Anonymity's Influence on Cryptocurrency Criminal Behavior

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Sam Galletta

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kent Wayland, Department of Engineering and Society

Introduction

In the Fall of 2013, the FBI seized over $3 billion worth of Bitcoin from the accounts of Ross Ulbricht, better known by his online moniker Dread Pirate Roberts (DPR). Ulbricht was the owner of a dark web marketplace known as the Silk Road, which facilitated millions of transactions of illicit goods. This was just of the tip of the iceberg of cryptocurrency related crimes. Over the past decade since the Silk Road scandal, we have seen countless headlines exposing the dark side of cryptocurrency, most recently the collapse and scandal around FTX which led to the arrest of Sam Bankman-Fried. These high-profile cases are still just a crumb of the vast iceberg of criminal uses of cryptocurrency, many of which will probably never be uncovered.

There are many properties of cryptocurrencies that make them ideal for committing illegal acts, but one that seems to be constant across some of the most popular cryptocurrencies is the untraceable and anonymous nature of transactions. Total anonymity or even just perceived anonymity can lead one to act in ways that they normally wouldn't, and often in more deviant ways. Through writing this paper, I plan to analyze how anonymity influences one's behavior and how those ideas can be applied to the use of cryptocurrency by criminals. This research could prove to be very valuable in uncovering some of the pitfalls of cryptocurrency technology and how there may need to be changes made in cryptocurrency regulations and laws.

Background

The Silk Road marketplace was founded in 2011 by Ulbricht and was a place where users were able to use Bitcoin as a payment method to hide their identities and avoid governmental

intervention. The marketplace served as a medium for users to buy and sell illegal items like stolen merchandise, forgeries, hacking devices, and most notably narcotics, which accounted for 70% of the products sold on the Silk Road. The Silk Road prohibited the sale of anything with the intent to harm or defraud including child pornography, assassinations, and weapons, but many other dark web marketplaces, inspired by the Silk Road, did not exercise these prohibitions (Christin, 2013).

The social implications of an online marketplace, like the Silk Road, backed by cryptocurrency, like Bitcoin, expand vastly across many different areas. For one, a marketplace like this makes illicit goods, especially narcotics, extremely easily accessible. With the current state of the drug market around the world and the damage it is doing to communities, easily accessible drugs via online anonymous transactions accelerates the amount of drugs going into circulation. Another social implication of crypto use for illicit transactions is the fact that cryptocurrencies are very loosely regulated by the government. With cryptocurrency only rising to popularity over the last decade or so, its novelty lends itself to its lack of regulation, allowing criminals a lot more space to operate without breaking laws (Valdeolmillos et al., 2020). The novelty of cryptocurrency also means that authoritative actors, like the FBI for example, need to formulate new techniques to discover and catch these cyber criminals. Undercover sting operations, rather than taking place in an isolated parking lot in the middle of the night, now must take place on dark web chat forums, behind a keyboard and screen.

This scandal involving DPR, the Silk Road, and Bitcoin shined the light on the darker side of crypto and exposed some of the weak points of cryptocurrency that could be exploited to aid criminal acts. The weak point that I want to focus on is the anonymous nature of crypto transactions. Little to no personal identifying factors are tied to a crypto wallet, making them

ideal for criminals who want to stay under the radar. The loss of individuality and self-awareness due to perceived or total anonymity through using cryptocurrencies can lead people to act in more deviant ways. This change in behavior is important to understand when discussing cyber-crime, as it can help provide some insight on a criminal's motives and why the sense of anonymity promotes criminal behavior. The anonymous nature of cryptocurrency transactions makes them ideal for the sale and purchase of illicit goods, as you cannot be easily identified by the government or other regulating actors.

