# DETECTING ILLICIT CRYPTOCURRENCY MINING

## GOVERNMENT RESPONCES TO CRYPTOCURRENCIES' EFFECTS ON CRIME AND CYBERCRIME

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Joseph Davidson

November 1, 2021

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.

ADVISORS

Catherine Baritaud, Department of Engineering and Society

Daniel Graham, Rosanne Vrugtman, Department of Computer Science

As recently as the summer of 2021 the US witnessed one of the most disruptive cyberattacks in history. The Colonial Pipeline, which transports huge volumes of gas and jet fuel to the Southeast, was shut down due to a ransomware attack that demanded cryptocurrency as payment (Turton & Mehrotra, 2021). This is just one of many increasingly common examples of cyberattacks using cryptocurrencies as a convenient means of receiving ransoms or financial benefit. In other instances, white-collar crime becomes more attractive when cryptocurrencies are involved due to their increased anonymity (Braaten et al., 2019). It has become apparent that cryptocurrencies are and continue to become an important component of modern cybercrime. In addition, they are being used in sophisticated ways in many different types of attacks, both as a source of ransom and as a direct target of attacks.

Cybersecurity has become increasingly important to the physical infrastructure and political stability of our world. Additionally, cryptocurrencies are poised to continue to play a greater role in the cyberattacks that will happen in the years to come. Understanding the complex interplay between these two systems is therefore critical to mitigating the negative impacts of cryptocurrencies. The dynamic impacts of cryptocurrencies on cybersecurity provide much of the motivation for this research.

The technical portion of this research is a state-of-the-art paper that focuses on methods for detecting illicit cryptocurrency mining with a focus on machine learning methods of detection. The technical portion, therefore, is a synthesis of concepts from CS 4630 – Defense Against the Dark Arts and CS 4774 – Machine Learning. Additionally, the technical portion will explore the various benefits of different types of detection, from machine learning and decision tree-based approaches to more simplistic malware fragment analysis.

The STS portion of this research will focus on how cryptocurrencies are broadly affecting cybercrime and what different government responses have been to these developments. Specifically, to complete the STS portion of this research Actor Network Theory, developed by Latour (2005), will be used to analyze the relationships between governments and a variety of cryptocurrency users. Additionally, this research will examine the various approaches that different governments, including the United States, the European Union and China, have taken in responding to cryptocurrencies.

The technical and STS portions of this research are tightly coupled together with both portions hoping to improve the information available on how cryptocurrencies interact with cybercrime. Additionally, both portions seek to better understand the complex factors that influence these systems and means of mitigating the negative side effects of cryptocurrencies. The work for this research will be carried out in the 2022 spring semester at the University of Virginia, School of Engineering and Applied Science.

## DETECTING ILLICIT CRYPTOCURRENCY MINING

As cryptocurrencies have become more valuable and widely used, they have increasingly become the target of cyberattacks, whether as a source of ransom or directly being mined from a host computer (Konoth et al. 2018). In particular, cryptojacking, when bad actors use a victim's computer processing power without permission to mine for cryptocurrencies, has become widespread. A basic depiction of cryptojacking and its costs can be seen in Figure 1. The figure shows the outlines of what occurs whenever cryptojacking takes place by depicting the interactions between a cybercriminal and a victim. When cryptojacking occurs "there are real costs associated with extra energy use, sluggish performance, and even failures of equipment due

to heavy use" (Leithauser, 2019).

