TMT : Tool for Monitoring Illegal Transactions using Anonymous Web and Blockchain Technology

[Chasing Cryptocurrency Account on the Dark Web]

Nohyun Kwak
GSIS, KAIST
nhkwak@kaist.ac.kr

Sejin Jeong
GSIS, KAIST
skyshiri@kaist.ac.kr

ABSTRACT

Keywords

Dark Web; Blockchain; De-anonymizing

1. INTRODUCTION

Dark web, like the nuance of its name, refers to the web used for illegal transactions such as weapons or drugs, using Tor's anonymity. Tor is free software that enables anonymous communication. Its use is originally intended to protect personal privacy. Tor is networked with volunteer nodes acting as onion routers to hide the user's location and usage. The dark web has the same anonymity because it uses tor as a network layer.

With the recent use of blockchain technology, the famous crypto currency, such as bitcoin or ethereum has emerged. Crypto currency uses blockchain technology to record transactions in blocks and share them in a distributed environment. Since each block generates a hash value of the current block based on the hash value of the previous block and verifies the integrity, it is difficult to modulate the block. Because crypto currency uses only public key information for transactions, trading is possible without sacrificing anonymity. Thus, the crypto currency is often used for illegal purposes based on anonymity. For example, there was a case in which a hacker forcibly encrypted victim's files with ransomware and threatened to pay a bitcoin to decrypt them. This shows that the transaction with bitcoin is used as an illegal means of payment because it has anonymity.

The combination of dark web and crypto currency makes it more difficult to track illegal transactions online because they can hide transactions anonymously.

In this paper, we propose a tool to detect and track illegal transactions based on the combination of dark web and crypto currency. The key ideas for this are as follows. Assuming that the site found on the dark web is for illegal activity, we crawl the dark web and find the crypto currency account information. These account information is categorized into the nature of sites such as weapons, drugs, and gambling, and accounts associated with these accounts are also registered as blacklist. Blacklisted accounts are anonymous public key information, so it is not easy to identify them and arrest the criminals. However, if Blacklisted accounts have transactions with trackable accounts, the tool we propose will detect them quickly and notify investigators, and investigators will have clues to track anonymous accounts. Traceable accounts are comprised of deanonymized accounts (for example, accounts opened to pay for cryptocurrency in online or offline stores) and deanonymizable accounts (for example, accounts where the actual user is identified by the police's request for cooperation).

In short, our tool's goal is to quickly detect blacklisted illegal accounts on the dark web as they deal with trackable accounts and to provide information to investigators to arrest criminals.

Our contributions We analyze transactions related to illegal activity on dark web. And we propose TMIT which is a tool for monitoring illegal and anonymous transactions.

WOODSTOCK '97 El Paso, Texas USA

ACM ISBN 0-12345-67-8/90/01…$15.00

DOI: 10.475/123_4

2. BACKGROUND

2.1 Dark Web

Dark web is World Wide Web content that exists on darknets, overlay networks which use the Internet but require specific software, configurations or authorization to access. Dark web forms a small part of the deep web, which is not indexed by search engines. So dark web can be used for hiding criminal activity. Individuals can access dark web using special software such as Tor(The Onion Router). Tor relies on the volunteer computer network to route the user's web traffic through a set of other user computers, so that traffic cannot be traced back to the original user. Once on dark web, users navigate through the same directory as the "Hidden Wiki", which organizes sites by category, just like Wikipedia. Individuals can also search the dark web using a search engine. Search engines are used to search for contraband such as broad or unspecified drugs, guns or counterfeit bills. In dark Web, individuals can communicate through methods such as secure e-mail, web chat, or personal messaging hosted on Tor.

2.2 Blockchain

Blockchain is a continuously growing list of records, called blocks, which is linked and secured using cryptography. Each block contains hash as a link to a previous block, a timestamp and transaction data. By design, blockchain is inher-

