PACIFIC FORUM
INTERNATIONAL

IMAGINED CURRENCIES: HOW THE DPRK USES CRYPTOCURRENCY TO BLUNT SANCTIONS

BY MICHAEL BUCKALEW

ISSUES & INSIGHTS
VOL. 21, WP 14
NOVEMBER 2021

Pacific Forum

Based in Honolulu, the Pacific Forum (www.pacforum.org) is a foreign policy research institute focused on the Asia-Pacific Region. Founded in 1975, the Pacific Forum collaborates with a broad network of research institutes from around the Pacific Rim, drawing on Asian perspectives and disseminating project findings and recommendations to global leaders, governments, and members of the public throughout the region. The Forum's programs encompass current and emerging political, security, economic, and maritime policy issues, and works to help stimulate cooperative policies through rigorous research, analyses and dialogues.

PACIFIC FORUM

Imagined Currencies: How the DPRK Uses Cryptocurrency to Blunt Sanctions

By
Michael Buckalew

ISSUES & INSIGHTS

WORKING PAPER

VOL. 21, WP14 | November 2021

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This research provides a contemporary study of how and why the Democratic Peoples' Republic of Korea (DPRK) chose to integrate cryptocurrency into its sanctions evasion strategy, as well as the US government's response to this via its financial services regulatory and federal law enforcement agencies. The increased coverage and efficacy of US and international sanctions, especially during and since President Obama's second term (2013-2017) forced the DPRK to find new sources of revenue to maintain elite domestic support and fund their weapons programs. The creation and proliferation of cryptocurrency, which allows for both a digital store of value and a means of exchange outside of the traditional international finance system, opened up an entirely new means by which the DPRK was able to obtain and move funds. Much the DPRK's cryptocurrency is obtained by the through the use of illicit methods and their success has blunted the impact of sanctions as a policy tool. As a result, US financial services regulators and law enforcement have moved to regulate cryptocurrency and crack down on illegal activities associated with it, such as ransomware payments. However, US regulations regarding cryptocurrency remain largely fragmented across agencies and various local jurisdictions.

This research highlights the underappreciated role played by the US Treasury Department and the semi-independent agencies under its aegis in turning policy goals into enforceable administrative law. It also finds a high degree of continuity in the development and application of sanctions between the Obama and Trump administrations against the DPRK. Furthermore, this study demonstrates the need for policymakers to develop a more comprehensive US legal framework around regulation of cryptocurrency to close off growing illicit revenue generation by hostile actors. The study then briefly touches on the increased importance of the DPRK's digital activities during COVID-19. Finally, this study outlines three potential methods by which to manage risks posed by cryptocurrency: 1) a public-private partnership to create s standards setting or certification organization to self-police the industry; 2) the US government using its sovereign authority to legislate and regulate; or 3) an outright banning of cryptocurrency activities in the United States.

Glossary of Terms

AEC	Anonymity-Enhanced Cryptocurrency; also commonly referred to as privacy coins
AML	Anti-Money Laundering
(A) Blockchain	A digital ledger of transactions that is duplicated and distributed across an entire network of computer systems
Blockchain technology	Computer operating network software (nodes) that enable, validate, and store transactional records on a distributed digital ledger
BSA	US Bank Secrecy Act
CBDC	Central Bank Digital Currency; a generic term for a third version of currency (in additional to cash and reserves) that could be used as an electronic record or digital token to represent the digital form of a nation's currency
Chain-Hopping	A practice where individuals or entities move from one cryptocurrency to another, sometimes for the purpose of obfuscating the origins of funds or assets
CIP	Customer Identification Program; a minimum set of standards for financial institutions to verify a customer's identity in connection with opening an account at a financial institution or processing a transaction subject to certain conditions
Cryptocurrency	A type of digital asset traded online through the use of a blockchain; also commonly referred to as a digital or virtual currency
Cryptocurrency Wallet	A digital account, which allows the accountholder (the user) to store, send and receive cryptocurrency.
DLT	Distributed Ledger Technology; a digital system for recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time
DOJ	US Department of Justice
CVC	Convertible Virtual Currency; a cryptocurrency that is able to be exchanged for legal tender / fiat currency, but lacks legal tender status