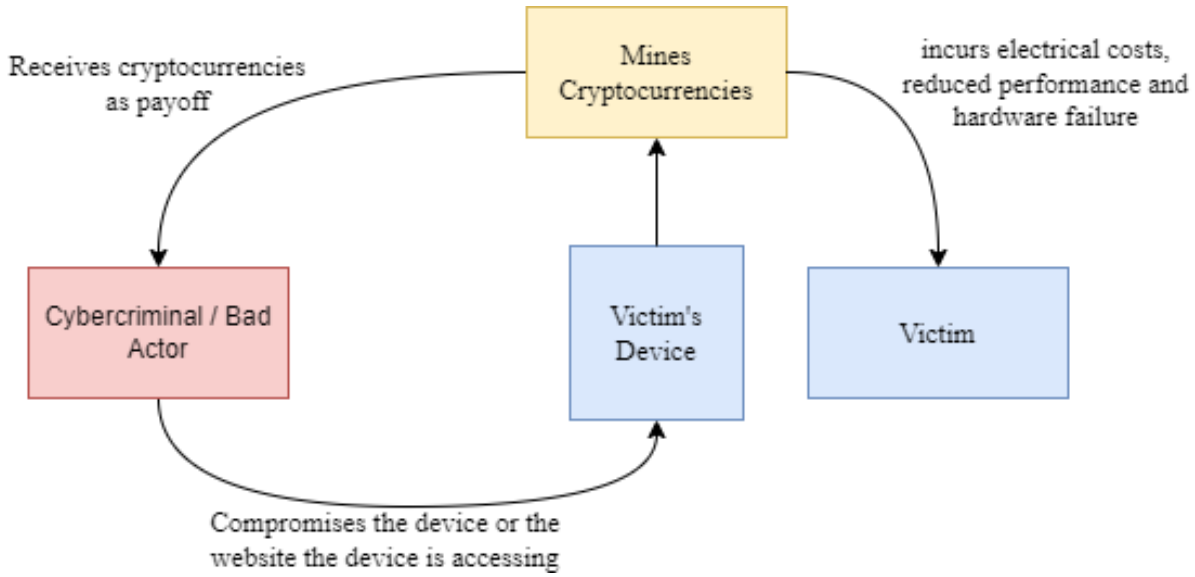


Figure 1: What is Cryptojacking? This diagram shows the basic outlines of cryptojacking on the broadest conceptual level. Showing how the cybercriminal gains the benefits while the victim is burdened with all the costs. (Created by Joseph Davidson (2021)).

All of these costs compound greatly when it is considered how common these attacks have become. In the first quarter of 2021, cryptojacking reportedly increased by over four times from the last quarter and with some four hundred thousand users reportedly having an encounter with cryptojacking (BI India Bureau, 2021).

The objective of the technical portion of the research is to develop an understanding of the wide-range of various approaches that have been created in order to detect cryptojacking, with a focus on machine learning approaches. There are several different ways that currently exist to detect cryptojacking in a variety of circumstances. One of the most common ways of identifying malware uses fragment analysis, this is also a very common approach for detecting cryptojacking (Romano et al., 2020). While this method cannot identify all variations of these attacks it serves as a good baseline to build on. In addition to fragment analysis there are machine learning approaches (Handaya et al. 2020). There are approaches that analysis

WebSocket payloads to detect potential communication between attackers and a victim's device (Saad et al., 2019). Additionally, there are methods that focus on behavior-based decision tree analysis in order to identify the common patterns of cryptojacking (Tanana et al., 2020).

Cryptojacking detection is important for a variety of reasons. Primarily, this is important because detection is the first step needed to create defenses against cryptojacking. Without the ability to discriminate between malware and normal software, users are unable to prevent malware from being executed on their devices. Furthermore, due to the difficulty of casually identifying when cryptojacking is occurring, it is necessary to possess a reliable set of methods to automatically detect and prevent this type of malware. In addition to the need for automatic detection, these detection methods need to be robust enough to handle large changes in the approach that cryptojackers use. As an example, when CoinHive, a cryptocurrency mining API, was shut down in March of 2019 many mining operations significantly changed the code they use to cryptojack, resulting in some detection methods no longer functioning properly (Varlioglu, 2020). Additionally, understanding methods for detecting this form of cybercrime will make future detections easier for a variety of cyber-attacks.

The technical portion of this research will create a synthesis of cybersecurity and machine learning in the form of a state-of-the-art report on the different methods that have and are being developed to detect when cryptojacking occurs. This will be in the form of a scholarly review article, which seeks to summarize and evaluate a collection of research from other published scholarly sources. The anticipated outcome is a report that consolidates the various methods of detection into a single comparative document that also seeks to understand each methods' strengths and weaknesses with an increased focus on machine learning applications.

## GOVERNMENT RESPONCES TO CRYPTOCURRENCIES' EFFECTS ON CRIME AND CYBERCRIME

Cryptocurrencies are taking up an increasingly prominent role in certain types of crime. In one example, hackers used an infected piece of software to mine for cryptocurrency on government websites (Finkle et al., 2018). As mentioned at the beginning of this prospectus, the Colonial Pipeline was shut down due to a ransomware attack that demanded cryptocurrency as payment, showing that cryptocurrency related cybercrime can have huge impacts on the economy (Turton & Mehrotra, 2021).

