes/../../as",
      "sprintf":"\u0e3f%01.8f",
      "balance":0.00091565,
      "balance_string":"\u0e3f0.00091565",
      "unconfirmed_balance":0.00091565,
      "unconfirmed_balance_string":"\u0e3f0.00091565",
      "deposit_address":"mrXEs8Kbj7mcMU1ZAq84Kdm85Vdd2Xg2b2",
      "deposit_address_qrcode_uri":"bitcoin:mrXEs8Kbj7mcMU1ZAq84Kdm85Vdd2Xg2b2",
    }
  },
  "result":"success"
}

```

### Get transactions

Retrieve past transaction info (deposits, withdrawals and transfers to other users) of the currently logged in user.

Used by the [wallets\_transactions] shortcode UI to display a paginated table of transactions.

**URI path:** /wallets/get\_transactions/SYMBOL/COUNT/FROM

#### Parameters:

- **SYMBOL:** The coin's symbol, e.g. BTC, LTC, etc. Only transactions regarding this coin will be retrieved.
- **COUNT:** Retrieve this many transactions
- **FROM:** Start retrieving transactions from this offset (for pagination)

**Required capabilities:** has\_wallets, list\_wallet\_transactions

**Example response:**

```
{
  "transactions": [
    {
      "category": "deposit",
      "account": "1",
      "other_account": null,
      "address": "1rXEs8Kbj7mcMU1ZAq84Kdm85Vdd2Xg2b2",
      "txid": "c9c30612ea6ec2509c4505463b6f965ac25e8e2cff6451e480aa3b307377df97",
      "symbol": "BTC",
      "amount": "0.0000100000",
      "fee": "0.0000000000",
      "comment": null,
      "created_time": "2016-12-17 15:22:14",
      "updated_time": "2016-12-30 11:33:14",
      "confirmations": "3249",
      "other_account_name": null,
      "amount_string": "\u00e3f0.00001000",
      "fee_string": "\u00e3f0.00000000"
    },
    {
      "category": "move",
      "account": "1",
      "other_account": "2",
      "address": "",
      "txid": "move-58629b173cb8f0.44669543-send",
      "symbol": "BTC",
      "amount": "-0.0000133400",
      "fee": "0.0000010000",
      "comment": "comment test",
      "created_time": "2016-12-27 16:47:19",
      "updated_time": "2016-12-27 16:47:19",
      "confirmations": "0",
      "other_account_name": "luser",
      "amount_string": "\u00e3f-0.00001334",
      "fee_string": "\u00e3f0.00000100"
    },
    {
      "category": "withdraw",
      "account": "1",
      "other_account": null,
      "address": "1i1B4pkLQ2VmLZwhuEGto3NAJdeh4xJr1W",
      "txid": "fed08f9a90c526f2bb791059a8718d422b8fdcb55f719bd36b6e3d9717e815e0",
      "symbol": "BTC",
      "amount": "-0.0000600000",

```

```

        "fee": "0.0000500000",
        "comment": "withdrawing bitcoins",
        "created_time": "2016-12-30 11:44:37",
        "updated_time": "2016-12-30 12:46:41",
        "confirmations": "12",
        "other_account_name": null,
        "amount_string": "\u00e3f-0.00006000",
        "fee_string": "\u00e3f0.00005000"
    }
],
    "result": "success"
}

```

*All times are GMT.*

#### Move funds to another user

Transfers funds to another user. The transfer fee that the administrator has set in the coin adapter is charged to the sender.

**URI path:** `/?__wallets_action=do_move&__wallets_symbol=SYMBOL&__wallets_move_toaccount=TOACCOUNT`

#### Parameters:

- **SYMBOL:** The symbol of the coins to move, e.g. BTC, LTC, etc.
- **TOACCOUNT:** User ID of the recipient. The IDs are accessible via `get_user_info`.
- **AMOUNT:** The amount of coins to transfer, excluding any transaction fees. This is the amount that the recipient is to receive.
- **COMMENT:** A descriptive string that the sender attaches to the transaction.

**Required capabilities:** `has_wallets, send_funds_to_user`

#### Example response:

