SCTR's Pune Institute of Computer Technology
Dhankawadi, Pune

A PROJECT REPORT ON
"E-Voting System"

SUBMITTED BY
41141 Kalme Akash Namdev
41124 Dhawale Harsh Vijay

Under the guidance of
Prof. S. W. Jadhav

DEPARTMENT OF COMPUTER ENGINEERING
Academic Year 2023-24

DEPARTMENT OF COMPUTER ENGINEERING

SCTR's Pune Institute of Computer Technology
Dhankawadi, Pune, Maharashtra 411043

CERTIFICATE

This is to certify that the SPPU Curriculum-based Mini Project titled 'E-Voting System based on Blockchain Technology'

Submitted by

41141 Akash Kalme
41124 Harsh Dhawale

has satisfactorily completed the curriculum-based Mini Project under the guidance of Prof. S. W. Jadhav towards the partial fulfillment of the final year of Computer Engineering Semester VII, Academic Year 2023-24 of Savitribai Phule Pune University.

Date:

Place: PUNE **Name & Sign of Project Guide:**

Acknowledgment

It gives me great pleasure to present the mini project on - Build a machine learning model that predicts the type of people who survived the Titanic shipwreck using passenger data (i.e. name, age, gender, socio-economic class, etc.).

First of all, I would like to take this opportunity to thank my guide Prof. S. W. Jadhav for giving me all the help and guidance needed. I am grateful for his kind support and valuable suggestions that proved to be beneficial in the overall completion of this project.

I am thankful to our Head of the Computer Engineering Department, Dr. G. V. Kale, for her indispensable support and suggestions throughout the internship work. I would also genuinely like to express my gratitude to the CC, Prof. Samadhan Jadhav, for his constant guidance.

Finally, I would again like to thank my mentor, Prof. S. W. Jadhav for his constant help and support during the overall process.

❖ Title

E-Voting System based on Blockchain Technology.

❖ Problem Statement

Develop a Blockchain based application dApp (de-centralized app) or Solidity Program for e-voting system.

❖ Objectives

The primary objective of this report is to identify, analyze, and provide recommendations for addressing the vulnerabilities present in the "Ballot" smart contract. These vulnerabilities are associated with the contract's voting and delegation processes. The overarching goal is to enhance the security, integrity, and fairness of the voting system facilitated by the contract. Specific objectives include:

- Identify and describe the security vulnerabilities in the "Ballot" smart contract.
- Evaluate the implications of these vulnerabilities on the contract's functionality and potential misuse.
- Provide clear and actionable recommendations for mitigating these vulnerabilities and improving the contract's security.
- Ensure that the voting system operates as intended, preventing unauthorized multiple voting, and maintaining transparent and reliable outcomes.

❖ Introduction

Smart contracts, powered by blockchain technology, have gained immense popularity for their potential to create decentralized applications and automated processes. One common application of smart contracts is creating voting systems that can ensure transparency, security, and fairness in various decision-making processes. This report focuses on a specific smart contract named "Ballot," which is designed to facilitate a voting process with delegation capabilities.

The "Ballot" smart contract in question exhibits a vulnerability that allows any user to vote multiple times without proper restrictions or checks. This security flaw undermines the integrity of the voting process and can lead to manipulative or malicious voting behavior. The key issues and concerns are as follows:

a. Unrestricted Voting: The current implementation of the "Ballot" contract does not enforce proper restrictions on voting. As a result, users can cast multiple votes, potentially skewing the voting outcome and undermining the democratic process.

b. Lack of Identity Verification: The contract does not incorporate identity verification mechanisms to ensure that each voter can vote only once. In a real-world scenario, voters should be uniquely identified and restricted to a single vote.

c. Lack of Authentication: The contract lacks proper authentication mechanisms

for voters, allowing anyone to impersonate another user and vote on their behalf.

d. Potential Double Voting: The contract does not maintain a proper record of voters who have already cast their votes. This omission makes it possible for a user to repeatedly vote for different proposals or delegate votes to other addresses.

e. Chain of Delegation: While the contract attempts to prevent looped delegation, it does not consider other potential complexities, such as the possibility of cycles forming within the delegation chain.

f. Lack of Access Control: The contract does not differentiate between the chairperson, who has special privileges, and regular voters. As a result, the chairperson's actions are not clearly distinct from those of regular voters, which could lead to confusion and misuse.

