



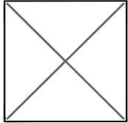


Product Requirement Document (PRD) - Version: 1.0



Template Name	Money Transfer system using Blockchain
Goals & Objective	<p>We all transfer money. The goal of this website is to provide a secure and efficient platform for individuals and businesses to transfer money using blockchain technology.</p> <p>From this website user/miner can :</p> <ul style="list-style-type: none"> - Send & Receive money with low cost transaction fee - Can see transparent ledger where all activity of transaction is shown - Can see block information - Miners can mine blocks - Miners can verify blocks - User/Miners can update their profile information
Client Information	
Product Type	Web Application
Domain	Web2
Access Layers	User, Miner
Design Required	Yes

Phase	Item No	Specification [Role]	User Story	Acceptance Criteria	UI Screen / Wireframe	Tags
Feature: 1		Auth Feature				
phase 1	1	Signup [Miner] [User]	<ul style="list-style-type: none"> - Enter Full name (input) - Enter unregistered email (input) - Enter password (input) [Logic: At least 8 characters long, atleast one special character] - Enter password again (input) [Logic: should match password input] - Choose user type [user,miner] - Click Signup (button) [Logic: If the email is unique, user will be registered to the system (database)] - Signin (link) [Logic: redirect user to Login page] 	<ul style="list-style-type: none"> - Email (input) field should only accept valid unregistered email address as input, otherwise will show an 'email already used' message. - Password (input) should be minimum 8 characters long. Otherwise show an invalid message. - Re-password (input) should match password. Otherwise show 'password do not match' message. - User type must be selected. Otherwise show 'Please select a user type'. - On clicking signup button, credential will be stored in database, user will be redirected to his dashboard. - A copy of the login information will be sent to his email. 	<div> <h3>Signup</h3> <p>Name : <input type="text"/></p> <p>Email <input type="text"/></p> <p>Password <input type="password"/></p> <p>re-Password <input type="password"/></p> <p>User type <input type="radio"/> User <input type="radio"/> Miner</p> <p><input type="button" value="Signup"/> Sign in</p> </div>	signup
phase 1	2	Signin [Miner] [User]	<ul style="list-style-type: none"> - Enter Email (input) - Enter password (input) - signin (button) - signup (link) - forgot password (link) 	<ul style="list-style-type: none"> - Email must match database email - password must match database password - User go to dashboard (if email & password match with database) - User is prompt with an error. "Email or password does not match!". (if email & password match with database) - clicking signup should take user to signup page - clicking forgot password should take him to forgot password page 	<div> <h3>Signin</h3> <p>Email <input type="text"/></p> <p>Password <input type="password"/></p> <p><input type="button" value="Signin"/> Sign up</p> <p>Forgot password?</p> </div>	signin

phase 1	3	Forgot password[Miner] [User]	<ul style="list-style-type: none"> - Enter email (input) - Press send code (button) - Enter new password (input) - Re-type new password (input) - click on change passowrd to update password (button) 	<ul style="list-style-type: none"> - email must match DB email or promt "No email found!" - pressing send code will print a message "code sent!" and the code can be found at user info row. - enter new password [At least 8 characters long, atleast one special character] - re-type new password [it should match new password] - clicking submit button will show user -> "password changed" if all info match criteria or it'll indicate what's wrong 	<div> <div>Change password</div> <div> <div>Email</div> <input type="text"/> <div>Send code</div> </div> <div> <div>Code</div> <input type="text"/> </div> <div> <div>Password</div> <input type="text"/> </div> <div> <div>Re-Password</div> <input type="text"/> </div> <div>Submit</div> </div>	forgot_password
