Task1

- 笔记作者：weidu
- 原文作者：Wesley Joon-Wie Tann..
- 原文题目：Towards Safer Smart Contracts: A Sequence Learning Approach to Detecting Security Threats
- 原文来源：AI 2016: Advances in Artificial Intelligence

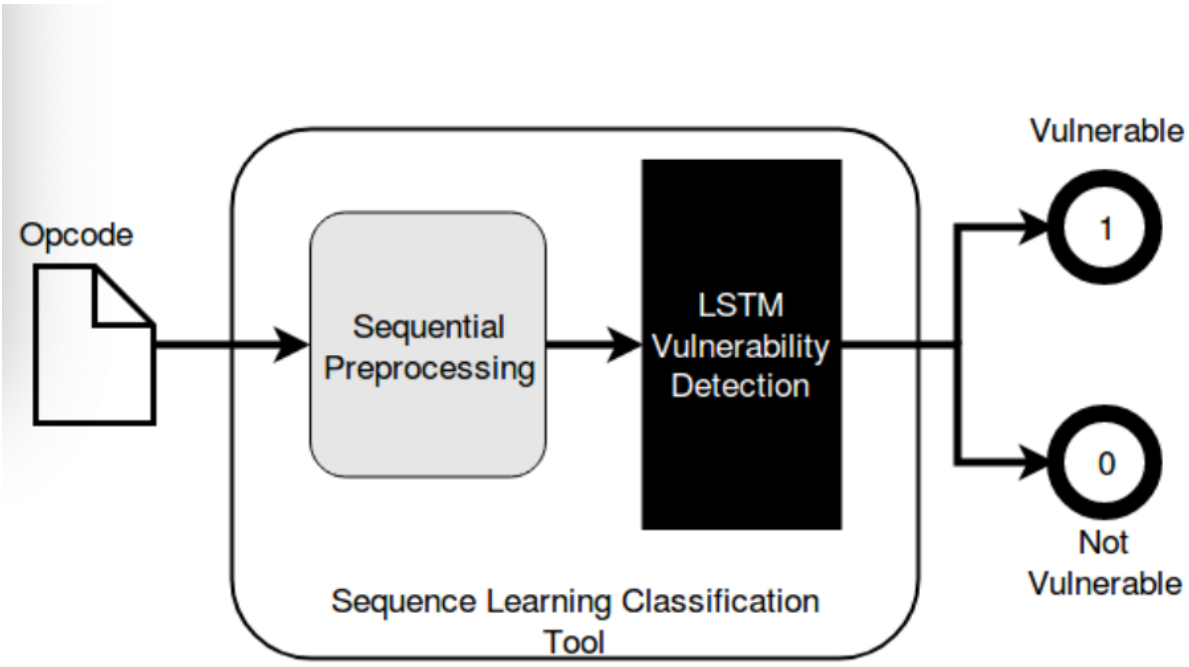
文章主要内容

区块链的火热发展催生了智能合约等新型互联网应用程序，但是合约代码具有永固性，一旦部署代码不可更改，所以智能合约安全的研究和防范显得尤为重要，本文提供了一种线型模型LSTM来检测已经部署的合约代码是否具安全。

