NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

School of Computer Science and Engineering
College of Engineering

Designing a Security Evolution tool for Blockchain Smart Contracts

Technology stack

VueJS as JavaScript framework

Flask to host trained model as a service

Keras as a neural-network library for model training

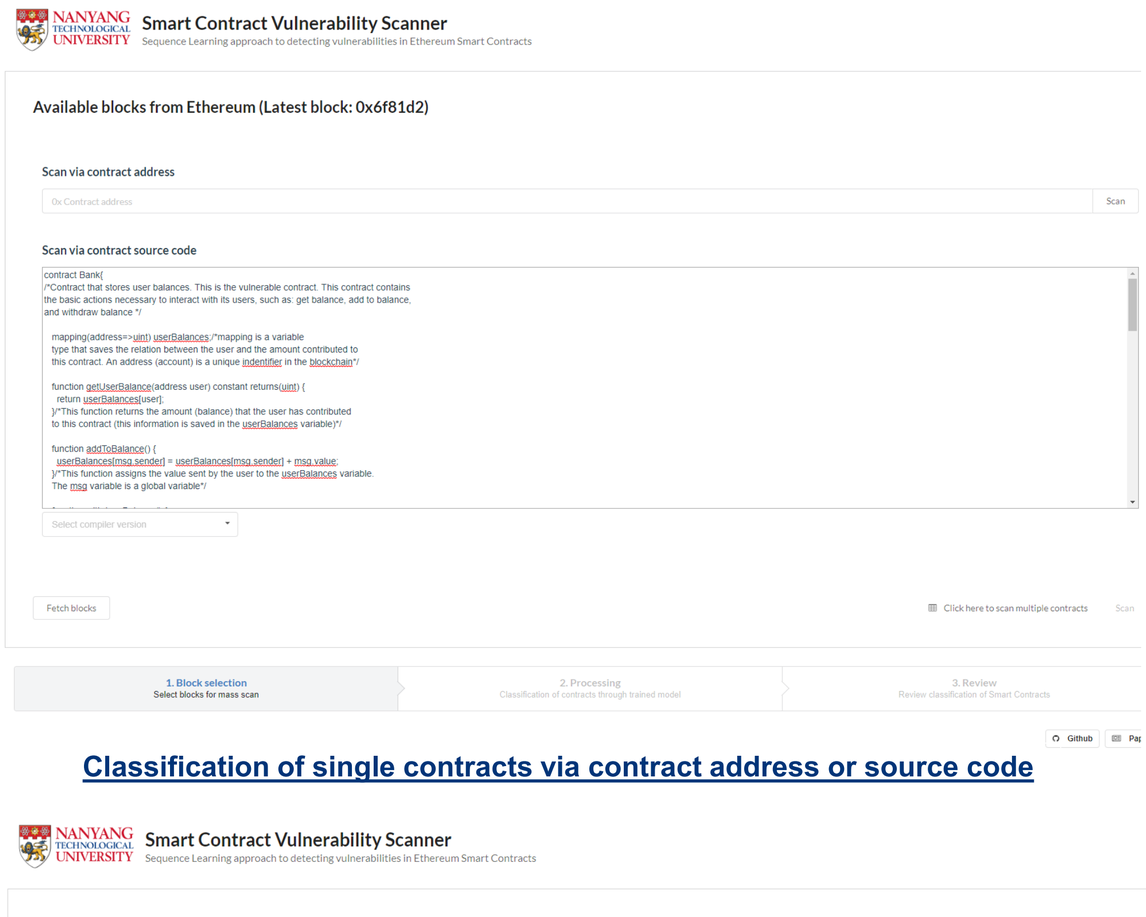
Infura for access to Ethereum main-net

Smart Contract Vulnerabilities

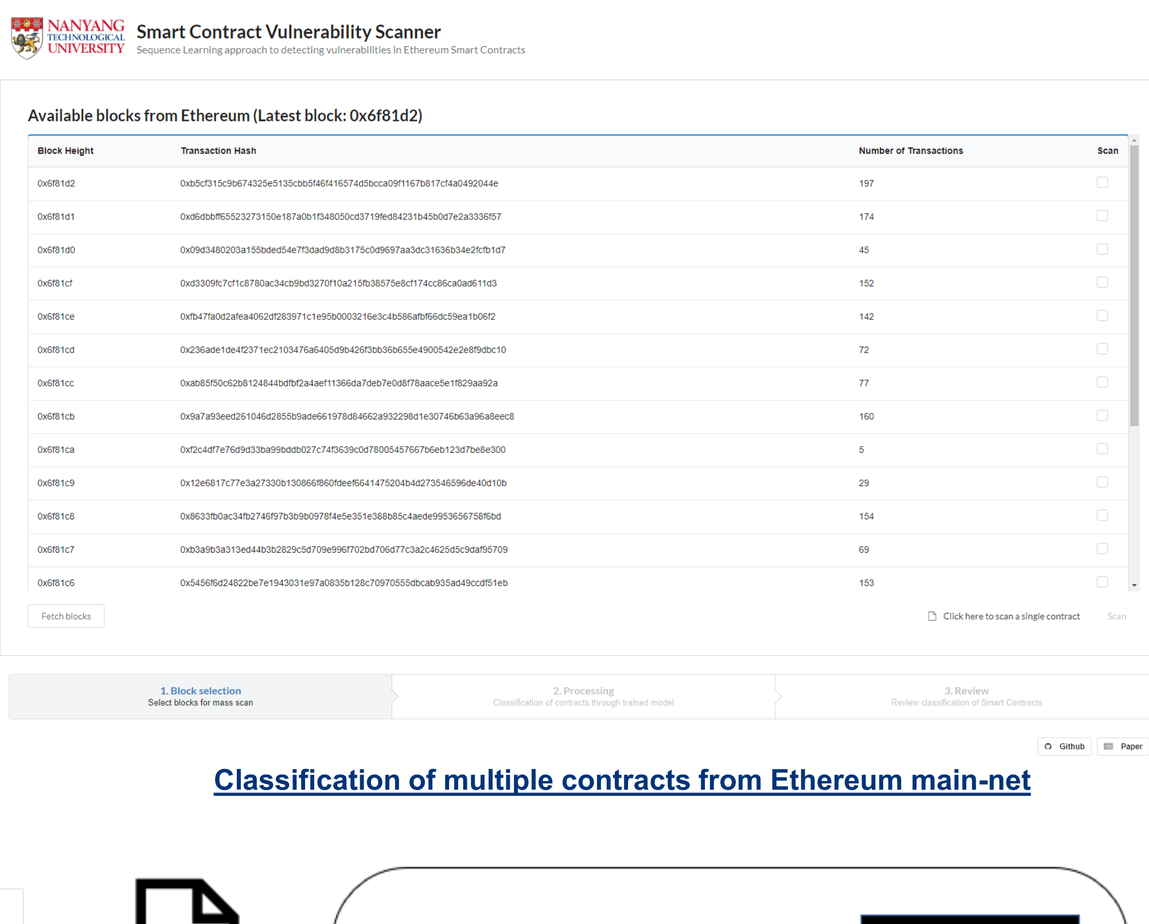
Past security incidents of smart contracts on the Ethereum blockchain has proved to be disastrous - incurring losses of upwards of a few hundred million USD to date. In this project, we aim to contribute to the security landscape of smart contracts by proposing an efficient smart contract vulnerability detection system.

Application of Deep Learning

A long-short term memory (LSTM) trained on approximately 1 million contracts serves as a classifier for identifying security threats. This approach takes less than 1/10 the time required for an analysis by prominent symbolic analysis tools while achieving high test accuracies, allowing us to classify smart contracts at scale.



Classification of single contracts via contract address or source code



Classification of multiple contracts from Ethereum main-net

Vulnerability scores indicating model's confidence

LSTM Performance Metrics

Test Accuracy	99.40%	Precision score	64.11%
Recall score	89.81%	F1 score	74.81%
		ROC AUC score	94.69%

Student: Han Xing Jie Supervisor: Dr Sourav Sen Gupta