CS381 Exercise 20

Name: Zhang Yupeng

Student ID: 5130309468

1. Is Bitcoin anonymous?

Solution:

Bitcoin is not anonymous. Some effort is required to protect your privacy with Bitcoin. All Bitcoin transactions are stored publicly and permanently on the network, which means anyone can see the balance and transactions of any Bitcoin address. However, the identity of the user behind an address remains unknown until information is revealed during a purchase or in other circumstances. This is one reason why Bitcoin addresses should only be used once. Always remember that it is your responsibility to adopt good practices in order to protect your privacy.

2. What is the purpose of mining?

Solution:

Mining is a distributed consensus system that is used to confirm waiting transactions by including them in the block chain. It enforces a chronological order in the block chain, protects the neutrality of the network, and allows different computers to agree on the state of the system. To be confirmed, transactions must be packed in a block that fits very strict cryptographic rules that will be verified by the network. These rules prevent previous blocks from being modified because doing so would invalidate all following blocks. Mining also creates the equivalent of a competitive lottery that prevents any individual from easily adding new blocks consecutively in the block chain. This way, no individuals can control what is included in the block chain or replace parts of the block chain to roll back their own spends.