```

{
    "result": "success"
}

```

#### Withdraw funds to an external address

Transfers funds to another address on the coin's network. The withdrawal fee that the administrator has set in the coin adapter is charged to the sender.

**URI path:** `/?__wallets_action=do_withdraw&__wallets_symbol=SYMBOL&__wallets_withdraw_address=ADDRESS`

#### Parameters:

- **SYMBOL:** The symbol of the coins to move, e.g. BTC, LTC, etc.
- **ADDRESS:** The external address to send coins to.

- **AMOUNT:** The amount of coins to transfer, excluding any transaction fees. This is the amount that the recipient address is to receive.
- **COMMENT:** A descriptive string that the sender attaches to the withdrawal.
- **COMMENT\_TO:** A descriptive string that the sender attaches to the address.

**Required capabilities:** has\_wallets, withdraw\_funds\_from\_wallet

**Example response:**

```
{
  "result": "success"
}
```

## Notification API

### Notify

Notifies the wallets plugin that an event has occurred. The plugin then fires a WordPress action of the form `wallets_notify_TYPE_SYMBOL` with a single `MESSAGE` argument, and adapters can decide how to handle this. The notification API does not require login.

In practice this mechanism is useful for receiving deposits and for updating the confirmation counts of transactions.

For the bitcoin daemon, the `-walletnotify` parameter must be made to call `/wallets/notify/BTC/wallet/TXID` where `TXID` is a transaction ID, and `-blocknotify` must be made to call `/wallets/notify/BTC/block/BLOCKHASH` where `BLOCKHASH` is the hash of the latest block announced on the blockchain.

In general it is the responsibility of coin adapters to inform you of how to set up notification.

**URI path:** `/wallets/notify/SYMBOL/TYPE/MESSAGE`

**Parameters:**

- **SYMBOL:** The symbol of the coin that this notification is about, e.g. BTC, LTC, etc.
- **TYPE:** The notification type, such as wallet, block, alert, etc.
- **MESSAGE:** A string that is the payload of the notification.

**Example response:**

```
{
  "result": "success"
}
```

## **PHP API**

The Bitcoin and Altcoin Wallets WordPress plugin offers a PHP API.

### **Purpose**

- You can access the API from your theme to perform transactions on behalf of your users.
- You can develop plugins that utilise the PHP API.
- You can install plugins that the Dashed-Slug releases to extend functionality. Many such plugins are on the roadmap.

### **How to call**

First you must call `Dashed_Slug_Wallets::get_instance()` to get an instance of the wallets plugin class. Refer to the auto-generated PHPdoc for a complete reference of what you can do and access.

### **Security caution**

As a side note, this also means that you must double-check what themes and plugins are installed on your site. Every piece of code that your site runs must be trustworthy for security reasons. Do not install themes or plugins from unknown sources without checking the code thoroughly. You should be already aware of this.

## Multi-site (aka network) installations

As of version 2.2.3, the **Bitcoin and Altcoin Wallets** plugin can be installed on multi-site WordPress installations.

As of version 2.4.0, the plugin will behave differently depending on whether it is *network-activated*, or activated on individual blogs.

### Activating on individual blogs

The *superadmin* installs the plugin via the network administrative pages and **does not** network-activate it.

Administrators can then activate the plugin on individual blogs and view the *Wallets* menu.

User roles who have the `manage_options` capability (usually administrators) will gain the `manage_wallets` capability and be able to configure settings, setup adapters, view and approve transactions, etc.

All settings can be set to be different between blogs.

Users will maintain separate wallets on each blog. Transactions stored in the database are bound to a blog and only appear on that blog.

Administrators can choose to install *coin adapters* or *feature extensions* on a blog-by-blog basis.

### Network-activating

The *superadmin* installs the plugin via the network administrative pages and proceeds to network-activate it.

Site administrators can not activate or deactivate the plugin on individual blogs, nor can they view the *Wallets* menu.

User roles who have the `manage_network` capability (usually super-admins) will gain the `manage_wallets` capability and be able to configure settings, setup adapters, view and approve transactions, etc. Site administrators will not be able to configure wallets settings.

Users will maintain one balance per coin accross the network.

Transactions stored in the database of the network can appear on all blogs in the network.

The network admin can choose to install *coin adapters*.

Blog administrators cannot install *coin adapters*, but they can install *feature extensions* on a blog-by-blog basis.

## Troubleshooting

### I do not see the UI elements in the frontend.

1. Check that you have added the shortcodes correctly or that you are displaying the widgets in the right widget area.
2. Check that you are logged in.
3. Check that you are logged in as a user with the right capabilities, including `has_wallets`. The needed capabilities for each UI element are listed in the *Shortcodes* section of this document.
4. Check that at least one coin adapter is online. Go to *Wallets* → *Adapters* and check the *status* column of each adapter.

If you have checked all of the above:

5. Contact support. If possible, check your JavaScript console for errors. If you find any, report them when you describe your issue.

### I am getting a warning about cron “The wp\_cron job has not run in a while and might be disabled.”

1. Manually visit the following link in your browser, replacing *example.com* with the domain name for your site. This should trigger cron once and execute a single batch of transactions.

