User Manual of Assignment 2

Machine Problem: Distributed Coin Flipping Game Using Ethereum

Jiabao LIN, 3035673521

Introduction

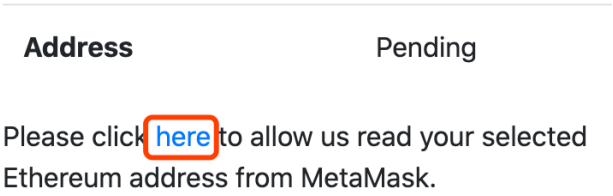
It is a coin flipping game. It has the following characteristics:

- **Highly anoymous and confidential.** Users cannot see the counterparties' username (accountID) in the game and game history. In game history, only the user's index and winner's index will be provided. Unless the counterparties go to the Ethereum Blockchain Explorer to track the transactions one by one, they will never know your actual accountID.
- **High speed.** The banker (dealer) is implemented within the contract, no real-person dealer is needed. Therefore, the speed of the game will be much faster (at least 16.7% faster if the users always act in time). This part is discussed in Design Document.
- **Light weight.** There is no server/backend actually needed, all the user/game/transaction information are stored in the blockchain. Even with GitHub Pages, a full functional site can be hosted without any effort.
- **Multiple players.** More than 2 players in each round of game is supported. The people who initialize the game can decide how many players are allowed in this round.

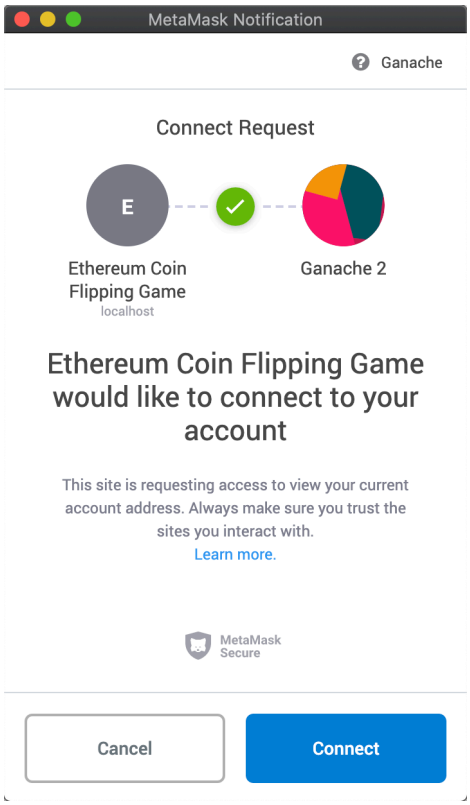
First Login

You need to install MetaMask in your browser, which could help you interact with the Ethereum Blockchain.

When you open this site for the first time, you need to click the link to allow the site interact with you accounts in MetaMask.



A MetaMask Notification will popup, click Connect to allow the conntection.

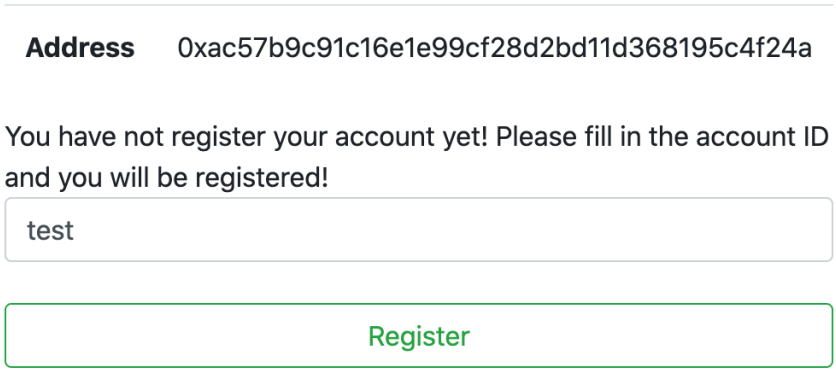


Once the site is successfully connected to MetaMask, it will refresh on its own, and you will be able to proceed.

