SCHOOL OF STUDIES, ENGINEERING &TECHNOLOGY

GURU GHASIDAS VISHWAVIDYALAYA

BILASPUR, C.G., INDIA

REPORT ON SEMINAR

7TH SEMESTER

DEPARTMENT OF COMPUTER SCIENCE AND TECHNOLOGY

SUMBMITTED TO	SUBMITTED BY
DR PRINCY MATLANI	SHARMA VISHAL RAJESH 19103359(53) SALMAN KHAN 19103354(48)

CERTIFICATE

OF INTERNSHIP

THIS CERTIFICATE HAS BEEN PRESENTED TO

SALMAN KHAN

FOR SUCCESSFULLY COMPLETING THE 12 WEEK INTERNSHIP PROGRAM AT CODEDAMN DELHI AS BLOCKCHAIN INTERN

11 AUGUST 2022

DATE

DIRECTOR
CODEDAMN

DETECTING MELICIOUS ACCOUNT IN PERMISIONLESS BLOCKCHAIN

The temporal nature of graphs modeling blockchain accounts as nodes and transactions as directed edges – enables us to understand the behavior (malicious or benign) of the accounts. Predictive classification of accounts as malicious or benign could help users of the permissionless blockchain platforms to operate securely. Motivated by this, we introduce temporal features such as burst and attractiveness on top of several already used graph properties such as the node degree and clustering coefficient. Using identified features, we train various Machine Learning (ML) algorithms and identify the algorithm that performs the best in characterizing the accounts as malicious. We then study the behavior of the accounts over different temporal granularities of the dataset before assigning them malicious tags. For Ethereum blockchain, we identify that for the entire dataset the ExtraTreesClassifier performs the best among supervised ML algorithms. On the other hand, using cosine similarity on top of the results provided by unsupervised ML algorithms such as K-Means on the entire dataset, we were able to detect 554 more suspicious accounts. Further, using behavior change analysis for accounts, we identify 814 unique suspicious accounts across different temporal granularities.