Lab 5
Applying these crypto staff - bitcoin

Goals:

1. Study how crypto-currency works.
2. Learn how to use GENI to run a computer network experiment.
3. Apply cryptography knowledge in a real-life scenario, such as bitcoin.

Preliminary Information:

- Watch the following video: https://spectrum.ieee.org/video/computing/networks/video-the-bitcoin-blockchain-explained
- Read this article carefully: https://spectrum.ieee.org/computing/networks/blockchains-how-they-work-and-why-theyll-change-the-world

Part 1: GENI Lab

1. Complete the following GENI lab: https://witestlab.poly.edu/blog/get-rich-on-fake-bitcoins/
2. Write a report answering the following questions:
   a. Describe the exact steps that were needed before the Bitcoin transaction in the experiment was spendable.
   b. How did the block chain reach consensus? Describe the steps in detail and give node numbers if needed.
   You may include screenshots from your experiments.

Part 2: Bitcoin Vulnerabilities & Applications:

1. Browse through the bitcoin vulnerabilities: https://en.bitcoin.it/wiki/Weaknesses
2. Write a report (minimum 300 words) that answers the following questions:
   a. Pick a vulnerability from the: “Might be a problem” category. Can you give an example (Proof of Concept, PoC) how one would implement the vulnerability that you picked from this category? Use technical details, what tools or techniques would you apply.
   b. “Probably not a problem” category: From this category read about the weakness: “Breaking the cryptography”. Comment on this based on your knowledge in cryptography. Do you agree or disagree that this is probably not a problem?
3. Find (or think) an application of the block chain other than cryptocurrency. Write a paragraph (minimum 300 words) about this application. Include any sources that you may have used with IEEE reference style.

Sources:

- If you want to learn a lot of technical details about bitcoin, there is a good book and lectures by Princeton professors in this page: http://bitcoinbook.cs.princeton.edu/
• Developers documentation: [https://bitcoin.org/en/bitcoin-for-developers](https://bitcoin.org/en/bitcoin-for-developers)