28th RSEP International Conference on Economics, Finance & Business
24-25 November 2022, University of Washington Rome Center, Rome, Italy

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-73146-5-9/December 2022

Iqbal, S. & Law, K. pp.37-41

Digital Coin Laundry - Anonymizing Mechanisms that Enable the Obscuring of the Public Blockchain

Saddam Iqbal[a] & Kurtz Law[b]
[a] *Ph.D. Candidate at Babes Bolyai University, Romania*
E-mail: saddam.iqbal@econ.ubbclu.ro
[b]*Ph.D. Candidate at the Bucharest University of Economic Studies*

DOI: https://doi.org/10.19275/RSEPCONFERENCES222

Abstract

The objective of this paper is to explore methods of how cybercriminals exploit virtual assets and anonymizing tools to obliterate the chain of transactions on the publicly identified blockchain. To merely enjoy the proceeds of virtual assets obtained through illegal means such as the following: stolen funds, sanctions evaders, scams, darknet market, ransomware, child abuse material, illicit actor organization, and/or terrorism financing. Methods such as using the following technologies, mixers, decentralized platforms, privacy wallets, or all to achieve (a) lower transparency (b) higher financial privacy, and (c) higher obfuscation of financial flows. This is an ongoing study to examine the loopholes in the virtual assets, and blockchain ecosystem and propose practical solutions to minimize crime in cyberspace. This can be found beneficial to the regulated exchanges and financial watchdogs to increase surveillance of illicit activities on the blockchain and become more robust in their countermeasures against cybercrime.

Keywords: knowledge management, anti-money laundering, money laundering mechanisms
Jel codes: G21, G22, G28, G30

1. Introduction

In 2008, under the presumed pseudonym "Satoshi Nakamoto", a revolutionary decentralized electronic cash system was launched to disrupt the conventional centuries-old centralized financial monetary system (Deloitte, n.d.). It was released as an open-source software solution, allowing the sending and receiving of online payments directly without banks involvement. According to the FATF (2014) decentralized, mathematical-based virtual currencies, transact through cryptographic proof, and each transaction is protected through a digital signature using a public key, which needs to prove the ownership of the private key. Crosby, et al. (2016), identify that verification is broadcasted via a public ledger known as the blockchain where transactions are recorded with timestamps to prevent double payments or alterations of transaction records. Consequently, internet money came into existence to perform online payments which was neither dependent on a nationalized central government nor financial institutions and eliminated the so-called trusted third parties, intermediaries, a central banking system.

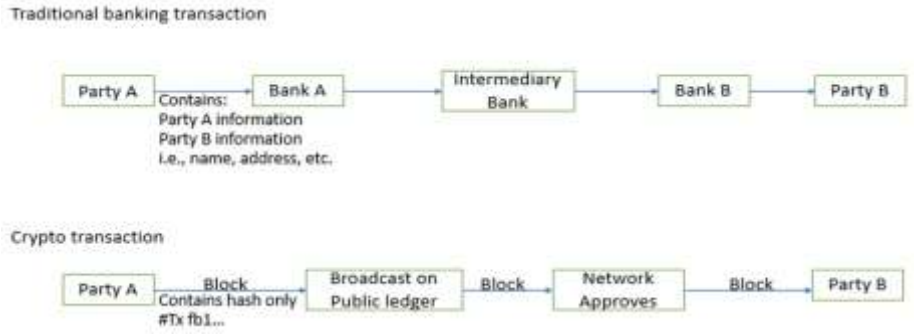

Figure 1. Traditional Banking Transaction vs Crypto Transaction

Source: Authors' Own Material

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-73146-5-9/December 2022

Iqbal, S. & Law, K. pp.37-41

2. Literature Review

While cryptocurrencies are still relatively new, technology has a tendency to evolve at a rapid pace. This seems true for human attitudes and familiarity with new technologies (Arvantis, et al. 2011). However, while cryptocurrencies have been seen as a 'new wave of the future' for payment methods, it has also created a new source of high potential tools for criminals to move and store elicit funds (FATF, 2014). This is because criminals continuously seek new ways to subvert transactions anonymously (OECD, 2019). Therefore, cryptocurrencies' strengths have become their weakness.

One of the strongest merits of cryptocurrencies has been the blockchain technology which supposedly ensures trust, transparency, security and reliability (Golosova and Romanovs, 2018). Golosova and Romanovs explain that through the blockchain, a hash is generated each time the cryptocurrency is created and changes hands. Additionally, the hash is generated automatically and is unchangeable. Therefore, as more blocks are added to the chain, the safer and more reliable the blockchain should become. Furthermore, Lin and Liao (2020) identified blockchain as a combination of cryptography and an economic model working on a peer to peer decentralized network. Nonetheless, it has been suggested that cryptocurrencies have become a popular method of transacting illicit funds by criminals and terrorist organizations (Europol, 2021; Paesano, 2021).