Feature: 2 Dashboard						
phase 1	4	Menu [User]	<ul style="list-style-type: none"> - Dashboard(link) - Send money(link) - public ledger (link) - Latest Blocks (link) - View Profile(link) - Edit profile(link) - change profile photo(link) - change password(link) 	<ul style="list-style-type: none"> - clicking dashboard will take user to dashboard page - go to send money page on click - go to public ledger on Click - go to Latest blocks page on click - go to view profile page on click - go to edit profile page on Click - go to change profile page on Click - go to change password page on Click 	<div> <div>User Menu</div> <div> <div>Dashboard</div> <div>Send Money</div> <div>Public Ledger</div> <div>Latest Blocks</div> <div>View Profile</div> <div>Edit Profile</div> <div>Change Profile Photo</div> <div>Change Password</div> </div> </div>	Menu
phase 1	5	Menu[Miner]	<ul style="list-style-type: none"> - Dashboard(link) - Send money(link) - public ledger(link) - Latest blocks(link) - Mempool(link) - Mine Blocks(link) - Verify Blocks(link) - View Profile(link) - Edit profile(link) - change profile photo(link) - change password(link) 	<ul style="list-style-type: none"> - clicking dashboard will take user to dashboard page - go to send money page on click - go to public ledger on Click - go to Latest blocks page on click - go to mempool page on click - go to mine blocks page on click - go to verify blocks page on click - go to view profile page on click - go to edit profile page on Click - go to change profile page on Click - go to change password page on Click 	<div> <div>Miner Menu</div> <div> <div>Dashboard</div> <div>Send Money</div> <div>Public Ledger</div> <div>Latest Blocks</div> <div>Mempool</div> <div>Mine Block</div> <div>Verify Blocks</div> <div>View Profile</div> <div>Edit Profile</div> <div>Change Profile Photo</div> <div>Change Password</div> </div> </div>	
phase 1	6	Dashboard [Miner] [User]	<ul style="list-style-type: none"> - Balance (text) - trx history(link) - public key (text) - private key(text) - bitcoin address(text) 	<ul style="list-style-type: none"> - show appropriate Balance (should not be less than 0) - clicking trx history link will take user to trx history page - public key is shown - private key is only shown when clicked - bitcoin address is shown 	<div> <div>Dashboard</div> <div> <div>Welcome, Shamim</div> <div>Balance : 123BTC</div> <div>View Trx History</div> <div>pub key : 112sadfa</div> <div>private key : Click to view</div> <div>Bitcoin Address : 123adfzxaefd</div> </div> </div>	
Feature: 3 Top bar and Bottom Bar						

phase 2	11	Latest Blocks[user][miner]	<ul style="list-style-type: none">- Block number (text)- Time(text)- Number of trx(text)- size(mb in text)- Miner(name)	<ul style="list-style-type: none">- full row is clickable- once clicked it'll redirect to another page [block view page where block details will be shown]- Block number should be in desending order [latest block should be in the top]- Block Size should be in MB- Number of trx should be in number [negative number not allowed]- Miner name	<div>Latest Block</div> <div> Logged in as, caeshamim42 Logout</div> <table><thead><tr><th>Block Numbe</th><th>Time</th><th>Number of transactions</th><th>Size</th><th>Miner</th></tr></thead><tbody><tr><td>77550</td><td>12:46:33</td><td>122</td><td>3.3MB</td><td>BCT.com</td></tr><tr><td>77549</td><td>12:40:15</td><td>452</td><td>0.56MB</td><td>Antpool</td></tr><tr><td>77548</td><td>12:35:27</td><td>354</td><td>3MB</td><td>Binance pool</td></tr><tr><td>77547</td><td>12:27:02</td><td>752</td><td>2.4MB</td><td>Foundry usa</td></tr><tr><td>77546</td><td>12:20:13</td><td>246</td><td>8.6MB</td><td>Acusjk</td></tr></tbody></table> <div>Copyright © 2023</div>	Block Numbe	Time	Number of transactions	Size	Miner	77550	12:46:33	122	3.3MB	BCT.com	77549	12:40:15	452	0.56MB	Antpool	77548	12:35:27	354	3MB	Binance pool	77547	12:27:02	752	2.4MB	Foundry usa	77546	12:20:13	246	8.6MB	Acusjk