User

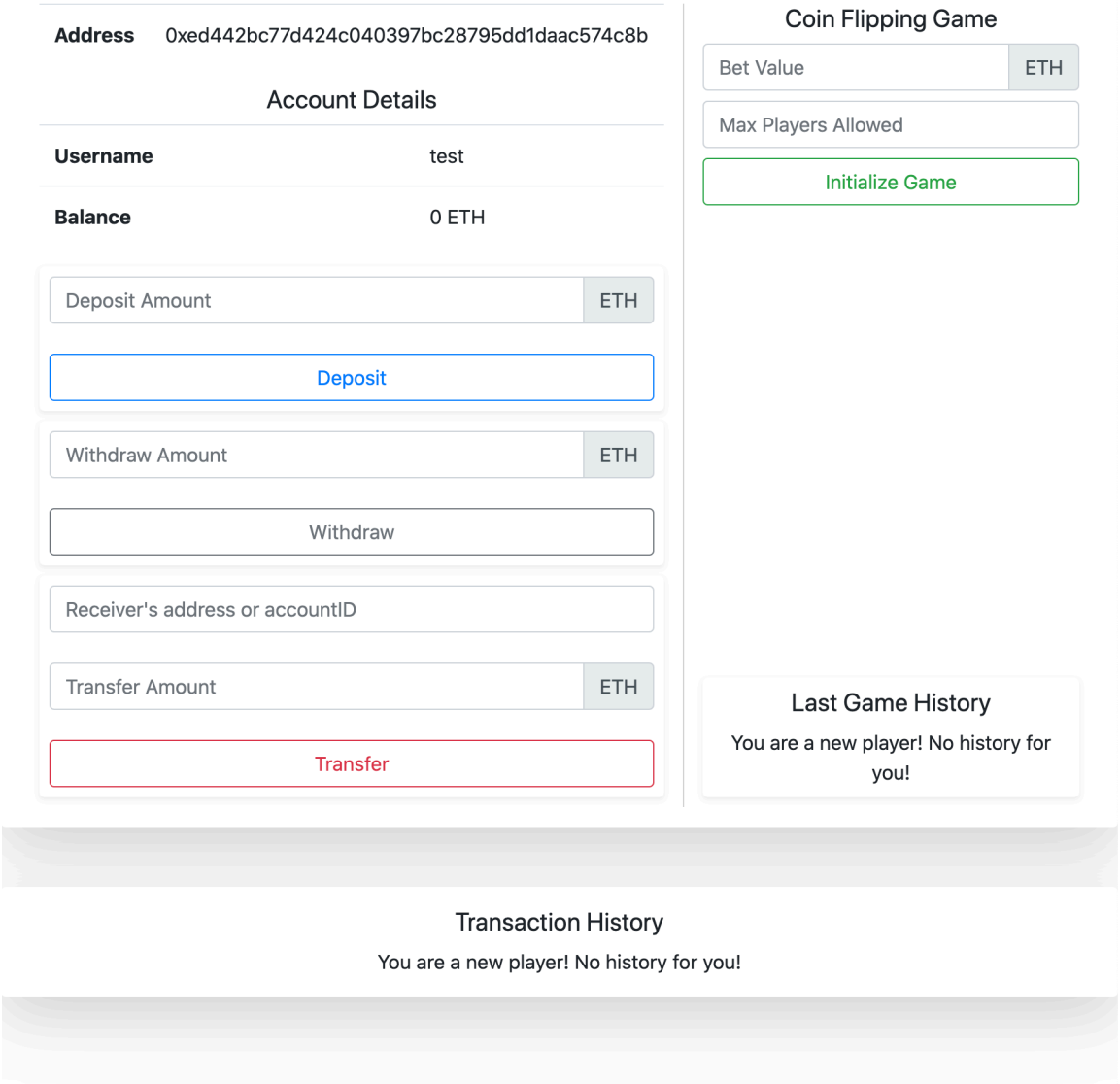
Registration

If it is the first time for you to login, you will need to register and account in the begining. Choose an ID and click `Register` button.



You need to notice that, your ID cannot start with `0x`, as this prefix is reserved for the addresses.

MetaMask will pop up to alert you that it will send a transaction to register this account. Click `Confirm` and your account will be prepare in the next block. You can refresh the page to check if the next block is successfully mined. If yes, you will get into this page.



Balance Management

The Ether you deposited into this contract will be keeped in track by the balance sheet in this contract, no one else can modify it except you.

Deposit/Withdraw

Input the value in the input box, click `Deposit` or `Withdraw`. MetaMask will pop up to let you confirm the interaction with the Blockchain.

If you are going to withdraw, please make sure the balance is enough in your account, otherwise you will not be able to withdraw anything.

Transfer

You can transfer you balance to other registered users within the contract. Once the transaction has been initiated, you cannot recall and the balance is moved immediately.

You can directly input the receiver's address or accountID to transfer your balance to that account. The website will directly tell whether your input is an address or an accountID.

If that address/accountID is not registered, your transaction will fail and your asset is safe.

Transaction History

The transaction history within 24 hours will be accessible. Once you successfully deposit/withdraw/transfer, the transaction history will refresh automatically. The outdated transaction history cannot be retrieved anymore because an contract-level (backend-level) block is implemented.