According to Alsalami and Zhang (2019) on the one hand, cryptocurrencies do not hide users' identities and as a result, creates a legitimate fear of unfair treatment caused by inadequate anonymity. Balthasar and Hernandez-Castro (2017) describes Bitcoin as having pseudo-anonymity as transactions are visible and traceable, but no names are stored in the blockchain. On the other hand, Sharma, et al. (2022), identify two main threat models, these being; "global passive adversaries" and "adversaries that control a subset of corrupted nodes". They suggest that these two threats enable adversaries to identify transactions originators or intermediaries using timing. Therefore, to prevent such threats requires the functionality of a mixer such as shown in the figure 2.

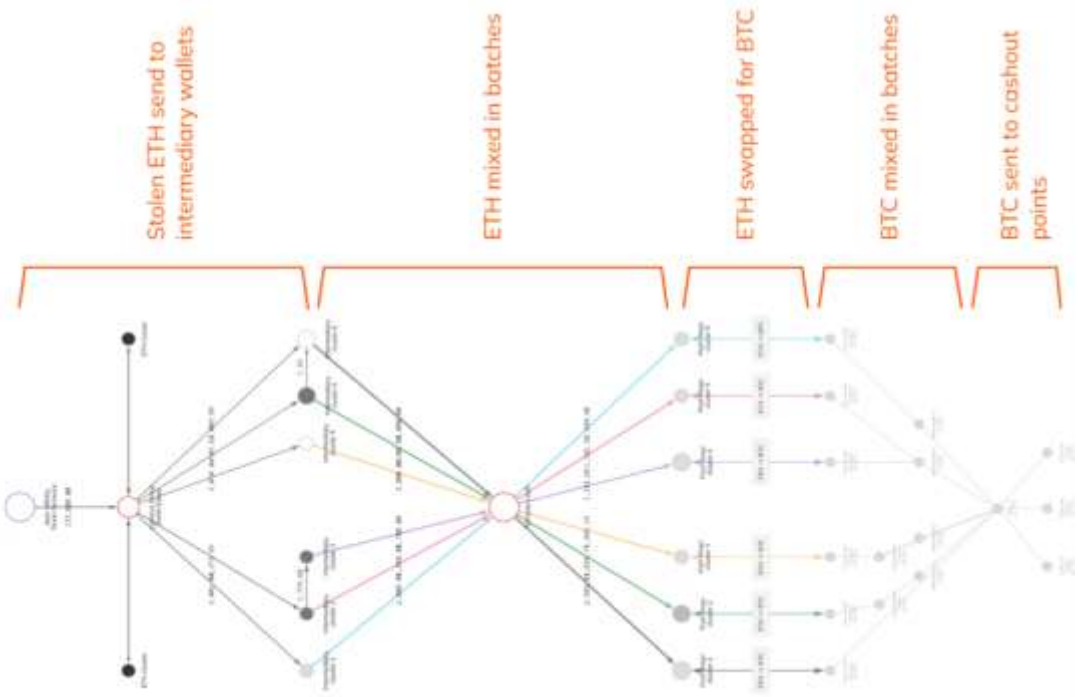

Figure 2. Example of a Mixer: Tornado Cash Mixer
Source: https://securityaffairs.co/wordpress/135524/apt/30m-stolen-axie-infinity-recovered.html

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-73146-5-9/December 2022

Iqbal, S. & Law, K. pp.37-41

While data and privacy are two rights upheld by EU treaties and in the EU Charter of Fundamental Rights, article 8 of the charter also contains an explicit right to personal data protection (European Data Protection Supervisor, 2022). It may then be argued that mixers offer a legitimate legal mechanism for people to upheld their rights to privacy by applying obfuscation techniques to prevent transactional analysis threats (Pakki, 2020). However, the Tornado Cash Mixer as shown in figure 2, was determined to have laundered more than $7 billion of virtual currency since its inception in 2019. This included more than $455 million that was stolen by the Lazarus group, a state sponsored hacking collective from the Democratic People's Republic of Korea (U.S. Department of the Treasury, 2022).

Nelson, et al. (2021), state that there is a need for an optimal combination of legal oversight, regulatory compliance, value stability, data privacy and cryptocurrency performance. Indeed, it is inferred that legitimate users of cryptocurrencies have already accepted the need for 'transparent yet private digital currencies'. The question therefore arises as to whether mixers truly have a place in the modern e-banking world, where criminals can cheaply and efficiently subvert AML functions at will.

