laws

MDPI

Article

Cryptocurrencies as a Threat to U.S. Homeland Security Interests

Austen D. Givens

School of Business and Justice Studies, Utica University, Utica, NY 13502, USA; adgivens@utica.edu

Abstract: The use of cryptocurrencies in transnational criminal activities has grown in recent years. The scholarly literature on cryptocurrencies recognizes this trend. Yet, there has been comparatively little attention paid to the degree to which cryptocurrencies pose a direct threat to U.S. homeland security interests. This article fills a gap in the scholarly literature on cryptocurrencies by presenting evidence that cryptocurrencies are a threat to U.S. homeland security interests, specifically because of their uses for financing terrorism, enabling human and drug trafficking, and evading international financial sanctions.

Keywords: cryptocurrency; homeland security; terrorism; trafficking; sanctions

1. Introduction

North Korea is subject to United Nations financial sanctions designed to curtail North Korea's nuclear and ballistic missile programs since 2006 (Nichols 2024). These sanctions prohibit U.N. member states from trading arms with North Korea and freeze the assets of those associated with North Korea's nuclear program (Council on Foreign Relations 2022). But according to U.N. monitors, in March 2024 North Korea laundered some $147.5 million dollars through a virtual currency platform called Tornado Cash (Nichols 2024). Tornado Cash is a cryptocurrency mixer whose purpose is to obfuscate the source and destination of funds. Using hackers to steal cryptocurrency from virtual currency exchanges, then laundering the stolen cryptocurrency, offers North Korea a way to circumvent the effect of United Nations sanctions to obtain financing for its nuclear and ballistic missile programs (ONDI 2024, p. 22).

Cryptocurrencies are a type of digital money (Giudici et al. 2020, p. 8). While the notion of digital money is not new, cryptocurrencies first emerged in their modern form with the creation of Bitcoin in 2009 (Dwyer 2015). A second cryptocurrency called Ethereum was created in 2015, and with it, the notion of self-executing financial contracts involving Ethereum that require no outside intervention (Liang et al. 2018).

Cryptocurrencies have become popular because of numerous features. Since they are digital, they have the potential to reach the unbanked who may live in remote areas without ready access to financial institutions. They may also yield gains as investment vehicles. They are de-centralized, in that their issuance and circulation is not controlled by a single entity, such as a government. To generate new cryptocurrency, individuals must use computers to solve complex mathematical equations in a process dubbed "mining" (Tredinnick 2019, p. 40). All transactions, including transfers of ownership, involving cryptocurrencies are recorded in a public ledger, known as a blockchain (Giudici et al. 2020, p. 3).

Cryptocurrencies also have privacy features. The identities of parties in the blockchain are pseudonymous, meaning that while the parties' virtual identities may be public, their true identities can remain hidden (Jaffe 2022). The blockchain itself is de-centralized,

check for updates

Academic Editors: Kyung-Shick Choi and Patricia Easteal

Received: 31 July 2024
Revised: 10 December 2024
Accepted: 23 December 2024
Published: 29 December 2024

Citation: Givens, Austen D. 2025. Cryptocurrencies as a Threat to U.S. Homeland Security Interests. *Laws* 14: 2. https://doi.org/10.3390/laws14010002

making it virtually impossible for an unauthorized third party to alter records about cryptocurrency transactions (Giudici et al. 2020, p. 3; Tredinnick 2019, p. 42). When cryptocurrencies are moved, such as via the sale of a fixed good, cryptocurrencies transfer from one digital wallet to another, and the transaction is recorded in the blockchain (Tredinnick 2019, p. 42).

In bypassing U.N. sanctions via cryptocurrency use, North Korea can continue to pay for the development of nuclear weapons and ballistic missiles. This activity directly endangers two of North Korea's neighbors—Japan and South Korea—which are vulnerable to North Korean missile attacks. And this activity also poses risks to the United States. In particular, North Korea's development of hypersonic ballistic missiles, which are designed to evade missile defense systems, presents a direct threat to the U.S. homeland (ONDI 2024, p. 22). North Korea exploits cryptocurrencies to threaten U.S. homeland security, which this article defines as the whole-of-society effort to protect the U.S. homeland from dangerous people and things, and to facilitate the recovery from the effects of these dangerous people and things when they cause harm inside the United States (Givens et al. 2018, p. 2).

