Cryptocurrencies

Jan 3-11 2018

Group 3
Dr. Eric Falkenstein and Mackenzie Mikkelsen
Jacob Gotto, Changlin Xie, Yuanyang Ruan, Jiahui Chen, Tianzi Guo
CryptoCurrency Project

- Learn how cryptos and Ethereum contracts work
- How to set up wallet
  - Transfer, trade coins/tokens
- How a simple contract works
  - How to interact with contracts
Tasks 1 (Eric)

- How does one set up a wallet?
- How much does it cost to send a coin?
- How much does it cost to change one coin into another
- How difficult is it to trade tokens?
  - How long does a transaction take?
  - What is the bid-ask?
Tasks 2 (Mackenzie Mikkelsen)

- Create simple Ethereum contract
  - Personal tokens
- Create contract that swaps tokens
  - Interact with contract on testnet
Transactions of Cryptocurrency

we used different wallets to transfer these different cryptocurrency, the transactions are composed of:

- coin(from)/coin(to)
- mining fee (usually listed in the transaction id)
- time sent and received
- how much was sent and received
- Can view transactions on blockchain
Cost of Swapping one Currency to Another

Used ShapeShift

Total Cost is based on estimated value of crypto sent minus value of crypto received

Price volatility can generate ‘negative’ costs

<table>
<thead>
<tr>
<th>Out Currency</th>
<th>In Currency</th>
<th>Time (min)</th>
<th>Out Amount</th>
<th>In Amount</th>
<th>Mining Fee</th>
<th>Mining Currency</th>
<th>Out Currency Price USD</th>
<th>In Currency Price</th>
<th>In Currency Mining cost in USD</th>
<th>Total Cost at Mkt Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETH</td>
<td>BTC</td>
<td>8</td>
<td>0.060</td>
<td>0.002</td>
<td>0.0015 BTC</td>
<td>987</td>
<td>15,390</td>
<td></td>
<td>23.08</td>
<td>29.07</td>
</tr>
<tr>
<td>ETH</td>
<td>LTC</td>
<td>8</td>
<td>0.449</td>
<td>1.718</td>
<td>0.0008 ETH</td>
<td>992</td>
<td>255</td>
<td></td>
<td>0.20</td>
<td>6.68</td>
</tr>
<tr>
<td>ETH</td>
<td>ZEC</td>
<td>6</td>
<td>0.328</td>
<td>0.587</td>
<td>0.0001 ZEC</td>
<td>1,016</td>
<td>591</td>
<td></td>
<td>0.06</td>
<td>-13.63</td>
</tr>
<tr>
<td>ETH</td>
<td>BCH</td>
<td>6</td>
<td>0.443</td>
<td>0.172</td>
<td>0.0002 BCH</td>
<td>1,176</td>
<td>2,606</td>
<td></td>
<td>0.52</td>
<td>73.13</td>
</tr>
<tr>
<td>ETH</td>
<td>DSH</td>
<td>6</td>
<td>0.060</td>
<td>0.048</td>
<td>0.0020 DSH</td>
<td>992</td>
<td>1,100</td>
<td></td>
<td>2.20</td>
<td>6.26</td>
</tr>
<tr>
<td>BTC</td>
<td>ETH</td>
<td>12</td>
<td>0.029</td>
<td>0.462</td>
<td>0.0012 BTC</td>
<td>15,988</td>
<td>1,012</td>
<td></td>
<td>1.21</td>
<td>-6.89</td>
</tr>
<tr>
<td>ZEC</td>
<td>ETH</td>
<td>6</td>
<td>0.624</td>
<td>0.329</td>
<td>0.0120 ETH</td>
<td>586</td>
<td>1,000</td>
<td></td>
<td>12.00</td>
<td>36.61</td>
</tr>
<tr>
<td>LTC</td>
<td>ETH</td>
<td>9</td>
<td>1.434</td>
<td>0.392</td>
<td>0.0050 ETH</td>
<td>293</td>
<td>1,056</td>
<td></td>
<td>5.28</td>
<td>6.93</td>
</tr>
<tr>
<td>BCH</td>
<td>ETH</td>
<td>13</td>
<td>0.172</td>
<td>0.414</td>
<td>0.0080 ETH</td>
<td>2,599</td>
<td>978</td>
<td></td>
<td>7.82</td>
<td>42.03</td>
</tr>
<tr>
<td>DSH</td>
<td>ETH</td>
<td>3</td>
<td>0.220</td>
<td>0.190</td>
<td>0.0080 ETH</td>
<td>1,175</td>
<td>977</td>
<td></td>
<td>7.81</td>
<td>72.92</td>
</tr>
</tbody>
</table>

