Detecting Money Laundering by Analyzing Cryptocurrency Transaction Graph

Junwoo Seo, Kyoungmin Kim, Mookyu Park, Moosung Park, and Kyungho Lee

Abstract—As the cryptocurrency market grows, various crimes based on cryptocurrency have come to the fore. Among the various crimes using cryptocurrency, this paper focuses on the money laundering and presents a methodology to detect money laundering. Most cryptocurrencies can query transaction data. Based on the extracted transaction data, the paper presents a graph that expresses the address as node and the transaction data as edge. Then, one of the characteristics of money laundering, a mixer pattern, is used to find a wallet address that is supposed to participate in money laundering in the graph. To find a mixer pattern in a transaction graph, the paper uses the subgraph isomorphism algorithm.

Research Keywords—Anti Money Laundering, Cryptocurrency, Graph Analysis, Money Laundering, Transaction Graph

1 INTRODUCTION

On January 3, 2009, the first Cryptocurrency, Bitcoin, was born by Satoshi Nakamoto. Over time, with the introduction of Bitcoin, various cryptocurrencies such as Ethereum, Ripple, and Litecoin have emerged and to this day the cryptocurrency world is constantly growing. The reason why the cryptocurrency world grows so fast that the cryptocurrency market cap reaches 600 billion dollars is because people are not simply enthusiastic about the new currency but are fascinated by the core technology of the cryptocurrency. The blockchain. Blockchain has the great advantage of decentralizing information, making it easy to share an integrity-guaranteed information. This gives cryptocurrencies many advantages for honest individuals [1]. For example, it can reduce transaction fees, ensure privacy in online transactions, or replace financial systems in countries where the financial system is immature. Cryptocurrency with this great technique, however, has a dark side. Because of the anonymity of transactions, the lack of regulation related to cryptocurrency, it is often involved in crime such as a means of payment for ransomware, for drug and weapon smuggling, prostitution, and money laundering.

This paper presents a methodology for detecting transaction related to money laundering through graph analysis in numerous cryptocurrency transactions. The next section is about related researches that are related to money laundering and cryptocurrency. The third section presents a methodology for finding nodes involved in money laundering in the entire transaction graph. The final section is the conclusion of this paper.

- *Junwoo Seo is with the Department of Cyber Defense(CYDF), Korea University. E-mail: junuseo@korea.ac.kr.*
- *Kyoungmin Kim is with the Department of Cyber Defense (CYDF), Korea University. E-mail: richard2104@korea.ac.kr*
- *Mookyu Park is with the Institute of Cyber Security & Privacy (ICSP), Korea University. E-mail: ctupmk@korea.ac.kr.*
- *Moosung Park is with Agency for Defense Development(ADD), Republic of Korea. E-mail: parkms@add.re.kr.*
- *Kyungho Lee (corresponding author) is with the Institute of Cyber Security & Privacy(ICSP), Korea University. E-mail: kevinlee@korea.ac.kr.*

2 RELATED WORKS

In this section, the paper introduces some preliminary studies related to this paper. Preliminary studies are divided into two types: Analysis on the relationship between cryptocurrency and money laundering and a technical analysis of the cryptocurrency transaction graph.

2.1 Cryptocurrency and Money Laundering

Christian Brenig et al. analyzed contextual and transactional factors that facilitate money laundering using cryptocurrency. As a result, from a criminal perspective, they pointed out that ML using cryptocurrency has economic incentives [1]. However, this study remains the first step in investigat-

ing money laundering and lacks specific analysis of contextual and transactional factors. David Bååth and Felix Zellhorn presented the benefits of bitcoin in ML in three ways [2]. First, the decentralized structure makes Anti Money Laundering (AML) method of monitoring existing intermediaries difficult. Second, all transactions are recorded in the blockchain, but it is extremely difficult to link the transaction with the actual person. Third, the speed and ease of transferring bitcoins are superior to the traditional cash. In addition to this, the suitability of cryptocurrency for ML was discussed by Sarah Meiklejohn et al. in computer science, Robert Stokes in law, and Victor Dostov and Pavel Shust in economics [3], [4], [5].

2.2 Analysis of Cryptocurrency Transaction Graph

Michael Fleder et al. have created a transaction graph to explore level of anonymity in Bitcoin and have linked it with real people. Based on the address information and transaction information disclosed on the Internet, it was able to match the actual person and the address, and it was possible to eliminate some anonymity [6].

Dorit Ron and Adi Shamir downloaded the entire bitcoin transaction and analyzed many statistical characteristics of the transaction graph. As a result, they found that hundreds of transactions moving more than 50,000 bitcoins were descendants of a single transaction performed in November 2010. This paper presented the possibility of tracking funds through the transaction graph [7].

3 Methodology of Detecting ML in Cryptocurrency Transaction

In this section, the paper proposes a method to detect money laundering activity in a cryptocurrency transaction.

