

EFFICACY OF ECONOMIC SANCTIONS IN THE FACE OF CRYPTOCURRENCY

TICHA UNGBORIBOONPISAL*

I. INTRODUCTION	221
II. OVERVIEW OF INTERNATIONAL ECONOMIC SANCTIONS	223
A. <i>Definitions</i>	223
B. <i>Current State of Play</i>	224
III. CHARACTERISTICS OF CRYPTOCURRENCY THAT FACILITATE THE EVASION OF SANCTIONS	225
A. <i>Characteristics</i>	225
B. <i>Examples of its Use</i>	227
IV. GAPS IN THE SANCTIONS EXPLOITED BY CRYPTOCURRENCY	229
A. <i>Deficiencies in the Language of the UNSC Resolutions</i>	229
B. <i>Challenges in the Implementation of Financial Sanctions</i>	230
C. <i>Challenges of the Working Procedure of the UNSC</i>	231
D. <i>Other General Gaps and Challenges</i>	232
V. SOLUTIONS FOR IMPROVING THE EFFICACY OF THE SANCTIONS	233
A. <i>Domestic Framework</i>	233
B. <i>International Framework</i>	234
VI. CONCLUSION	235

I. INTRODUCTION

In the past several years, cryptocurrency has increasingly been used by sanctioned States in an effort to evade economic sanctions. For instance, cryptocurrency has been used to settle trade,¹ engage in money laundering, and commit cyber hack-

* LL.M. Candidate 2022-2023, NYU School of Law. The author would like to thank Maiko Takeuchi for her insightful and constructive comments, which serve as a helpful starting point for this research.

1. Tom Wilson, *Iran Makes First Import Order Using Cryptocurrency-Report*, REUTERS (Aug. 9, 2022, 8:14 AM), <https://www.reuters.com/business/fi>

ing.² No international treaty is in place that specifically regulates cryptocurrency. Instead, there is only national legislation, often with varying policies, which can range from a total ban of the use of cryptocurrency, to partial bans on cryptocurrency as a means of payment, to wholesale legalization of cryptocurrency.³ This discrepancy may create gaps where neither national nor international regulation can reach, thus facilitating cryptocurrency's misuse as a tool to evade economic sanctions. For example, in the case of North Korea, the "[o]ngoing deficiencies in the implementation by Member States of financial sanctions, combined with the deceptive practices of the Democratic People's Republic of Korea, enabled the country to continue to access the international financial system."⁴ Although it is argued that crypto-based transactions and crypto markets only account for a small portion of the global currency market,⁵ the recent incidents of economic sanction evasion emphasize the importance and necessity for this issue to be addressed soon before cryptocurrency becomes more sophisticated and more dominant. This paper focuses on economic sanctions imposed by the United Nations Security Council (UNSC).

nance/iran-makes-first-import-order-using-cryptocurrency-tasnim-2022-08-09/.

2. Choe Sang-Hun & David Yaffe-Bellany, *How North Korea Used Crypto to Hack Its Way Through the Pandemic*, N.Y. TIMES (July 1, 2022), <https://www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html>; Priscilla Moriuchi, *North Korea Turning to Cryptos to Counter Economic Sanctions*, THE HILL (Jan. 22, 2018, 2:15 PM), <https://thehill.com/opinion/international/370114-north-korea-turning-to-cryptos-to-counter-economic-sanctions/>; Tom Mitchelhill, *Infamous North Korean Hacker Group Identified as Suspect for \$100M Harmony Attack*, COINTELEGRAPH (June 30, 2022), <https://cointelegraph.com/news/infamous-north-korean-hacker-group-identified-as-suspect-for-100m-harmony-attack>.

3. See Law Library of Congress, *Regulation of Cryptocurrency Around the World*, GLOBAL LEGAL RESEARCH CENTER (June 2018), <https://www.loc.gov/item/2018298387/>.

4. U.N. President of the S.C., Note by the President of the S.C., at 4, U.N. Doc. S/2019/691 (2019) [hereinafter Note by the President of the S.C. 691].