Methods

While gathering evidence for my research, I decided that a bottom-up approach would best suit my needs. I wanted to start with the broadest aspects of my topic and methodically narrow down my research. My focus when beginning research was to gather articles that had some general information about cryptocurrency related crimes and some articles that had information about anonymization and behavior. This ensured that I would have an ample amount of background and a good understanding of some of the previous research that has been done on these topics. I then moved to narrow down my research by collecting articles pertaining to anonymity and crime. As these articles were more closely related to my research question, I will be able to more easily apply the ideas mentioned in these articles to my argument. I also found it useful to gather evidence discussing the anonymous nature of cryptocurrencies. I found it difficult to gather articles directly discussing my research topic which I found to be a good thing, meaning there is not much existing research about this topic. By applying and combining the principles discussed in the above articles that I have gathered, I will be able to synthesize an original research project and solidify my argument.

Aggressive Behavior and Anonymity

Being in a state of anonymity can lead one to behave in ways that are abnormal to their usual behaviors. Acting under the guise of an anonymous state can have some positive impacts on behavior, but it often leads individuals to act in more violent and even evil ways. When analyzing how anonymity can lead one to behave in a criminal manner, it is important to understand a phenomenon called deindividuation. Deindividuation is a theory in the realm of social psychology that suggests a loss of self-awareness can lead individuals to behave in a more deviant manner. Deindividuation can be caused by a variety of external factors such as the immersion of an individual in a group and perceived or total anonymity (Chang, 2008). Much of the existing research around deindividuation focuses on the negative effects on social behavior. Andrew Silke investigates the connection of deindividuation and anonymity in a 2003 study that focuses on violent assaults in Northern Ireland from 1994 to 1996. He compiled a database of 500 attacks during that timeframe and coded each case into a series of categories, some of which were the severity of the injuries and whether the assailant was wearing a disguise. In cases where severe physical harm was administered and where the assault was accompanied by vandalism at the scene, a higher percentage of offenders opted to hide their identity than to commit the crime undisguised (Silke, 2003). These findings suggest that individuals under the assumption of anonymity display not only a more extreme amount of aggression but also a wider variety of aggressive acts. This study supports the claims of deindividuation theory, specifically that anonymity facilitates aggression and deviant behavior.

Silke's study built on a 1969 experiment carried out by an American psychologist, Phillip Zimbardo, who also set out to explore how people would be more inclined to participate in violent or aggressive activities when their identities were hidden. A group of students was gathered where half of them would wear hoods to conceal their identities while the other half

were given name tags. Individuals from each group were instructed to administer electric shocks to other individuals. The findings showed that individuals who had their identities hidden administered shocks more frequently and for longer periods of time compared to those who were easily identifiable. This disregard for the well-being of others by the first group suggests that individuals feel almost desensitized once they are anonymous (Zimbardo, 1969). The results of this experiment, like the findings of Silke's study, supported the existing beliefs about deindividuation theory by solidifying an undeniable connection between anonymity, the loss of individual identity, and aggressive behavior.

While these two studies help clarify the connection between anonymity and aggression in a real-world setting, it is valuable to understand how the same principles could be applied to an online setting. The internet can facilitate aggressive behavior due to the variety of avenues that an assailant may take to become anonymous. Technologies like Tor, a dark web browser that allows for anonymous surfing, make concealing your online identity very simple while also making tracing one over the internet much more difficult (Woodhams et al., 2021). Even simpler, creating social media accounts under fake identities are another way for individuals to achieve a level of anonymity online. Although this way is not nearly as secure as using a browser like Tor, this amount of perceived anonymity can still affect the behavior of an individual. A prime example of how the use of online monikers can lead to aggressive behavior is cyberbullying. According to the CDC, 67% of message related cyberbullying attacks occurred through instant messaging platforms while the remaining percentages occurred through text messaging and email (CDC, 2011). This could be due to the increased level of anonymity or perceived anonymity on an IM platform as you can use a made-up username that has no ties to your personal identity like an email or phone number would (Barlett, 2015). Online anonymity can

also lead to more serious forms of malevolent behavior. Use of a dark web browser can fully abstract an individual's personal information rendering them totally anonymous and completely untraceable. This is part of the reason why we often see the dark web being used as a medium to commit serious crimes, one of which is the sexual exploitation and abuse of children. A Europol study has shown that since 2016 there has been a significant increase in not only the amount of dark web forums dedicated to child pornography, but also the amount of material exchanged on these forums. They also found that along with the increased amount of content, the material has become more extreme and violent (Europol, 2020). While these trends do not immediately suggest that the sole reason these individuals exchange child pornography is because of their online anonymity, the connection is undeniable. Perpetrators are fully aware of the untraceable nature of the dark web and understand that there is reduced amount of risk of them getting caught (Woodhams et al., 2021).