In more traditional crime, cryptocurrencies have also become an attractive tool that is being used in a variety of situations. In some cases, white-collar crime becomes more common and attractive when cryptocurrencies are involved. This trend seems to be due to, in large part, the increased anonymity that cryptocurrencies provide (Braaten et al., 2019). Additionally, cryptocurrencies have been used as a new and efficient way to launder money. Some estimates put the amount laundered in 2018 at close to $1.5 billion (Crosman, 2018). In the past several years cryptocurrencies have become increasingly prominent in cybercrime and traditional crime. These examples help to show that cryptocurrencies have and are being used in significant ways to promote illegal activities and these show the significant need to better understanding the role that cryptocurrencies play in crime.

The objective of this research is to identity and understand the different considerations related to government actions and regulations in regard to cryptocurrencies. Additionally, a major objective is to understand how cryptocurrencies have impacted cybercrime and more traditional crimes.

The general approach this research will take is to analyze the various human and non-human actors in the system by using Actor Network Theory (Latour, 2005). Some of the complex roles that cryptocurrencies play can be seen in Figure 2. This figure shows, generally, how governments are attempting to balance a variety of considerations when making determinations on how to regulate and treat cryptocurrencies. Governments must balance the desire for economic growth with the clear lack of oversight that cryptocurrencies afford to their users.

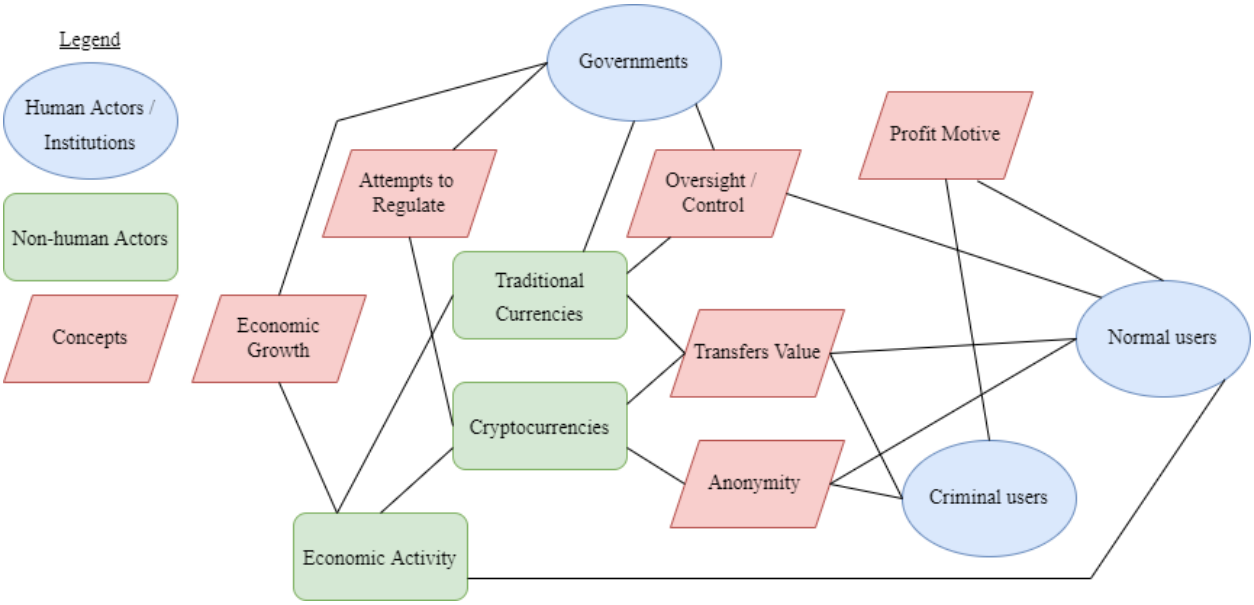


Figure 2 - Actor Network Theory for Cryptocurrencies and Governments. This figure shows the basic relationships that contextualize the place cryptocurrencies have in the economy and the motivations of human actors from governments to criminal and normal users. (Created by Joseph Davidson (2021)).

The ANT diagram in Figure 2 also helps to illustrate how the desires of criminal users and normal users are remarkably similar. Both type of users in general desire the greater anonymity that cryptocurrencies provide, as well as their decentralized nature. In addition to this, both groups of users need cryptocurrencies to transfer value in order for them to be useful. These two

aspects together provide the ability for criminal users to launder money and collect ransoms more effectively with cryptocurrencies.

Figure 3 helps to illustrate why cryptocurrencies are a desirable choice for criminals to use. As shown cryptocurrencies allow for relatively anonymous transactions, they provide an easy method of laundering the funds and there is minimal government oversight. All of these factors help to make cryptocurrencies a useful tool for illicit activity.

