Blockchain and cryptocurrency

Workshop 1
Bitcoin wallet

- Bitaddress.org

Public and private key cryptography

Private Key → Elliptic Curve Multiplication (One-Way) → Public Key

Public Key → Hashing Function (One-Way) → Bitcoin Address
Exploring Bitcoin transactions

- https://live.blockcypher.com/btc/
- https://www.blockchain.com/explorer
- https://coinmarketcap.com/currencies/bitcoin/
Ethereum wallet

- https://www.myetherwallet.com/
- https://metamask.io/index.html
- https://enjin.io/wallet

Public and private key cryptography
Exploring Ethereum transactions

- https://live.blockcypher.com/eth
- https://coinmarketcap.com/currencies/ethereum/
Cryptocurrency exchanges

- Trade cryptocurrencies

[Logos of Binance, Kraken, Bittrex, Coinbase]
Crypto wallets

● Store public and private keys
● Send and receive cryptocurrency
● Track the cryptocurrency balance
● Wallet could be:
  ○ Paper wallet
  ○ Hardware wallet
  ○ Software wallet
Hot and cold wallets

- What is a *hot wallet*?
- What is a *cold wallet*?
- Are cryptocurrency wallets *secure* to use?

*Take 5 minutes and find answers of these questions*
Hot wallet

Hot wallet is like keeping a lot of cash in your pocket wallet and carry all the time with you.

In cryptocurrency world, hot wallet:

- Online and connected to internet
  - Instant trades (transactions)
  - Instant withdrawals
- Easy to use
- Cryptocurrency is less secure

Cryptocurrency exchanges are an example of hot wallet.
Cold wallet

● Not online or connected to internet
  ○ Completely offline
● Secure
● Not ideal for instant trades (transactions)

Paper and hardware wallets are an example of cold storage
ERC-20 token

- Ethereum platform based crypto tokens
  - Tradeable, spendable
- Standard for ERC-20 tokens
  - Token Name
  - Symbol
  - Decimal (up to 18)
  - `totalSupply`
  - `balanceOf`
  - `transfer`
  - `transferFrom`
  - `approve`
  - `allowance`
ERC-721 token

- Ethereum platform based tokens
  - Non-fungible tokens (NFTs)
    - Collectible digital assets
  - Tokenize ownership of any arbitrary data

- NFTs
  - Crypto Kitties
  - Sorare

- Resources
  - https://docs.alchemy.com/docs/how-to-develop-an-nft-smart-contract-erc721-with-alchemy
  - https://nft-generator.art
  - NFTs marketplace
    - https://opensea.io
Let’s create our own ERC-20 token

- Create an account on MetaMask
  - [https://metamask.io/index.html](https://metamask.io/index.html)

- Add Ether
  - [https://faucet.metamask.io/](https://faucet.metamask.io/)
  - [https://app.mycrypto.com/faucet](https://app.mycrypto.com/faucet)

- Create token using Token Mint
  - [https://tokenmint.net/](https://tokenmint.net/)
    - Goerli test network
Phases of launching an ICO

- Ideation phase
- Competitors analysis
- Legal side research
- Write a white paper
- Create ICO token
- Launch a website
- Marketing
Workshop tasks
Task 1

Explore Bitcoin blockchain and provide the following details.

<table>
<thead>
<tr>
<th>Current price in USD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Recent Block**

<table>
<thead>
<tr>
<th>Block height and time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transactions in recent block</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total BTC sent</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total fees paid</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Block size</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Merkle root of block</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Previous block hash</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Add screenshot of block details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

### Task 2

Explore Ethereum blockchain and provide the following details.

<table>
<thead>
<tr>
<th>Current price in USD</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recent Block</strong></td>
</tr>
<tr>
<td>Block height and time</td>
</tr>
<tr>
<td>Transactions in recent block</td>
</tr>
<tr>
<td>Total ETH sent</td>
</tr>
<tr>
<td>Total fees paid</td>
</tr>
<tr>
<td>Block size</td>
</tr>
<tr>
<td>Merkle root of block</td>
</tr>
<tr>
<td>Previous block hash</td>
</tr>
<tr>
<td>Add screenshot of block details</td>
</tr>
</tbody>
</table>
Task 3 - Ethereum wallet

Create Ethereum wallet using MetaMask:

- Go to https://metamask.io/index.html
- Install MetaMask Chrome extension
- Create MetaMask account
- Create Ethereum wallet

Provides the following details:

- Ethereum address
- Etherscan screenshot of your Ethereum address
  - https://etherscan.io/
Task 4 - Get Ether in MetaMask wallet

Get Ether in your Ropsten Test Network using MetaMask Ether wallet:

- Select Ropsten Test Network from MetaMask
- Go to https://faucet.metamask.io/ or
  - https://app.mycrypto.com/faucet
- Connect with Ropstren Test Network
- Click on “request 1 Ether from faucet” button
- Explore transaction hash

Provides the following details:

- From address where you received Ether
- Screenshot of transaction details page
Task 5 - Create ERC-20 token

Get Ether in your test Ropsten network using MetaMask Ether wallet:

- Go to [https://tokenmint.net](https://tokenmint.net)
- Connect with Goerli Test Network
- Request Ethers
- Explore transaction hash
- Provide token details and deploy contract

Provides the following details:

- Deployed **smart contract address**
- Screenshot of transaction details page
Workshop report submission

This assignment must be submitted individually as one PDF document via Course Website as BCT1_YourLastName.pdf

**Deadline:** Before the next lecture

Report that are handed in after the deadline 50% of the points will be deducted