Anonymity in Cryptocurrency

Cryptocurrencies tend to be the main medium of payment for transactions that occur on dark web marketplaces. This is largely in part to the anonymous nature of transactions and untraceable crypto wallets. Even with tens of thousands of different cryptocurrencies to choose from, dark web users often opt for Bitcoin when completing illegal transactions because of its wide availability, decentralized blockchain, and anonymous network (Amarasinghe, 2019). But how anonymous is Bitcoin? Is a user completely untraceable or is it possible for somebody to follow the tracks to uncover the user's identity? To address this question, it is important to understand the difference between pseudonymity and anonymity. Data is pseudonymous when some identifying information has been removed but the data can ultimately be linked back to the subject. When data is anonymous, all identifying factors that link the subject to the data have

been completely removed. While it is widely accepted by the public that Bitcoin transactions are fully anonymous, that is actually not the case. Although Bitcoin users are identified by a public key rather than their personal information, it has been proven that Bitcoin transactions can be linked back to real world identities, making them pseudonymous. There are some known workarounds to achieve a higher level of anonymity, the most popular and simplest of them being mixing transactions of different users. By mixing the transactions of different users, the path from a transaction to a user's identity is more difficult to follow, increasing the degree of anonymity (Amarasinghe, 2019). This increased level of anonymity is highly sought after by cyber criminals, making these mixing protocols much more popular.

While anonymity through cryptocurrency is one of the ways that online attackers abstract their identity, the use of anonymous networks like Tor prove to be just as useful. Tor, the dark web browsing platform discussed previously, facilitates a variety of illegal online activities like drug trafficking, human sex trafficking, and the sale of pirated media, to name a few. The combination of participating in illegal activities in an anonymous browser while making payments through an anonymous or pseudonymous cryptocurrency seems to be the most common route for cybercriminals looking to preserve their privacy (Lee, 2019). The two work together hand in hand to help facilitate crime, and each technology would not be as successful without the help of the other. The dark web does not only serve as a place for sellers to list products and buyers to show interest anonymously, but it is also a medium for anonymous communication between the two parties. This communication is essential in the transaction process because buyers need to know the seller's Bitcoin wallet address to transfer the payment. It is crucial that the transfer of the address is done through an anonymous network otherwise it completely negates the pseudonymity of the Bitcoin, allowing the address to be easily traced

back to a name (Lee, 2019). The anonymity of cryptocurrency would also be deemed useless by cybercriminals without the help of dark web browser technology. By removing the level of anonymity that a criminal achieves with anonymous browsing, there is more room for a link to be established between the cryptocurrency address and true identity.

Discussion

While there is a distinct connection between anonymity and aggressive behavior along with anonymity tied to cryptocurrency, is it safe to say that cybercriminals do what they do because of the anonymity? It is hard to establish a singular source of causation for cybercrime, but anonymity must not be overlooked. From the studies presented above, we can confirm that there is an established notion that individuals who believe that their identity is hidden will tend to act more aggressively or violently. Silke's study showed through an analysis of real-world violent attacks that perpetrators with a higher level of anonymity committed more extreme and a wider variety of aggressive acts. Zimbardo's findings suggested similar trends in a laboratory setting. When we try to apply these same principles to the sale of illicit goods in online marketplaces using cryptocurrency, is there enough evidence to support the claim that anonymity causes this behavior online? The use of cryptocurrency provides the highest level of anonymity when compared to other forms of payment like cash or credit cards. This is because many cryptocurrencies use public keys to identify accounts and not any personal identifying information. It is definitely safe to say that the anonymity assumed from using cryptocurrencies for illegal transactions influences the criminal to act the way they do. Deindividuation theory helps support these claims by reinforcing how the loss of self-awareness through anonymization will lead people behave more aggressively and violently. By hiding their identities, criminals assume less responsibility for their actions and will tend to act in a more deviant manner, similar

to how subjects in the Zimbardo study showed that they were desensitized by administering shocks more frequently for longer periods of time. But on another note, a criminal may already be inclined to commit the crime, regardless of their identity being hidden. The motives behind criminal acts vary vastly from case to case, which is also why it is hard to generalize causation. To say that the anonymous nature of cryptocurrencies is a cause of online crime is not a long shot, but I believe that it is a topic for future research.