5. Kashyap Kompella & James Cooper, *Cryptocurrencies Are No Threat to the Efficacy of International Sanctions*, THE HILL (Mar. 9, 2022), <https://thehill.com/opinion/finance/597269-cryptocurrencies-are-no-threat-to-the-efficacy-of-international-sanctions/>.

II. OVERVIEW OF INTERNATIONAL ECONOMIC SANCTIONS

A. Definitions

Economic sanctions are “the withdrawal of customary trade and financial relations for foreign- and security-policy purposes.”⁶ The UNSC has the authority to impose economic sanctions, which is derived from Article 41 of Chapter VII of the U.N. Charter.⁷ One of the aims of economic sanctions is to put pressure on the economy of the target States in order to make them yield to the issues of concern of the UNSC—for example, a threat to international peace and security. The sanctions are, in principle, legally binding upon U.N. Member States (UNMS).⁸ UNMS are responsible for implementing sanctions at the national level. Therefore, they are required to adopt national implementation measures and make sure that the individuals concerned comply with them.⁹ The only exception for non-compliance is provided in Article 50 of the UN Charter.¹⁰

Efficacy in the context of economic sanctions may denote “(1) the extent to which States actually comply with the UNSC resolutions by prohibiting commercial or financial relations with the target States; (2) the extent to which such prohibition actually impacts the economy of the target States; or (3) the extent to which the target State actually modifies its behavior as a result of the impacts on its economy.”¹¹ However, it

6. Jonathan Masters, *What Are Economic Sanctions?*, COUNCIL ON FOREIGN RELATIONS (Aug. 12, 2019, 8:00 AM), <https://www.cfr.org/background/what-are-economic-sanctions>.

7. U.N. Charter art. 41 (“the Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations”).

8. U.N. Charter art. 25, art. 48, ¶ 2.

9. Paul Szasz, *The Law of Economic Sanctions*, 71 INT’L L. STUD. 455, 459 (1998).

10. U.N. Charter art. 50 (“if preventive or enforcement measures against any state are taken by the Security Council, any other state, whether a Member of the United Nations or not, which finds itself confronted with special economic problems arising from the carrying out of those measures shall have the right to consult the Security Council with regard to a solution of those problems”).

11. Szasz, *supra* note 9, at 473.

should be noted that efficacy is difficult to gauge, as it depends on several factors and it cannot be measured in a vacuum.¹²

B. *Current State of Play*

As of 2022, a total of thirty regimes have been imposed.¹³ They are targeted at States, elite government officials responsible for the administration, or particular individuals or entities that fuel the conflict.¹⁴ The Sanctions Committee monitors the enforcement of sanctions.¹⁵

At present, active economic sanctions have been imposed on a number of countries with different measures. Sanctions against Somalia (imposed in 1992) include an arms embargo.¹⁶ Those against Sudan (imposed in 2005) also include asset freezes on individuals.¹⁷ One of the most robust economic sanctions regimes is against the Democratic People's Republic of Korea (DPRK). Due to its proliferation of nuclear weapons, which poses a threat to international peace and security, the UNSC has consequently imposed economic sanctions upon the DPRK. By UNSC resolution 1718 (2006), most sanctions are directed at physical items, for example equipment or supplies of nuclear weapons, including export bans on certain items. Moreover, they also include measures to “. . . freeze immediately the funds, *other financial assets* and economic resources which are on their territories at the date of adoption of this resolution or at any time thereafter, that are owned or controlled, directly or indirectly, by the persons or entities by designated by the Committee or the Security Council. . . or by persons or entities acting on their behalf or at their direction. . .”¹⁸

In 2016, the UNSC resolution 2321 added new measures, such as prohibiting DPRK diplomats from practicing *commercial activities* by referring to obligations under the Vienna Con-

12. *Subsidiary Organs of the United Nations Security Council: Fact Sheets 2022*, U.N.S.C. SUBSIDIARY ORGANS, 4 (2022), https://www.un.org/securitycouncil/sites/www.un.org/securitycouncil/files/subsidiary_organs_factsheets.pdf.

