WESTERN SYDNEY
UNIVERSITY

Forensic/Investigatory Tool used to track money laundering through anonymous bitcoin mixers

Mukul Chhabra

19572970

A project proposal submitted for 300597 Master Project 1

in partial fulfilment of the requirements for the degree of

Master of Information and Communication Technology

Supervisor: Dr Aruna Jamdagni

School of Computing, Engineering and Mathematics

Western Sydney University

September, 2019

1. Table of Contents

Introduction

This project proposal is prepared to identify the best forensic tools for detecting fraudulent money-laundering activities through Bitcoin mixers. Money laundering is a criminal activity which transfers money from different sources to destinations including borders, for illegal purposes by avoiding transaction records and identifications. These amounts fund terrorism, drugs, crimes and many other illegal activities. With advancement in technology, money-laundering is now being done through digital cash, and cryptocurrencies. Bitcoin has been one of the most used cryptocurrencies for money-laundering, due to its anonymity. The anonymity comes from Bitcoin mixers who change the sources of Bitcoins, making it appear as a newly generated currency from a node. Each time these nodes are changed and the track through which the Bitcoin arrived is deleted, making it impossible for agencies to determine its sources. Money-laundering has a great impact on our societies, it promotes illegal activities and decelerates economic growth of countries. Taxes are avoided and levies are bypassed, with tax agencies losing billions every year, it affects the prosperity of nations. On other hand, criminal activities sky-rocket due to illegal money, sale of drugs on our streets has increased, and all this illegal cash is laundered through online platforms now.

Worst to come, agencies have been trying to detect the sources of these currencies, but in vain. The digital era has made it very easy for these launderers to transfer money with high-level of anonymity. Cross-borders transfers now have no control, making it more and more difficult to track down on the transactions.

This project will help us to identify the best tool to detect fraudulent money-laundering activities, by Bitcoin mixers and gives us an overview of the tool to be used. The data which would be generated and the outcomes and results from the software.

Background

Bitcoin is a digital cryptocurrency which was developed in the year 2009 by Satoshi Nakamoto, it is a decentralised currency which makes it capable of transferring between peers without any intermediaries. It is created as an outcome for mining, for which transactions are verified or authorised by a network of nodes and registered in a ledger called "Blockchain" (Nakamoto, 2008). As the popularity of Bitcoin grew, it was being used as a medium for money laundering by bitcoin mixers and resulted in large amounts of money being transferred to groups. As bitcoins could be exchanged for other currencies or could be used to pay for online transactions, it grew as a popular illegal currency for transactions throughout the world. Hundreds of researches have been conducted to identify the paths of these transactions, researchers have also developed tools and software's to track bitcoins and illegal transactions over the internet and dark web. Current tools use analytics of Blockchain to track Bitcoin transactions, with this technology a mere percentage of them are tracked, as the transactions are completed on dark web (Sirer, 2013).

Money-laundering is centuries old criminal activity, with changing technologies and digital era, its constantly changing its channels and ways of doing it. Crypto-currencies have emerged as one of the most popular methods of laundering money and cashing-out, it is reported that over 40% of criminal transactions and payments have been made using Bitcoin. Dark web has accounted for nearly 50% of these transactions and cybercriminals are using technology and protocols to avoid being caught, while hiding the IP Addresses or using a clone address to deceive the systems. Bitcoin grew as a popular medium for criminals, as it enables users to make direct transfers without the interference of banks, thus decentralising the payment gateway (Tim Ruffing, 2017). Researchers have long been working into solving this problem, by techniques and tools to track the Bitcoins and control the transactions over the web, over this Bitcoin Mixers evolved to break the transactional link between the transactions. Bitcoin Mixers provide a virtual service which generates a new address for bitcoins and pays-out bitcoins from its own reserve to the address provided by the customer and charges a fee to provide this service. This cuts the link between the Bitcoins deposits and makes it appear as an anonymous transaction. It also provides the customer with a link to verify the link of transactions, a Zero percent link is shown if the mixing service is performed correctly (Malte Möser, 2013) (Möser, 2013).

This proposal will identify potential tools and technologies which can be used to track Bitcoin transactions and prevention techniques to reduce money-laundering through anonymous mixers.

