GOVERNMENT RESPONSES TO CRYPTOCURRENCIES' EFFECTS ON CYBERCRIME

A Research Paper submitted to the Department of Engineering and Society
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By

Joseph Davidson

March 28, 2022

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
Catherine D. Baritaud, Department of Engineering and Society

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 perceived 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. Professor Daniel Graham served as the advisor for the technical portion of this research. The STS portion of this research, with Catherine Baritaud as an advisor, is a review of government policies related to cryptocurrencies. Additionally, this research seeks to identify the broad categories of government responses to these developments. Specifically, to complete the STS portion of this research Actor Network Theory, developed by Latour (2005), is used to analyze the relationships between governments and a variety of

cryptocurrency users. Additionally, Actor Network Theory is used to analyze the motivations behind different government actions and responses. Using this STS framework and prospective in this research will allow for a more meaning understanding of how the different actors are impacting the complex sociotechnical system being developed around 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 cryptocurrencies, cybersecurity, and the institutions and organization involved in them. Finally, both portions of research are looking at means of mitigating the negative side effects of cryptocurrencies; one from a technical prospective and the other from a social (i.e. policy) prospective.

GOVERNMENT RESPONCES TO CRYPTOCURRENCIES' EFFECTS ON 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, 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).

Before government responses to cryptocurrency can be fully understood, it is important to consider why criminals and cybercriminals might use cryptocurrencies over traditional means of exchange. One important caveat before continuing discussing cryptocurrencies as a whole is

that not all of them operate within the exact same design specifications. While the majority of main-stream cryptocurrencies follow Bitcoin's pseudo-anonymity as discussed by Alsalami et al. (2019), some relatively niche cryptocurrencies, such a Zcash, employ different means of cryptography that generally seek to enhance anonymity (Silfversten, 2020). These factors create different considerations when discussing their use and government actions in response. All this being said, Bitcoin and Ethereum, the two most popular cryptocurrencies by market share, make up nearly two-thirds of the total value of all cryptocurrencies and both have a similar cryptographic strategy (Chinchalkar, 2021). With this in mind, for the remainder of this research paper when referring to cryptocurrencies it may be assumed that Bitcoin and those closely related to it cryptographically are being discussed.

APPEAL OF CRYPTOCURRENCIES FOR CRIMINAL ACTIVITY

Even though cryptocurrencies were not designed as a tool for criminal activity, they have become a popular means of extracting ransoms and facilitating other illegal activities (Myre, 2021). Figure 1 on page 4 helps to illustrate why cryptocurrencies are a desirable choice for criminals to use. As shown, cryptocurrencies allow for relatively anonymous transactions, although not completely as will be discussed later in this paper. Additionally, they provide an easy method of laundering funds and there is minimal government oversight when compared to traditional currencies. All of these factors help to make cryptocurrencies a useful tool for illicit activity.

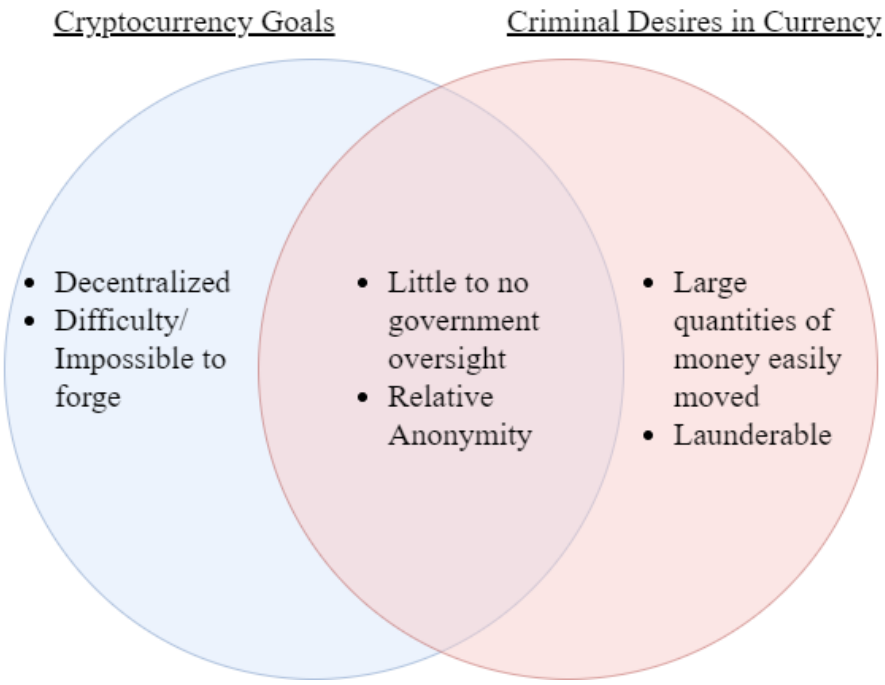

Figure 1. Cryptocurrency Goals vs Criminal Desires in Currency. This diagram shows the overlapping goals and desires that make cryptocurrencies appealing to criminals. (Created by Davidson (2021)).

