

## **DAT 510: Assignment 3**

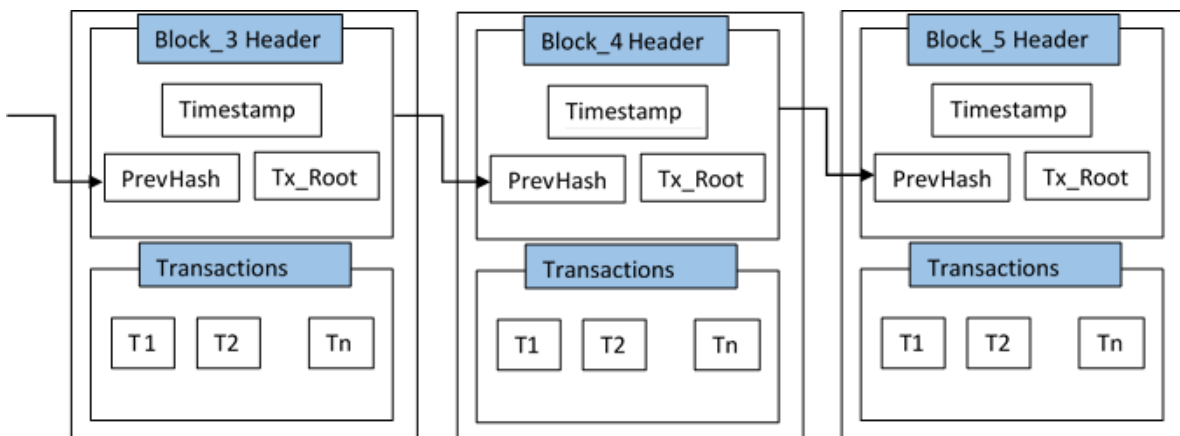
Submission Deadline: 23:59 Monday, Nov. 4, 2019

## Part 1 (50%)

### Simplified Blockchain

In this part you will implement a simplified Blockchain (40%). Each block should contain the following components

- Hash of transaction/s (follow Merkle tree)
- Previous block hash
- Transaction/s
- Timestamp



- Tx\_Root or Mekanle root: represents the hash value of all the transactions in the block.
- Prev\_Hash: represent the hash value of the previous block header.
- Timestamp : represents the time when a block was created.
- Transactions: All the transactions in the block. It can be 1 or more. If more than 1 it should follow the property of merkle root\*

Your program should be able to:

- Input transaction/s for a block.
- Create the block and display the entire block, which include the previous block header hash. Also display the hash of that block header.
- Must be able to repeat the above steps.
- Finally should display all the blocks added in the blockchain.
- For the first block you can hardcode the block and the values.

Breifly explain the features that you used to implement your simplified blockchain in the report. (10%)

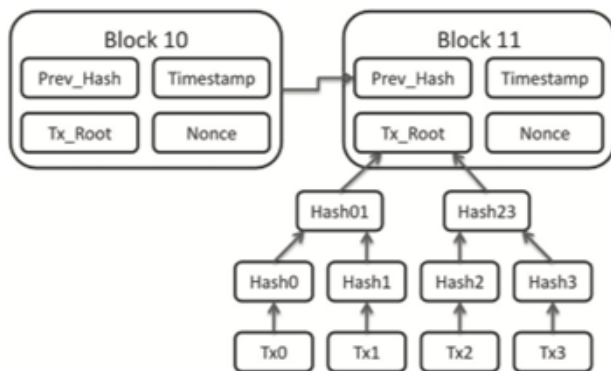
## Part 2 (50%)

Write a detailed report on the below given topics:

- Blockchain and Types of Blockchain (20%)
- Role of Digital signature in Blockchain Architecture(10%)
- Consensus Algorithm in Blockchain. Briefly explain PoW and PoS (20%)

Extra details:

- \*Part1: Merkle root: in the below fig Tx\_Root



# Assignment Submission

**Deadline:** 23:59, Monday, Nov. 4 2019 (submit your assignment through canvas)

## Final submission:

### 1. Source Code

- Source code submitted for the assignment should be your own code. If you have used sources from the internet everything should be added to the references. If you used someone's code without reference, that will also be treated as plagiarism.
- Source code should be single, compressed directory in .tar.gz or .zip format.
- Directory should contain a file called README that describes the contents of the directory and any special instructions needed to run your programs (i.e. if it requires and packages, commands to install the package. describe any command-line arguments with the required parameters).
- You may use any reasonable programming language for part one of the assignment. Reasonable languages include: Java, C, C++, Python, MatLab, R and others with permission of Racin Gudmestad or Dhanya Therese Jose (Email: [dhanya.t.jose@uis.no](mailto:dhanya.t.jose@uis.no) )
- You should **NOT** use available libraries/packages/classes for implementing the core functionality of the assignment.

### 2. A **separate** report with PDF format

- Texts in the report should be readable by human, and recognizable by machine;
- Other formats will **NOT** be opened, read, and will be considered missing;
- Report should follow the formal report style guide in next page.
- Each student should write an individual report. Each report will be checked for plagiarism. If it is copied from some where else, you will fail the assignment.

NOTE: If you encounter problem with upload archive file (e.g. \*.zip, \*.tar) to the website <https://uis.instructure.com/>, you should be able to upload after you add extension .txt to your archive file (e.g., \*.tar  $\Rightarrow$  \*.tar.txt).

**Note:** The assignment is individual and can **NOT** be solved in groups.

# Project Title

## Abstract

A one-paragraph summary of the entire assignment - your choices of cryptographic primitives and their parameters, procedure, test results, and analysis.

## Introduction

A description of the scientific background for your project, including previous work that your project builds on. (Remember to cite your sources!) The final sentence (analogous to the thesis statement in a term paper) is the objective of your experiment.

## Part1:

## Design and Implementation

A detailed description (in paragraph format) of the design, procedure, and implementation of your project. This should be the main part of the report.

## Test Results

Results of testing the software, as you observed/recorded them. Note that this section is only for observations you make during testing. Your analysis belongs in the Discussion section.

## Part2:

Write a detailed report on given topics

## Discussion

Your analysis of what your testing results mean, and your analysis.

## Conclusion

A short paragraph that restates the objective from your introduction and relates it to your results and discussion, and describes any future improvements that you would recommend.

Works Cited A bibliography of all of the sources you got information from in your report.