```
http://example.com/wp-cron.php?doing_wp_cron
```

2. Setup a unix cron job to trigger that URL via curl at regular intervals. For example this will trigger cron every five minutes:

```
*/5 * * * * curl http://example.com/wp-cron.php?doing_wp_cron  
> /dev/null 2>&1
```

3. Alternatively, you can setup the above curl command in CPanel if you prefer. See here for details.

### I am getting a warning about cron “WordPress cron is disabled.”

1. Check if the constant `DISABLE_WP_CRON` is set to `false` in your `wp-config.php` file. If it is, delete the line and cron should be enabled again.
2. If you cannot find the constant in `wp-config.php`, some other plugin might be setting the constant. Search the code of the other plugins or try disabling them to figure out which plugin is causing this.



## Coin Adapter development

In *Bitcoin and Altcoin Wallets*, connectivity to the various local and cloud wallets is provided by *Coin adapters*.

Coin adapters:

1. Perform the on-chain transfers (withdrawals).
2. Notify the plugin for any incoming deposits.
3. Provide information about a coin and the wallet service.
4. Provide settings that control communication with the wallet.

Coin adapters do not worry about accounting or internal fund transfers. This is done by the main plugin.

### Coin adapter simple example

When the `wallets_declare_adapters` action is triggered, include a file that will contain the adapter.

```
function myplugin_wallets_declare_adapters() {  
    include 'myplugin-coin-adapter-class.php';  
}
```

```
add_action( 'wallets_declare_adapters', 'myplugin_wallets_declare_adapters' );
```

The adapter itself must be a class that derives from `Dashed_Slug_Wallets_Coin_Adapter`.

The class must have a no-argument constructor. You do not instantiate your class. *Bitcoin and Altcoin Wallets* will create a single instance of each class you declare.

Simply study the `Dashed_Slug_Wallets_Coin_Adapter` class file and override all methods needed in your implementation.

For example, a Litecoin wallet might begin as follows:

```
class MyPlugin_Adapter extends Dashed_Slug_Wallets_Coin_Adapter {  
  
    public function get_symbol() {  
        return 'LTC';  
    }  
  
    public function get_name() {  
        return 'Litecoin';  
    }  
  
    // etc...  
}
```

The adapter's submenu normally appears under the wallets menu.

On the action `admin_menu`, *Bitcoin and Altcoin Wallets* triggers the `wallets_admin_menu` action.

Adapters normally bind the `action_wallets_admin_menu()` function to this action upon construction. This is the function that binds the adapter settings.

You might want to override it to provide additional settings:

```
public function action_wallets_admin_menu() {  
    parent::action_wallets_admin_menu();  
  
    // bind additional settings...  
}
```

Or to hide the settings altogether and possibly provide your own page.

