3.3.0 Account Creation

3.3.0.0 Types of Accounts

User Account - This will be the basic account that all users will have. It will have limited functionality.

Frozen Account- If the user fails to login several times the account will have to be authenticated through an email verification process

Super User Account - will be able to modify databases and have greater functionality than the standard user account. Access to this type of account will be heavily restricted.

3.3.0.1 Information

Email - will be used to authenticate account and used to send updates to the user. The email will be stored as a representation of the email rather than simple plaintext.

Password- used in conjunction with the email to grant access to the user’s Goodcoin account and ethereum account. Each password and email will be hashed with a salt on the database to ensure security to users in the event of an attack.

First Name/Last Name - used to personalize emails and web page

*3*.3.0.2 Successful Account Creation

Upon successful account creation the user will be able taken to the login page and they will be able to log in through that page with their new credentials after they verify their email address.

The user will also have created an Ethereum account that they will be able to interface with to conduct any transactions.

3.3.1 Login Page

3.3.1.0 Login

This feature will provide a user access to their Goodcoin and Ethereum accounts. The login page will prompt the user for their email and password.

3.3.1.0.1 Successful Attempt

Grants the user access to the account and logs their current IP Address and location.

If the user is successful but from an IP address that is not on file the user must authenticate their account for that IP address.

User is redirected to the main page in order to continue their interaction with Goodcoin.

After a successful attempt the user will be able to whitelist their IP address and be able to log in from that address without verification in the future. The user may also request that the whitelisted IP addresses are the only IP addresses that are allowed to attempt to access the account without email verification. If an IP address attempts to access the account that is not whitelisted then any attempt that is not from the whitelisted email addresses will not be able to access the account and an email will be sent and the unverified attempts will be logged.

3.3.1.0.2 Unsuccessful Attempt

Denies the user access to the account and logs their current IP address and location.

After 4 failed attempts the user will be locked out of their account, the account will be frozen and the user must authenticate their account through email verification.

If the users’ account is frozen through unauthorized attempts then the IP address of the unverified attempts will be banned from accessing the account.

Every incorrect attempt sends the IP address and location of the attempt

3.3.2 Email Authentication

Email Authentication will be used as a part of two step verification to ensure that the person who is logging in is who they say they are and that they have access to the account.

3.3.2.0 Sending and Verifying Email

The email will be sent out to the email on file containing a single use, time sensitive code or web link that will be used to verify their account.

3.3.2.1 Email Verification page

The email verification code will be a nonce code that is unique to the user and will have to be input onto the email verification page with their email in order to verify the account and grant the user access to the account.

3.3.3 Wallets

There will be two kinds of wallets, the hot wallet and the cold wallet.

3.3.3.0 Cold Wallet

The cold wallet will be the main source of currency for Goodcoin. The cold wallet will be almost exclusively offline and will house the majority of the coins. This is done to protect the main storage of coins in case there is an attack on the system. The cold wallet will be stored on its own separate server that will only wake if the hot wallet has run out of funds. The cold wallet will only be able to interact with the hot wallet, no single user will be able to interact with the cold wallet.

3.3.3.1 Hot Wallet

The hot wallet will house a vast minority of the coins. The hot wallet will be the portion of the coins accessed when a transaction is to be made. Each transaction will first be verified on the block chain for its veracity before being executed and having the funds removed from the hot wallet. The hot wallet will be able to access the cold wallet in the event there are not enough coins in the hot wallet to cover a particular transaction or if the amount of coins in the wallet is zero.

3.3.4 Server

The server will house the

Other NonFunctional Requirements

Security Requirements

 HTTPS/SSL

The web page will be secured through a secure socket layer, this level of security will provide users with piece of mind that their information will be safely and securely handled.

                      Firewall on servers

The web server and main server will be protected with a firewall that will only allow certain ports to be accessed and will only allow certain types of information through the firewall

                       Parameterized SQL injection

There will be parameterized SQL injection to ensure the databases cannot be directly attacked through any sort of injection attack when inputting information into any of the fields.

                        Ip Address monitoring

IP addresses will be monitored during sessions to prevent any sort of hijacking attack. If the IP address of a user changes during a session then they will be automatically logged out and have the change recorded. The User will then have to log back in securely.

                        Inactivity monitoring

The user’s session will be tracked not only for IP address change but also for activity on the page and in the app. If the user does not have any sort of interactivity with Goodcoin for over 5 minutes they will be automatically logged out and will have to relogin.

                        Encryption Used

The types of encryption that will be used include AES-256 as well as SHA-256, these encryption standards will be mainly used on the database and for sending sensitive information. There will also be Pgp protection on the emails to ensure an attacker cannot intercept an email.

**Legal Requirements**

Goodcoin will be fully legal as it will be a side chain of the Ethereum block chain. The users will only be able to interact with their own currency and it will be managed over the Ethereum network. Legal troubles arise when the coin begins to exchange with banks and various entities of that type.