Totals: 60.18 253.11
Cost and Time to Transfer Cryptos

- One address to another

<table>
<thead>
<tr>
<th>Currency</th>
<th>Time (min)</th>
<th>Amount</th>
<th>Mining Fee</th>
<th>Price USD</th>
<th>Mining cost in USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSH (regular)</td>
<td>12</td>
<td>0.208</td>
<td>0.002</td>
<td>1,150</td>
<td>2.3</td>
</tr>
<tr>
<td>DSH (private)</td>
<td>3</td>
<td>0.150</td>
<td>0.0001</td>
<td>1,150</td>
<td>0.12</td>
</tr>
<tr>
<td>DSH (instant)</td>
<td>1</td>
<td>0.049</td>
<td>0.0001</td>
<td>1,150</td>
<td>0.12</td>
</tr>
<tr>
<td>LTC</td>
<td>1</td>
<td>1.435</td>
<td>0.001</td>
<td>294</td>
<td>0.29</td>
</tr>
<tr>
<td>BCH</td>
<td>3</td>
<td>0.172</td>
<td>0.0002</td>
<td>2,606</td>
<td>0.52</td>
</tr>
<tr>
<td>ZEC</td>
<td>1</td>
<td>0.624</td>
<td>0.0001</td>
<td>591</td>
<td>0.06</td>
</tr>
<tr>
<td>BTC</td>
<td>2</td>
<td>0.030</td>
<td>0.0018</td>
<td>15,000</td>
<td>27</td>
</tr>
<tr>
<td>ETH</td>
<td>15</td>
<td>0.450</td>
<td>0.0033</td>
<td>1,012</td>
<td>3.34</td>
</tr>
</tbody>
</table>
Tokens

1. A token is simply a custom cryptocurrency

What is a ERC20 token?

‘ERC’ stands for "Ethereum Request for Comments".

‘20’ is the unique proposal ID number.

‘ERC20’ is the standard Ethereum token

List of all ERC 20 tokens can be found here - https://etherscan.io/tokens
2. Based on Ethereum Blockchain

Difference between ERC20 tokens and a standalone currency (like Bitcoin):

ERC20 tokens piggyback on the Ethereum network, hosted by Ethereum addresses and sent by Ethereum transactions.

All ERC20 tokens transact on the same network that our Ethereum wallet uses.

Hence, an ETH address is also the address used for tokens.
## Total token market capitalization

$73$ Billion total (there are hundreds)

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Platform</th>
<th>Market Cap</th>
<th>Price</th>
<th>Volume (24h)</th>
<th>Circulating Supply</th>
<th>Change (24h)</th>
<th>Price Graph (7d)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>🔧 EOS</td>
<td>Ethereum</td>
<td>$8,561,378,575</td>
<td>$14.29</td>
<td>$2,335,730,000</td>
<td>598,991,015</td>
<td>18.72%</td>
<td><img src="image1" alt="Price Graph" /></td>
</tr>
<tr>
<td>2</td>
<td>💰 TRON</td>
<td>Ethereum</td>
<td>$7,114,611,908</td>
<td>$0.108210</td>
<td>$714,507,000</td>
<td>65,748,192,476</td>
<td>-6.35%</td>
<td><img src="image2" alt="Price Graph" /></td>
</tr>
<tr>
<td>3</td>
<td>🎉 ICON</td>
<td>Ethereum</td>
<td>$3,750,234,008</td>
<td>$9.91</td>
<td>$122,727,000</td>
<td>378,545,005</td>
<td>3.23%</td>
<td><img src="image3" alt="Price Graph" /></td>
</tr>
<tr>
<td>4</td>
<td>☻ Binance Coin</td>
<td>Ethereum</td>
<td>$2,329,631,096</td>
<td>$23.53</td>
<td>$517,473,000</td>
<td>99,014,000</td>
<td>14.94%</td>
<td><img src="image4" alt="Price Graph" /></td>
</tr>
<tr>
<td>5</td>
<td>🤝 OmiseGO</td>
<td>Ethereum</td>
<td>$2,307,284,138</td>
<td>$22.61</td>
<td>$84,533,000</td>
<td>102,042,552</td>
<td>-0.80%</td>
<td><img src="image5" alt="Price Graph" /></td>
</tr>
</tbody>
</table>
Where do tokens trade?

Top tokens trade on large exchanges (approx. 50% of token market capitalization)

  E.g. Poloniex, Kraken

Second tier tokens trade on decentralized exchanges

  E.g. EtherDelta (Most popular contract in Ethereum)
## trading tokens on Etherdelta

<table>
<thead>
<tr>
<th></th>
<th>PnL (%)</th>
<th>PnL (ETH)</th>
<th>Bid-Ask (%)</th>
<th>Bid-Ask (ETH)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIBE(1)</td>
<td>-11.2%</td>
<td>-0.036</td>
<td>50%</td>
<td>0.0009-0.0015</td>
</tr>
<tr>
<td>VIBE(2)</td>
<td>-39.1%</td>
<td>-0.022</td>
<td>50%</td>
<td>0.0009-0.0015</td>
</tr>
<tr>
<td>SPANK</td>
<td>+ 6.13%</td>
<td>+0.013</td>
<td>18%</td>
<td>0.000375-0.00045</td>
</tr>
<tr>
<td>AION</td>
<td>-42.52%</td>
<td>-0.111</td>
<td>25%</td>
<td>0.006 - 0.0075</td>
</tr>
</tbody>
</table>