Anonymity of Cryptocurrencies

While the views on Bitcoin and other cryptocurrencies' anonymity differ among various users, there is a substantial segment that greatly value and believe that Bitcoin is anonymous (Ghesmati, 2022). In many ways cryptocurrencies are anonymous. Transactions use wallet addresses, which are alpha-numeric sequences, instead of names and accounts. Additionally, every transaction can use a new public and private key, as is recommended by cryptocurrency enthusiasts. Even with these measures, when cryptocurrencies are converted into traditional fiat currencies ownership can be more easily established and the chain of transactions can be more easily traced (Galston, 2021).

One common means of increasing the anonymity of cryptocurrencies is to employ a technology / service known as a mixer (Tran et al., 2018). These mixers function by collecting a

large number of transactions and ‘mixing’ up which coins go to which individuals. This process allows the transfer of cryptocurrencies from one account to another to be preformed in a manner similar to a direct transaction, while also breaking the chain of traceability and obfuscating payments.

Limited Government Oversight

In addition to the anonymity that cryptocurrencies provide over traditional currencies, they also have substantially less inherent government oversight and control. This is often an appealing feature for legitimate uses and illegitimate ones. Whereas traditional fiat currencies are directly managed by governments through their monetary policy and central banks, cryptocurrencies are not managed by any central authority. This separation from government control is certainly not complete and there are many factors that governments can impact and control even with the decentralized model of cryptocurrencies.

Domains of Cryptocurrency's Use in Crime

In addition to their use in ransoms, cryptocurrencies appear prominently in a variety of other crimes. The Cryptocurrency Enforcement Framework, authored by the Office of the Deputy Attorney General’s Cyber-Digital Task Force (2020), lays out a large number of different crimes and illicit activities that have used cryptocurrencies since their creation. Specifically, the framework lists three major categories of illicit uses that pertain to cryptocurrencies.

The first major category consists of using cryptocurrencies to facilitate or acquire illegal goods or activities, such as purchasing illicit drugs or funding terrorism. The next major category includes using cryptocurrencies for tax evasion and to launder money. Cryptocurrencies have been used as an efficient means for laundering money. Some estimates put the amount laundered in 2018 at close to $1.5 billion (Crosman, 2018). Additionally, in some cases white-collar crime

becomes more common and attractive when cryptocurrencies are involved (Braaten et al., 2019). Finally, the framework includes crimes directly related to cryptocurrencies, such as theft of cryptocurrencies from exchanges, illegally mining cryptocurrencies on an unauthorized device, and their use in ransoms.

CURRENT AND PLANNED REGUALATIONS

The use of cryptocurrencies in illicit ways has not gone unnoticed by governments. In many US states, legislation exists or has been purposed in an attempt to bring cryptocurrencies 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).

Enforcement of Existing Laws

In addition to any new regulations that are being proposed and implemented, many governments are using their existing framework of laws to mitigate and punish criminal activity. For example, many US laws that apply to traditional fiat currency also have been applied to cryptocurrencies. Often this is due to the deliberately constructed language of these pieces of legislation allowing them to be broad enough to adapt to new financial situations. In the Cryptocurrency Enforcement Framework, the US Department of Justice (2020) lays out the various laws and regulatory bodies that currently have authority to enforce cryptocurrency related laws and regulations. Broadly, the US DOJ lays out the current laws and policies that it has previously used to prosecute criminal behavior and misuse of cryptocurrencies. Of these the DOJ focuses on two main categories. The first of these are the laws related to using

cryptocurrencies to facilitate other illegal activities, like purchasing drugs or other contraband. The second major category focuses on regulating exchanges, banks, and other financial structures that can facilitate money laundering or the obfuscation of digital funds.

A recent example of this type of enforcement can be seen in the US Department of Justice seizing $2.3 million worth of Bitcoin from the group responsible for the Colonial Pipeline attack (Department of Justice, 2021). Likewise, the Department of Justice seized over $4.5 billion worth of Bitcoin in early 2022 that was initially stolen in 2016 and was being laundered (Benner, 2022). In other instances the US has shut down exchanges and mixing services that did not meet required record keeping standards and arrested their operators (FinCEN, 2020).