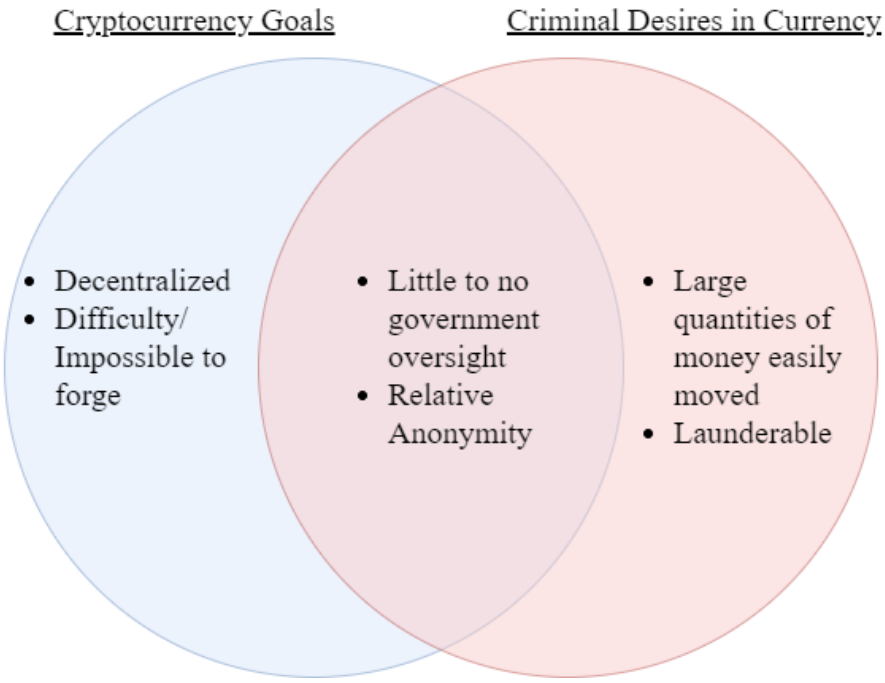


Figure 3 - Cryptocurrency Goals vs Criminal Desires in Currency. This diagram shows the overlapping goals and desires that make cryptocurrencies appealing to criminals. (Created by Joseph Davidson (2021)).

The use of cryptocurrencies in illegal ways has not gone unnoticed by governments. In many US states, legislation exists or has been purposed in an attempt to bring crypto currencies more generally under the supervision and regulation of governments (Morton, 2021). In addition to these efforts at regulation, the European Commission has proposed legislation that would seek to ensure that cryptocurrency transactions are traceable within the European Union (Jones, 2021).

These new regulations seek to eliminate the anonymity of cryptocurrencies, which would substantially reduce their ability to be used for laundering and ransoms. The United States federal government has also increased efforts to mitigate the negative impacts of cryptocurrency related cybercrime. Recently, the US Department of Justice seized $2.3 million worth of Bitcoin from the group responsible for the Colonial Pipeline attack (Department of Justice, 2021). Beyond planned or concrete government action there have been increasing calls for governments to do even more to reign in cryptocurrencies. In some cases, there have been calls for stiffer regulation and potentially the crippling or elimination of cryptocurrencies altogether (Rosenzweig, 2021). In China regulators have done exactly this and banned all transactions using and the mining of cryptocurrencies (John, 2021). These examples help to show that governments have and are planning on responding in a diverse number of ways to manage the impacts of cryptocurrencies on the economy and society.

This STS topic, will examine research on how cryptocurrencies are influencing cybersecurity. Additionally, this work will seek to understand how a variety of governments are responding to and seeking to regulate cryptocurrencies. Primarily focusing on the United States and European Union. The goal of this work is to better understand the approaches being used to mitigate the negative impacts of cryptocurrencies and how they differ between regions.

## CRYPTOCURRENCIES - A DYNAMIC FRONT IN CYBERSECURITY

Cybersecurity is one of the vital pillars of security in our world today. A system cannot be secure if it does not take cybersecurity carefully into consideration. Cryptocurrencies are poised to continue to play a greater role in the cyber-attacks that will happen in the years to come. This means that cryptocurrencies have become a vitally important factor to understand and

ensure robust cybersecurity. Understanding how cryptocurrencies impact these various systems will be necessary in order to appropriately respond. Additionally, it is vital to understand the various approaches that are currently being used or are proposed to manage and mitigate the negative effects of cryptocurrencies. Overall, this research hopes to consider both the technical and societal factors that are at play in cryptocurrencies and their impacts on government and cybersecurity. This will be done by examining technical means of mitigating cryptojacking, such as machine learning methods, and by studying the societal and governmental responses to cryptocurrencies and their impacts.