There are good reasons to examine the risks that cryptocurrencies pose to U.S. homeland security in particular, as opposed to the security interests of a different individual state or a collection of nations. As one of the world's leading superpowers, the domestic security measures taken in the United States can have ripple effects upon those of other countries. The U.S. homeland security threat environment is increasingly understood by scholars as international in scale, despite the domestic-sounding focus (Givens et al. 2018). Researchers have been interested in U.S. homeland security for many years, to the point of creating refereed journals such as *Homeland Security Affairs* and the *Journal of Homeland Security and Emergency Management*. In addition, cryptocurrencies are the subject of growing U.S. legal and regulatory scrutiny, meaning that the policy milieu surrounding cryptocurrencies in the United States is ever-changing.

Funding the development of hypersonic ballistic missiles is not the only way that cryptocurrencies can pose a threat to U.S. homeland security. Cryptocurrencies facilitate transnational criminal transactions. Human trafficking, for example, can be accomplished through the use of Bitcoin or Ethereum on Dark Web marketplaces (Kethineni and Cao 2020). Drug trafficking, particularly through the purchase of narcotics via the Dark Web, is also facilitated through the use of cryptocurrencies (Kethineni and Cao 2020). Financing drug trafficking in this way can directly harm drug consumers located inside the United States. Terrorist groups like Hamas and the Islamic State of Iraq and Syria (ISIS) have accepted donations in cryptocurrency, demonstrating the possibilities that cryptocurrencies create for the evasion of international financial sanctions (Rosen et al. 2023; PBS News 2023). It is also the case that ducking sanctions in this way creates a means through which terrorist organizations might be able to pay for and execute attacks on the U.S. homeland.

Despite mounting public evidence that the use of cryptocurrencies can pose a threat to U.S. homeland security, the scholarly literature on illicit uses of cryptocurrencies tends to focus mostly on the role of cryptocurrencies in transnational criminal transactions. For example, Kethineni and Cao (2020) highlight the fact that the growth in popularity of cryptocurrencies has come with a corresponding rise in the use of cryptocurrencies for activities like human trafficking and the movement of narcotics. Gundur et al. (2021), in a global survey of criminal transaction methods, note that cryptocurrencies can make an ideal vehicle for money laundering.

Scholars have paid comparatively little attention to cryptocurrencies as a U.S. homeland security problem, however. In one of the few papers on cryptocurrencies and national security, George (2018) notes that cryptocurrencies can be leveraged to fund lone wolf-style terrorist attacks and permits regimes in countries like Iran and North Korea to evade

sanctions (pp. 9–10). He does not, however, describe cryptocurrencies as a homeland security challenge, nor does he analyze in detail the extent to which cryptocurrencies can be leveraged to engage in activities like human trafficking. One report notes that malicious actors can exploit the under-developed regulatory regime for cryptocurrencies to create safe havens for transnational criminal organizations (Gold and McBride 2019, pp. 35–36). Like George, however, this report does not frame cryptocurrencies as a homeland security issue.

In a graduate thesis on the subject, Frebowitz (2018) is perhaps the only researcher to assert that cryptocurrencies have become a homeland security concern (p. 4). He notes that multiple scholars have identified the terrorism–Bitcoin nexus, wherein terrorists raise funds via cryptocurrencies, as evidence of the degree to which cryptocurrencies have become a homeland security issue (Frebowitz 2018, pp. 6–7). Crucially, however, while Frebowitz describes cryptocurrencies as a homeland security issue, he does so on the grounds that the unregulated nature of cryptocurrencies limits nations' abilities to enforce homeland security policies, not as a homeland security threat *per se* (Frebowitz 2018, p. 90). He also cautions that there is disagreement among scholars about the extent to which terrorists' use of cryptocurrencies to raise funds has become mainstream (Frebowitz 2018, pp. 7–8).

This article argues that cryptocurrencies have become a threat to U.S. homeland security specifically because of their use to finance terrorism and facilitate drug and human trafficking, as well as to fund rogue regimes. In advancing this argument, this article synthesizes the existing scholarship on cryptocurrencies used within transnational criminal transactions as well as the much smaller body of literature on cryptocurrencies and national security.

The fact that cryptocurrencies represent a homeland security threat does not mean that their global use needs to be restricted in some way, however. Many investors, for instance, buy cryptocurrency in the hope of amassing financial returns, which is a perfectly legitimate activity. Others rely on cryptocurrencies as a store of value for business transactions. Still others accrue cryptocurrency precisely because of its pseudonymous quality, valuing the fact that it exists beyond the reach of banking and financial regulators. Yet, by recognizing cryptocurrencies as a threat to U.S. homeland security interests, policymakers can design appropriate measures to address their use and abuse by terrorists, traffickers, and rogue states.