❖ Scope

The scope of this report is focused on the security vulnerabilities within the "Ballot" smart contract. It encompasses the following key areas:

- Voting Process Security: The report will examine the contract's voting process to identify vulnerabilities that allow users to vote multiple times, impersonate others, or manipulate the vote count. It will propose solutions to address these issues and ensure that each voter can cast only one vote.

- Delegation Mechanism Security: The contract's delegation feature will be scrutinized for potential vulnerabilities that may permit improper delegation, including looped delegation. The report will offer recommendations to enhance the delegation process's integrity and fairness.

- Authentication and Access Control: It will assess the contract's authentication mechanisms and access control to determine if unauthorized users can take actions reserved for the chairperson. Solutions to clearly differentiate between chairperson privileges and regular voter actions will be proposed.

- Algorithmic Enhancements: The report will evaluate the contract's algorithms for determining winning proposals and ensure that the process is accurate and secure.

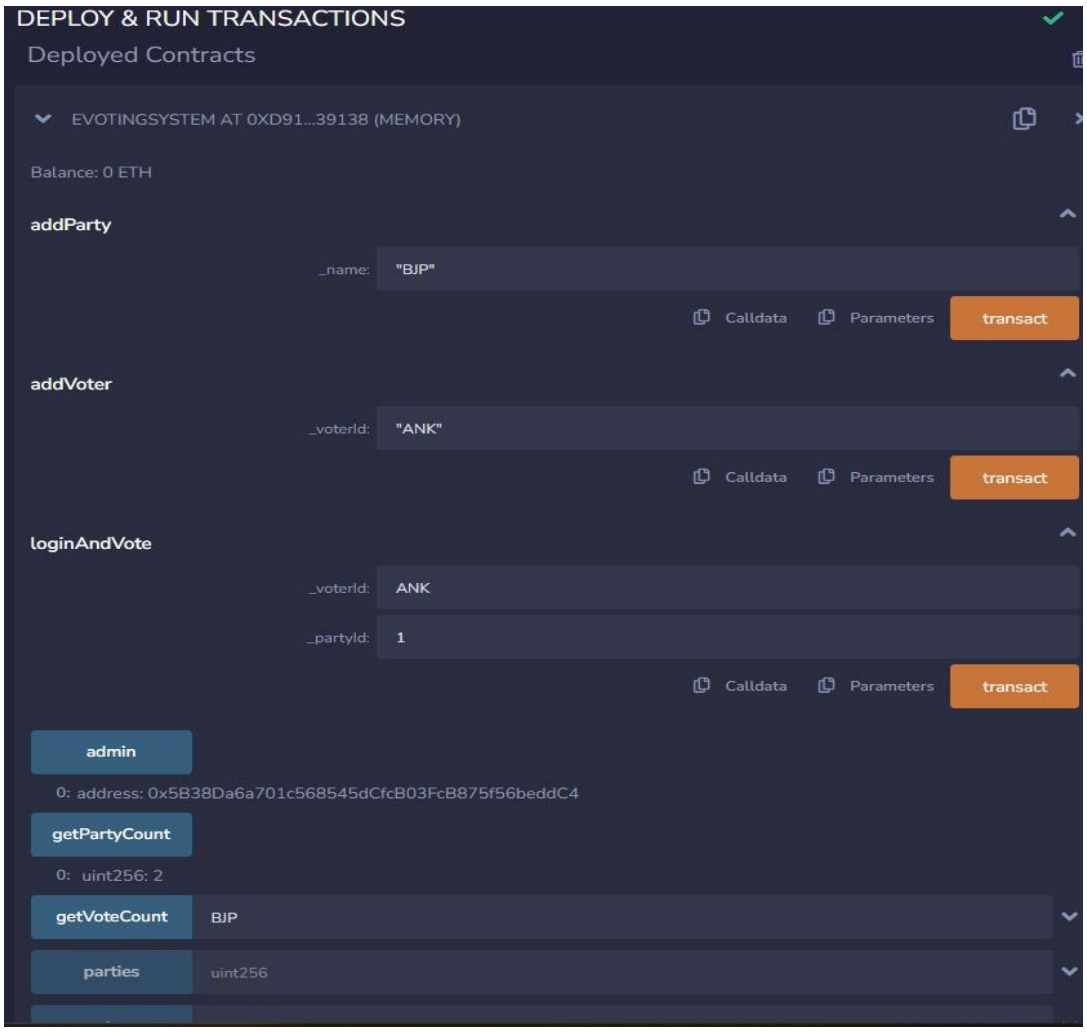
- Contract-Level Scope: The report will focus solely on the security aspects of the contract and will not address broader concerns related to gas efficiency, code optimization, or other non-security-related matters.

