Blockchain and cryptocurrency

Workshop 1
Bitcoin wallet

- Bitaddress.org
- https://walletgenerator.net/

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://live.blockcypher.com/btc/)
- [https://www.blockchain.com/explorer](https://www.blockchain.com/explorer)
- [https://coinmarketcap.com/currencies/bitcoin/](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://live.blockcypher.com/eth)
- [https://coinmarketcap.com/currencies/ethereum/](https://coinmarketcap.com/currencies/ethereum/)
Cryptocurrency exchanges

- Trade cryptocurrencies

[Logos of Binance, Bittrex, Kraken, and 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 15 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`
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/)
- Create token using Token Mint
  - [https://tokenmint.io/app/#/token](https://tokenmint.io/app/#/token)
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 and provide the following table

<table>
<thead>
<tr>
<th>Current price in USD</th>
<th>$11,335.74 USD</th>
</tr>
</thead>
</table>

**Recent Block**

<table>
<thead>
<tr>
<th>Block height and time</th>
<th>646,552, 2020-09-03 13:31</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions in recent block</td>
<td>1,664 Transactions</td>
</tr>
<tr>
<td>Total BTC sent</td>
<td>4,809.3745 BTC</td>
</tr>
<tr>
<td>Total fees paid</td>
<td>0.862 BTC</td>
</tr>
<tr>
<td>Block size</td>
<td></td>
</tr>
<tr>
<td>Merkle root of block</td>
<td></td>
</tr>
<tr>
<td>Previous block hash</td>
<td>000000000000000000000000dcee71742c6e735baf69c68fea90f12f9614ed481d240</td>
</tr>
</tbody>
</table>
### Task 2

- Explore Ethereum and provide the following table

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

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

- Select Ropsten Test Network from MetaMask
- Go to [https://faucet.metamask.io/](https://faucet.metamask.io/)
- Connect with Ropsten 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.io/app/#/token](https://tokenmint.io/app/#/token)
- 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
Workshop report submission

All assignments must be submitted individually as one 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
Presentation 1

● Work in groups
  ○ Team of 2-3 members

● Prepare slides to speak in the next class
  ○ 3-5 minutes presentation
Presentation 1

- Work in groups
  - Team of 2-3 members
- Prepare slides to speak in the next class
  - 2-3 minutes presentation

Focus on these two questions when preparing for the slides:

1. What is it? and
2. How it is related to the blockchain?
Topics

1. What is the Genesis block and coinbase transaction?
2. What are blockchain oracles and role within Blockchain-based applications?
3. What is the role of Blockchain in the healthcare domain?
4. What is the role of Blockchain in the supply chain?
5. What is solidity and what is solidity used for?
6. What is Corda and CorDapp?
7. What are the Defi coins? And the difference with ICOs?
8. Who is a Craig wright?
9. What was a DAO attack?
10. What was a silk road dark web and who was operating?
11. List some cryptocurrency/Bitcoin scams.
12. What is an EstCoin?
13. What is the Guardtime Blockchain project?