Of particular relevance to this article is convenience theory, first posited by Petter Gottschalk in 2017, which in the context of criminal behavior refers to time and effort savings (p. 3). Transaction costs are lowered through convenience, but the likelihood of one being caught increases. Gottschalk underlines that convenience is linked with the three primary dimensions of white-collar crime—illegal financial gain, organizational ease in hiding illegal transactions, and the justification of illegal behavior (Gottschalk 2017, p. 4).

Convenience theory is integral to understanding cryptocurrencies as a threat to homeland security as defined in this article. The saving of time and effort achieved through the use of cryptocurrencies facilitates terrorism, human and drug trafficking, as well as the funding of rogue regimes hostile to the United States.

The first part of this article provides background material on cryptocurrencies, highlighting the ways that cryptocurrencies function as well as how they can be exploited to harm U.S. homeland security. The second part of this article explores in depth how terrorists can leverage cryptocurrencies to plan and execute terrorist attacks. The third part of this article describes how cryptocurrencies are used to facilitate human and drug trafficking. The fourth part of this article examines how rogue regimes use cryptocurrencies to raise money. The final part of this article summarizes the article's findings and provides suggestions for future research in this area.

2. Cryptocurrencies: A Short Primer on Their Appeal

Cryptocurrencies' value is dictated by market conditions. Put simply, cryptocurrency is worth whatever a buyer believes it to be worth, reflecting any number of input variables, including, for example, the value of mining itself, or speculation. And cryptocurrencies are notoriously volatile, making them a fickle store of value (Tredinnick 2019, p. 39).

Malicious actors can use cryptocurrencies in myriad ways to harm U.S. homeland security interests. For example, because they are not controlled by governments, terrorist organizations may use cryptocurrencies to finance the planning of attacks. Human smugglers can employ cryptocurrencies to facilitate payments among themselves or between themselves and clients, evading detection by bank authorities and compromising border security in the process. Narcotics traffickers can leverage cryptocurrencies to move money between the production and shipping ends of their operations, endangering lives inside the United States. Rogue regimes, such as Iran and North Korea, can also use cryptocurrencies to launder the proceeds of ill-gotten money. These are not all the ways that cryptocurrencies can pose a threat to U.S. homeland security, but they are among the ways that have the most direct connection to U.S. homeland security concerns.

3. Terrorism

Terrorism refers to the use of violence or threats of violence against primarily civilian targets to achieve a political or social goal (Ganor 2002, p. 288). A universally accepted definition of terrorism remains elusive, though terrorism itself has been defined many times (Ramsay 2015, p. 2). In conceptualizing terrorism, this article envisions actions like those carried out by organizations such as Hezbollah, Hamas, and Al-Qaeda, three groups designated as terrorists by the U.S. Department of State (DOS n.d.). Countering terrorism remains, at the time of the writing, one of the U.S. Department of Homeland Security's top priorities (Department of Homeland Security 2023). Activities which facilitate terrorist attacks, therefore, necessarily qualify as homeland security threats.

Planning and executing terrorist attacks requires money. Funds are necessary to finance the procurement of materials that can be used to construct bombs, for example. Moving would-be terrorists from place to place requires money for transportation, food, and lodging, not unlike the expenses associated with a typical business. The 9/11 Commission estimated that the 11 September 2001 terrorist attacks cost between $400,000 and $500,000 to execute (National Commission 2004). The expenses associated with the 9/11 terrorist attacks included the costs of visas and passports, as well as transportation to the United States (National Commission 2004).

However, there are extensive measures in place to detect the movement of illicit terrorist funds. As one scholar notes, the post-9/11 effort to counter terrorist financing has been among the most successful counterterrorism initiatives (Clunan 2006, p. 569). U.S. regulatory and reporting requirements around suspicious transactions are one way that terrorist financing is interdicted (Clunan 2006, p. 585). There is a broad international consensus on the need to thwart terrorist financing (Malakoutikhah 2020, p. 5). These domestic and international measures raise the risk of terrorists being detected in their efforts to move money to support terrorist operations. There is a natural incentive for terrorists to seek alternate means to move money to support their operations. Cryptocurrencies provide such an avenue, and they do so while lowering the time and effort required to move money vis-à-vis more conventional financing methods, which is consistent with Gottschalk's convenience theory.

