

# SPOTCOIN – a technical overview

Spring 2017

## Project

***Spotcoin.net** is an online trading platform to buy and sell cryptocurrencies with fiat currency. The platform is designed to be flexible and is adjusted to the customer who can intuitively operate the system without any technical support.*

## System architecture :

*Customers have excess to a live cryptocurrency exchange table by different currencies and public market place without signing in. The trade data is the marketplace, and the marketplace data is open to the public.*

*Customers can register to get further access by a valid email address and password including at least 8 characters.*

*The customer Email should be verified for account activation.*

*After successful registration customers are launched to an active market place page.*

## Marketplace

*The most important function in marketplace is the ability to fill buy-sell application data. This blank is placed on left side.*

*The application form can be filled as following:*

*While filling the application, customer must choose the suitable cryptocurrency to buy or sell, choose **RealWallet** (where money will be held from), price per coin, total will be summarized as well as an amount of money which will be held after placing an order. (In case of **Sell**, customer should have on wallet 100 (one hundred) unit in corresponding currency. In case of **Buy** it's 1% (one percent) of Total). While placing an order of buying as well as selling cryptocurrency customer can indicate if he/she wants to sell/buy cryptocurrency partially.*

**Remark:** Placed order won't be shown on public marketplace immediately. Our administrator, after review of order, will change status from pending to approved or canceled.

If an order is approved by administrator, it will be shown on marketplace as well as in placed orders unless it will only be shown on Archived Orders blank. Our administrators are working 24/7 on the live site.

On the right side of page, on marketplace blank is placed information about existing trades, in this table and also accept trade.

on marketplace we can also view **Placed Orders** – with ability of canceling trade or just view status.

## Wallet

On wallet customers can see available amount of money in different currencies and all transactions with detailed information. The REALWALLET is specific to SpotCoin and it displays amounts available in the selected currency with the built in FX trade fees between different currencies and the best price for crypto currencies. For example, if a customer has ONLY \$100 USD in their account, the REALWALLET will display the corresponding amounts in Euro and British Pounds (or other currencies) post – FX fees, and a corresponding BTC amount post – SpotCoin fees.

## Notifications

In this part of webpage customers can view received System notifications or Warnings. Notices can be for account actions, news, or other activity as deemed by the administrators.

## Account overview

In the page **View Account** customers must verify their identity by filling up provided fields. **Spotcoin** administration will review an application manually.

In this page customers can update profile or enable **Two-Factor Authentication** or **change password**;

## Server infrastructure

The server software and services for website to operate:

- Unmanaged Server with root access.
- Server must have regular updates managed by system administrator, to avoid legacy software for better performance and security.
- NGINX web server has to be installed on server, there are several languages used on website, it is mandatory to have universal reverse proxy server software (nginx) to serve visitors, nginx caching will help server to use less compute resources and operate faster.
- We use MongoDB and MySQL server softwares, to handle databases, server must have SSD flash drives for better I/O.
- Site static content (CSS styles, JavaScript codes, Images) hosted on CDN servers, that will help visitors from around the world, open website much faster. CDN save our server resources and reduces network loads.
- Website must have horizontal scaling, to add compute and storage resources, in case, if visitors count will increase.
- Every website resource must have Cache-Control and expires HTTP headers, to control caching and increase cache times, if content is always static.
- Server must have remote backup location to save all website data and databases on remote server, in case, if hardware, or server software fails.
- Firewall software must be installed on server, both iptables with access rules and fail2ban for SSH security, additionally for better filtering CSF plugin can be installed.
- All ports except 80 (HTTP), 443(HTTPS) ports are blocked for public, only accepted IP addresses will have access to it.
- HTML files are cached using NGINX caching, plus Cloudflare CND cache control value must be higher than 1 hour.

- *MySQL database queries has to be cached using memcached in-memory caching system, to avoid unplanned downtimes and slow query times.*
- *Web server hardware requirements:*

**Processor:** Minimum 1.8 Ghz **Intel Xeon / AMD** Opteron 4 Cores/4 Threads  
**RAM:** 16 GB or more  
**Disk:** 250GB SSD or more

- *Database server hardware requirements:*

**Processor:** Minimum 1.8 Ghz **Intel Xeon / AMD** Opteron 4 Cores/4 Threads  
**RAM:** 16 GB or more  
**Disk:** 100GB SSD or more

- *Blockchain server hardware requirements:*

**Processor:** Minimum 1.8 Ghz **Intel Xeon / AMD** Opteron 4 Cores/4 Threads  
**RAM:** 16 GB or more  
**Disk:** 500GB SATA or SAS

- *Server must have Ubuntu Linux 16.04 LTS (Long-time Support) operating system installed on it, only 64bit version is acceptable.*

## Security

- *Website is always working on SSL(HTTPS) technology to avoid, third person interruption to client-to-site connections to steal passwords, or other private data, SSL (Secure socket layer) is responsible to secure data transmission between server and client, only client and server knows data as they have public and private SSL keys to encrypt and decrypt data sent by server or user.*
- *We use 2FA separate passwords and two-step verification with each device and service, users have option to use Google 2FA authenticator to secure their account.*
- *Website must have certificate provided by Comodo, DigiCert or Verisign. Only several certificates are compatible with every browser.*
- *Website has additional security layer, named as CSRF token generation, to avoid password hacking and bad requests sent by visitors trying to hack our system, csrf itself ensures, that client visited using web browser and has fresh CSRF key to send any data to server, if user will try using same CSRF token, all requests will be blocked and logged as hack attempt.*

- *All data sent to website are sanitized and cleaned to avoid SQL injection.*
- *We check for strong passwords on account creation and password reset.*
- *Root access and password authentication has to be disabled, instead we will be using encrypted key-based authentication, server must have RSA key file on it, only person with private key file, and pin for that private RSA will have access to the server, addition to the key-based authentication, user must have sudoer password to use server to install or modify anything on server.*
- *All critical data that grants visitor login access, passwords and private information about user itself are encrypted using OpenSSL technology with AES-256-CBC encryption algorithm, the data encrypted with AES-256-CBC is irreversible, no one can decrypt.*
- *Additional hashes, such as link generated with random one time token for email verification, password recovery and other keys are also generated using OpenSSL 256bit encryption (AES-256-CBC).*

## Technologies we use

- *PHP and Node.js (Javascript) are used as backend programing languages.*
- *Express.js and Laravel PHP are used as backend programming frameworks for better security and stability.*
- *Several technologies are used on frontend, Ember.js (Javascript) is used as main frontend framework, in addition jQuery and jQuery plugins are used as well, such as alerts, notifications, datatables and several other.*
- *To build interface HTML5 with Twitter bootstrap is used.*
- *To process bitcoin transactions, wallets and balances additional software is used, named as BitCore.*
- *For security purposes we use Site-to-Site VPN to connect all servers to bitcore node, to avoid public data, or credentials being leaked.*

- Browser quality control and compatibilities between versions.

Development will be held on DEVELOPMENT server. We can test individual functions or UX's visual side here, or test webpage generally on different devices or browsers.

**Involvement of Customer**

customer will be given a server STAGING. where will be uploaded already tested version of webpage. On this server customer will be provided with the ability to come familiar with existing functions, test and find out more about working process and status (what have we already done and what's new step)