B. M. S. COLLEGE OF ENGINEERING BENGALURU
Autonomous Institute, Affiliated to VTU

A Technical Seminar Report based on Technical Activity

Prevention of Pool Hopping using Smart Contracts

Submitted in partial fulfillment for the award of degree of

Bachelor of Engineering
in
Computer Science and Engineering

Submitted by:
M Ananta Naga Rajesh
1BM21CS098

Work carried out at

Internal Guide
Namratha M
Assistant Professor
B. M. S. College of Engineering

Department of Computer Science and Engineering
B. M. S. College of Engineering
Bull Temple Road, Basavanagudi, Bangalore 560 019
2022-2023

B. M. S. COLLEGE OF ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

DECLARATION

I, **M ANANTA NAGA RAJESH (1BM21CS098)** student of 4th Semester, B.E, Department of Computer Science and Engineering, B. M. S College of Engineering, Bangalore, hereby declare that, this technical seminar entitled " **Prevention of pool hopping using Smart Contracts** " has been carried out under the guidance of **NAMRATHA M,** Assistant Professor, Department of CSE, BMS College of Engineering, Bangalore during the academic semester June-September 2023. I also declare that to the best of my knowledge and belief, the technical seminar report is not from part of any other report by any other students.

Signature of the Candidate

M ANANTA NAGA RAJESH (1BM21CS098)

B. M. S. COLLEGE OF ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the Technical Seminar titled "**Prevention of pool hopping using Smart Contracts**" has been carried out by **M ANANTA NAGA RAJESH (1BM21CS098)** during the academic year 2022-2023.

Signature of the Guide   Signature of the Head of the Department

Signature of Examiners with date

1. Internal Examiner   _____

2. External Examiner   _____

Abstract

We have written a research paper on "Prevention of Pool Hopping using Smart Contracts, and we described the solutions for which the miners jump from one pool to the other which leads to network stability. So, we described everything in this paper from the point when miner enter the mining pool up to when the miner leaves the pool.

In the process of onboarding miners to the network, a critical step involves verifying their miner certification. Each miner possesses a unique miner address associated with their individual certificate, which is necessary for receiving rewards. The pool manager, while respecting the miner's privacy, accesses this certificate by requesting the miner's address. This certificate details the miner's history, particularly focusing on their Hop-Count, past smart contract (SC) upholds, and SC violations.

To assess a miner's risk to the mining pool, both the Hop-Count (α) and SC-violated (μ) components are evaluated. When both values are zero, the miner is considered safe for inclusion in the pool. However, if either or both values are greater than zero, indicating a potential risk due to hopping behavior, a smart contract is initiated. This contract requires miners with a high Hop-Count to submit coins as an escrow, acting as a penalty if they prematurely leave the mining pool. The escrow serves as a deterrent, ensuring miners remain committed to completing their mining tasks. The terms of the smart contract mandate the escrow requirement, with the specific amount determined based on the miner's history of upholding or violating prior smart contracts. Miners with a reliable history may need a smaller escrow, reflecting their trustworthiness. This approach effectively discourages pool hopping behavior and promotes a fair and secure mining environment.

Table of Contents