3. Data & Methodology

This research holds to the premise that mixing of coins service enables modern money laundering schemes to occur. New technology capabilities include decentralized financing technologies such as mixers and cryptocurrency un-hosted wallets (HM Treasury, 2020; Fletcher, et al., 2021).

As a result, our primary research questions are:

1. How do anonymizing tools obliterate the chain of blockchain transactions?
2. How are suspicious cryptocurrencies sent to cash-out points?

This paper represents the early stages of an ongoing research which utilizes both third party data and a systematic review of literature. These methods were chosen to enable triangulation of data results to occur, as well as to gather a wide range of views on the topics. Advantages of a systematic review includes the ability to gain a holistic view of the subject and enables abstraction of overarching themes (Petticrew and Roberts, 2006).

A bot identifier surveillance model is proposed that enables surveillance of virtual asset service providers whether it be a mixing service provider or an exchange. This would ensure that originator identities can be verified and the beneficiaries so that all types of virtual asset service providers can implement appropriate anti-money-laundering (AML) controls and perform enhanced due diligence. The proposed mechanism is shown in figure 3.

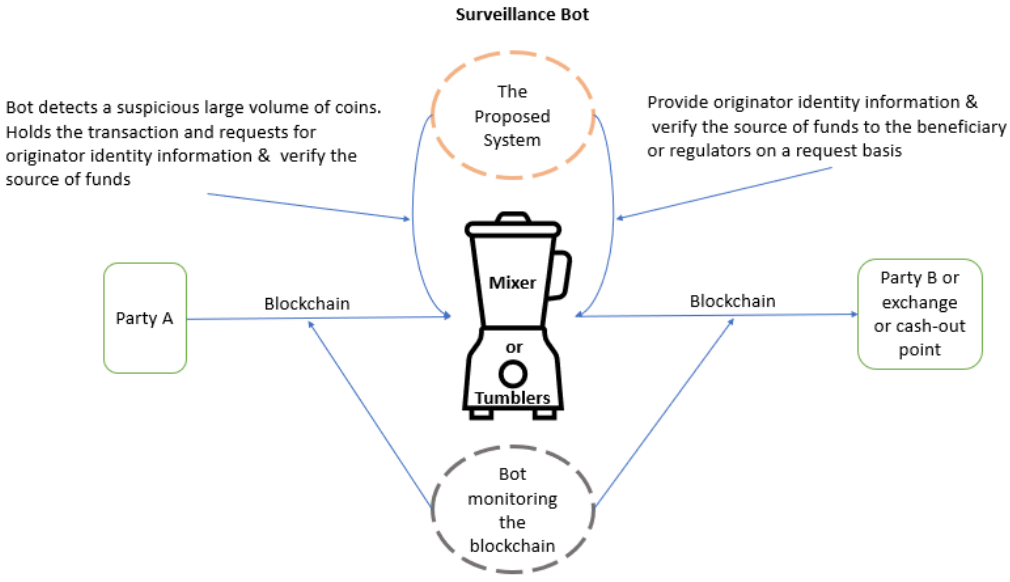

Figure 3. Proposed Surveillance Bot
Source: Authors' Own Material

4. Discussion and Findings

Some of the key issues with this mechanism include ameliorating the public sentiment as described earlier by Alsalami and Zhang (2019) and Sharma, et al. (2022), as well as handling legal concerns regarding data privacy from the EU, and the rest of the world. However, current success rate of using legal mixers by criminal organizations to transact black money into white without fear of being caught, may expedite legal reforms. Additionally, as more criminal finances continue to accumulate, more criminals will be emboldened to use this method of money laundering. Other issues include the potential for misuse or abuse of the system. Four primary mechanisms are proposed, a) suitable authority level, b) appropriate training and education of objectives and data protection methods, c) accountability and responsibility, and d) oversight by a recognized and independent AML task force. Cooperation between international AML agencies as well as interference from governments is likely to be an obstacle to the long-term sustainability of the system. Potentially, a collective task force may enable surveillance to be a solution to the issue. However, historically increased complexity of internal communication tends to lead to less efficiency with some nations obstructing others or using systems for political maneuvering. Thus, a third-party independent but trusted task force would be preferable.