Beyond the United States, the European Union is also using existing laws and regulations in order to curtail some of the negative impacts that cryptocurrencies have had in promoting and facilitating crime. For some aspects of cryptocurrency regulation the European Union has been relying on their existing suite of anti-money laundering/combating the financing of terrorism (AML/CFT) regulations and directives (Bąkowski, 2021). This strategy is similar to that of the United States. Additionally, the EU is applying some of the regulatory practices that were designed for post-trading activities and securities markets in order to provide some framework for regulation to cryptocurrency trading (European Securities and Markets Authority, 2017).

In both of these cases, the United States and European Union have been attempting to bring some degree of regulation to cryptocurrencies and the markets that trade and exchange them. However, in many ways the current application of these laws, laws that were not written with cryptocurrencies and digital-assets in mind, has been somewhat cumbersome and incomplete. In response to this difficulty there are currently initiatives in a several governments

under way to create new laws and regulations that will fill in the gaps of those currently in place and tailor them specifically to the needs of cryptocurrencies.

Establishment of New Regulations and Laws

While many of these new regulations and laws have yet to be formally written and passed, the broad outlines for them have been established. In the United States the White House and Congress have both been working to create the next generation of laws and regulations to more fully integrate cryptocurrencies and digital assets into the current economic and financial framework. The US Congress has not yet settled on a single approach for how to move forward with legislation to update these regulations. In 2021 alone over thirty bills were introduced into congress relating to cryptocurrency regulation (Brett, 2021). In addition to congressional action, the White House (2022) released an executive order seeking to create a more unified interagency response to cryptocurrencies and cryptocurrency related crimes. This executive order also calls for increased scrutiny in how digital assets can help to facilitate cybercrimes with a focus on finding additional ways to mitigate these effects.

The European Union is also pushing to adopt additional legislation to fill in the gaps in regulatory information. In a recent press release the European Commission (2021) described the updated versions of their AML/CFT rules. These new rules seek to create a more robust system for ensuring digital assets in particular are not being used in illicit ways that compromise the safety of society. Many of these efforts to update and reform regulations and guidelines have been in line with the standards of the Financial Action Task Force, an intergovernmental standard creating body that focuses on financial crimes.

Other Approaches to Cryptocurrencies

Beyond seeking to regulate and manage the use of cryptocurrencies and digital assets, some governments have gone further to the point of banning almost all use of cryptocurrencies within their nations. The most prominent example of banning or severally restricting cryptocurrencies comes from China. After years of increasing restrictions, the People's Bank of China effectively banned all use of cryptocurrencies within China (BBC News, 2021). While China may be the largest economy to place a ban on cryptocurrencies, it certainly is not the only one. Over forty nations have effectively banned or severely restricted cryptocurrencies within their borders, often by limiting how banks are able to interact with the digital assets and by disallowing exchanges from being established (Quiroz-Gutierrez, 2022).

Impacts of Government Enforcement and Regulation

While some government actions, such as China's ban on cryptocurrency transactions and mining, have temporarily reduced the appeal of cryptocurrencies, most current regulatory and enforcement actions do not seem to have the same effect (John, 2021). There are voices that have called for even stricter regulations as a means of bringing cryptocurrencies inline with more traditional financial markets (Rosenzweig, 2021). As it stands, most of the regulations in place today primarily seek to prevent cryptocurrencies from being used as a tool for criminal activities while in most cases maintaining their usefulness within the economy. The next generation of laws and regulations seems to aim less at preventing criminal acts and is more focused on implementing consumer and investor protections.

USING ACTOR NETWORK THEORY TO ANALYZE GOVERNMENT MOTIVATIONS

In order to understand the motivations and complex factors that exist within the cryptocurrency space, it is important to analyze the various human and non-human actors in the system by using Actor Network Theory (ANT) (Latour, 2005). In this way, ANT reveals how the actors associated with cryptocurrencies' use and their regulation are interrelated to each other. Additionally as Figure 2 shows, each actor within the network has many connections to a variety of other actors that are often opposing and complexly interwoven themselves. This figure shows 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 activity and growth with the clear lack of oversight that cryptocurrencies afford to their users.