## REFERENCES


BI India Bureau. (2021, June 8). Cryptojacking scams are on the rise once again, after declining for two years. https://www.businessinsider.in/cryptocurrency/news/cryptojacking-scams-are-on-the-rise-once-again-after-declining-for-two-years/articleshow/83335965.cms

Braaten, C. N., & Vaughn, M. S. (2019). Convenience theory of cryptocurrency crime: A content analysis of U.S. federal court decisions. *Deviant Behavior*, *42*(8), 958–978. https://doi.org/10.1080/01639625.2019.1706706

Crosman, P. (2018). Crypto money laundering up threefold in 2018: Report. *American Banker, 183*(128), 1.

Davidson, J. (2021). *Actor network theory diagram for cryptocurrencies and governments*. [Figure 2]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Davidson, J. (2021). *Cryptocurrency goals vs criminal desires in currency.* [Figure 3]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Davidson, J. (2021). *What is cryptojacking?* [Figure 1]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Department of Justice. (2021, June 7). *Department of justice seizes $2.3 million in cryptocurrency paid to the ransomware extortionists Darkside*. https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

Finkle, J., Hosenball, M., & Wallis, D. (2018). Thousands of U.K. and U.S. websites infected with cryto-mining malware. *CIO (13284045)*, 4.

Handaya, W. B. T., Yusoff M. N., Jantan A. (2020). Machine learning approach for detection of fileless cryptocurrency mining malware. *Journal of Physics: Conference Series, 1450*.

Jones, H. (2021, July 20). *EU to tighten rules on cryptoasset transfers*. Reuters. https://www.reuters.com/technology/eu-tighten-rules-cryptoasset-transfers-2021-07-20/

John, A., Shen, S., & Wilson, T. (2021, September 27). *China's top regulators ban crypto trading and mining, sending bitcoin tumbling*. Reuters. https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/

Konoth, R. K., Vineti, E., Moonsamy, V., Lindorfer, M., Kruegel, C., Bos, H., & Vigna, G. (2018). MineSweeper: an in-depth look into drive-by cryptocurrency mining and its defense. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. Published. https://doi.org/10.1145/3243734.3243858

Latour, B. (2005). Reassembling the social: An introduction to the actor-network theory. Oxford, England: Oxford University Press.

Leithauser, T. (2019). Report: 2M cyber incidents caused $45B in losses in 2018. *Cybersecurity Policy Report*. Published. https://www.proquest.com/advancedtechaerospace/docview/2266935077/3B2E0F02C38D4340PQ/1?accountid=14678

Morton, H. (2021, May 14). *Cryptocurrency 2021 Legislation*. National Conference of State Legislatures. https://www.ncsl.org/research/financial-services-and-commerce/cryptocurrency-2021-legislation.aspx

Romano, A., Zheng, Y., & Wang, W. (2020). MinerRay. Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering. Published. https://doi.org/10.1145/3324884.3416580

Rosenzweig, P. (2021, August 31). Opinion | There's a better way to stop ransomware attacks. *The New York Times.* https://www.nytimes.com/2021/08/31/opinion/ransomware-bitcoin-cybersecurity.html

Saad, M., Khormali, A., & Mohaisen, A. (2019). Dine and dash: Static, dynamic, and economic analysis of in-browser cryptojacking. 2019 APWG Symposium on Electronic Crime Research (ECrime). Published. https://doi.org/10.1109/ecrime47957.2019.9037576

Tanana, D., & Tanana, G. (2020). Advanced behavior-based technique for cryptojacking malware detection. 14th International Conference on Signal Processing and Communication Systems (ICSPCS). Published. https://doi.org/10.1109/icspcs50536.2020.9310048

Turton, W., & Mehrotra, K. (2021, June 4). *Hackers breached colonial pipeline using compromised password*. Bloomberg. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Varlioglu, S., Gonen, B., Ozer, M., & Bastug, M. (2020). Is cryptojacking dead after coinhive shutdown? *2020 3rd International Conference on Information and Computer Technologies (ICICT)*. Published. https://doi.org/10.1109/icict50521.2020.00068