Block Numbe	Time	Number of transactions	Size	Miner																															
77550	12:46:33	122	3.3MB	BCT.com																															
77549	12:40:15	452	0.56MB	Antpool																															
77548	12:35:27	354	3MB	Binance pool																															
77547	12:27:02	752	2.4MB	Foundry usa																															
77546	12:20:13	246	8.6MB	Acusjk																															
Feature: 7 Mempool																																			
phase 2	12	Mempool[miner]	<ul style="list-style-type: none">- unconfirmed trx ids (text)- trx fee (in btc)- click add button(button)- number of added trx(number)- total fees(number)- go(button)	<ul style="list-style-type: none">- add button must add the corresponding transaction [after clicking add button, the row should disspear from the list and added to the block]- the trx list should be in decending order by the fee. [maximum fee transaction should appear on top]- total number of trx added should appear in the bottom of demo block- total fees of added trx- go button should take miner to mine block page.	<div>Latest Block</div> <div> Logged in as, caeshamim42 Logout</div> <table><thead><tr><th>Block Numbe</th><th>Time</th><th>Number of transactions</th><th>Size</th><th>Miner</th></tr></thead><tbody><tr><td>77550</td><td>12:46:33</td><td>122</td><td>3.3MB</td><td>BCT.com</td></tr><tr><td>77549</td><td>12:40:15</td><td>452</td><td>0.56MB</td><td>Antpool</td></tr><tr><td>77548</td><td>12:35:27</td><td>354</td><td>3MB</td><td>Binance pool</td></tr><tr><td>77547</td><td>12:27:02</td><td>752</td><td>2.4MB</td><td>Foundry usa</td></tr><tr><td>77546</td><td>12:20:13</td><td>246</td><td>8.6MB</td><td>Acusjk</td></tr></tbody></table> <div>Copyright © 2023</div>	Block Numbe	Time	Number of transactions	Size	Miner	77550	12:46:33	122	3.3MB	BCT.com	77549	12:40:15	452	0.56MB	Antpool	77548	12:35:27	354	3MB	Binance pool	77547	12:27:02	752	2.4MB	Foundry usa	77546	12:20:13	246	8.6MB	Acusjk
Block Numbe	Time	Number of transactions	Size	Miner																															
77550	12:46:33	122	3.3MB	BCT.com																															
77549	12:40:15	452	0.56MB	Antpool																															
77548	12:35:27	354	3MB	Binance pool																															
77547	12:27:02	752	2.4MB	Foundry usa																															
77546	12:20:13	246	8.6MB	Acusjk																															
Feature: 8 Mine Blocks																																			
phase 2	13	Mine Blocks[miner]	<ul style="list-style-type: none">- current block no(number)- nonce(can be input)- data(all transactions)- prev hash(previous block hash)- hash(current hash with given data)- try mining with given nonce(button - it'll generate a hash with given nonce,blockno,data,prevhash and check if it's less than target)- mine (it'll try all possible nonce to find a hash which is less than target)	<ul style="list-style-type: none">- block number should be 1 + previous block number. Genesis block number is 1- default nonce value is one- data should include all valid transaction in the block- prev hash should be the hash of previous block- "try mining with given nonce" button will try to mine using the given nonce- mine button will find a valid hash that is less than the target and notify miner that it's ready to be added to the verification list	<div>Mine Blocks</div> <div><div>Block No: <input type="text" value="02"/></div><div>Nonce: <input type="text" value="215458"/></div><div>Data: <input type="text" value="1233.34BTC"/></div><div>Previous Hash: <input type="text" value="8428934398498347"/></div><div>Hash: <input type="text" value="5434583479534985"/></div><div><input type="button" value="Mine with given Nonce"/> <input type="button" value="Mine"/></div></div>																														