Leveraging cryptocurrencies to direct funds toward the planning and execution of terrorist attacks is one way that cryptocurrencies can present a threat to U.S. homeland security (Lee and Choi 2021, pp. 364–65). There are two primary means through which

terrorists or would-be terrorists can employ cryptocurrencies. The first is fundraising (Clunan 2006, p. 570). This type of activity can be used to raise money for propaganda, such as that of the terrorist organization ISIS (Mahood and Rane 2016, pp. 25–26). It can also be used to carry out operations, as in the 9/11 terrorist attacks (Clunan 2006, p. 570). Moreover, cryptocurrency fundraising can leveraged for training, such as the construction of improvised explosive devices (IEDs) (Clunan 2006, p. 570).

There is evidence that terrorists have employed cryptocurrencies in precisely this manner. Following the 7 October 2023 attack by Hamas on Israel, the U.S. Treasury Department sanctioned a Gaza-based virtual currency exchange (Rosen et al. 2023, p. 1). Perhaps more significantly, the Department entered into a multibillion dollar settlement with Binance, a cryptocurrency firm, for Binance's failure to report dealings with terrorist organizations (Rosen et al. 2023, p. 1). These efforts follow a flurry of activity 2020 by the U.S. Department of Justice to seize the cryptocurrency assets of multiple terrorist organizations, including Al-Qaeda and ISIS (Department of Justice 2020a). These actions demonstrate that terrorist activity using cryptocurrencies is more than merely a theoretical concern. Terrorist organizations have used cryptocurrencies to advance their goals.

4. Human and Drug Trafficking

Human trafficking refers to the "use of force, fraud, or coercion to obtain some type of labor or commercial sex act" (Department of Homeland Security 2022b). Drug trafficking means the movement of illicit narcotics as part of the larger cycle of drugs, involving their cultivation, production, and consumption (Jenner 2013, p. 65). In each case, this article refers to the illegal forms of these activities; the voluntary movement of individuals across state lines for labor does not qualify as human trafficking, nor does the correct use of prescription medication under direct medical supervision qualify as drug trafficking. Combatting human and drug trafficking is a high operational priority for the U.S. Department of Homeland Security (Department of Homeland Security 2024).

Both human and drug traffickers require funding. Yet, there are numerous legal and regulatory mechanisms in place to combat the flow of money. As of 2020, the U.S. Department of the Treasury had identified some 20 financial and behavioral indicators of human trafficking that it shared in a supplemental advisory document with corporate executives and managers (Department of the Treasury 2020, p. 2). These indicators include the use of front companies or third parties who insist on being physically present for every aspect of a business transaction (Department of the Treasury 2020, pp. 3, 6). An extensive list of federal laws protects human trafficking victims and punishes human traffickers (Department of Homeland Security 2022a). The U.S. Department of Homeland Security has a dedicated Center for Countering Human Trafficking (Department of Homeland Security 2024). The list of legal barriers to human trafficking, therefore, is extensive.

Efforts to combat the flow of illegal drugs into the United States have been underway since at least the early 1970s, costing more than a trillion dollars (Crandall 2020, p. 3). These efforts include the work of U.S. Customs and Border Patrol agents (CBP), which is a component agency of the U.S. Department of Homeland Security, at U.S. borders to seize drug shipments. They include efforts to stem the tide of money to which narcotics traffickers must have access in order do business. The Anti-Drug Abuse Act of 1988, for instance, prohibits financial institutions from issuing checks or money orders greater than $3000 without first obtaining proper identification and verifying account ownership (U.S. Congress n.d.). Much more recently, in 2021, President Biden signed an Executive Order authorizing the Secretary of the Treasury to impose sanctions on anyone involved in providing substantial financial, material, or technological support in support of the narcotics trade (Biden 2021).

Narcotics and human traffickers, however, have clever ways of circumventing these restrictions on the movement of their money. Perhaps the most prevalent method is laundering money, that is, intentionally concealing the source of funds and converting it through mixing processes into currency that is viewed as legitimate in origin (Alasmari 2012, pp. 139–40). By converting funds in this way, traffickers can continue their trade. But, as noted above, a thicket of laws and regulations and executive orders is designed to impede traffickers and to detect money laundering (DeFeo 1990). This means that narcotics and human traffickers have incentives to turn to alternate methods to continue moving money and plying their respective trades.