EO	An executive order issued by Office of the President of the United States
FATF	Financial Action Task Force; an international organization based in Paris whose mission it is to issue advisories, draft reports, and make recommendations regarding best practices related to anti-money laundering
DPRK	Democratic People's Republic of Korea; commonly referred to as North Korea
FinCEN	US Financial Crimes Enforcement Network; a bureau of the United States Department of the Treasury
IEEPA	International Emergency Economic Powers Act; a law passed by the US Congress to empower the president to impose sanctions on designated entities (e.g. DPRK)
Mixer	A mechanism used to break the connection between an address sending CVC and the addresses receiving CVC, effectively making it difficult to impossible to trace transactions; also sometimes referred to as a 'tumbler.'
NY DFS	New York Department of Financial Services
OFAC	US Office of Foreign Assets Control; an office in the US Treasury Department which administers and enforces economic sanctions programs against designated countries and groups of individuals (e.g. terrorists, narcotics traffickers, and state entities).
Private Key	A cryptographic key used with an algorithm to encrypt and decrypt code; when used with cryptocurrencies, this key allows a user to access their cryptocurrency
Public Key	A cryptographic key that can be obtained and used by anyone to encrypt messages intended for a particular recipient, such that the encrypted messages can be deciphered only by using a second key that is known only to the recipient; in the case of cryptocurrencies, this is a code that allows users to receive cryptocurrencies into their accounts
ROK	Republic of Korea; commonly referred to as South Korea
Stablecoin	A type of cryptocurrency that is pegged to a fiat currency (such as USD)
SWIFT	A global member-owned cooperative which provides financial transaction messaging and transfer services

USD	United States Dollars
USA PATRIOT Act	A law passed in October 2001 by the US Congress in response to the 9/11 terrorist attacks, which provides enhanced anti-money laundering and counter financing of terrorism provisions.
WPK	Workers' Party of Korea; sometimes referred to as the (DRPK) or the North Korean communist party

Notes Regarding Romanization of Korean Names and Words

All Korean words used in this work have been Romanized according to the Revised Romanization system. The only exceptions to this are direct quotations from authors who have published in English using a different spelling of particular names or words or where well-known names of people or places use another form of romanization. Additionally, Korean names are written with surnames followed by given names, unless otherwise listed in direct quotations.

INTRODUCTION

Over the past few years, there has been a significant shift in the Democratic Peoples' Republic of Korea's (DPRK)[1] illicit revenue acquisition, f due to the proliferation of cryptocurrency. The funds acquired via cryptocurrency are utilized for the development of weapons programs and to sustain support among domestic elites for the regime. The DPRK has increasingly turned to cryptocurrency[2] and cybercrime to obtain revenue, accounting for 10-15% of the DPRK's foreign exchange earnings.[3]

The highest-priority US policy objective regarding the DPRK is addressing their missile and nuclear weapons programs. However, the political and military situation in Northeast Asia limits options that the United States can pursue. This leads to differing approaches by the two parties to advance their goals. The DPRK often takes indirect, obscured actions, while the US works more publicly with allies and partners in the region to discourage proliferation. However, the emergence of cryptocurrency,[4] beginning with Bitcoin in 2008 introduced a new variable in the dynamic of US-DPRK interactions: 1) since the 2010s, the DPRK uses cryptocurrency to obtain and move revenue, while subverting the US sanctions regime[5] and, 2) the United States has responded by adjusting its policies to limit the DPRK's access to cryptocurrency funds through its law enforcement, financial regulatory agencies.

