Abstract

Ethereum is a development platform upon which smart contracts can be built and deployed. Smart contracts allow credible transactions to be executed without the intervention of third parties. They are also irreversible and completely trackable. The cryptocurrency of Ethereum is known as Ether which can be transferred between users by sending Ether from one user's address to another. All history of Ether owning and transferring, as well as smart contract deployment and interactions, are available on the public ledger known as the Ethereum Blockchain. While the transactional data available contains information such as the users' addresses, their true identity is hidden.

The decentralisation of the Ethereum blockchain, coupled with the pseudo-anonymity of its users, has paved the way for an unregulated technology in which users can deploy applications and transfer cryptocurrency from one user's address to another. It is hard to near impossible for law enforcement to detect suspicious patterns on the blockchain, thus making it an attractive environment for malicious activity.

Interest in detecting suspicious behaviour has gained a lot of interest from various parties over the last number of years with different means of identification being explored such as Ponzi schemes and using the Markov Logic Network and Markov Random Fields to exploit underlying links between potentially fraudulent users in the network.

In this thesis we explore the use of unsupervised learning as a means of detecting patterns in the Ethereum transactional data. We evaluate the accuracy of the patterns formed and investigate whether or not anomalies occur. This study provides a good starting point for future work to advance in the area of detecting suspicious behaviour on the Ethereum Network.