```
public function action_wallets_admin_menu() { }
```

## Coin adapters class hierarchy

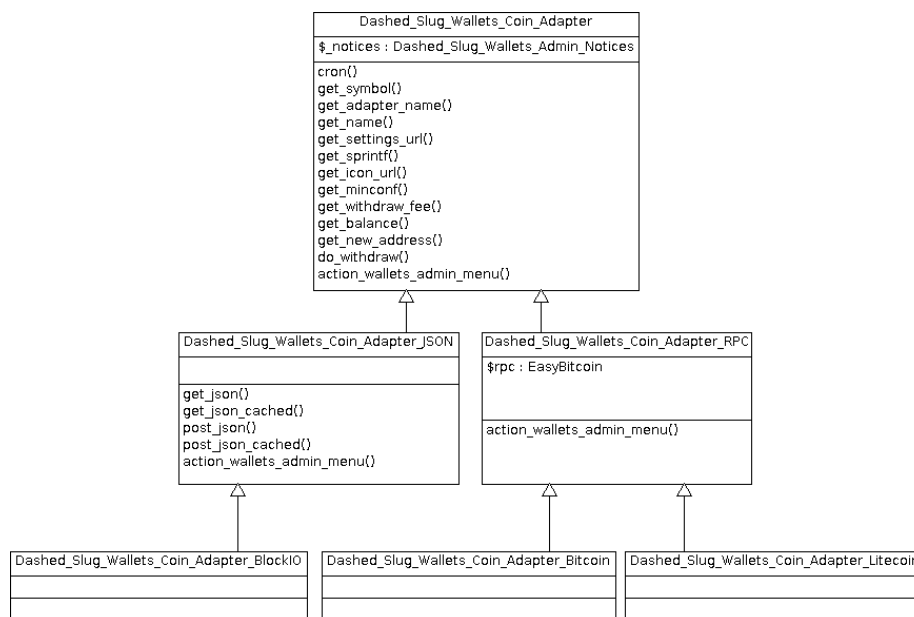


Figure 2: Coin adapters class hierarchy

You do not have to extend directly from `Dashed_Slug_Wallets_Coin_Adapter`.

### `Dashed_Slug_Wallets_Coin_Adapter_RPC`

If your wallet is a Bitcoin-like wallet daemon with an RPC API, you might want to derive from `Dashed_Slug_Wallets_Coin_Adapter_RPC`. This is an abstract class that uses EasyBitcoin-PHP to communicate with a wallet.

### `Dashed_Slug_Wallets_Coin_Adapter_JSON`

If you need to do GET or POST requests to an API that returns JSON, consider deriving from `Dashed_Slug_Wallets_Coin_Adapter_JSON`. This provides the following helpers: `get_json()`, `get_json_cached()`, `post_json()`, `post_json_cached()`.

## Withdraw address validators

You can bind JavaScript validator functions to coins. Whenever a user enters a withdrawal address into the [wallets\_withdraw] UI, your function can test that address for consistency and warn the user if the address does not pass validation. For example, here's how to hook a validation function for Litecoin:

```
$.fn.walletsBindWithdrawAddressValidator(  
    'LTC',  
    function ( val ) {  
        var bytes;  
  
        try {  
            bytes = bs58check.decode( val );  
        } catch ( e ) {  
            return false;  
        }  
  
        if ( bytes.length != 21 )  
            return false;  
  
        var version = bytes[0];  
  
        return 0x30 == version;  
    }  
);
```

The above code binds a validator function to the LTC symbol. The code does a bs58check and a version check to validate a Litecoin address. The bs58check object from bitcoinjs is always available.

To make sure that your code runs after the wallets code, enqueue it with these dependencies:

```
function action_wp_enqueue_scripts() {  
    wp_enqueue_script(  
        'wallets_litecoin_validator',  
        plugins_url( 'wallets-litecoin-validator.js',  
            "wallets-litecoin/assets/scripts/wallets-litecoin-validator.js" ),  
        array( 'wallets_ko', 'bs58check' ),  
        false,  
        true  
    );  
}  
add_action( 'wp_enqueue_scripts', 'action_wp_enqueue_scripts' );
```

This ensures that your script only runs after \$.fn.walletsBindWithdrawAddressValidator and bs58check are loaded.

## **Contact and support**

Please use the support forum on WordPress.org for all issues and inquiries regarding the plugin.

Please use the appropriate support forum for the plugin's extensions.

You are welcome to send in any problems, questions, suggestions, thoughts, etc.

For all other communication, please contact [info@dashed-slug.net](mailto:info@dashed-slug.net).