13. *Id.*

14. Kristen E. Boon, *The Legal Framework of Security Council Sanctions in Terminating Security Council Sanctions*, INT'L PEACE INST. 2,4 (2014).

15. U.N.S.C. Subsidiary Organs, *supra* note 12.

16. S.C. Res. 733, ¶ 5 (Jan. 23, 1992).

17. S.C. Res. 1591, ¶ 3(e) (Mar. 29, 2005).

18. S.C. Res. 1718, ¶ 8(d) (Oct. 14, 2006) (emphasis added).

vention on Diplomatic Relations of 1961,¹⁹ prohibiting public and private financial support from within UNMS territories for trade with DPRK,²⁰ expelling an individual if it is determined that the individual is working on behalf of or at the direction of a DPRK bank or financial institution,²¹ and calling on UNMS to exercise vigilance on the practice of DPRK sending nationals to work abroad for the purpose of *earning hard currency* to fund its nuclear programs.²² The subsequent UNSC resolutions also expand these measures to cover more individuals and entities.

III. CHARACTERISTICS OF CRYPTOCURRENCY THAT FACILITATE THE EVASION OF SANCTIONS

A. Characteristics

Cryptocurrencies create a “troubling new opportunity to avoid international sanctions”²³ and are “harder to trace, can be laundered many times and are independent from government regulation.”²⁴ Although its value is highly volatile, it can be extremely valuable when converted to fiat currency.²⁵ The following characteristics, in short, incentivize businesses and individuals (and sanctioned States) to enter into this novel monetary system and consequently impact the efficacy of economic sanctions.

The first and most important characteristic of cryptocurrency is anonymity throughout the chain of crypto-based transactions. Even though every crypto-based transaction is recorded in a blockchain, there are a myriad of methods to en-

19. *Id.* ¶ 17.

20. *Id.* ¶ 32.

21. *Id.* ¶ 33.

22. *Id.* ¶ 34.

23. Cari Stinebower et al., *Russia-Ukraine Conflict Increases Regulatory Risks for Sanctions Evasion Through Crypto-Based Transaction*, WINSTON & STRAWN LLP (July 27, 2022), <https://www.winston.com/en/global-trade-and-foreign-policy-insights/russiaukraine-conflict-increases-regulatory-risks-for-sanctions-evasion-through-crypto-based-transactions.html> (quoting ATT’Y GEN. CYBER DIGIT. TASK FORCE, CRYPTOCURRENCY ENFORCEMENT FRAMEWORK (2020)).

24. U.N. President of the S.C., Note by the President of the S.C., ¶ 114, U.N. Doc. S/2019/171 (2019) [hereinafter Note by the President of S.C. 171].

25. On September 14, 2022, 1 Bitcoin is equal to about \$19,950 and 1 Ether is equal to about \$1,597. <https://www.coindesk.com/data/>.

hance anonymity or obscure—even change—the owner’s identity, origin, and amount of funds. Ownership of cryptocurrency is not necessarily attributable to people or businesses, as it can be put in a “tumbler” or “mixer” in order to hide or change the owner’s identity.²⁶ The most notable privacy coin, also referred to as anonymity-enhanced cryptocurrencies, is Monero, which adopts technology which can hide transaction amounts and automatically conceal addresses for each transaction to ensure only the transaction sender and receiver know of a payment’s destination. Even though all crypto-based transactions are recorded permanently,²⁷ it may still be difficult to identify the senders and receivers.

The second characteristic is its decentralized nature, including a lack of third-party oversight, absence of a centralized leadership, and the use of a proof-of-work (PoW) consensus mechanism. In other words, transactions can be completed without the use of intermediaries. Moreover, as there is no centralized leadership for most cryptocurrency,²⁸ no one can be held accountable to orders from a regulator to freeze certain accounts or stop suspicious transactions. The PoW, a means to verify transactions without the involvement of a third party, enhances this difficulty.²⁹

26. Deane R. Konowicz, *The New Game: Cryptocurrency Challenges US Economic Sanctions* (May 3, 2018) (Paper submitted to the Faculty of the United States Naval War College Newport, RI, in partial satisfaction of the requirements of the Department of National Security Affairs).