Feature: 9 Verify Blocks																																			
phase 2	14	Verify Blocks[miner]	<ul style="list-style-type: none">- current block no(uneditable number)- nonce(uneditable text)- data(all transactions)- prev hash(uneditable previous block hash)- hash(current hash with given data)- miners can verify a mined block whether hash value meets the target condition or not- after verifying miner will confirm the block and if 51% miner confirm that the block does not contain any tampered data, then the block will be added to the chain- verify(button)- confirm(button)	<ul style="list-style-type: none">- block number should be 1 + previous block number. Genesis block number is 1 and has no prev hash- correct nonce value should be set- data should include all transaction in the block- prev hash should be the hash of previous block- clicking on confirm will not work before verifying- clicking on verify will prompt will a message "It's a valid block!".- Clicking on confirm button will increment <row = number of confirmation>	<div>Verify Block</div> <div><div>Block</div><div>Confirmations : 3</div><div>Block No : 2</div><div>Nonce : 12312</div><div>Data :</div><div><div>Shamim -> asif 5BTC</div><div>Abdur -> Taifur 0.234 BTC</div><div>•</div><div>•</div><div>•</div></div><div>Prev Hash : 0000123sdfa13ssa4312</div><div>Hash : 0000tttsdfa13ssa4312</div><div><input type="button" value="Verify"/> <input type="button" value="Confirm"/></div></div>																														

Feature: 10		Profile			
phase 1	15	View Profile[miner][user]	<ul style="list-style-type: none"> - Full name of user (view) - phone number of user (view) - date of birth of user (view) - gender of user (view) - user type (miner/user) - edit (link button) 	<ul style="list-style-type: none"> - No null values - Edit button should take user to edit page 	<div> <div>Profile</div> <div> Name : Md Shamim Ahmed Email : xys@gmail.com Phone : 012312 Date of Birth : 01-01-1999 gender : Male User Type : Miner Edit </div>  </div>
phase 1	16	Edit Profile[miner][user]	<ul style="list-style-type: none"> - can edit name - can edit email - can edit phone - can edit date of birth - can edit gender - can click on save button 	<ul style="list-style-type: none"> - No null values - email should be in correct format [xyz@abc.com] - phone number should be in correct format [11 digits] - date of birth should be in at least 15 years - clicking save button will either prompt with an error if above rules do not meet or a prompt notifying the user about successful change 	<div> <div>Edit Profile</div> <div> Name : <input type="text" value="Md Shamim Ahmed"/> Email : <input type="text" value="xys@gmail.com"/> Phone : <input type="text" value="012312"/> Date of Birth : <input type="text" value=""/> / <input type="text" value=""/> / <input type="text" value=""/> gender : <input type="radio"/> Male <input type="radio"/> Female <input type="button" value="Confirm"/> </div> </div>
phase 1	17	Change Profile Photo[miner][user]	<ul style="list-style-type: none"> - current image of user/miner is shown - user can choose new photo from device - after choosing new photo, user can confirm by pressing confirm button 	<ul style="list-style-type: none"> - current image/ default image is shown - input file should be an image and not any other format [png,jpg format] - cofirm button should redirect user to view profile page 	<div> <div>Change profile picture</div> <div>  <input type="button" value="+"/> Choose File <input type="button" value="Confirm"/> </div> </div>
phase 1	18	Change Password[miner][user]	<ul style="list-style-type: none"> - type current password - type new password - type new password again 	<ul style="list-style-type: none"> - user can type current password [it should match database password] - Password (input) should be minimum 8 characters long. Otherwise show an invalid message. - Re-password (input) should match password. Otherwise show 'password do not match' message. - On clicking signup button, credential will be stored in database, user will be prompted with a message. [sucessfully changed / something went wrong] 	<div> <div>Change Password</div> <div> Current Password <input type="text"/> * Password: <input type="text"/>  * Re-type password: <input type="text"/> <input type="button" value="Change"/> </div> </div>