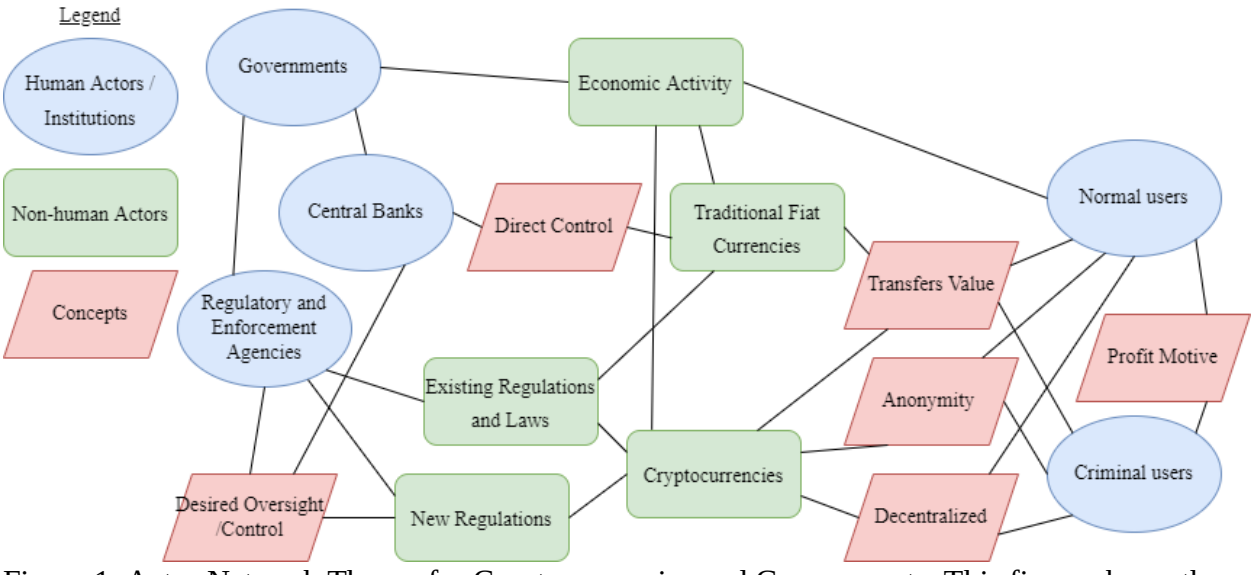

Figure 1. Actor Network Theory for Cryptocurrencies and Governments. This figure shows the basic relationships that contextualize the place cryptocurrencies have in the economy and the motivations of human actors from governments to criminal and normal users. (Created by Davidson (2022)).

Furthermore, any attempt to alter the fundamental principles of cryptocurrencies, such as their anonymity and decentralized structure, through regulations or other government policies would potentially negatively impact legitimate use even while mitigating criminal use. Figure 2 on the previous page helps to show this by displaying the shared features that normal users and criminal users both value in cryptocurrencies.

In places like the United States and European Union, where governments have primarily sought to curtail any criminal activity related to cryptocurrencies and digital assets, there has been a stronger emphasis on balance between economic stability and technical innovation. Up to this point, many government regulations and resources have been devoted to reducing the ability of criminals to use cryptocurrencies as an easy means of money laundering and other criminal acts. In a recently released executive order from the White House (2022), the President stated that it was in the United States' interest to pursue the potential benefits that cryptocurrencies and their surrounding technology could provide, while also seeking to minimize or eliminate the negative impacts. Similarly, in Europe regulators have sought to pursue laws and practices that prevent the issues that digital assets create, while still allowing the technology to develop in hopes of reaping the benefits of it (European Securities and Markets Authority, 2017).

In the examples of the US and the EU it is clear that these governments have recognized the potential benefits this relatively new technology could provide to economic activity and efficiency. Therefore, these governments are seeking to let cryptocurrencies develop in hopes of realizing those potiential benefits. That being said, they also have a very clear incentive to prevent illicit use of cryptocurrencies and eliminate this type of use to the best of their abilities.

In stark contrast to the US and the EU are countries which have actually or effectively banned cryptocurrencies altogether. China being the largest example of this. While it is difficult

to make generalizations about such a large group of nations, over forty have issued these types of restrictions and bans; the motivating reasons for most of these nations seems to be a great desire for continued control of monetary resources. There is also the obvious fact that without access to cryptocurrencies it is much more difficult if not impossible to use them for money laundering and other criminal activities.

In the end, what governments choose to do about cryptocurrencies and their affects on the economy and cybercrime can largely be traced to the balance between desired control of critical economic factors and the desire for innovation and the economic growth. Which path different governments have taken can largely be informed by their general attitudes toward maintaining control within their nations. While virtually all national governments require some degree of control over monetary policy and other economic aspects, some are significantly more willing to allow their citizens additional autonomy.

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. In this context 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. In addition to the potential threats that cryptocurrencies present, they also present potential benefits to the efficiency and accessibility of economic resources throughout a society.