Conclusion

There is undeniable evidence that being anonymous influences people to behave differently, often times in negative ways. Many cryptocurrencies grant users a level of anonymity that cannot be achieved through other traditional currencies. This paper is meant to serve as the bridge between social psychology and cryptocurrency technology. By analyzing multiple social psychology studies, I was able to reinforce the theories of deindividuation. I also made it a point of importance to make it clear what degree of anonymity is achievable through the use of cryptocurrencies and what other technologies increase an online aggressor's level of anonymity. While my research serves mostly as a brief overview of the two topics and discusses the bridge across them, I think there is a lot of room for future research to be done. One route of extended research could explore if the level of anonymity achieved through using cryptocurrency has a direct correlation do online behavior, especially in dark web marketplaces. While anonymity may not be a sole cause of cybercrime because motives for crime vary case by case, there may still be some correlation that is worth exploring.

Bibliography

Amarasinghe, Niluka & Boyen, Xavier & McKague, Matthew. (2019). A Survey of Anonymity of Cryptocurrencies. ACSW 2019: Proceedings of the Australasian Computer Science Week Multiconference. 1-10. 10.1145/3290688.3290693.

Barlett, C. P. (2015). Anonymously hurting others online: The effect of anonymity on cyberbullying frequency. *Psychology of Popular Media Culture, 4*(2), 70–79. https://doi.org/10.1037/a0034335

Bray, J. (2016). *Anonymity, Cybercrime and the Connection to Cryptocurrency* (Doctoral dissertation, Eastern Kentucky University).

Center for Disease Control. (2011). Electronic aggression: Emerging adolescent health issue. Retrieved from http://www.cdc.gov/features/electronicaggression/.

Chang, J.K. (2008). The Role of Anonymity in Deindividuated Behavior : A Comparison of Deindividuation Theory and the Social Identity Model of Deindividuation Effects (SIDE).

Christin, N. (2013, May). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international conference on World Wide Web* (pp. 213-224).

Europol, (2020). Exploiting isolation: Offenders and victims of online child sexual abuse during the Covid-19 pandemic. The Hague: Europol.

Lee, Seunghyeon & Yoon, Changhoon & Kang, Heedo & Kim, Yeonkeun & Kim, Yongdae & Han, Dongsu & Son, Sooel & Seungwon, Shin. (2019). Cybercriminal Minds: An

investigative study of cryptocurrency abuses in the Dark Web. Network and Distributed Systems Security (NDSS) Symposium 2019 24-27 February 2019, San Diego

Silke A. (2003). Deindividuation, anonymity, and violence: findings from Northern Ireland. *The Journal of social psychology*, *143*(4), 493–499. https://doi.org/10.1080/00224540309598458

Valdeolmillos, D., Mezquita, Y., González-Briones, A., Prieto, J., Corchado, J.M. (2020). Blockchain Technology: A Review of the Current Challenges of Cryptocurrency. In: Prieto, J., Das, A., Ferretti, S., Pinto, A., Corchado, J. (eds) Blockchain and Applications. BLOCKCHAIN 2019. Advances in Intelligent Systems and Computing, vol 1010 . Springer, Cham.

Woodhams, J., Kloess, J. A., Jose, B., & Hamilton-Giachritsis, C. E. (2021). Characteristics and Behaviors of Anonymous Users of Dark Web Platforms Suspected of Child Sexual Offenses. *Frontiers in psychology*, *12*, 623668. https://doi.org/10.3389/fpsyg.2021.623668

Zimbardo, P. G. (1969). The human choice: Individuation, reason, and order versus deindividuation, impulse, and chaos. *Nebraska Symposium on Motivation*, *17*, 237–307.