Objective

This research aims at determining the channels of Bitcoin mixers and detect fraudulent activities, including money-laundering by using tools and techniques. This will help governments and law enforcement agencies such as federal governments, tax offices, revenue offices, security exchanges and other financial agencies to track down illegal transactions and block funding of money to groups and gangs for criminal activities.

Hypothesis

- Elliptic Forensic tool is best to track money-Laundering. There are three other tools which are identical in nature to Elliptic, of which CipherTrace tool is robust.
- Visualisation and statistical analysis will be used to track Bitcoin Mixers.
- CipherTrace and Elliptic are the best tools to detect anonymity of Bitcoin mixers and fraudulent money laundering.

Methodology

To perform this research, Elliptic Forensic analysis tool will be used, the other tool which could be used is the CipherTrace, which uses Blockchain technology to detect money-laundering and Bitcoin Mixers. Blockchain technology enables the digital information to be distributed between nodes and networks but disables it from being copied.

Elliptic tool identifies money-laundering through machine-learning algorithms and matching the data of money with agencies across the world. The tool uses Ip Addresses, internet packets from the source, by decrypting the data, the software identifies if the transfer is legitimate or has abnormalities, such as anonymous source and destination and other attributes, like destination IP, receiver details.

It detects anonymity of the transactions with the help of algorithms and techniques which identify the MAC address and IP addresses of source, if any discrepancies are noticed, the transaction is flagged and investigated.

Elliptic tool can perform investigations usingstatistical data to identify crimes and illicit transactions by mixers and users using cryptocurrency. This tool helps to identify anonymous and pseudonymous cryptocurrencies which are used to facilitate criminal activities. It uses strong analytical systems and uses proprietary data to identify the people involved and generate evidence of illegal activities, this is done by linking identities with real profiles on Bitcoin Blockchain.Elliptic tool uses data which is collected deep from the web, and links it with history of transactions and transfer of cryptocurrencies (Robinson, 2018).

Elliptic's Bitcoin Big-Bang visualisation demonstrates the transfers of Bitcoin's over a few years and performs analysis with the data collected. The visualisation tool provides insights of dark web, Bitcoin Mixers and the use of Tor Protocols to perform transfers across the borders.

A statistical analysis is performed on the data, which was collected over years by Elliptic team, this data is private and Elliptic owns the rights to data. They have harvested this data over the years, using various tools and techniques. This data is the records of the detected Bitcoin transactions through web, dark-web such as silk way, it has been collected by Elliptic over years and used in their algorithms, which runs the transaction through the database to match any historic sources and destinations flagged as illicit. Elliptic tool performs statistical analysis using the data from their database, which will give an outcome of any matches and historical routes of illicit money-laundering (Khatri, 2019).