Another critical issue could also be the potential malicious attack on the surveillance system itself. This may be achieved by the use of a disgruntled employee such as through physical interference, or through cybercrime. The potential for both high-profile scandals, and data leakage would be high. Further, data governance is crucial in how blockchain data will be monitored, collected, and processed. This as aforementioned will bridge cooperation between the mixers service providers and international AML agencies. As the data collected will be a valuable asset and treated as substantial evidence for compliance officers and global regulators. It must be a timely and accurate data feed that will steer the investigation direction. Lastly, cyber security since the proposed surveillance bot will be facing incoming suspicious coins by skilled hackers who would be experts in subverting cryptocurrency wallets. Weakness in cyber security can be led to non-detection by hackers.

5. Conclusions

This study represents the early findings of an ongoing study. Future endeavours will be made in constructing a prototype to investigate the efficacy of the model, as well as creating use cases for oversight protocols. A series of small focus groups with sample demographics from a) members of the general public, b) financial institutions' compliance officers and c) members of government and/or law enforcement officers will be held. The purpose of these focus groups will be to determine levels of resistance/acceptance, and perceived difficulties or solutions for them. Limitations of this study includes a need to gain access to sample demographics from other nationalities, including 3rd world countries and nations with reported higher crime rates.

Acknowledgment: This study was conducted as part of a doctoral program at the Babes Bolyai University and at the Bucharest University of Economic Studies.

References

Alsalami, N. and Zhang, B. (2019). SoK: A Study of Anonymity in Cryptocurrencies. Proceedings of the 2019 IEEE Conference on Dependable and Secure Computing. Accessed: 11/Nov/2022 from: https://ieeexplore.ieee.org/document/8937681

Arvantis, T., Williams, D., Knight, J., Baber, C., Gargalakos, M., Sotiriou, S. and Bogner, F.X. (2011). A Human Factors Study of Technology Acceptance of a Prototype Mobile Augmented Reality System for Science Education. Advanced Science Letters. Vol.4(11-12). 3342-3352.

Crosby, M., Nachiappan, N., Pattanayak, P., Verma, S. and Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. Applied Innovation Review. Issue.2. June. 2016. Accessed: 13/Nov/2022 from: http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf

Deloitte. (n.d.). Bitcoin, Blockchain & Distributed Ledgers: Caught Between Promise and Reality. Centre for the Edge. Australia. Accessed: 12/Nov/2022 from: https://www2.deloitte.com/content/dam/Deloitte/au/Images/infographics/au-deloitte-technology-bitcoin-blockchain-distributed-ledgers-180416.pdf

European Data Protection Supervisor. (2022). Data Protection. Data Protection Notice. Accessed: 15/Nov/2022 from: https://edps.europa.eu/data-protection/data-protection_en

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-73146-5-9/December 2022

Iqbal, S. & Law, K. pp.37-41

Europol. (2021). Cryptocurrencies: Tracing the Evolution of Criminal Finances. Europol Spotlight. Report Series, Publications Office of the European Union, Luxembourg.

FATF. (2014). Virtual Currencies. Key Definitions and Potential AML/CFT Risks. FATF Reports. Accessed 11/Nov/2022 from: https://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Golosova, J. and Romanovs, A. (2018). The Advantages and Disadvantages of the Blockchain Technology. Proceedings of the 2018 IEEE, 6th Workshop on Advances in Information, Electronic and Electrical Engineering. Accessed 12/Nov/2022 from: https://ieeexplore.ieee.org/document/8592253

Lin, I. C. and Liao, T.C. (2017). A Survey of Blockchain Security Issues and Challenges. International Journal of Network Security. Vol.19(5). 653-659.

Nelson, J.S., Bulkin, A., Carlson, S. and Stanley, A. (2021). Transparent yet Private Digital Currency. Sweetbridge Whitepaper. Accessed: 13/Nov/2022 from: https://sweetbridge.com/wp-content/uploads/2021/07/Sweetbridge-Whitepaper-Transparent-yet-Private-Digital-Currency.pdf

OECD. (2019). Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors. Organization for Economic Co-Operation and Development. Available at: https://www.oecd.org/tax/crime/money-laundering-and-terrorist-financing-awareness-handbook-for-tax-examiners-and-tax-auditors.pdf

Paesano, F. (2021). Cryptocurrencies and Money Laundering Investigations. Basel Institute on Governance. Quick Guide Series 01. Accessed 12/Nov/2022 from: https://baselgovernance.org/sites/default/files/2021-08/QG%20crypto%20money%20laundering%20updated.pdf

Petticrew, M. and Roberts, H. (2006). Systematic Reviews in Social Sciences: A Practical Guide. Blackwell Publishing. Available at: https://onlinelibrary.wiley.com/doi/book/10.1002/9780470754887

U.S. Department of the Treasury. (2022). U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash. August, 8, 2022. Press Release. Accessed 13/Nov/2022 from: https://home.treasury.gov/news/press-releases/jy0916