The study seeks to address two broad research questions: 1) How has cryptocurrency changed the DPRK's capabilities and tactics in circumventing sanctions? 2) How have US sanctions and anti-money laundering policies towards the DPRK changed in response? These questions are assessed via a case study comparing the evolution of the DPRK's illicit revenue generation and how US regulatory and enforcement policies have adapted. The analysis is conducted through the lens of social constructivist theory, where actors (state and non-states) make decisions based on perceptions themselves and perceptions of others.

This study is divided into five sections. Section 1 provides a background on cryptocurrency, including its regulation in the United States. Gaps in existing literature are noted, along with how this study addresses them. Section 2 covers the methodology and theoretical structure of the paper, including critiques of social constructivism as an analytical method. It also notes the impact of (coronavirus) COVID-19 pandemic as an intervening variable. Section 3 details and assesses changes in the DPRK's illicit revenue generation since the proliferation of cryptocurrency. Section 4 provides background and an analysis of the US policy response in

[1] For the sake of clarity and consistency, I will refer to North Korea as the Democratic People's Republic of Korea (DPRK), unless directly quoting source materials.
[2] Mathew Ha and David Maxwell, "Kim Jong Un's 'All Purpose Sword': North Korean Cyber-Enabled Economic Warfare," Washington, DC, Foundation for Defense of Democracies (October 2018), 10. https://www.fdd.org/wp-content/uploads/2018/09/REPORT_NorthKorea_CEEW.pdf
[3] Patrick Howell O'Neill, "North Korea's plan to cultivate an army of cybercrime masterminds," CyberScoop, April 11, 2021. https://www.cyberscoop.com/north-korea-lazarus-group-bangladesh-bank-donald-trump-xi-jinping/.
[4] Also commonly referred to as "digital currencies" or "virtual currencies".
[5] Matt Burgess, "North Korea's elite hackers are funding nukes with crypto raids," Wired, April 3, 2019, https://www.wired.co.uk/article/north-korea-hackers-apt38-cryptocurrency.

relation to cyberattacks and money laundering via cryptocurrency. Section 5 looks at how well the theoretical structure of this paper applied to the case study, policy implications, recommendations, and future avenues of potential inquiry.

SECTION 1: EXISTING LITERATURE ON CRYPTOCURRENCY, GAPS AND HOW THIS WORK SEEKS TO ADDRESS THEM

What is Cryptocurrency and How Does It Work?

The US Department of Justice (DOJ)[6] defines cryptocurrency as "a type of virtual asset that uses cryptography to secure financial transactions."[7] In the context of a recent sanctions breach criminal case, it was also defined as "a decentralized, peer-to-peer form of electronic currency that can be digitally traded and functions as (1) a medium of exchange; (2) a unit of account; and/or (3) a store of value, but does not have legal tender status."[8] In effect, cryptocurrency serves many of the same functions of money, but without the backing of a centralized authority.

While there are many types of cryptocurrencies, Bitcoin is by far the most common by trade volume and market cap value. [9] Other popular cryptocurrencies include Ethereum, Ripple, Litecoin, Bitcoin Cash, Dash, and anonymity-enhanced cryptocurrencies (AEC)[10] such as ZCash and Monero.[11] A unit of cryptocurrency is called a "coin" or "token," depending on its underlying software. Coins are exchanged or traded in a series of transactions recorded as entries on a blockchain, the shared ledger maintained on every computer—each referred to as a node—connected to the cryptocurrency's networks (see Figure 1 for additional details). The software running on the nodes processes, validates, and stores the transaction records, keeping the distributed digital ledger on each node in sync by using a consensus mechanism. While the methods for determining consensus vary, the key principle is that each block of transactions on the ledger incorporates an encrypted data string derived from the preceding block, thereby chaining the entries together—hence, a blockchain—in a way that makes tampering with the ledger's values effectively impossible. Most cryptocurrencies use permissionless and public ledgers, meaning anyone can view it at any time, so long as they have appropriate software. See Figure 2 and Figure 3, which provide visual depictions of how a blockchain works and how cryptocurrency transactions are conducted.