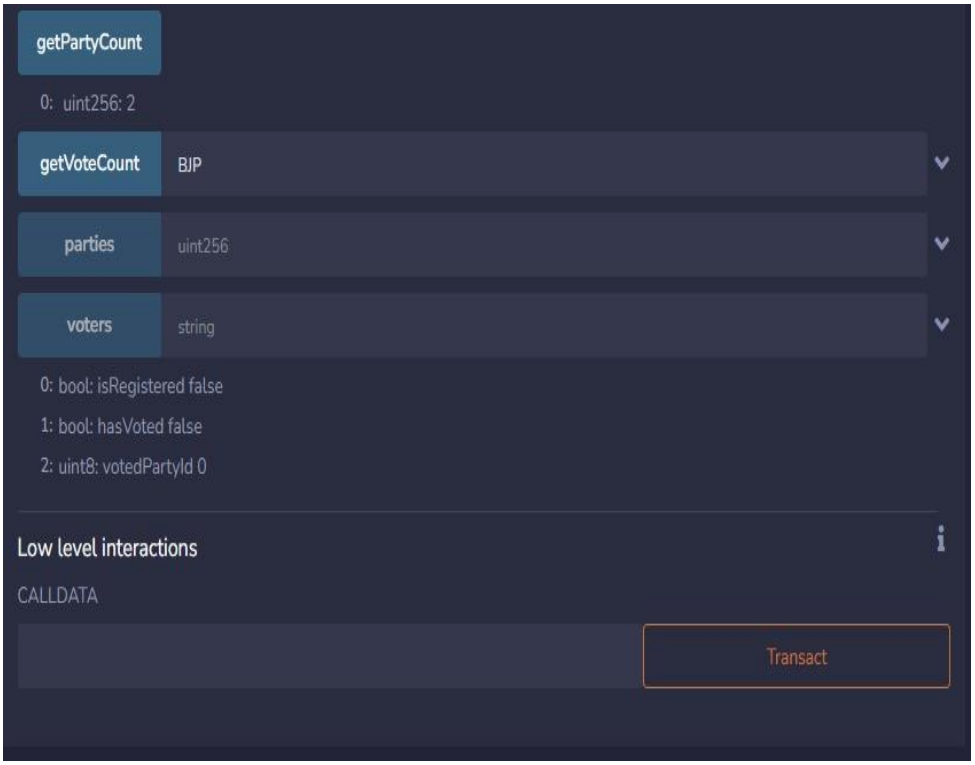
❖ Methodology

The "Ballot" contract implements a voting process along with vote delegation. The key algorithms used in the contract include:

- Voting Weight: Each voter has a weight that accumulates based on delegation. This weight is used to influence the outcome of the vote.
- Delegation: Voters can delegate their votes to other addresses, creating a chain of delegation. The contract checks for looped delegation to prevent cycles.
- Vote Casting: Voters can cast their votes for specific proposals by providing the index of the proposal they wish to support. The contract updates the vote count for the chosen proposal.
- Winning Proposal: The contract calculates the winning proposal by identifying the proposal with the highest vote count.
- Access Control: The contract has basic access control, allowing the chairperson to grant voting rights and manage the voting process.

❖ Results





❖ Conclusion

An E-Voting System using Solidity has the potential to enhance the transparency, security, and accessibility of elections. While it offers numerous benefits, it must also address challenges related to cybersecurity, identity verification, and public trust to ensure its successful adoption and continued use in the democratic process.