UC-278 Cyber Security in Blockchain

INTRO/ABSTRACT

Blockchain is a growing technology that utilizes a decentralized record of transactions for currencies, financials, healthcare, supply chains, etc. Although a robust system, it is not impenetrable as this project will explain and demonstrate many of the shortcomings of blockchain and provide solutions to these weaknesses. The attacks demonstrated are as follows: Transaction Order Dependence, Denial of Service, Replay Attacks, Writing of Arbitrary Storage, Weak Randomness, and Honeypot Attack.

METHODS

Technology and Resources used are as follows:

- **Google Site**
  - Hosts our research, instructions, and modules
- **Remix IDE**
  - Used for developing code and deploying smart contracts
  - Uses the **Solidity** language for building contracts on the blockchain
- **GitHub**
  - Houses our code available to view and download
  - Version Control
- **Test Networks/Accounts**
  - Using **Ganache Truffle Suite** to generate test network with accounts
  - Using **MetaMask** with Goerli Test Network

RESULTS

The results are very optimistic for future work in blockchain. Five of the six modules have coded solutions presented that are efficient and viable. One of the six has no codable solution as of now, however has many alternative protections as well as beneficial advice. Further research could be in implementing these solutions in practical applications such as live contracts.

We researched, designed, and developed six modules to showcase blockchain attacks and robust solutions to prevent these attacks.

QR Code to our website. If you would like to see the project, background information, our research, results and its demonstration modules check it out!

KENNESAW STATE UNIVERSITY
COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING

Memebers: Eric Cooper, Alex Fortson, Eric Weese
Owner: Dr. Yong Shi Advisor: Sharon Perry