---

[6] Unless otherwise noted, all government regulatory agencies, courts, etc. should be assumed to be from the United States.

[7] US Department of Justice, "Department of Justice Launches Global Action Against NetWalker Ransomware," January 27, 2021, 1. https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware. (DOJ 2021a)

[8] US Southern District of New York Federal Court, "United States of America v. Virgil Griffith Sealed Complaint," July 2020, 3. https://www.justice.gov/usao-sdny/press-release/file/1222646/download.

[9] Yahoo! Finance, "Top Cryptos by Volume (all currencies, 24hr)," https://finance.yahoo.com/u/yahoo-finance/watchlists/crypto-top-volume-24hr/. As of August 29, 2021, Bitcoin had an average three-month trading volume of 26.26 billion, followed by Ethereum at 23.25 billion.

[10] Also commonly referred to as 'privacy coins', providing additional protections to hide the identities of the persons or entities involved in the transactions.

[11] Megan McBride and Zach Gold, "Cryptocurrency: Implications for Special Operations Forces," CNA Analysis & Solutions, August 2019, 5. https://doi.org/10.1007/s10551-018-3923-1.

A blockchain allows a user to initiate transactions with other users (e.g. an individual, company or another entity) through the use of public and private keys to process and complete them. Private keys are in and of themselves anonymous,[12] so long as a user does not share their information with others. Transactional records and public keys are viewable at any time, while personal identifiers are not.[13] However, "[o]nce the public address and private key are united, blockchain suddenly appears to be a pseudonymous system."[14]Additionally, there are also different kinds of coins promoted based on certain features (e.g. stability, anonymity, etc.). AECs are especially important in this study, given the DPRK's preference for using them and other tools which are used to obfuscate illicit money transmission.

How Cryptocurrency is Regulated in the United States

The fragmented US regulatory framework for cryptocurrency presents another significant challenge to addressing illegal activities which utilize the technology. Different federal agencies address certain functions of cryptocurrency based on their mandates and respective agency cultures. Table 1 below provides a short summary of these approaches.

Table 1: US Federal Regulation of Cryptocurrency

Agency	How Cryptocurrency is Regulated
Commodity Futures Trading Commission (CFTC)	As a commodity, under the Commodity Exchange Act; additionally the agency regulates cryptocurrency exchanges offering derivatives (e.g. futures contracts) products on certain digital exchanges[15]
Financial Crimes Enforcement Network (FinCEN)	Regulates cryptocurrency businesses as money service businesses (MSB) under the Bank Secrecy Act (BSA)
Internal Revenue Service (IRS)	Property for US federal tax purposes[16]
Office of the Comptroller of the Currency (OCC)	Allows for cryptocurrency custodial services for customers by national banks and federal savings

[12] Anonymous data is any information from which the person the data relates to can't be identified. Pseudonymous data allows for some form of reidentification, even if it's indirect or remote.
[13] McBride and Gold, 13.
[14] Wacsman, "Answering One of Blockchain's Biggest Questions: Anonymity or Pseudonymity?" Jan. 29, 2019, https://medium.com/@Wachsman_/answering-one-of-blockchains-biggest-questions-anonymity-or-pseudonymity-5c9ada879e87.
[15] Commodity Futures Trading Commission, "Final Interpretative Guidance: Retail Commodity Transactions Involving Certain Digital Assets," June 24, 2021, https://www.cftc.gov/LawRegulation/FederalRegister/finalrules/2020-11827.html.
[16] Internal Revenue Service, "Frequently Asked Questions on Virtual Currency Transactions," https://www.irs.gov/individuals/international-taxpayers/frequently-asked-questions-on-virtual-currency-transactions, accessed July 6, 2021. See Question 2: "Virtual currency is treated as property and general tax principles applicable to property transactions apply to transactions using virtual currency."