Feature: 11		Transaction details			

phase 3	19	Transaction Details[miner][user]	<ul style="list-style-type: none"> - user can see unique hash id - user can see trx status(pending/confirmed) - user can see the amount - user can see fee - user can see from where the money coming - user can see to where the money is going - user can click 'More' to see more about this transaction 	<ul style="list-style-type: none"> - hash id must be unique - trx status must be set - amount should be number and positive value - fee should be a number - the address of sender must be shown - the address of receiver is also shown - clickable link to more details about this transaction 	<div>Transaction details</div>  <p>Logged in as, cseashamim47 Logout</p> <p>Hash id → 54dge24Fh56</p> <p>status → pending</p> <p>Amount → 542BTC</p> <p>Fee → 10BTC</p> <p>From → dfk452R5dJg</p> <p>To → 5dfh2f5r2f25</p> <p>more</p> <p>Copyright © 2023</p>	
phase 3	20	More[miner][user]	<ul style="list-style-type: none"> - user can see unique hash id - user can see trx status(pending/confirmed) - user can see the amount - user can see fee - user can see from where the money coming - user can see to where the money is going - trx Time is shown - age of the trx is shown - input and input vlaue is shown - output and output value is shown - fee is shown - size of the trx also can be seen 	<ul style="list-style-type: none"> - hash id must be unique - trx status must be set - amount should be number and positive value - fee should be a number - the address of sender must be shown - the address of receiver is also shown - trx time : when the trx happened is set to see - age = current time - trx time - input (integer number) & input value(decimal) - output (integer number) & output value(decimal) - fee must be set - size of trx in bytes 	<div>Transaction details</div>  <p>Logged in as, cseashamim47 Logout</p> <p>Hash id → 54dge24Fh56</p> <p>status → pending</p> <p>Amount → 542BTC</p> <p>Fee → 10BTC</p> <p>From → dfk452R5dJg</p> <p>To → 5dfh2f5r2f25</p> <p>Time → 12:24:52</p> <p>Age → 6 minute</p> <p>Inputs → 2 BTC</p> <p>Input value → 10BTC</p> <p>Output → 2 BTC</p> <p>Output value → 9 BTC</p> <p>Copyright © 2023</p>	
Feature: 12		Block details				
phase 3	21	Bitcoin Block[miner][user]	<ul style="list-style-type: none"> - Block number - miner name - block BTC(sum of all trx) - value(BTC in dollar) - more(link) 	Everything should be valid & verified	<div>Block details</div>  <p>Logged in as, cseashamim47 Logout</p> <p>Block Number : 2</p> <p>Miner : allox_4b</p> <p>BTC : 0.38</p> <p>Value : 60 BTC</p> <p>More</p> <p>Copyright © 2023</p>	
phase 3	22	More[miner][user]	<ul style="list-style-type: none"> - Block number - miner name - block BTC(sum of all trx) - value(BTC in dollar) - distance(mins since mined) - depth(number of blocks that have been added after this block+1) - trx(number of transactions) - input(number of inputs) - output(number of outputs) - fees(total fees generated to verify all transaction) - Reward(block reward. currently 6.5 btc) - Nonce(number) - size (mb) 	Everything should be valid & verified	<div>Block details</div>  <p>Logged in as, cseashamim47 Logout</p> <p>Block Number : 2</p> <p>Miner : allox_4b</p> <p>BTC : 0.38</p> <p>Value : 60 BTC</p> <p>Distance : 4 minutes</p> <p>depth : 3</p> <p>trx : 4545213</p> <p>input : 2</p> <p>output : 2</p> <p>Fees : 42 BTC</p> <p>Reward : 6.5 BTC</p> <p>Nonce : 263</p> <p>Size : 0.3 MB</p> <p>confirmations : okay</p> <p>Copyright © 2023</p>	
Feature: 13		Notification				