Because cryptocurrencies exist mostly beyond the reach of financial industry regulators, cryptocurrencies offer a way for human and narco-traffickers to transfer funds from digital wallet to digital wallet without detection. In line with convenience theory, human and drug traffickers have turned to alternative measures like cryptocurrencies to lower the transaction costs of moving their money. While it is true that the U.S. Department of Justice has taken enforcement action against cryptocurrency exchanges and even shut down Dark Web sites peddling drugs and human beings, the fact remains that cryptocurrency is an attractive financial vehicle for malicious actors (Department of Justice 2020b, pp. 5–6; Devon 2023; Department of Justice 2022). For example, a U.S. Government Accountability Office report from 2021 indicated that 15 of 27 online sex marketplaces studied accepted virtual currency (Government Accountability Office 2021a, p. 23). The use of other methods to increase the anonymity of cryptocurrency, such as coin mixers that obfuscate the origins of cryptocurrenices, also demonstrates that cryptocurrencies remain attractive for human and narcotics traffickers (Government Accountability Office 2021b, pp. 69–74).

5. Rogue Regimes

A rogue state is a country that engages in erratic behavior, subjugates its population, is hostile to the free world, and breaches established international rules and norms in many areas (Becker 2005, p. ix). It may also pursue the development of weapons of mass destruction (WMD) (Becker 2005, p. ix). There is evidence that rogue regimes hostile to the United States, such as Iran and North Korea, have used cryptocurrencies to launder money to evade international sanctions and further their own interests. In this way, their actions demonstrate convenience theory at work, for the use of these alternative means provides a clearer path to move money without detection, ultimately lowering transaction costs. Because these regimes directly and indirectly menace the United States, this activity represents a homeland security threat.

Iran is subject to a battery of U.S. financial sanctions designed to prevent it from developing nuclear weapons (Thomas 2023, p. 1). These take the form of primary sanctions, which target U.S. persons and entities, as well as secondary sanctions, which focus upon non-U.S. persons (Thomas 2023, p. 1). Iran is also a U.S.-designated state sponsor of terrorism and has backed groups, such as Hezbollah, which have directly attacked U.S. interests (Department of State 2020). There is evidence that the government of Iran has actively promoted cryptocurrency mining as a way to raise money (Reuters 2021). This is somewhat understandable, a this creates a path for the regime effectively to evade sanctions, which have had devastating effects on the Iranian economy. This activity has even been promoted openly by the Iranian government to prevent capital flight and encourage investment in the country's currency, the rial (Gholipour 2021).

North Korea, too, is the target of an array of U.S. sanctions to prevent the development of nuclear weapons and ballistic missiles (Manyin and Nikitin 2024, p. 2). There exist United Nations sanctions with the same aims (Council on Foreign Relations 2022). The potential development of these weapons is not a theoretical concern. Between 2006 and 2017, North

Korea tested six nuclear devices and launched scores of ballistic missiles (Manyin and Nikitin 2024, p. 2). But North Korea, like Iran, has learned that cryptocurrencies can be used to evade these sanctions. Scholars at the Belfer Center for Science and International Affairs at Harvard University note that North Korea stole some $250 million in cryptocurrency in 2018 via the Lazarus Group, a hacking organization (Kim et al. 2022, p. 2). Estimates of North Korean gains from cryptocurrency theft are upwards of several hundred million dollars (Kim et al. 2022, pp. 3–4). The regime allegedly also engages in cryptomining and cryptojacking, a practice that involves using malicious software to hijack computers and secretly use them to mine cryptocurrency (Kim et al. 2022, pp. 5–7). Combined with its cyberwarfare capabilities, the portrait that emerges is of a North Korean state that possesses forbidable cyber prowess (Hwang and Choi 2021, p. 5).

These actions by Iran and North Korea demonstrate that their respective regimes are using cryptocurrency to avoid the consequences of international financial sanctions whose purpose is to deter their production of nuclear weapons and ballistic missiles. Because the proliferation of these weapons constitutes a threat to U.S. homeland security, and their proliferation is at least partially funded through cryptocurrency, we can understand cryptocurrencies themselves to be a homeland security threat.

6. Conclusions and Recommendations

This article advanced the novel argument that cryptocurrencies today constitute a threat to U.S. homeland security and that Gottschalk's convenience theory is integral to understanding cryptocurrencies as a homeland security threat. There is evidence that cryptocurrencies have been used to fund terrorist activity. Cryptocurrency helps to finance the trafficking of narcotics and human beings. Digital currencies are also being used, at least in part, to fund the weapons proliferation activities of rogue regimes like those of Iran and North Korea.