3.1 Mixer Process in Cryptocurrency Transaction

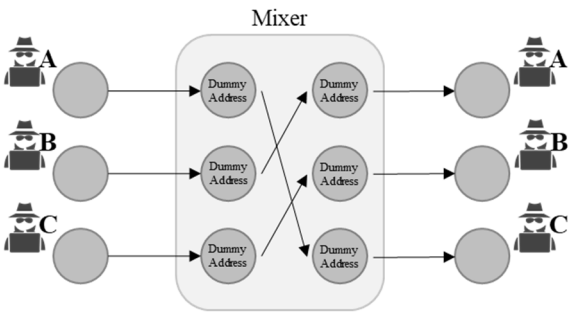

Fig. 1. The mixer process while money laundering by cryptocurrency

ML makes it hard to know which money belongs to whom and where it comes from, making it hard to track the flow of money. In ML using cryptocurrency, various shuffling services such as Bitmixer.io and Helix Mixer exist. The anonymity of the transaction is strengthened by hiding the correlation between the input and output addresses. The more the number of nodes and edges (addresses and transactions) participating in the ML, the anonymity increases. This process is called "mixer". Due to the ease of creating a new address, the mixer typically occurs as shown in Figure 1. In the figure, node represents a wallet address and edge represents a transaction. This mixer service usually leaves the same trace as the Mixer part of Figure 1, because the mixing method is not completely random. This paper proposes a method to detect money laundering by detecting such traces.

3.2 Detecting Mixer Process in Transaction Graph

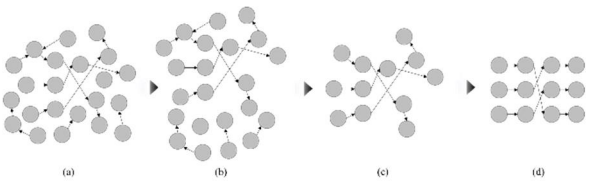

Fig. 2. Detecting mixer pattern in transaction graph

Figure 2 shows the process of finding a mixer process in a cryptocurrency transaction graph. In Figure 2, (a) is the natural state in which all the wallet addresses and transactions are represented. In the case of Bitcoin, for example, the number of known wallets exceeds 21 million. The subgraph isomorphism problem is known as NP-complete, so the smaller the graph set to search, the better detecting algorithm performs. Therefore, disconnected node sets should be separated as in (b). For the separated graphs, we can find a mixer pattern as in (c) by performing a subgraph isomorphism algorithm with (d) as a subgraph.

4 Conclusions

The UN is strengthening economic sanctions against North Korea, which has launched a ballistic missile and conducted its sixth nuclear test. North Korea secured new source of funds using cryptocurrency. In this situation, the technology that can trace how North Korea is doing money laundering is very important. This paper presents a methodology for finding the wallet address involved in money laundering in the transaction graph using the mixer pattern that appears when money launder-

ing is carried out. Future research attempts to provide a more meaningful detecting solution by linking this wallet address with the real world.

ACKNOWLEDGMENT

This work was supported by Defense Acquisition Program Administration and Agency for Defense Development under contract. (UD060048AD)

REFERENCES

[1] Brenig, Christian, Rafael Accorsi, and Günter Müller. "Economic Analysis of Cryptocurrency Backed Money Laundering." ECIS. 2015.
[2] Bååth, David, and Felix Zellhorn. "How to combat money laundering in Bitcoin? An institutional and game theoretic approach to anti-money laundering prevention measures aimed at Bitcoin." (2016).
[3] Meiklejohn, Sarah, et al. "A fistful of bitcoins: characterizing payments among men with no names." Proceedings of the 2013 conference on Internet measurement conference. ACM, 2013.
[4] Stokes, Robert. "Virtual money laundering: the case of Bitcoin and the Linden dollar." Information & Communications Technology Law 21.3 (2012): 221-236.
[5] Dostov, Victor, and Pavel Shust. "Cryptocurrencies: an unconventional challenge to the AML/CFT regulators?." Journal of Financial Crime 21.3 (2014): 249-263.
[6] Fleder, Michael, Michael S. Kester, and Sudeep Pillai. "Bitcoin transaction graph analysis." arXiv preprint arXiv:1502.01657 (2015).
[7] Ron, Dorit, and Adi Shamir. "Quantitative analysis of the full bitcoin transaction graph." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2013.

Junwoo Seo is currently a B.S student in the Department of Cyber Defense(CYDF) of Korea University since 2015. His research interests include Risk management, Cryptocurrency and Blockchain.

Kyoungmin Kim is currently a B.S student in the Department of Cyber Defense(CYDF) of Korea University since 2015. His research interests include Risk management and Blockchain.

Mookyu Park received the B.S. degrees from Sejong University in 2014, Currently he is an Ph. D student in the Center for Information Security Technologies(CIST) of Korea University since 2014. His research interests include Data minig and Risk management.

Moosung Park received the B.S. degrees from Sogang University of in 1988, M.S. degrees from Sogang University in 1990, Ph. D degrees from Kwangwoon University in 2004. Currently he works for Agency for Defense Development. His research interests include Cyber defense and Cyber sitautional awareness.

Kyungho Lee received the B.S. degrees from Sogang University of in 1989, M.S. degrees from Sogang University in 1997, Ph. D degrees from Korea University in 2009. Currently he is Associate Professor in the Department of Cyber Defense and the Center for Information Security Technologies(CIST) of Korea University. His research interests include Risk management, Information security consulting, Privacy policy and Privacy impact assessment.