Office of Foreign Assets Control (OFAC)	Application of economic and trade sanctions enforcement authority administered by the Treasury Department
Securities and Exchange Commission (SEC)	Many cryptocurrency tokens are treated as investment contracts under US securities law; additionally the agency has purview to regulate when initial coin offerings are utilized to raise capital or companies engage in securities transactions utilizing cryptocurrency[17]

Source: Department of Justice. Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework. October 1, 2020, 23-33.[18]

In additional to federal law, three US states serve as important hubs for cryptocurrency: California, New York, and Wyoming. Silicon Valley, California is the heart of the financial technology (fintech) industry, of which cryptocurrency is a major component. California legalized the use of cryptocurrency to transmit payments and purchase goods in 2014[19] and expanded upon it 2019, allowing the state's consumer enforcement agency to regulate cryptocurrency.[20] Finally, cryptocurrency companies have largely been exempted from money transmission regulations.[21]

New York is another key jurisdiction for cryptocurrency given its importance as a financial center. In 2015, the New York Department of Financial Services (NY DFS), issued regulations to oversee cryptocurrency businesses under its BitLicense Program.[22] To receive and maintain a license, companies and individuals must: 1) obtain a license from the state, 2) file financial reports, 3) manage records, 4) meet specific capital requirements; 5) be subject to potential regulatory examination; and; 6) be required to safeguard their customers' interests.[23] The license is required in order to engage in the following activities:

> 1) receiving Virtual Currency for transmission or transmitting Virtual Currency; 2) storing, holding, or maintaining custody or control of Virtual Currency on behalf of

[17] Gary Gensler, "Testimony Before the Subcommittee on Financial Services and General Government, US House Appropriations Committee," US Securities and Exchange Commission, May 26, 2021, https://www.sec.gov/news/testimony/gensler-2021-05-26.
[18] US Department of Justice, "Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework," Oct. 1, 2020, https://www.justice.gov/archives/ag/page/file/1326061/download. (DOJ 2020a), 23-33.
[19] State of California, "Assembly Bill 129: Lawful Money," 2014, http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab_0101-0150/ab_129_cfa_20140128_174724_asm_floor.html.
[20] See State of California, "Assembly Bill 1864: Department of Financial Protection and Innovation," 2019., https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1864 and Sebastian Sinclair. "California Governor Signs Law Bringing State 'New Tools' to Regulate Crypto Coindesk," Sept. 29, 2020, https://www.coindesk.com/california-governor-newsom-law-regulation-crypto.
[21] Buckley, LLP, "California DBO opinion letters cover activities exempt from MTA licensing," Aug. 7, 2020, https://buckleyfirm.com/blog/2020-08-07/california-dbo-opinion-letters-cover-activities-exempt-mta-licensing.
[22] Jane Kim, "Suffocate or Innovate: An Observation of California's Regulatory Framework for Cryptocurrency," Loyola of Los Angeles Law Review, Vol 52. No. 3, Article 4, Feb. 2, 2019, https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=3058&context=llr.
[23] Kim, 349-350.

> others; 3) buying and selling Virtual Currency as a customer business; 4) performing exchange services as a customer business; or 5) controlling, administering, or issuing a Virtual Currency.[24]

Wyoming is widely considered the "Wild West" of the cryptocurrency industry given the high degree of activity and significant body of law enacted in the state. Wyoming has gained a reputation for having deregulated fiscal and energy markets and allows for a wide range of permissible cryptocurrency activities in the state. This includes: 1) property rights; 2) a fintech regulatory sandbox, 3) state-chartered depository institutions and; 4) allows for "qualified custodians" for digital assets.[25]

How and Why is Cryptocurrency Useful for Illegal Activities?

Cryptocurrency funds are held in individual users' wallets, until the user either wants to buy a good or service, convert it into another cryptocurrency, or convert it into a fiat currency. For purchases, users transfer cryptocurrency directly to another user's address, although some exchanges have escrow-like systems, which allow for easier dispute resolution.[26] Converting cryptocurrency into fiat currency (and the reverse) is typically handled by exchanges, which are financial services providers that buy and sell cryptocurrencies with users, or via peer-to-peer exchanges.