To address the threat that cryptocurrencies pose to U.S. homeland security interests, it is necessary to balance the efforts to monitor their use with the need for continuing the free and open exchange of cryptocurrencies for legitimate, lawful reasons. At present, the U.S. Securities and Exchange Commission (SEC) is the chief federal regulatory body with responsibility for the cryptocurrency market. A tighter degree of integration between the SEC and homeland security-focused agencies such as the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), and the Department of Homeland Security would be a logical, achievable policy response to the recognition that cryptocurrencies threaten homeland security interests. Moreover, greater collaboration between cryptocurrency exchanges and federal law enforcement officials—specifically with a view to interdicting illegal activity that threatens homeland security interests—would be a natural step to take. However, it must be acknowledged that such a measure could meet resistance from cryptocurrency exchange leaders who may bristle at the prospect of coordinating with law enforcement agencies. Nonetheless, prior research has demonstrated that such public-private sector partnerships can yield important outcomes in the homeland security sphere, suggesting that cooperation in this area is realistic and achievable, too (Busch and Givens 2014).

Additional measures that could further bolster protection against bad actors using cryptocurrencies to threaten U.S. homeland security interests include strengthening incident response policies (Hwang and Choi 2021, pp. 20–21). If organizations become aware that cryptocurrencies are being used to facilitate activities like terrorism, escalatory measures, which involve notifying federal homeland security agencies and not just the SEC, would be helpful for overall situational awareness. Furthermore, law enforcement officials can

buttress deterrence policies by aggressively investigating and prosecuting crimes which involve the utilization of cryptocurrencies (Lee and Choi 2021, pp. 378–79).

Future research on this topic could focus upon ancillary areas of homeland security in which cryptocurrencies also play a role, with a view to informing policy decisions. For example, to what extent does cryptocurrency fund attempts at visa fraud? Knowing this information could help investigators to reduce the amount of visa fraud that occurs each year. Is there a place for cryptocurrency in disaster recovery funding, and if so, could it be used in some way to defraud the United States? Policymakers would do well to examine this issue, given the proliferation of natural disasters that takes place annually in the United States. Other lines of inquiry could explore the traceability of cryptocurrencies. Because convenience is integral to their use by malicious actors, the development of tools to trace cryptocurrency transactions makes it more likely that their use will be reduced. As cryptocurrency use continues to proliferate, these and similar questions will need to be explored.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The author declares no conflicts of interest.

References

Alasmari, Khaled A. A. 2012. Cleaning up Dirty Money: The Illegal Narcotics Trade and Money Laundering. *Economics & Sociology* 5: 139–48.

Becker, Jasper. 2005. *Rogue Regime: Kim Jong Il and the Looming Threat of North Korea*. Oxford: Oxford University Press.

Biden, Joseph Robinette. 2021. Executive order on Imposing Sanctions on Foreign Persons Involved in the Global Illicit Drug Trade. December 15. Available online: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/15/executive-order-on-imposing-sanctions-on-foreign-persons-involved-in-the-global-illicit-drug-trade/ (accessed on 29 July 2024).

Busch, Nathan E., and Austen D. Givens. 2014. *The Business of Counterterrorism: Public-Private Partnerships in Homeland Security*. New York: Peter Lang.

Clunan, Anne. 2006. The Fight against Terrorist Financing. *Political Science Quarterly* 121: 569–96. [CrossRef]

Council on Foreign Relations. 2022. What to Know About Sanctions on North Korea. July 27. Available online: https://www.cfr.org/backgrounder/north-korea-sanctions-un-nuclear-weapons (accessed on 27 December 2024).

Crandall, Russell. 2020. *Drugs and Thugs: The History and Future of America's War on Drugs*. New Haven: Yale University Press.

DeFeo, Michael A. 1990. Depriving International Narcotics Traffickers and Other Organized Criminals of Illegal Proceeds and Combatting Money Laundering. *Denver Journal of International Law & Policy* 18: 405–15.

Department of Homeland Security. 2022a. Human Trafficking Laws & Regulations. November 9. Available online: https://www.dhs.gov/human-trafficking-laws-regulations (accessed on 29 July 2024).

Department of Homeland Security. 2022b. What Is Human Trafficking? September 22. Available online: https://www.dhs.gov/blue-campaign/what-human-trafficking (accessed on 29 July 2024).

Department of Homeland Security. 2023. Counter Terrorism and Homeland Security Threats. May 30. Available online: https://www.dhs.gov/counter-terrorism-and-homeland-security-threats (accessed on 29 July 2024).

Department of Homeland Security. 2024. DHS Center for Countering Human Trafficking. July 2. Available online: https://www.dhs.gov/dhs-center-countering-human-trafficking (accessed on 29 July 2024).

