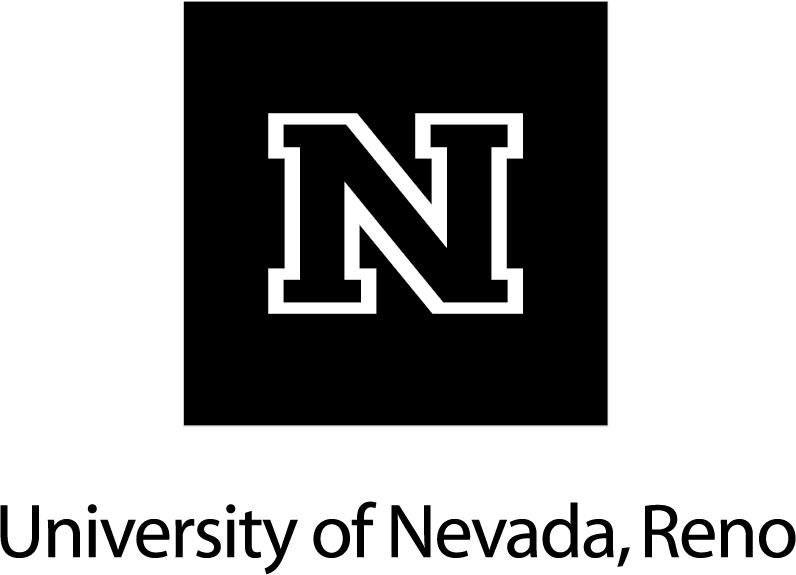
**Department of Computer Science and Engineering**

**University of Nevada, Reno**



Course No.: **CS 705**

Course Name: **Cryptography and Blockchain**

Assignment No.: **1**

Assignment Name: **Bitcoin**

Date of Submission: **April 16, 2020**

Student Name: **Farhan Sadique**

NSHE ID: **8001062452**

**Part 1: Answer the following questions: 5pt (1+1+1+2)**

Please read the bitcoin white paper <https://bitcoin.org/bitcoin.pdf> and respond to the following questions:

1. Double Spending: Please explain how Bitcoin addressed double spending.

**Answer:** Bitcoin addresses double-spending by keeping a public record of all transactions using a peer-to-peer (P2P) network. Bitcoin ensures that records cannot be modified by an attacker using proof-of-work (PoW) that quickly becomes computationally impractical for the attacker to change if honest nodes control a majority of CPU power.

1. Proof of Work (Mining): In your own words please explain how Bitcoin deters denial of service attacks or other service abusers.

**Answer:** Since bitcoin runs on a peer-to-peer distributed network, it is really difficult to take the network down using denial-of-service (DoS) attacks. Because to take down the bitcoin network, a malicious party must take down every single miner node. For a traditional network, the attacker must attack only one server or one gateway which is easier to do than attacking thousands of miners with varying network capacity.

However, network DoS is not the only type of DoS attack on bitcoin network. Malicious users can slow down the network by posting a lot of small transactions (e.g. 1 cent) on the block. Since, bitcoin only allows 1 block to be mined every 10 minutes, this can deny legitimate users to complete their transactions.

This second type of DoS attacks take care of themselves, because of the transaction fees of each transaction. The attacker will continuously lose his/her bitcoin as transaction fees because of making a lot of small transactions. As a result, he/she will eventually be left with no bitcoin to transact bringing an end to the DoS attack.

1. Incentives: How does Bitcoin incentivize nodes to mine on the network? What are some other effects of these incentives (positive, negative, neutral)?

**Answer:** Bitcoin provides two types of incentives: transaction fee and mining reward. The mining reward is the first transaction of each block and is offered as a reward for mining a block. This is done to attract miners initially. However, there is only a limited number of coins to be mined (21 million for bitcoin), and after that the incentives are provided by transaction fees only.

These incentives encourage miners to stay honest, because stealing bitcoins require a lot of CPU power to show PoW for all earlier blocks again. Rather than doing that, a node is better off mining bitcoins honestly using the same CPU power. Also, as he acquires more coins, he is more likely to use his CPU power to protect the system rather than undermine it.

One of the negative effects of providing mining rewards is a lot of people are investing their CPU power just to mine blocks. This is essentially a waste of electricity and CPU power. Moreover, mining groups with large CPU power can perform hash attacks on the bitcoin block chain if they suddenly stop mining when the PoW burden is high.

1. Competing Chains: If there are two blockchains with divergent histories, which blockchain does Bitcoin protocol tell miners to mine on?

**Answer:** Miners will mine on the longer chain which essentially has more proof of work (PoW). This ensures that so long as honest nodes control more than 50% of the total mining power, the network remains stable.

This is the same reason for which bitcoin does not allow miners to use their mining rewards until their mined block is buried under at least 100 newer blocks. However, bitcoin design is conservative because, there is less than 1% probability of getting two divergent chains with 7 blocks or more in each.

**Part 2: Develop and write a report: 25pt (5+1+2+4+2+1+5+2+3)**

Please review the python source codes from lecture 2 (Building smallest blockchain.txt) and lecture 3 (PoW-2.txt). The first application shows a chain of blocks, but it does not provide any proof of work. Second code shows how to build a simple proof of work, but it does not show any block chain. Using the knowledge of these two codes please build a simple local blockchain application where there will be 3-4 users (Alice, Bob, Charlie,….). They will exchange some values (like currency) to each other. Then these transactions will be gathered and stored in the blockchain. Before storing, the miners should validate the transactions and perform proof of work to create the block and store it in the chain. You can have as much as features in your application as you wish but not less than the below:

1. Make use of merkle tree to store the transaction hash. **5**
2. Predefined transaction pools between the users.**1**
3. You need be able to demonstrate creating genesis block and then adding following blocks in the chain. **2**
4. Demonstrate that miners are solving PoW puzzle and one get selected who solves it first. **4**
5. Demonstrate and explain how integrity and verifiability are ensured. **2**
6. The block should contain atleast the Hash=H(root hash of merkle tree, prev hash, nonce, timestamp) **1**
7. Also please make sure:
   1. Clear and all step by step explanation **5**
   2. Showing the full blockchain in output as well as in report. **2**
8. Explain the benefits of using merkle tree in this context. What would happen if you would not use the merkle tree to store all the transactions’ hash? **3**

You can use any platform to build this application.

***Prepare a report (like the Ethereum application manuals) and explain each and every possible function, provide screen shot of your code and output.***

***Please submit all answers in one pdf. This assignment carries 30 marks but later your marks will be converted to out of 10.***