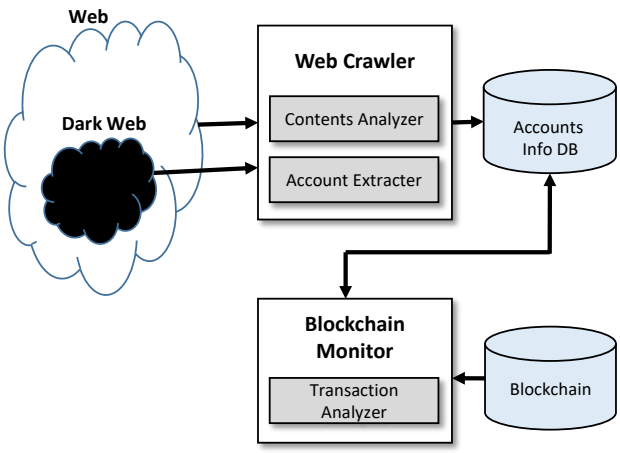

Figure 1: TMIT Architecture

ently resistant to modification of the data. Blockchain can serve as open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. For use as a distributed ledger, blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered without the alteration of all subsequent blocks, which needs a collusion of the network majority. Blockchain is secure by design and example of a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain. The first distributed blockchain was conceptualised in 2008 and implemented the following year as a core component of the digital currency bitcoin, where it serves as the public ledger for all transactions.

3. DESIGN

Figure 1 shows the overall architecture for de-anonymizing illegal transactions: First, the web crawler collects the account information of the crypto currency on the dark web and normal web. Then it set up the account found on the dark web to the account associated with the illegal transaction and set the legitimate and trackable account of the normal web to a trackable account. Based on the stored accounts, the blockchain monitor keeps track of the transactions of those accounts in the blockchain and checks whether there is a connection between trackable accounts and illegal accounts. If a connection is found between two account groups, it is considered to have found a link to de-anonymize. Figure 2 shows the relationship between two account groups in a graphical representation. When red nodes are accounts on the blacklist and green nodes are trackable accounts, you can see that there is a trade between an illegal account and a trackable account.

3.1 Illegal Accounts

The illegal account we monitor is an account associated with illegal activities on the dark web. Therefore, we categorized the illegal activities as follows in consideration of

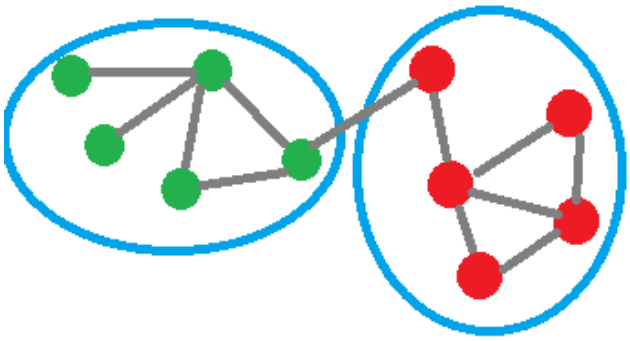

Figure 2: Graphical analysis for illegal account

the seriousness.

- **RA-5 (More than 5 years sentence)** Sale of stolen goods, Contract murder, Transactions of weapons or drugs
- **RA-3 (More than 3 years sentence)** Transactions of adult contents or counterfeit bills
- **RA-1 (3 years or less)** Request for hacking, Gambling, Transactions of personal information

Since the accounts linked directly to the accounts associated with the above activities are also likely to be illegal accounts, they also need to be monitored. We therefore defined a range of influence (RA) as a value that indicates the extent to which we monitor these activities. Accounts with depths within the value of RA are also tracked, centered on accounts associated with the activities listed above. In other words, depth is monitored deeply for serious criminal activity and monitored to a lesser extent for less serious criminal activity. The categorized criteria and score can be changed in any case. In this paper, we only present concepts for defining and prototyping accounts associated with Illegal Accounts.

3.2 Web Crawler

The web crawler scrapes the web site and analyzes the contents for finding the account information of crypto currency. For example, bitcoin's account information consists of a string in the format Base58. Therefore, if the HTML document is parsed from the dark web and the string exists, the string is added to the blacklist as an account associated with the illegal transaction. In a similar way, legitimate and trackable accounts extracted from the normal web are added to the trackable list.

3.3 Blockchain Monitor

To remove the anonymity of an illegal account on the dark web, the blockchain monitor checks that the account in the blacklist is associated with a trackable account. To do this, the transaction of two account groups should be continuously monitored and the transaction should be converted into a graph data structure and analyzed.

4. IMPLEMENTATION

4.1 Web Crawler

4.2 Blockchain Monitor

Not yet

5. EVALUATION

We will evaluate the performance for monitoring illegal transaction.

6. DISCUSSION

Maybe the limitation of our research and future work will be discussed.

7. RELATED WORK

Not yet

8. CONCLUSIONS

Not yet