Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

InIT Institut für angewandte Informationstechnologie

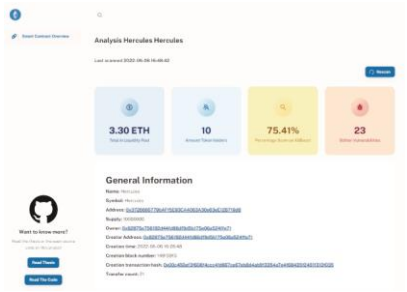
Smart Contract Scam Checker for Decentralized Finance (SCSC)

Diplomierende
Pascal Ackermann
Stefano Tassone

Dozent
Gürkan Gür

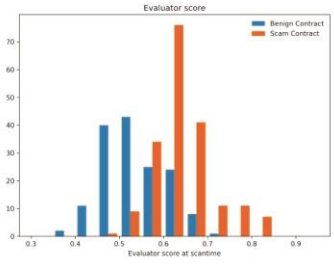
Die Anzahl der Betrugsfälle im Decentralized Finance (DeFi) ist beträchtlich hoch. Es ist wahrscheinlicher, dass ein neu veröffentlichter Smart Contract ein Betrug ist, als dass er legitim ist. Ziel dieses Projekts war es daher, mit Hilfe verschiedener Indikatoren und Live-Daten, die von DeFi-Diensten für Ethereum gesammelt wurden, Wege zur frühzeitigen Erkennung solcher Betrügereien zu finden. Zu diesem Zweck haben wir gängige Betrugsfälle analysiert und sieben Indikatoren implementiert. Diese Indikatoren sammeln Daten von externen APIs und verarbeiten sie mit Hilfe von Logik, Best Practices sowie statistischen Beobachtungen aus dem Datensatz, der während der Erstellung dieses Projekts gesammelt wurde.

Es wurden drei Ansätze für die Bewertungen der Daten implementiert. Als erstes wurde der gewichtete Durchschnitt der Indikatorwerte für die Klassifizierung verwendet, zweitens wurde über eine Support Vector Machine basierende Entscheidung bewertet und drittens wurde ein XGBoost-Modell genutzt, welches auf dem gesammelten Datensatz trainiert wurde. Die experimentellen Ergebnisse zeigen auf, dass unsere vorgeschlagene Lösung erfolgreich zwischen offensichtlichem Betrügen und eindeutig gutartigen Smart Contracts unterscheiden kann. Im Testdatensatz zeigt der gewichtete Durchschnitts-Klassifikator eine Genauigkeit von 71%, der Support Vector Machine-Klassifikator eine Genauigkeit von 83% und der XGBoost-Klassifikator eine Genauigkeit von 86%. Die Ergebnisse des Testdatensatzes zeigen jedoch, dass es schwierig ist, neu erstellte Smart Contracts als legitim zu kennzeichnen.



Detailansicht der SCSC Smart Contract Analyse

Als zukünftige Arbeit und als mögliche Erweiterung unserer aktuellen Bachelorarbeit wäre es wichtig, das Problem der fehlenden Informationen aufgrund der frühen Analyse neu erstellter Smart Contracts anzugehen. Diese Informationen sind für einige unserer Indikatoren entscheidend. Darüber hinaus ist ein grösserer und ausgewogenerer Testdatensatz von entscheidender Bedeutung, um die schwache Identifizierungsleistung für legitime Smart Contracts mit unseren vorgeschlagenen Ansätzen zu untersuchen. Um diese Schwäche zu reduzieren, wäre ein regelmässiger Rescan oder eine längere Zeitspanne zwischen Erhalt und der automatischen Analyse der Smart Contracts von Vorteil.



Verteilung der eigenen SCSC Wertung