NATIONAL INSTITUTE OF TECHNOLOGY TIRUCHIRAPPALLI – 620 015

TITLE : Analysis of Smart Contract vulnerability and extension of Oyente Tool.

KEYWORDS : Smart Contract, Ethereum, Oyente, Cryptocurrency, Vulnerabilities.

TEAM MEMBERS

- AYUSH SHARMA(106117018)
- MAYANK GARG(106117048)

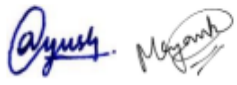
PROJECT GUIDE : Dr. KUNWAR SINGH

PROJECT ABSTRACT : Oyente follows a modular design. It consists of four main components, namely CFGBuilder, Explorer, CoreAnalysis, and Validator. CFGBuilder constructs a Control Flow Graph of the contract, where nodes are basic execution blocks, and edges represent execution jumps between the blocks. Explorer is the main module that symbolically executes the contract. The output of Explorer is then fed to the CoreAnalysis. Finally, Validator filters out some false positives before reporting to the users. The old Oyente tool was able to detect the following 7 vulnerabilities :

• Integer Overflow
• Integer Underflow
• Call Stack depth attack
• Transaction ordering Dependence
• Timestamp Dependence
• Re-entrancy vulnerability
• Parity Multisig Bug

We have found 2 new vulnerabilities and have added them to the Oyente tool. And we have also improved an existing vulnerability Transaction Ordering Dependence. So now our Oyente tool is more efficient in detecting any possible attacks in future and warn us in advance. The newly added features to Oyente tool are:

• Contract Referencing
• TX_Origin
• Efficient Transaction Ordering Dependence



Signature of Student

Signature of Guide