27. Alexander Culafi, *Monero and the Complicated World of Privacy Coins*, SEARCHSECURITY (Jan. 24, 2022), <https://www.techtarget.com/search-security/news/252512394/Monero-and-the-complicated-world-of-privacy-coins>.

28. See, e.g., *Introduction to Ethereum Governance*, ETHEREUM (Oct. 6, 2022), <https://ethereum.org/en/governance/> (“No one person owns or controls the Ethereum protocol. . .”); *Frequently Asked Questions*, BITCOIN, <https://bitcoin.org/en/faq#who-created-bitcoin> (stating “nobody owns the Bitcoin network much like no one owns the technology behind email. Bitcoin is controlled by all Bitcoin users around the world”); *FAQ*, MONERO, <https://www.getmonero.org/get-started/faq/> (stating “Monero is an open source community project. Meaning that there is no company who runs it and there is no CEO who hires people”).

29. See, e.g., *The Great Chain of Being Sure About Things*, THE ECONOMIST (Oct. 31, 2015), <https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things>; *Proof-of-Stake vs. Proof-of-Work: Differences Explained*, COINTELEGRAPH, <https://cointelegraph.com/blockchain-for->

The final complicating characteristic is the piece-meal, and often inconsistent, regulation across different countries. The nation-by-nation regulation has left a vacuum in certain circumstances, for example whether to legalize cryptocurrency in whole or in part, in what manner it should be taxed, how to incorporate it into anti-money laundering laws and regulations, or which agency should be the main regulator. The fact that regulations have not yet covered cryptocurrency in many aspects and that there has yet to be a consensus on how to regulate cryptocurrency allow it to slip through economic sanctions.

B. *Examples of its Use*

DPRK has been reportedly using technology in various ways to evade the economic sanctions imposed on it by the UNSC, especially assets freezes, for the purpose of generating income, gaining access to the global financial system, and generally obtaining funds to support its nuclear programs. From cyberattacks against banks, businesses, and cryptocurrency exchanges, crypto ransom, and laundering of proceeds to crypto mining through crypto-jacking attacks, DPRK operations are increasingly sophisticated, shifting from earning fiat currency to cryptocurrency and resulting in significant financial loss.³⁰

A means of obscuring the theft of cryptocurrency is to create multiple transactions using one-time cryptocurrency wallets. Transferring stolen cryptocurrency through thousands of separate transactions can spread out and hide transactions across multiple countries before converting to fiat currency.³¹ For example, the WannaCry ransomware in 2017, which was allegedly backed by the North Korean regime,³² affected more than 150 countries and demanded payments of ransom in Bitcoin. After the attacker received the proceeds, the attacker

beginners/proof-of-stake-vs-proof-of-work:-differences-explained (explaining the technical processes behind cryptocurrency).

30. Note by the President of S.C. 691, *supra* note 4, at 4; Note by the President of S.C. 171, *supra* note 24, at 51.

31. Note by the President of S.C. 691, *supra* note 4, ¶ 62.

32. See Press Release, *North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*, U.S. Dep't of Justice (Sept. 6, 2018), <https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and> (charging a North Korean Citizen for his involvement in the conspiracy).

laundered Bitcoin multiple virtual currencies across different jurisdictions to conceal transactions and finally converted to Monero, which had a higher privacy protection.³³ Another instance of cryptocurrency theft was the Bithumb attack in 2017, where \$7 million of funds in Bitcoin and Ether were stolen.³⁴ The proceeds were transferred through YoBit in a complex series of hundreds of transactions, converted and cashed out entirely.³⁵

To enhance the difficulty of tracking the stolen funds, hackers have used “mixer” to conceal the origins of their cryptocurrencies by pooling coins, “mixing” them, then swapping them for different coins.³⁶ As recently as June 2022, \$100 million worth of cryptocurrency was stolen from Harmony Protocol. The mixing service was then used to send stolen Ether totaling around 30,000 ETH through multiple transactions.³⁷