Besides permitted activities, cryptocurrency is also utilized for illegal means. The existence of payment mechanisms that are both digital and anonymous have facilitated the growth of online black markets, such as the now defunct "Silk Road."[27] Digital hackers and extortionists of all types now routinely request cryptocurrency for quick, efficient, and easily verifiable ransom payments.[28] Importantly, these illicit financial activities are frequently conducted via cryptocurrency due to the difficulties that government regulatory and law enforcement agencies have in tracking the transactions:

> Blockchain analysis can be rendered less effective by a number of factors, including the scale of a blockchain network, the extent of peer-to-peer activity (i.e., transactions between unhosted wallets), the use of anonymizing technologies to obscure transaction information, and a lack of information concerning the identity of transferors and recipients in particular transactions.[29]

---

[24] New York Department of Financial Services, BitLicense FAQs, last accessed March 30, 2021, https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/bitlicense_faqs.
[25] Caitlin Long, "What Do Wyoming's 13 New Blockchain Laws Mean?" March 4, 2019. https://www.forbes.com/sites/caitlinlong/2019/03/04/what-do-wyomings-new-blockchain-laws-mean/?sh=a65f6a85fde6.
[26] Foley, et. al., 1804.
[27] Sean Foley, Jonathan R. Karlsen, Talis J. Putniņš, "Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed through Cryptocurrencies," Oxford University, *The Society for Financial Studies*, 2019, https://academic.oup.com/rfs/article/32/5/1798/5427781, 1799.
[28] Angelena Bradfield and Stephanie Wake, "Top 7 Things to Know About Ransomware and Why Criminals Prefer Crypto Payments, Bank Policy Institute, May 12, 2021, https://bpi.com/top-7-things-to-know-about-ransomware-and-why-criminals-prefer-crypto-payments/.
[29] US Financial Crimes Enforcement Network, "Proposed Rulemaking: Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," US Federal Register. Dec. 23, 2020, 12. https://www.federalregister.gov/documents/2020/12/23/2020-28437/requirements-for-certain-

Transactions are often conducted in a number of ways which evade existing US financial services laws: 1) via unregulated peer-to-peer networks, 2) via unhosted wallets or those hosted by a foreign financial institution that not subject effective anti-money laundering (AML) regulations, including recordkeeping and reporting requirements.[30] With these factors taken together, it is unsurprising that individual criminals, crime syndicates, and illicit state actors prefer cryptocurrency as both the means and method of payment in the conduct of illegal activities.

Literature on Cryptocurrency

This review will focus on published works by central bank authorities and other researchers looking at legitimate usage purposes and illicit applications by non-state, state, and sub-state actors. The US Federal Reserve and other central banks have released numerous works on the technological and applications of blockchain and cryptocurrency. Badev and Chen's study looks at the applications of cryptography for secure transactions and the maintenance of distributed ledgers.[31] Both Lindsay[32] along with Pandy and Crow[33] assess potential applications for (distributed ledger technology) DLT's applications by government regulators and for use in processing payments. Related to this is the interest of central banks to develop a Central Bank Digital Currency (CBDC).[34] Cheng, Lawson, and Wong's study addresses what a sound legal framework should include for CBDC: 1) clear legal authority; 2) legal tender status; 3) AML and countering the financing of terrorism, and addressing sanctions evasion; 4) privacy and; 5) legal roles and responsibilities.[35] Finally, the Bank of International Settlements[36] published a study which designed a prudential treatment standard for cryptoassets. Together these works provide insights on the views of banking authorities relative to blockchain and cryptocurrency's utilities and risks.

Other economics studies focus more on theoretical aspects of cryptocurrency. Shaw discusses cryptocurrency in terms of its challenges to existing monetary models, the role of social

---

transactions-involving-convertible-virtual-currency-or-digital-assets. Hereafter referred to as FinCEN 2020c.