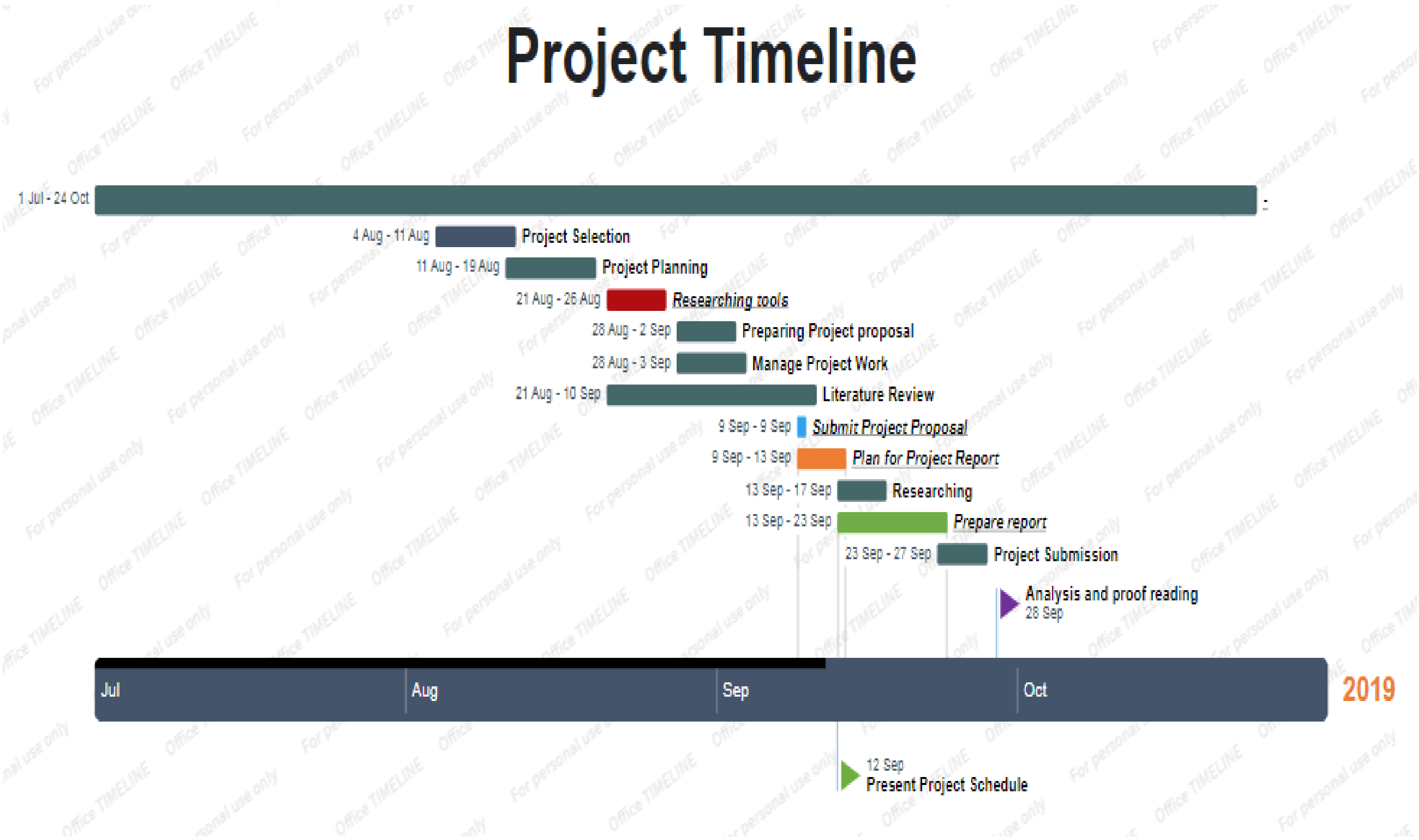
Expected outcomes

Cryptocurrency has only emerged in the recent years with the digitisation of transactions and banking. Data collection is still underway to completely understand the market of

Bitcoin and money-laundering, with many methods evolving and less involvement from authorities, this area will take an enormous time to completely understand the topic (Stefano Bistarelli, 2018).

This research will provide the analysis and overview of the area and propose the best tool to investigate money-laundering by bitcoin mixers. This will be demonstrated by using Elliptic and CipherTrace tool simultaneously, and then analysing the final outcomes from both tools.Providing graphical data of the routes of Bitcoin transfers, this research will help us to select the best tool to investigate money-laundering.

Program of work



Bibliography

Khatri, Y., 2019. *THE BLOCK.* [Online] Available at: https://www.theblockcrypto.com/2019/08/02/blockchain-analytics-startup-elliptic-mit-researchers-collaborate-to-detect-money-laundering-in-bitcoin-using-deep-learning-techniques/
[Accessed 28 August 2019].

Malte Möser, R. B. D. B., 2013. *An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem.* Münster, IEEE.

Möser, M., 2013. *Anonymity of Bitcoin Transactions- An Analysis of Mixing Services.* Münster, University of Münster.

Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. pp. 1-9.

Robinson, Y. J. F. a. T., 2018. *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services,* s.l.: Center on Sanctions & Illicit Finance memorandum.

Sirer, I. E. a. E. G., 2013. *Majority is not Enough: Bitcoin Mining is Vulnerable,* New York: Department of Computer Science, Cornell University.

Stefano Bistarelli, M. P. a. F. S., 2018. *Visualising Bitcoin Flows of Ransomware,* Perugia: ITASEC.

Tim Ruffing, P. M.-S. A. K., 2017. *P2P Mixing and Unlinkable Bitcoin Transactions,* Purdue: s.n.