Department of Justice. 2020a. Global Disruption of Three Terror Finance Cyber-Enabled Campaigns. Available online: https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns (accessed on 29 July 2024).

Department of Justice. 2020b. Report of the Attorney General's Cyber Digital Task Force. October. Available online: https://www.justice.gov/d9/pages/attachments/2021/01/20/cryptocurrency_white_paper.final_.pdf (accessed on 29 July 2024).

Department of Justice. 2022. Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace. April 5. Available online: https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace (accessed on 29 July 2024).

Department of State. 2020. Country Reports on Terrorism 2020: Iran. Available online: https://www.state.gov/reports/country-reports-on-terrorism-2020/iran (accessed on 14 October 2024).

Department of State. n.d. Foreign Terrorist Organizations. Available online: https://www.state.gov/foreign-terrorist-organizations/ (accessed on 29 July 2024).

Department of the Treasury. 2020. Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity. October 15. Available online: https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL_0.pdf (accessed on 29 July 2024).

Devon, Cheyenne. 2023. A Crypto Exchange Allegedly Processed over $700 Million Worth of Illicit Funds Before the Department of Justice Shut it Down. CNBC.com. January 20. Available online: https://www.cnbc.com/2023/01/20/justice-dept-shuts-down-crypto-exchange-that-processed-illicit-funds.html (accessed on 29 July 2024).

Dwyer, Gerald P. 2015. The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability* 17: 81–91. [CrossRef]

Frebowitz, Ryan L. 2018. Cryptocurrency and State Sovereignty. Naval Postgraduate School. Available online: https://apps.dtic.mil/sti/pdfs/AD1059865.pdf (accessed on 16 July 2024).

Ganor, Boaz. 2002. Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter? *Policy Practice and Research: An International Journal* 3: 287–304. [CrossRef]

George, Derek R. 2018. Cryptocurrencies: Emergent Threat to National Security. Marine Corps University. Available online: https://apps.dtic.mil/sti/trecms/pdf/AD1179035.pdf (accessed on 16 July 2024).

Gholipour, Benham. 2021. Official Report: Iran Could Use Cryptocurrencies to Avoid Sanctions. March 2. Iranwire.com. Available online: https://iranwire.com/en/features/69084/ (accessed on 29 July 2024).

Giudici, Giancarlo, Alistair Milne, and Dmitri Vinogradov. 2020. Cryptocurrencies: Market analysis and perspectives. *Journal of Industrial and Business Economics* 47: 1–18. [CrossRef]

Givens, Austen D., Nathan E. Busch, and Alan D. Bersin. 2018. Going Global: The International Dimensions of U.S. Homeland Security Policy. *Journal of Strategic Security* 11: 1–34. [CrossRef]

Gold, Zack, and Megan McBride. 2019. Cryptocurrency: A Primer for Policy-Makers. CNA. Available online: https://www.cna.org/archive/CNA_Files/pdf/crm-2019-u-020185-final.pdf (accessed on 16 July 2024).

Gottschalk, Petter. 2017. Convenience in White-Collar Crime: Introducing a Core Concept. BI Norwegian Business School. Available online: https://biopen.bi.no/bi-xmlui/bitstream/handle/11250/2479955/Gottschalk+_2016_DevBeh.pdf?sequence=2 (accessed on 16 July 2024).

Government Accountability Office. 2021a. Sex Trafficking: Online Platforms and Federal Prosecutions. Available online: https://www.gao.gov/assets/gao-21-385.pdf (accessed on 29 July 2024).

Government Accountability Office. 2021b. Virtual Currencies: Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking. Available online: https://www.gao.gov/assets/gao-22-105462.pdf (accessed on 29 July 2024).

Gundur, R. V., Michael Levi, Volkan Topalli, Marie Ouellet, Maria Stolyarova, Lennon Yao-Chung Chang, and Diego Dominguez Mejia. 2021. Evaluating Criminal Transaction Methods in Cyberspace as Understood in an International Context. April 16. Available online: https://www.crimrxiv.com/pub/48bmtkg0#n5jrqdrnooe (accessed on 16 July 2024).

Hwang, Jeeseon, and Kyung-Shick Choi. 2021. North Korean cyber attacks and policy responses: An interdisciplinary theoretical framework. *International Journal of Cybersecurity Intelligence and Cybercrime* 4: 4–24. [CrossRef]

Jaffe, Justin. 2022. A Beginner's Guide to Bitcoin and Cryptocurrency. CNET.com. June 21. Available online: https://www.cnet.com/personal-finance/investing/crypto/what-is-bitcoin/ (accessed on 29 July 2024).

