COMPUTING SUBJECT:	Blockchain with crypto currency
TYPE:	Mandatory project
IDENTIFICATION:	Blockchain
COPYRIGHT:	*Michael Claudius*
LEVEL:	High
TIME CONSUMPTION:	15-40 hours
EXTENT:	300 lines codes mainly auto-generated
OBJECTIVE:	Blockchain theory, application and implementation
PRECONDITIONS:	See special paper with useful links
COMMANDS:	

MANDATORY PROJECT: BLOCKCHAIN

The Mission

You are to gain knowledge on blockchain by setting up e.g. a smart contract and/or creating your own cryptocurrency utilizing the Ethereum tool. You shall do this in two steps/assignments:

1. Theoretical part, explaining the concepts of blockchain and bitcoin.
   This is an individual assignment, where the student upload his/her solution.
2. Practical part, install Ethereum and publish a token to a small group of participants.
   This can best be done in small groups.

As this topic is rather green and also new to you, the project is defined as an exploring project; meaning that a successful implementation of point 2 cannot be guaranteed, neither is it expected to be.

Purpose

The purpose of this project is to explore blockchain.

Useful links for blockchain

When surfing on the net it is easy to find many descriptions more or less useful, and in more or less updated versions. I have made a preliminary collection on the home page.

Hand in

It is important first to understand the theory, therefore the theoretical part, as .pdf file (3-5 pages), must be uploaded on Wiseflow not later than 16.00 5th April 2020. It is recommended to do as much as you can as early as possible, best before 26th March, so you and your mates can focus on the practical part afterwards.

The practical part as a .zip or .pdf file (depending on what you developed in your project) must be uploaded on Wiseflow not later than 16.00 5th April 2020.

The two parts are handed in together in one .zip file.

Theoretical part: Topics and questions

You can decide to follow the below mentioned points strictly answering one by one or to make report covering the topics.

Blockchain
Give a short general definition and description of blockchain network.
State the organisation of nodes.

Transactions
What is a transaction?
What is the content of a transaction?
How is hashing combined with digital signatures?

Block
What is a block?
What is the content of a block?
How are public/private keys used for digital signatures?
How is hashing used?'
How are blocks ordered in blockchain?

What is a Merkle tree?
Why is it used in the block to hold transactions?

Timestamping
What is idea of a a timestamp server ?
Notice the original ideas of Sato (E-coins) was changed somewhat later.
What is a blockchain timestamp?
For what and how is it used?

Proof of work
What is proof of work?
Describe the proof of work in blockchain.

The processing
What happens in the P2P when a new transaction is announced?
What happens if a node at the same time receives two or more different versions of the next block;

Double spending
What is the double spending problem?
How is it solved in blockchain?

Mining and miners
What is a miner?
Describer the purpose and work of a miner.
What happens if two miners simultaneously broadcast a new block to the blockchain?
How are miners rewarded?

Risks

What is the risk if honest nodes hold less than 50% of the CPU-power and a hostile attacker holds 50%+ CPU power?
How can the speed of mining challenge the 10 minutes' delay.
How to defend this risk?

Practical Part: Ethereum/fake e-coins

A. First you investigate Ethereum
What is Ethereum?
What are the differences between Bitcoin and Ethereum.

B. Second you are to create your own e-coin and do some transactions.
Create your own e-coin.
Make a wallet.
Create a transaction to yourself or to some friends

I can recommend a fast introduction to create token and later use it on Ropsten or Rinkeby test network.
https://medium.com/bitfwd/how-to-issue-your-own-token-on-ethereum-in-less-than-20-minutes-ac1f8f022793

https://ropsten.etherscan.io/

https://rinkeby.etherscan.io/

Prove the abovementioned points by giving a set of screen dumbs and add your comments/experiences on the way.
And/or by attaching some code examples.

If your group has good time if can make further investigations; e.g.

A interesting possibility is implementing blockchain in Javascript
https://www.youtube.com/watch?v=zVqczFZr124

Another interesting possibility is implementing blockchain in C#
https://www.c-sharpcorner.com/article/blockchain-basics-building-a-blockchain-in-net-core/

Some people might want to work directly with Ethereum, I don't recommend that !