It is also reported that a professional branch of the DPRK military has been engaging in cryptocurrency mining. Mining activity of Bitcoin and Monero has significantly increased in the DPRK,³⁸ as much as tenfold in 2019 alone.³⁹ Mining can be conducted through cyber-jacking by using malware to infect a computer to install a mining software and utilize its resources to generate cryptocurrency.⁴⁰

33. Note by the President of S.C. 691, *supra* note 4, at 28, ¶¶ 64-65.

34. Joseph Young, *New Report: North Korean Hackers Stole Funds from South Korean Cryptocurrency Exchanges*, COINTELEGRAPH (Jan. 21, 2018), <https://cointelegraph.com/news/new-report-north-korean-hackers-stole-funds-from-south-korean-cryptocurrency-exchanges>.

35. Note by the President of S.C. 691, *supra* note 4, at 28, ¶ 65.

36. See, e.g., Sander Lutz, *North Korean Attackers Behind \$100M Harmony Hack: Report*, DECRYPT (June 29, 2022), <https://decrypt.co/104138/north-korean-attackers-behind-100m-harmony-hack-report> (discussing mixing used to disguise funds stolen in the Harmony hack).

37. Jason Nelson, *Harmony Hackers Begin Laundering Ethereum Stolen from Horizon Bridge*, DECRYPT (June 27, 2022), <https://decrypt.co/103941/harmony-hackers-begin-laundering-stolen-horizon-bridge-funds>.

38. Note by the President of S.C. 691, *supra* note 4, at 28, ¶ 66.

39. Graham Smith, *New Report Finds North Korean Mining of XMR Increased Tenfold in 2019, Online Activity 300%*, BITCOIN.COM (Feb. 13, 2020), <https://news.bitcoin.com/north-korea-xmr-mining/>; Paddy Baker, *North Korea is Expanding its Monero Mining Operations, Says Report*, YAHOO! (Feb. 12, 2020), <https://www.yahoo.com/now/north-korea-expanding-monero-mining-142554186.html>.

40. Krisztian Sandor, *What is CryptoJacking? How to Protect Yourself Against Crypto Mining Malware*, COINDESK (Mar. 22, 2022, 9:24 AM), <https://>

IV. GAPS IN THE SANCTIONS EXPLOITED BY CRYPTOCURRENCY

As recently as November 2022,⁴¹ the DPRK launched cruise missiles off its west coast, despite nearly a dozen UNSC resolutions aiming to pressure the DPRK to denuclearize since 2006. Clearly, the efficacy of economic sanctions should be called into question. In particular, as pointed out in Part II, the DPRK can engage in proliferation financing through the use of cryptocurrency, whether it is legal or not. Targeted States can evade sanctions when they use cryptocurrency and other cyber tools to generate income and conceal such income through cyber means.⁴² This Part will argue that the gaps in economic sanctions stem from deficiencies in the language or terms used in the UNSC resolutions in the face of cryptocurrency, as well as the challenges in the implementation of the financial sanctions and the challenges of the working process of the UNSC itself.

A. *Deficiencies in the Language of the UNSC Resolutions*

The goal of the UNSC resolutions relating to the DPRK appear to be to reduce the DPRK's ability to gain income and financial resources to fund its nuclear programs. Sanctions imposed upon the DPRK aim to freeze the funds or assets that support the DPRK's nuclear and weapons programs. However, none of the resolutions mention a word about cryptocurrency.

Most of the relevant UNSC resolutions still identify "cash" and "foreign currency" as the main sources of income for sanctioned entities. Moreover, financial institutions and banks, as intermediaries in the traditional payment system, are the main targets. The measures restrict the number of bank accounts held by DPRK nationals, especially diplomats or embassies. These terms "freeze immediately the funds, other financial assets and economic resources which are on [UNMS] territo-

www.coindesk.com/learn/what-is-cryptojacking-how-to-protect-yourself-against-crypto-mining-malware/.

41. Gawon Bae et. al., *North Korea Claims Friday's Launch was a 'New Kind of Intercontinental Ballistic Missile'*, CNN (Nov. 18, 2022), <https://www.cnn.com/2022/11/17/asia/north-korea-ballistic-missile-friday-intl-hnk/index.html>.