Jenner, Matthew S. 2013. Drug Trafficking as a Transnational Crime. In *Handbook of Transnational Crime and Justice*, 2nd ed. Edited by Phillip Reichel and Jay Albanese. Thousand Oaks: Sage Publications, Inc., pp. 65–84.

Kethineni, Sesha, and Ying Cao. 2020. The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review* 30: 325–44. [CrossRef]

Kim, Heeu M., June Lee, and Rachel Paik. 2022. North Korean Cryptocurrency Operations: An Alternative Revenue Stream. May. Harvard Kennedy School, Belfer Center for Science and International Affairs, North Korea Cyber Working Group Policy Memo No. 1. Available online: https://www.belfercenter.org/publication/north-korean-cryptocurrency-operations-alternative-revenue-stream (accessed on 31 July 2024).

Lee, Hannarae, and Kyung-Shick Choi. 2021. Interrelationship between Bitcoin, Ransomware, and Terrorist Activities: Criminal Opportunity Assessment via Cyber-Routine Activities Theoretical Framework. *Victims & Offenders* 16: 363–84.

Liang, Jiaqi, Linjing Li, and Daniel Zeng. 2018. Evolutionary dynamics of cryptocurrency transaction networks: An empirical study. *PLoS ONE* 13: e0202202. [CrossRef] [PubMed]

Mahood, Samantha, and Halim Rane. 2016. Islamist narratives in ISIS recruitment propaganda. *The Journal of International Communication* 23: 15–35. [CrossRef]

Malakoutikhah, Zeynab. 2020. Financial Exclusion as a Consequence of Counter-Terrorism Financing. Available online: https://eprints.whiterose.ac.uk/151973/3/financial%20exclusion%20(3).pdf (accessed on 29 July 2024).

Manyin, Mark E., and Mary Beth D. Nikitin. 2024. U.S.-North Korea Relations. March 26. Congressional Research Service. Available online: https://crsreports.congress.gov/product/pdf/IF/IF10246 (accessed on 29 July 2024).

National Commission on Terrorist Attacks Upon the United States. 2004. Final Report of the National Commission on Terrorist Attacks Upon the United States: Executive Summary. Available online: https://911commission.gov/report/911Report_Exec.htm (accessed on 29 July 2024).

Nichols, Michelle. 2024. Exclusive: North Korea Laundered $147.5 mln in Stolen Crypto in March, SAY UN Experts. Reuters. May 14. Available online: https://www.reuters.com/technology/cybersecurity/north-korea-laundered-1475-mln-stolen-crypto-march-say-un-experts-2024-05-14/ (accessed on 16 July 2024).

Office of the Director of National Intelligence. 2024. Annual Threat Assessment of the U.S. Intelligence Community. February 5. Available online: https://www.odni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf (accessed on 16 July 2024).

PBS News. 2023. The Role of Cryptocurrency in Financing Terrorist Organizations. November 4. Available online: https://www.pbs.org/newshour/show/the-role-of-cryptocurrency-in-financing-terrorist-organizations (accessed on 16 July 2024).

Ramsay, Gilbert. 2015. Why terrorism can, but should not be defined. *Critical Studies on Terrorism* 8: 211–28. [CrossRef]

Reuters. 2021. Iran Uses Crypto Mining to Lessen Impact of Sanctions, Study Finds. May 21. Available online: https://www.reuters.com/technology/iran-uses-crypto-mining-lessen-impact-sanctions-study-finds-2021-05-21/ (accessed on 29 July 2024).

Rosen, Liana W., Paul Tierno, and Rena S. Miller. 2023. Terrorist Financing: Hamas and Cryptocurrency Fundraising. Congressional Research Service. November 27. Available online: https://crsreports.congress.gov/product/pdf/IF/IF12537 (accessed on 16 July 2024).

Thomas, Clayton. 2023. U.S. Sanctions on Iran. July 20. Congressional Research Service. Available online: https://crsreports.congress.gov/product/pdf/IF/IF12452 (accessed on 29 July 2024).

Tredinnick, Luke. 2019. Cryptocurrencies and the blockchain. *Business Information Review* 36: 39–44. [CrossRef]

U.S. Congress. n.d. H.R.5210—Anti-Drug Abuse Act of 1988. Available online: https://www.congress.gov/bill/100th-congress/house-bill/5210 (accessed on 29 July 2024).