DECLARATION

KRISHNAM CHATURVEDI, bearing USN **1EW17IS048** student of VIII semester B.E, in the Department of Information Science Engineering, East West Institute of Technology, Bangalore hereby declare that the Technical Seminar entitled “BLOCKEYE: Hunting for Defi Attacks On Blockchain” has been carried out by us under supervision of **Mrs. Anjana H S,** Asst. Prof Department of ISE, EWIT submitted in fulfilment of the course requirement for the award of the degree of bachelor of engineering in Information Science and Engineering of Visvesvaraya Technological University, Belagavi during the academic year 2020-2021. We further undertake that the matter embodies in the report has not been submitted previously for the award of any degree by us to any institution.

Krishnam Chaturvedi(1EW17IS048)

ABSTRACT

Decentralized finance, i.e., DeFi, has become the most popular type of application on many public blockchains (e.g., Ethereum) in recent years. Compared to the traditional finance, DeFi allows customers to flexibly participate in diverse blockchain financial services (e.g., lending, borrowing, collateral izing, exchanging etc.) via smart contracts at a relatively low cost of trust. However, the open nature of DeFi inevitably introduces a large attack surface, which is a severe threat to the security of participants' funds. In this paper, we proposed BLOCKEYE, a real-time attack detection system for DeFi projects on the Ethereum blockchain. Key capabilities provided by BLOCKEYE are twofold: (1) Potentially vulnerable DeFi projects are identified based on an automatic security analysis process, which performs symbolic reasoning on the data flow of important service states, e.g., asset price, and checks whether they can be externally manipulated. (2) Then, a transaction monitor is installed off chain for a vulnerable DeFi project. Transactions sent not only to that project but other associated projects as well are collected for further security analysis. A potential attack is flagged if a violation is detected on a critical invariant configured in BLOCKEYE, e.g., Benefit is achieved within a very short time and way much bigger than the cost. We applied BLOCKEYE in several popular DeFi projects and managed to discover potential security attacks that are unreported before

ACKNOWLEDGEMENT

Any achievement, be it scholastic or otherwise does not depend solely on the individual efforts but on the guidance, encouragement and cooperation of intellectuals, elders and friends. A number of personalities, in their own capacities have helped me in carrying out this project work. We would like to take this opportunity to thank them all.

First and foremost, we would like to thank **Dr. K Channakeshavalu**, Principal, EWIT, Bangalore, for his moral support towards completing our project work.

We would like to thank, **Dr. Suresh M B,** Professor and Head of Department of ISE, EWIT, Bangalore, for his valuable suggestions and expert advice.

We deeply express our sincere gratitude to our guide **Mrs. Anjana H S,** Asst. Prof Department of ISE, EWIT, Bangalore for her able guidance throughout the technical seminar and guiding us to organize the report in a systematic manner.

We thank my Parents, and all the faculty members of Department of Information science & Engineering for their constant support and encouragement.

Last, but not the least, we would like to thank our peers and friends who provided us with valuable suggestions to improve our seminar.

KRISHNAM CHATURVEDI (1EW17IS048)

TABLE OF CONTENTS

1. INTRODUCTION……………………………………………………………,…..01

2. What is DEFI?.......................…………………..…………………………..………03

2.1 DEFI Building Blocks,,………………………………………………………..…03

3. PROPOSED SYSTEM …….…………………;…………………………………...05

3.1 Functionalities.……………………………………………………………….…05

4. LITERATURE SURVEY……………..……..……………………………………..07

5. ATTACK DETECTION FOR DEFI….……….…………………………………...10

5.1 Overview……..…………………………...……………………………………..10

5.2 Oracle Analysis…………………………..……………………………………..10

5.3 AUTOMATIC ATTACK MONITORING…………………………………..„11

6. INCENTIVE STRUCTURES AND GOVERNANCE…………..……………….....12

7. SECURITY PROBLEMS IN DEFI PROJECTS………..……………………......14

7.1 The Blockeye Solution……..……………………………...….……….………..14

8. DEFI SERVICE CATEGORIES……………………………...………………...15

8.1 Uniswap and Sushiswap…….……………………….…………………….………..16

9. CHARACTERISTICS OF DEFI…………………………………………………...17

10. DEFI PROTOCOLS………………………………………………………….…..19

11. DEFI PRIMITIVES………………………………………………………….…...23

12.WHAT ARE FLASH LOANS?...,,................26

13.TECHNICAL SECURITY…………………………………………………………27

14.PRELIMINARY EVALUATION…………………………………………………..29

15. DEFI: USE CASE AAVE…………………………………………………………...31

16.OPEN RESEARCH CHALLENGES……………………………………………....33

17. DATA AVAILABILITY STATEMENT…………………………………………35

18.THE FUTURE OF DEFI……………………………………………………..36

CONCLUSION……………………………………………………………..38

REFERENCES……………………………………………………………..39

LIST OF FIGURES

Figure No	Title	Page no
3.1	The general architecture of BLOCKEYE	05
3.2	The input interface for BLOCKEYE.	06
5.1	The general workflow of BLOCKEYE	11
6.1	DeFi classification flowchart	13
10.1	A conceptual overview of the different constructs within the DeFi ecosystem.	19
13.1	The output interface for BLOCKEYE	29
17.1	Attack on the bZx project	35