Transaction History

Transaction ID	Type	Transaction Time	From	To	Amount
3	Transfer	27/4/2020 6:30:24 PM	test	test1	0.3 ETH
2	Withdraw	27/4/2020 6:29:46 PM	test	External Wallet	0.5 ETH
1	Deposit	27/4/2020 6:29:08 PM	External Wallet	test	1 ETH

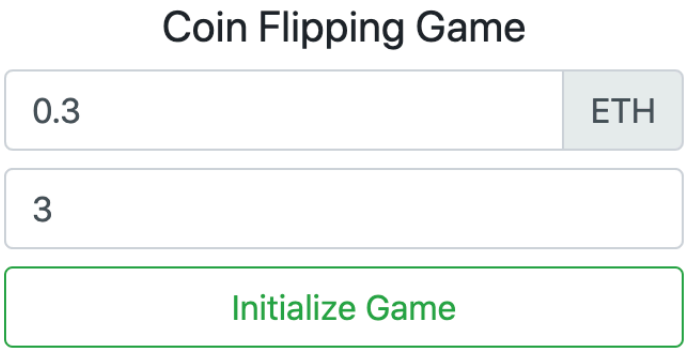
Game

Only 1 game is on-going every time, and only 2 players are allowed in each game.

Initialize Game

If there is no on-going game, you can input a bet value and click `Initialize Game` initialize a game.

Please make sure you have enough balance to initialize a game.

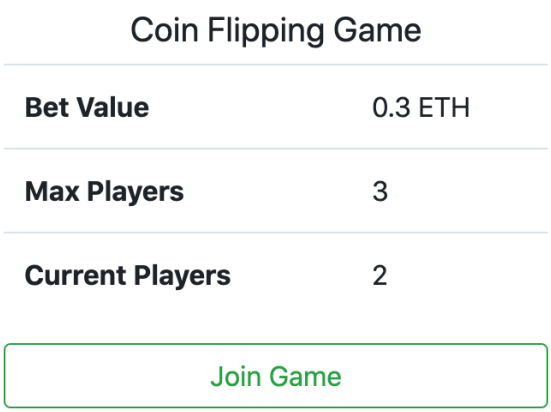


Once you successfully initialize a game, the bet value will be temporarily transferred from your balance to the banker's deposit to freeze those tokens.

Join Game

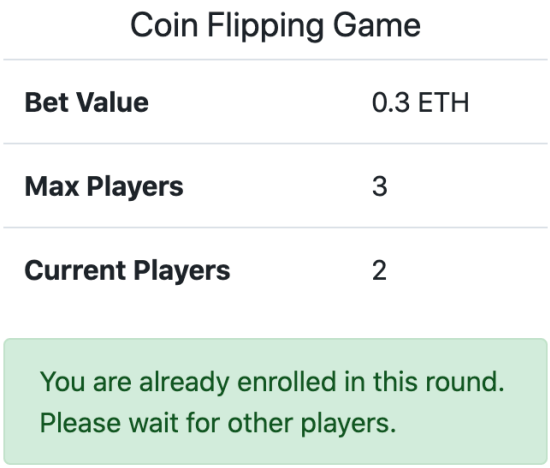
If there is an on-going game, the bet value of that game will be shown. If you appreciate that bet value, you can click `Join Game` to join that game. Otherwise, you can only wait for that game to end.

Please make sure you have enough balance to join a game.



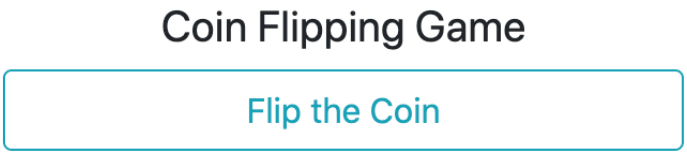
The same as initializing a game, once you successfully join a game, the bet value will be temporarily transferred from your balance to the banker's deposit to freeze those tokens.

If the user has successfully enrolled in this game, there will be an alert showing this information.



Flip Coin

Once the players reached the max players, the game will start automatically. You can flip the coin by clicking `Flip the Coin`.



Once you click the button, please do not refresh the page until 2 transactions was send! A random number is generated after clicking the button to keep you fair, if you refresh the site, the random number will be gone.

MetaMask will pop up twice during this process.

1. Send a transaction containing hashed random number.
2. Once all participants submitted the hashed random number, the random number in clear text version will be submitted automatically.

Once you have seen 2 transactions, you can refresh the page and check the winner.

Cheating Detection

If any participants are detected cheating, all the balance will be transfer back to the participants account. Currently, there will not be any punishment, and the reason is discussed in the Round 4 of Design Document.