[30] FinCEN 2020c, 6.

[31] Anton Badev and Matthew Chen. "Bitcoin: Technical Background and Data Analysis," Finance and Economics Discussion Series 2014-104. Washington: Board of Governors of the Federal Reserve System, Oct. 7, 2014, https://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf.

[32] Jay Lindsay, "Past the hype: getting practical with blockchain," Federal Reserve Bank of Boston, Feb. 6, 2019. https://www.bostonfed.org/-/media/Documents/one-time-pubs/2019/blockchain-white-paper.pdf?la=en.

[33] Susan M. Pandy and Marianne Crowe, "Trends in Distributed Ledger Technology, Cryptocurrency, Mobile P2P Payments, Fraud, and Authentication," Federal Reserve Bank of Boston, May 1, 2020. https://www.bostonfed.org/-/media/Documents/PaymentStrategies/MPIW-Meeting-Final-Report-20200501.pdf.

[34] Add to term list: "a government issued and regulated virtual form of a fiat currency of a particular nation, represented by an electronic record or digital token."

[35] Jess Cheng, Angela N. Lawson, and Paul Wong, "Preconditions for a general-purpose central bank digital currency," Finance and Economics Discussion Series. Washington: Board of Governors of the Federal Reserve System, February 24, 2021. https://www.federalreserve.gov/econres/notes/feds-notes/preconditions-for-a-general-purpose-central-bank-digital-currency-20210224.htm.

[36] An international financial institution owned by central banks based in Bern, Switzerland. The bank also has the BASEL Committee, which helps to set standards for other global banking regulators.

construction in the creation of value, and the transition of Bitcoin from a social experiment to a multi-billion dollar industry.[37] Additionally, a meta-study by Molling, Klein, Hopen, and Dalla Rosa give insights into the most frequently subjects covered cryptocurrency article topics published between 2007-2018.[38] These included: 1) economics, 2) definitions and applications of cryptocurrency, cryptocurrency laws and regulations and 4) crimes involving (or conducted via) cryptocurrency.[39]

Illicit uses of cryptocurrency look at both non-state and state actors. For examples of non-state actors, Irwin and Milad,[40] as well as Sountra[41] study the use of cryptocurrency to fund terrorism. Irwin and Dawson build on this work seeking to determine how global regulation of cryptocurrencies can assist with ransomware attribution and other cybercrime incidents.[42] Studies of state actors actions' related to cryptocurrency often focus on nations with an adversarial relationship with the United States. Fanusie and Logan compare the cryptocurrency activities of Venezuela, Russia, Iran, and China.[43] Similarly, Konowicz provides an analysis of cryptocurrency strategies by Russia, the DPRK, Venezuela, Iran, and Sudan to avoid US sanctions.[44] Rodima-Taylor and Grimes look at the challenges Bitcoin posed to state actors' power, looking at the US, China, and Russia.[45]

There are a number of studies which look more parsimoniously at the DPRK and their cryptocurrency activities. McBride and Gold analyze hypothetical scenarios regarding security challenges posed by hostile state actors including, but not limited to the DPRK.[46] They assert that, "[The DPRK] is confirmed to have been active in the cryptocurrency space—largely motivated by a desire to avoid crippling international sanctions and to fund its weapons of