42. U.N. President of the S.C., Note by the President of the S.C., 64 n. 185, U.N. Doc. S/2020/151 (2020) [hereinafter Note by the President of the S.C. 151].

ries.”⁴³ However, such language does not seem to capture the lifecycle of cryptocurrency, if at all. As will be elaborated in the next section, certain characteristics of cryptocurrency substantially facilitate evasion of sanction measures, complicating the implementation of the imposed sanctions.

B. *Challenges in the Implementation of Financial Sanctions*

Even if the above-mentioned sanctions were able to adequately cover cryptocurrency, there would still be challenges in the implementation of those sanctions due to the nature of cryptocurrency itself—namely its anonymity, decentralized nature, and the use of technology to “mine” cryptocurrency. In addition, inconsistency in the enforcement of sanctions and the lack of capacity of each State in its defense against cyber operations also pose serious gaps. In short, these low-risk, high-reward, increasingly sophisticated, difficult-to-detect attacks can frustrate attribution.⁴⁴

Anonymity is inherent in any cryptocurrency, making it highly difficult to track and trace the flow of crypto-based transactions and to identify relevant users engaging in the transactions without robust technology. Coupled with its decentralized nature, many questions will be left to the regulators responsible for implementing the sanctions. Such questions may include: Who would be held accountable? Who would be the recipient of orders to stop certain transaction or freeze crypto-based assets? More generally, cryptocurrency can be mined anywhere as long as there is internet connection and a computer. As noted earlier, the fact that mining activity of Bitcoin and Monero is significantly increasing in the DPRK possibly implies that sanction measures mandating the repatriation of DPRK nationals, including IT workers, as well as those relating to banks and financial institutions would not stop DPRK efforts from generating cryptocurrency in its territory or from launching more cyberattacks at cryptocurrency exchanges.

The success of sanctions also comes down to the consistency of enforcement by individual UNMS. As the implementation of sanction measures is subject to national interpreta-

43. S.C. Res. 1718, *supra* note 18.

44. Note by the President of the S.C. 151, *supra* note 42, at 64, ¶ 179.

tion, sanctioned States can make use of UNMS that narrowly interpret sanction measures. For example, with regard to a sanction measure prohibiting engaging in joint ventures with DPRK individuals and entities, Russia interpreted that a Russian company, whose sole founder is a DPRK citizen despite being registered as a Russian company, was not subject to the prohibition on joint ventures and cooperative entities.⁴⁵ Furthermore, some States have not yet adopted a comprehensive legal framework to regulate cryptocurrency, especially under the ambit of money laundering and terrorism-financing regime, which would ultimately affect the legal framework needed for the implementation of sanctions.

More importantly, effective implementation of sanctions hinges upon the capacity and resources of each State. As evidently shown by the above-mentioned examples of the use of cryptocurrency by the DPRK, its increasing sophistication and successes in the cyberattacks and cyber-jacking operation are concrete proof that victims—individuals, entities and even States—do not possess cyber defense tools and infrastructure needed to protect themselves.

C. *Challenges of the Working Procedure of the UNSC*

In addition to implementation being subject to national interpretation, the definitions of terms also depend on different domestic interpretations. For example, regarding the term “luxury goods” as provided in some UNSC resolutions, each country designates different goods that are on their domestic lists of prohibited luxury items. Collectibles are considered luxury in the European Union, the United States, and Singapore, but not in Russia, Australia, Republic of Korea and Japan. Artwork constitutes luxury items in the European Union, United States and Australia, but not in Canada and Russia.⁴⁶

In addition, negotiations among UNSC members regarding financial sanctions are highly politicized. Compromises

45. Maiko Takeuchi, *Smart Language: How to Address an Inherent Weakness Undermining the Implementation of U.N. Sanctions on North Korea*, 96 INT'L L. STUD. 58, 76 (2020).