Reward

The winner will receive the reward once the game ends. 95% of the total bet value will be transfer to your balance, and 5% will be the banker's commission.

Transaction History

Transaction ID	Type	Transaction Time	From	To	Amount
8	Reward	27/4/2020 6:46:40 PM	banker	test3	0.19 ETH
6	Bet	27/4/2020 6:39:14 PM	test3	banker	0.1 ETH
5	Deposit	27/4/2020 6:38:23 PM	External Wallet	test3	1 ETH

Game History

The game history of the previous round will be available on the page.

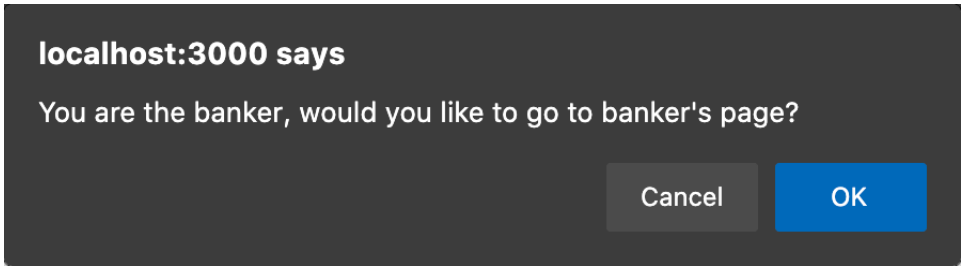
Last Game History

Game ID	1
Bet Value	0.5 ETH
Total Player	4
Your Index	3
Winner Index	3

To keep the privacy of the participants, only the indexes will be shown in this frame. You can find out how many participants are in this round, your index and the winner's index.

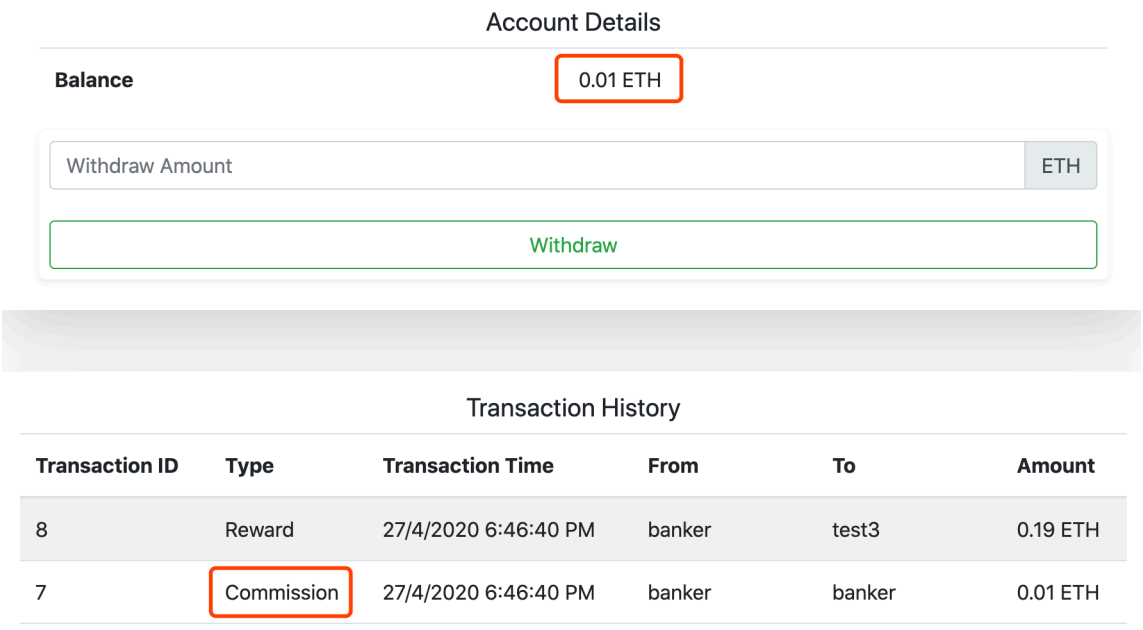
Banker

If a banker visit the site, an alert will pop up to ask whether it is going to the banker's site or not.



By clicking `OK`, the banker will automatically be redirected to the banker's panel.

This site is quite simple, banker can withdraw the commission earnings or check all the transaction histories of all users on this site, no other functions are provided.



All the functions of banker cannot be executed by normal users, they are blocked from both front-end and back-end.

Withdraw Commission

In each game, the banker will earn 5% of the total bet value as the commission fee. Therefore, from time to time, the banker will need to withdraw this balance. This balance can only be withdrawn to banker's address, which is the owner of this contract.

Track Transaction History

For administration purpose, the banker can also see all the transaction histories of all users.