Lab #5

CSCI 345  
By: Brandi Durham, Andrew Miller

Part 1.)

2A.) The steps needed for bitcoin to be spendable are as follows:  
 1.) A transaction is broadcast to every node in the network.

2.) Miners consolidate transactions and append to the current block.

3.) Mining nodes in a network find a hash that validates the current block.

4.) Nonce solution is broadcast to the network

5.) Once transaction has been verified by a few nodes (usually 6) the bitcoin from the original transaction is marked as spendable.

2B.) During the process of broadcasting and verifying transactions, often multiple solutions are found. This is also known as a fork. Consensus is reached because miners, which are tasked with verifying the transactions, are incentivised to mine based on the longest series of continuous nodes from the genesis node.

Part 2.)

2A.) Denial of Service Attack: To do an denial of service attack the hacker floods the Bitcoin servers with more traffic than they can handle. The attacker will send lots of data to one node, which could make it so busy that it cannot process other Bitcoin transactions. There are multiple tools the hacker could use to perform an DoS attack, such as MyDoom or Stacheldraht. There are different tools depending on how the hacker wants to implement the attack. If they want to have the user not know you are using their computer, the tool could be in malware on their computers that launches without the users knowledge, MyDoom. Or Stacheldraht which takes control of compromised systems to implement the attack. The hacker uses client programs to connect to the compromised systems. This type of attack has already been used against different parts of Bitcoins blockchain, such as Bitcoin Gold.

2B.) SHA-256 (A part of the SHA-2 family) and the Elliptic Curve Digital Signature Algorithm are used extensively throughout the bitcoin network and are considered very strong against brute force attack. In fact with current computational power and barring any undiscovered vulnerabilities it would take longer than the expected lifetime of the universe to break bitcoin’s cryptography. But like any technology imperfections are bound to exist, the bitcoin protocol was written in a somewhat modular way to allow for the upgrade to a more secure algorithm. Reflecting on this, the bitcoin protocol is not the weak link in the chain of transactions other side-channel, phishing, or bitcoin exchange hacks are far more likely to influence this technology in the future.

3.) Another use of blockchain technology is that of: A distributed asset ledger. This idea is that real world assets could be tracked by private numbers (keys) and the blockchain could act as a ledger to log history, verify ownership, and maintain transaction integrity. These assets could include real-estate, or physical assets such as laptops and workstations. This technology is already being tested in a pilot run by large organizations such as the: US Department of the Treasury, tracking high value laptops and other computer equipment that changes ownership on a daily basis. One advantage of such a system, is that assets could transfer to a new owner in almost instantaneously. Many banks are in the process of integrating a similar technology for more traditional asset tracking \*that is\* the use of blockchain technology to verify the integrity of monetary assets ownership and transactions. The implications of a distributed ledger technology on the banking infrastructure is revolutionary, as many systems of asset tracking exist but much of the banking infrastructure is aging, and blockchain technology could potentially prepare it for a more modern transaction paradigm. While such a technology is promising it could still potentially be vulnerable to similar attacks to bitcoin’s blockchain network, DOS attacks, Theft of Private keys on unencrypted devices/networks.

