Article Review #1

Cyber Victimization & Virtual Currencies: A Social Science Review of Cryptocurrency Romance Scams

OLD DOMINION UNIVERISTY

CYSE 201S – Cybersecurity & Social Science
September 27, 2025

By: Ethan Spruill

ODU Honor pledge

"I pledge to support the Honor System of Old Dominion University. I will refrain from any form of academic dishonesty or deception, such as cheating or plagiarism. I am aware that as a member of the academic community it is my responsibility to turn in all suspected violations of the Honor Code. I will report to a hearing if summoned."

X 

INTRODUCTION

Romance scams have been on the rise employing romantic tactics to deceive victims into being vulnerable to exploiting them. Recently, cryptocurrency has also been on the rise adding even more to these scams allowing the attackers to easily launder their money through currencies like Bitcoin and Ethereum. In 2023 alone there were 65,715 cases reported of romance scams losing a total of $1179 million, making this a 75-fold increase since 2020 [1]. If nothing is done about these scams to help regulate, especially within the crypto market these losses could continue to skyrocket as perpetrators gain more advanced tactics to work with going forward. This review takes a deep dive into "Modus Operandi and Blockchain Analysis of Romance Scams: Cryptocurrency-Driven Victimization" by Amy Lim and Kyung-shick Choi in which we will assess the methods, findings, and overall implications of this study, evaluating its contents through a social sciences lens.

REVIEW

This study relates to social science principles by looking into how human behavior interacts with exploitation through romance scams. Using the 107 cases, this article presents empirical evidence to show how victims are being taken advantage of and look at it through the lens of victimization. On top of these principles, it considers the overall societal impact these scams have and how we should go about combating them to better protect those who may be more vulnerable to these attacks. Using these core systems throughout their research they can effectively apply core principles of social science.

Research Framework

Before we dive deeper into this study's methodology and results let's first look at the framework they lay out for this article. The main research question they seem to follow is, how

do offenders use cryptocurrency in romance scams, and what patterns seem to affect the victim? In this study they take an initial approach of focusing on the perpetrator's actions rather than on what the victim may be doing on a case-to-case basis, thus giving a larger pattern of what may be affecting the victim the most in these kinds of scams based on tactic. We can assume with this intent that their hypothesis is, laundering techniques done in romance scams change the amount of financial harm for the victims. This can be backed up by their primary focus on the ways in which our victims were first contacted and how they became vulnerable through these dating apps, much as seen in Table 1 within the study [1]. Based on the data they have provided their Independent Variables (IVs) seem to be the type of cryptocurrency, deception strategy, laundering technique, and the deposit method all of which are the recorded data within each case study. While on the other hand for the Dependent Variables (DVs) consist of two main measurements: (1) Individual level of monetary loss and (2) The cluster level of total monetary loss [1]. With each of these parameters laid out for us we can now begin our deeper dive into the methods and analysis conducted throughout this study.

Research Methodology & Analysis

As stated in our article the approach taken in terms of method was a mixed-methods approach combing quantitative analysis and blockchain forensic techniques [1]. We can compare these techniques to those discussed by which we can conclude these methods presented as a combination of archival research, case studies, and survey-like data. The archival research portion comes from all the quantitative data coming from records of past incidents to make up their study. Our case studies are the obvious ones as they have taken real-world scenarios and highlighted them throughout their analysis such as US v. Marfo. Lastly, in a way we are using surveys as all the data records are based on self-reported incidents therefore survey-like data will

be portrayed. Overall, as they have stated, this article presents a very multi-method approach as it combines all forms of these methods seamlessly with quantitative data and a forensic outlook. The data itself was collected from Chainabuse.com from May 2022 to October 2024, totaling 783 reported romance scams which were brought down to 107 confirmed cases [1]. This data was then analyzed by first quantitatively looking at how the different laundering techniques and amount of monetary loss were correlated in which they could determine that there were significant associations between Mixer or Tornado Cash methods and significant monetary loss for the individuals [1]. On top of this they could also conclude that cryptocurrencies with less security checks were the easiest to scam victims out of larger sums as compared to the more highly used Bitcoin and Ethereum, but with the number of individuals using those two brings their overall losses on that currency to still be incredibly high. The final analysis of their data that was conducted was using their blockchain model where they mapped out different forms of money laundering techniques and demonstrated the steps, they would follow to scam their victims including Swap, Mixer, or Tornado Crash, Peel chain, and Self-Fund as seen in their Figure 2 [1].

Making Connections

Much of this study is very easily drawn back to our coursework, for example this article presents their main premise to be based on Human Factors, much like in our slides showing the cognitive analysis and emotional need to have these relationships and fulfill their requests due to that. This study also embodies the ideas revolving around Cyberpsychology that we have discussed by focusing on why these scams are effective and conducting a forensic approach to the paths these perpetrators may take. On top of all of this it also presents the continuing idea of Victimization to point out what our victim can do to avoid and be aware of these scams before it

is too late and can learn rather than feel blamed for everything or not fix their past mistakes. Lastly, we'll look at how this all relates to marginalized groups which in our case would be elderly and those who are less experienced in the digital sphere. As these areas of marginalized groups show the most vulnerability as they don't have the right awareness to realize the true situation they are trapped in. If we can better educate these groups, they would be far less susceptible to this form of attack and be less willing to fall into this false romance when asked for large amounts of money from someone they've never met in person.

CONCLUSION

This article presents a shift in policy that needs to be addressed to combat against these laundering techniques that are occurring on many cryptocurrency sites due to their lack of regulations that are in place. With this data laid out for the public to see if we can act on this sooner than later, we can help fix this growing issue and at least subdue some of these losses by making it harder for the scammers to operate under these exchange websites. Overall, this article contributes to society by giving proper psychological insight into how these human factors lead to vulnerability of our victims to these scams and demonstrates how we should go about fixing these issues directly with policies that they believe should be enacted.

REFERENCE

[1] Lim, A. & Choi, K. (2025). Modus Operandi and Blockchain Analysis of Romance Scams: Cryptocurrency Driven Victimization. International Journal of Cybersecurity Intelligence & Cybercrime, 8(2), - . DOI: https://doi.org/10.52306/2578-3289.1220