46. See Sasha Erskine, *North Korean Proliferation Financing and Designated Non-Financial Businesses and Professions*, ROYAL UNITED SERVICES INST. FOR DEFENCE AND SECURITY STUD., 10 (2022) (offering a table setting out the luxury good designations of various countries).

can also lead to unclear terminologies in the operative paragraphs.⁴⁷ Should there be a question over the interpretation of the terms of the UNSC resolutions, an official interpretation can hardly be issued by the UNSC for UNMS to follow. This lack of uniform official construction makes implementation more difficult, as competent authorities would need a legal basis to implement sanction measures in their domestic laws.⁴⁸

D. *Other General Gaps and Challenges*

The most recent UNSC resolution imposing sanctions was on December 22, 2017.⁴⁹ Since then, there have been many new individuals and entities engaging in sanctions evasion, particularly those using cyber operation—for instance, the notable Lazarus Group.⁵⁰ Therefore, it is crucial that UNSC update its list of individuals and entities to keep up with the new development. In addition, diplomatic privileges and immunities have also been abused. It has been acknowledged that there is a recurring trend whereby DPRK diplomats and their family members establish bank accounts for the purpose of sanctions evasion.⁵¹

International politics also play a key role in the result of a resolution and ultimate outcomes. Some resolutions regarding the DPRK were diluted in order to obtain the backing of China and Russia. Moreover, the UN Panel of Experts on North Korea indicated that both Russia and China have allowed DPRK laborers to overstay their visas, in clear violation of UN sanctions.⁵²

47. Takeuchi, *supra* note 45, at 69.

48. *Id.* at 72.

49. S.C. Res. 2397 (Dec. 22, 2017).

50. *Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups*, U.S. DEP'T OF THE TREASURY (Sept. 13, 2019) <https://home.treasury.gov/news/press-releases/sm774>.

51. Note by the President of the S.C. 151, *supra* note 42, at 65, ¶ 187.

52. Jason Bartlett, *Sanctions, Cyber, and Crypto: How Pyongyang Can Exploit the War in Ukraine*, THE DIPLOMAT (July 27, 2022), <https://thediplomat.com/2022/07/sanctions-cyber-and-crypto-how-pyongyang-can-exploit-the-war-in-ukraine/>.

V. SOLUTIONS FOR IMPROVING THE EFFICACY OF THE SANCTIONS

A. Domestic Framework

Effective implementation of sanctions by States is key to their success.⁵³ Therefore, it is crucial that States put in place domestic legal frameworks that address all aspects and life-cycles of cryptocurrency and crypto-based transactions. Related areas which would support regulation of cryptocurrency and safeguard against its misuse are anti-money laundering laws and regulations, laws on the countering of terrorism financing, and counter-proliferation financing compliance.

Clear and precise assignment of a regulatory authority responsible for cryptocurrency is also essential to avoid further gaps in the regulation. As crypto-based transactions could be made for the purposes of investment, payment of goods and services, or just as a commodity, most likely different types of transactions would fall under different regulatory authorities. Thus, States would need to ensure consistent and cooperative effort among their agencies, absent consideration of a new regulating body for cryptocurrency in every aspect.

Despite the decentralized nature of cryptocurrency, the Bitcoin ecosystem is actually de facto centralized. Cryptocurrency exchanges and wallets serve as repositories of cryptoassets, which could increase a degree of centralization to cryptocurrency.⁵⁴ Hence, regulatory authorities could target key players, for instance currency exchanges, mixers, or wallet services.⁵⁵ For example, regulators could take advantage of the available public database of crypto-based transactions⁵⁶ by imposing a degree of reporting obligations or a duty to conduct the “Know Your Customer” process upon those in-

53. Takeuchi, *supra* note 45, at 59.

54. Chris Burniske & Jack Tatar, *Investing Directly in Cryptoassets: Mining, Exchanges, and Wallets*, in CRYPTOASSETS: THE INNOVATIVE INVESTOR’S GUIDE TO BITCOIN AND BEYOND (McGraw-Hill, 2017).

55. See Rainer Böhme et al., *Bitcoin: Economics, Technology, and Governance*, 29 J. OF ECON. PERSPECTIVES 213, 231 (2015) (discussing measures that have been successfully used to target currency exchanges).

56. See, e.g., Blockchain.com

intermediaries.⁵⁷ This could support any investigation conducted by law enforcement officials.

