German University in Cairo
Faculty of MET (CSEN 1001 Computer and Network Security Course)
Dr. Amr El Mougy

Project Description

Deadline: 11:59pm Monday 23 of April

Guidelines

This project should be done in groups of maximum 4 students. You can share ideas, consult the TA, and search online. **However, all work done in this project must be done by the team members and the team members only**.

All team members should work on this project equally and no work should be done by anyone outside the team. Evaluations **will** be conducted at the end in order to verify that.

The main aim of this project is to test your knowledge of the security concepts taught in this course.

Please Register your team **here**.

All external assets used from the internet must be credited in the credits section of your report.

Any plagiarism detected will be penalized with a zero.

Administrative

- Team submission should be no later than **Sunday, March 4th, 2018.**
- Final submission due to **Monday, April 23rd, 2018** via MET Website.
- Teams of minimum 2 members and maximum 4 members are allowed.
- Grading:
  - Report: 20%.
  - Secure implementation of features: 80%.
  - 5% percent bonus is awarded if substantial work is shown.

German University in Cairo
Faculty of MET (CSEN 1001 Computer and Network Security Course)
Dr. Amr El Mougy

Description

What is the main Idea?

In this project, we will design a cryptocurrency similar to BitCoin. We will simulate a multi-user network, once a transaction is made, the user announces it to his near peers. Not all users get notified by the transaction, you can randomize the notification process. Once the user accumulate **n** transaction, he can form a block by accumulating transactions and doing a computationally expensive task (e.g. finding a nonce that hasn't be used in the ledger before) and append this nonce to the block. Once the block is formed, it can now be announced. After a block announcement, users who are notified about this block, will add it to their version of the ledger and the majority of them have to consent that this version of the ledger is the same version they have. Users with different version than this version will have to throw away their versions and adopt this one.

Deliverables

- ❖ A transaction will be treated as a black box with a transaction ID.
- ❖ A simulation of the network, with multiple users and the randomized process of announcing a transaction, making each transaction reach an arbitrary set of users.
- ❖ The design and implementation of the ledger based on the concept of the blockchain (hash linked list)
- ❖ The puzzle needed to announce the block, you can find a computationally expensive task that's used in famous blockchains and apply it in your system.
- ❖ The process of building a block out of a set of transactions, a hash to the preceding block and a nonce generated by the computationally expensive task.
- ❖ The process of announcing the block to an arbitrary set of users.
- ❖ Having the users consent that once they received the announced block, their ledger (blockchain) align with that of the other users. And having users with different versions of the ledger adopt the consented version instead.

Milestones

- **Milestone 1:**
  - Deliver the simulated network along with the transaction announcing process. As well as, a mechanism for announcing blocks. (i.e. announcing the blocks has to be considered when building the ledger and the simulated network).
  - Deadline: **April 2nd, 2018.**
- **Milestone 2:**
  - Deliver the remaining deliverables.
  - Deadline: **April 23rd, 2018.**