Total PnL: -0.156 ETH
SPANK—market depth on EtherDelta

Red - Buy

Green - Sell
AION—market depth on EtherDelta
VIBE—Market depth on EtherDelta
Example of a transaction

<table>
<thead>
<tr>
<th>Transaction Information</th>
<th>Tools &amp; Utilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transaction ID</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Addresses (sender &amp; receiver)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Time of transaction</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Block chain fee (gas cost)</strong></td>
<td></td>
</tr>
</tbody>
</table>

Function: trade(address token0, uint256 amount0, address token1, uint256 amount1, uint256 expires, uint256 nonce, address user, uint8 v, bytes32 r, bytes32 s, uint32 amount)
The total cost of transactions

Gas Cost = Gas Price * Gas Used by transaction

<table>
<thead>
<tr>
<th>Cryptocurrency</th>
<th>VIBE(1)</th>
<th>VIBE(2)</th>
<th>SPANK</th>
<th>AION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost (ETH)</td>
<td>0.008608</td>
<td>0.008906</td>
<td>0.015972</td>
<td>0.008572</td>
</tr>
</tbody>
</table>

Total mining cost: 0.042 ETH
PnL: -0.156

Conclusion: Main costs of buying and selling tokens involves crossing the bid-ask spread
Inefficient trading

It takes a long time to trade on EtherDelta, usually hours

Could not process market orders
Make our own token using Ethereum contract

1. Based on Ropsten Test Net---- a test network
2. Interacted with MetaMask test and Ethereum Wallet

avoids using real money and gas fee.
Make our own token

1. Write the code of token using common template
2. Publish and verify the source code on ropsten.etherscan.io
3. Share token address with group members to swap tokens
4. Add all tokens were created linked to our Ethereum Wallet
Create a Custom Token - ERC20 Tokens

```solidity
// ERC Token Standard #20 Interface

contract ERC20Interface {
    function totalSupply() public constant returns (uint);
    function balanceOf(address tokenOwner) public constant returns (uint balance);
    function allowance(address tokenOwner, address spender) public constant returns (uint remaining);
    function transfer(address to, uint tokens) public returns (bool success);
    function approve(address spender, uint tokens) public returns (bool success);
    function transferFrom(address from, address to, uint tokens) public returns (bool success);
    event Transfer(address indexed from, address indexed to, uint tokens);
    event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
}

string public constant name = "Token Name";
string public constant symbol = "SYM";
uint8 public constant decimals = 18; // 18 is the most common number of decimal places
```
The code for our Custom Token

how to create your own Token currency and to deploy it to the ethereum test network?

Our code:

https://gist.github.com/anonymous/8fee9900532350ed706f35ce8a5ac6d4

https://remix.ethereum.org/#optimize=false&version=soljson-v0.4.19+commit.c4cbbb05.js
Six tokens in Ethereum Wallet

To watch and interact with a contract already deployed on the blockchain, you need to know its address and the description of its interface in JSON format.

**CUSTOM CONTRACTS**

WATCH CONTRACT

**CUSTOM TOKENS**

Tokens are currencies and other fungibles built on the Ethereum platform. In order for accounts to watch for tokens and send them, you have to add their address to this list. You can create your own token by simply modifying this example of a custom token contract or learning more about Ethereum Tokens.

**WATCH TOKEN**
Token Address (Token ID)

Token Name

Token Symbol

Decimals

Total YY Token in this Account
Main Function of Token Contract

- `totalSupply()` returns the total number of tokens in circulation
- `balanceOf(...)` returns the number of tokens a given address owns
- `allowance(...)` returns the amount that user B is authorised to withdraw from user A’s account
- `transfer(...)` user A calls this to give user B some number of tokens
- `approve(...)` user A calls this to give user B authorization to take some number of A’s tokens
- `transferFrom(...)` user B calls this to take some number of A’s tokens, but only up to the approved amount
Token Swap Process

1. User A deposits his/her token into the Trade Swap Contract
2. User A creates an order in the Trade Swap Contract to exchange his/her token for another
3. User B deposits his/her token into the Trade Swap Contract
4. User B takes the order from User A knowing the address of A’s order
5. User A’s token is exchanged with User B’s token at the exchange rate in the contract.
Main functions of Swap Contract

function depositToken(...) deposit some token less than A’s approve to this swap contract

function withDrawToken(...) withdraw some number of token form this swap token to A’s token contract

function makeOrder(...) A publish a order in form of x number of a contract to y number of b contract for other users to take, and return a orderID

function takeOrder(...) B take an order from other users according to orderID

function cancelOrder(...) A cancel the order he/she has published according to orderID.