B. *International Framework*

Existing treaties could be utilized more robustly. For example, the UN Convention Against Transnational Organized Crime (UNTOC) broadly defines “transnational,” “organized criminal group,” and “property.”⁵⁸ These terms could be interpreted to cover cyber theft and cyber-jacking against cryptocurrency exchanges. Cooperation among law enforcement, technical assistance, and capacity building mechanisms under the UNTOC could be utilized.⁵⁹ Nonetheless, a challenge remains as to the prosecution since cyberattack on cryptocurrency exchanges could be conducted anywhere, which might complicate the arrest of a wrongdoer. Most importantly, the full and effective implementation of the UNTOC rests upon State Parties adopting appropriate measures and criminalizing relevant crimes in their domestic laws.

UNMS should also closely monitor abuse of diplomatic privileges and immunities under the Vienna Convention on Diplomatic Relations of 1961 (VCDR) by diplomats or their family members, in particular those relating to financial activities,⁶⁰ as they could use their privileges and immunities to aid the evasion of sanctions. Furthermore, existing international organizations could fill in the gap. There has been a proposal to use the International Monetary Fund (IMF) and the World

57. See, e.g., Mark Beardsworth et al., *UK Crypto Regulation: Cryptoasset Exchange and Custodian Wallet Providers Now Required to Report on Suspected Breaches*, PROGRAM ON CORPORATE COMPLIANCE AND ENFORCEMENT (Sept. 14, 2022), https://wp.nyu.edu/compliance_enforcement/2022/09/14/uk-crypto-regulation-cryptoasset-exchange-and-custodian-wallet-providers-now-required-to-report-on-suspected-breaches/ (providing an example of regulators imposing such duties on intermediaries).

58. U.N. Convention Against Transnational Organized Crime art. 2(d), *opened for signature* Dec. 12, 2000, 2225 U.N.T.S. 209 (stating “property shall mean assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets”).

59. *Id.* arts. 27-30.

60. Vienna Convention on Diplomatic Relations arts. 37, 42, Apr. 18, 1961, 500 U.N.T.S. 95.

Trade Organization (WTO) to chime in the cryptocurrency regulation.⁶¹

On the other hand, a new international treaty has also been proposed to mitigate sanctions evasion using cryptocurrency.⁶² However, questions remain as to whether provisions therein would duplicate existing mechanisms, which international organization(s) would be appropriate to take on the negotiation, and to what extent and what aspects cryptocurrency would be regulated. Also, challenges regarding different, if not opposite, national policies toward cryptocurrency, especially its legality, status, and scope of use, might cause reluctance for States to agree on the terms of the treaty. Thus, the underlying aim should be to facilitate compatibility, rather than imposing uniformity.

VI. CONCLUSION

Cryptocurrency poses serious threats to the efficacy of economic sanctions imposed by UNSC resolutions. Due to its nature, together with the deficiencies of UNSC resolutions and working procedure, sanctioned States are still able to access financial resources through the evasion of sanctions.

Efficacy of economic sanctions depend on their implementation by UNMS. In the short run, any effort should focus on effective implementation of sanctions at the national level through all-encompassing legal frameworks, coherent regulatory bodies, and measures targeting key players in the cryptocurrency market. In conjunction with such domestic focus, existing international mechanisms could also be used to cooperate among law enforcement, to support capacity-building, technical assistance, and training for domestic regulatory authorities. In the long run, an international treaty that is specifically tailored to the unique nature of cryptocurrency may be negotiated.

61. See Ed Howden, *The Crypto-Currency Conundrum: Regulating an Uncertain Future*, 29 EMORY INT'L L. REV. 741 (2015) (discussing how the IMF and WTO can be mobilized in this way).

62. See Emma K. Macfarlane, *Strengthening Sanctions: Solutions to Curtail the Evasion of International Economic Sanctions Through the Use of Cryptocurrency*, 42 MICH. J. INT'L L. 199 (2020) (arguing for the enactment of a new multilateral treaty to combat the use of cryptocurrency to evade sanctions).