通过训练模型来检测恶意的OPcode来判断代码是否安全。提供了一种新的研究方式

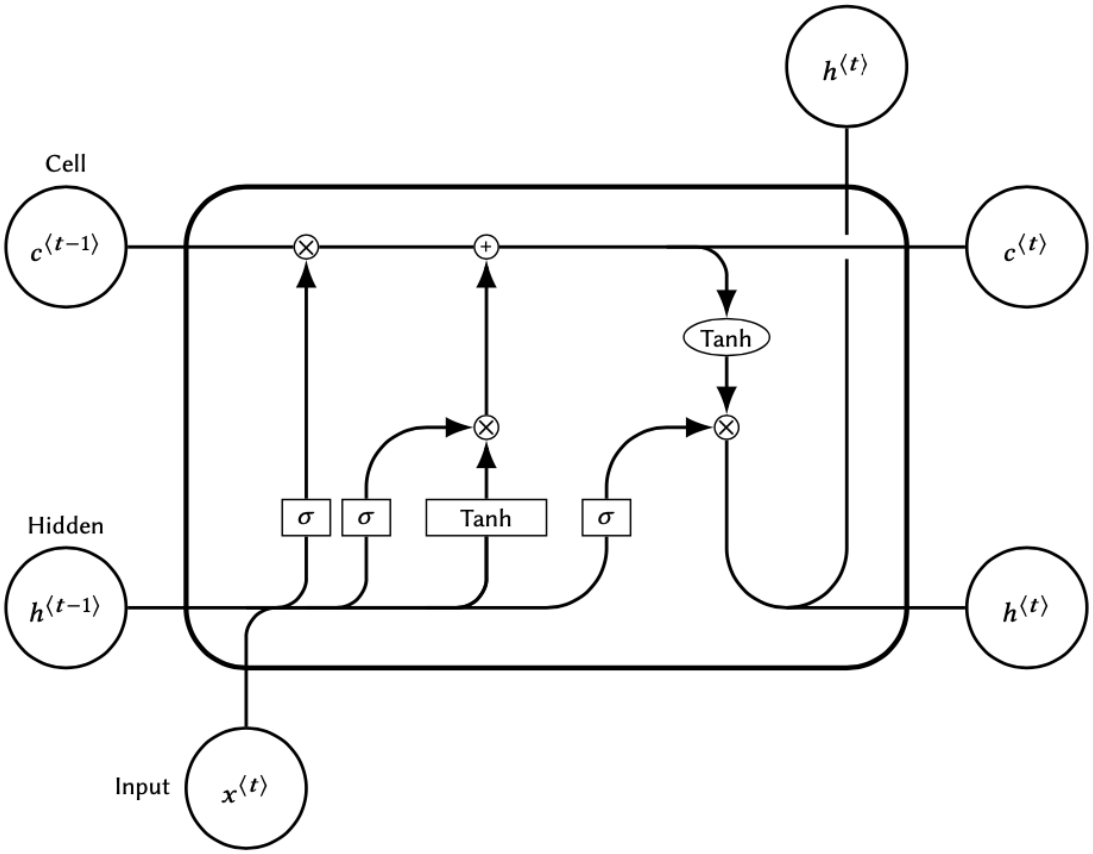
1、研究内容

架构：整个系统框架图如下所示，



收集opcode的数据集然后进行数据预处理，之后输入到LSTM网络,会返回出是否代码具有风险

LSTM网络的架构非常著名



因为LSTM这种模型可以有效的防止梯度消失问题，而且可以学到线性的模式，所以用来分析代码非常合适

数据集：使用的数据集来自Google Ethereum Opcode Sequence

并通过Maian进行LABLE

评估结果：

使用指标，准确率，精确度和召回率ROC等。

- the LSTM with 99.57% accuracy significantly outperformed MAIAN's 89% accuracy in detecting unsafe smart contracts.

Classification Performance Measure	LSTM %
Test Accuracy	99.57
Recall Score	89.90
Precision Score	82.49
F_1 Score	86.04
ROC AUC Score	94.81

Table 2: LSTM detection performance measures.

最终评估结果表明，LSTM的准确度为99.57%，在检测不安全的智能合约方面明显优于Maian的89%的准确度。

2、创新点

本文的主要创新点如下：

直接分析合约的opcode,不需要反汇编,也没有分析静态代码，使用LSTM模型，具有非常高的准确度

3、论文评论优缺点

总的来说，这篇论文是一篇特别优秀的论文，采用LSTM模型方法非常成功，提供了一种研究以太坊安全的新方法，而且我想借此论文再深入研究,该论文只探讨了合约是否具有漏洞,本质上是一个二分类问题,但是我们可以做多分类问题,

合约中的DASP漏洞就很有价值，我们可以复现训练一个双向的RNN来进行实现，或者Conv1D，准确度方面也不会差，而且训练的时间会大大缩短。