GOVERNMENT ACTION

Overall, governments have been responsive to cryptocurrencies and their impacts in the economic and cybersecurity arenas. Through a variety of actions, including regulations and enforcement, governments have sought to eliminate or mitigate the negative impacts of these digital currencies. Additionally, some governments have taken the step of effectively banning the use and production of cryptocurrencies within their borders. Often times the motivations that shape a particular government's actions are complex, but by using Actor Network Theory these motivations can become more apparent. Generally, these choices come down to a balance between government control and economic and technical benefits to society.

FUTURE WORK

While there is a large amount of information regarding government regulations and actions in response to cryptocurrencies, these actions are still in flux and will almost certainly change in the coming years. It is therefore important that this research and similar research like it be revisited as governments continue to change their approaches to managing this ongoing situation.

Additionally, it would be beneficial for future work in this area to look more into the costs and benefits of each individual type of government action to identify which are most appropriate. Beyond that, it could be beneficial for work to explore nongovernmental means of solving cryptocurrencies' problems as they relate to cybercrime.

REFERENCES

Alsalami, N., & Zhang, B. (2019). SoK: A systematic study of anonymity in cryptocurrencies. *2019 IEEE Conference on Dependable and Secure Computing (DSC)*. https://doi.org/10.1109/dsc47296.2019.8937681

Bąkowski, P. (2021, December). *Proposal for a regulation to fight money laundering and counter terrorist financing*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698862/EPRS_BRI(2021)698862_EN.pdf

China declares all crypto-currency transactions illegal. (2021, September 24). BBC News. https://www.bbc.com/news/technology-58678907

Benner, K. (2022, February 9). Justice Dept. Seizes $3.6 billion in bitcoin and arrests married couple. *The New York Times*. https://www.nytimes.com/2022/02/08/us/politics/ilya-lichtenstein-heather-morgan-bitcoin-laundering.html?searchResultPosition=1

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

Brett, J. (2021, December 29). *In 2021, congress has introduced 35 bills focused on U.S. crypto policy*. Forbes. https://www.forbes.com/sites/jasonbrett/2021/12/27/in-2021-congress-has-introduced-35-bills-focused-on-us-crypto-policy/?sh=7a48b468c9e8

Chinchalkar, A. (2021, December 20). *Crypto barrels toward 2022 after adding $1.5 trillion in value*. Bloomberg. https://www.bloomberg.com/news/articles/2021-12-20/cryptocurrencies-and-bitcoin-btc-2021-year-in-charts

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

Davidson, J. (2022). *Actor network theory diagram for cryptocurrencies and governments*. [Figure 2]. *STS Research Paper:* Government responsese to cryptocurrencies' effects on cybercrime (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 1]. *STS Research Paper:* Government responsese to cryptocurrencies' effects on cybercrime (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

European Commission. (2021, June 20). *Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3690

European Securities and Markets Authority. (2017, February). *Report: The distributed ledger technology applied to securities markets*. https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf

FinCEN. (2020, October). *First bitcoin "mixer" penalized by FinCEN for violating anti-money laundering laws*. https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws

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

Galston, E. (2021, June 16). *Untraceable bitcoin is a myth*. WSJ. https://www.wsj.com/articles/untraceable-bitcoin-is-a-myth-11623860828

Ghesmati, S., Fdhila, W., & Weippl, E. R. (2022). User-perceived privacy in blockchain. *Coordination of Decentralized Finance 2022*. https://eprint.iacr.org/2022/287.pdf

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/

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/

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

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

Myre, G. (2021, June 10). *How bitcoin has fueled ransomware attacks*. NPR. https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks

Quiroz-Gutierrez, M. (2022, January 5). Crypto is fully banned in China and 8 other countries. *Fortune*. https://fortune.com/2022/01/04/crypto-banned-china-other-countries/

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

Silfversten, E., Favaro, M., Slapakova, L., Ishikawa, S., Liu, J., & Salas, A. (2020). *Exploring the use of zcash cryptocurrency for illicit or criminal purposes*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR4400/RR4418/RAND_RR4418.pdf

The White House. (2022, March). Executive order on ensuring responsible development of digital assets. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/

Tran, M., Luu, L., Kang, M. S., Bentov, I., & Saxena, P. (2018). Obscuro. *Proceedings of the 34th Annual Computer Security Applications Conference*. https://doi.org/10.1145/3274694.3274750

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

United States Department of Justice, Office of the Deputy Attorney General, Cyber-Digital Task Force. (2020, October). *Cryptocurrency enforcement framework: Report of the attorney general's cyber digital task force*. https://www.justice.gov/cryptoreport