---

[37] Lynette Shaw, "The Meanings of New Money: Social Constructions of Value in the Rise of Digital Currencies," Ph.D. dissertation, 2016, University of Washington, Seattle.
[38] Graziela Molling, Amarolinda Klein, Norberto Hoppen and Rafael Dalla Rosa, "Cryptocurrency: A Mine of Controversies," Journal of Information Systems and Technology Management – Jistem USP, Vol. 1, 2020, https://doi.org/10.4301/s1807-1775202017010.
[39] Molling, et. al., 7.
[40] Angela S.M. Irwin and George Milad, "The use of Crypto-Currencies in Funding Violent Jihad," Macquarie University, Journal of Money Laundering Control, Vol 19, No. 4, Sydney, Australia, 2016, www.emeraldinsight.com/1368-5201.htm.
[41] Malik Amir Shahzad Sountra, "Cryptocurrency as a Modern Technique of Money Laundering and Terrorism Financing," LGU International Journal for Electronic Crime Investigation, Vol 3, Issue 4, October-December 2019.
[42] Angela S.M. Irwin and Caitlin Dawson, "Following the Cyber Money Trail: Global Challenges When Investigating Ransomware Attacks and How Regulation Can Help," Macquarie University, Journal of Money Laundering Control, Vol. 22, No. 1, Sydney, Australia, 2019, www.emeraldinsight.com/1368-5201.htm
[43] Yaya J. Fanusie and Trevor Logan, "Crypto Rogues: US State Adversaries Seeking Blockchain Sanctions Resistance," Foundation for the Defense of Democracies, July 2020, https://www.fdd.org/wp-content/uploads/2019/07/fdd-report-crypto-rogues.pdf.
[44] Deane R. Konowicz, "The New Game: Cryptocurrency Challenges US Economic Sanctions," United State Naval War College, Newport, RI. Feb. 8, 2018.
[45] Daivi Rodima-Taylor and William W. Grimes, "Cryptocurrencies and digital payment rails in networked global governance: perspectives on inclusion and innovation," in Bitcoin and beyond: Cryptocurrencies, blockchains, and global governance Malcolm Campbell-Verduyn, (ed.), London, UK, 89-90. http://hdl.handle.net/10419/181975
[46] See McBride and Gold.

mass destruction (WMD) program—since at least early 2017."[47] Clautice assesses several points: 1) the DPRK's embrace of cryptocurrency as a response to sanctions, 2) how the US utilized economic sanctions generally and, 3) how some countries have responded to DPRK cyber activities.[48] Relatedly, Ha and Maxwell[49] interpret the DPRK's efforts to be a type of asymmetric economic warfare. Finally, while being more of a general study, Bechtol's work details trends in the DPRK's illicit revenue generation including legacy Soviet weapons systems trade, diplomatic drug pouches, and cyberattacks in the international banking and financial system.[50]

SECTION 2: THEORY / METHODOLOGY

Methodology and Sources

This comparative case study looks at the DPRK's adoption and use of cryptocurrency to finance their policy goals and how the United States has responded to the DPRK's changing tactics. Source materials include press releases, public source announcements, guidance and rulemakings by US government agencies, and reports from the United Nations Security Council (UNSC) Panel of Experts.

Theory Structure for this Paper and Addressing Critiques

This work utilizes a social constructivist theoretical framework. Constructivist literature establishes that one's identity forms the basis of interests.[51] Ted Hopf, a leading constructivist scholar emphasizes the importance of norms and practice in developing a social context in international relations:

> Meaningful behavior, or action, is only possible only within an inter-subjective social context. Actors develop their relations with, and understandings of, others through the media of norms and practices. In the absence of norms, exercises of power, or actions, would be devoid of meaning. Constitutive norms define an identity by specifying the actions that will cause Others to recognize that identity and respond to it appropriately.[52]

[47] McBride and Gold, 20.
[48] Thomas Clautice, "Nation State Involvement in Cryptocurrency and the Impact to Economic Sanctions," La Salle University, Economic Crimes Forensics Program, May 20, 2019, https://digitalcommons.lasalle.edu/ecf_capstones/43.
[49] See Ha and Maxwell.
[50] Bruce E. Bechtol Jr., "North Korea Military Proliferation in the Middle East and Africa," The University Press of Kentucky, 2018.
[51] Ted Hopf. "The Promise of Constructivism in International Relations Theory," International Security, Volume 23, No. 1, Summer 1998, 175; Alexander Wendt, "Anarchy is what states make of it: the social construction of power politics," in International Organization, Vol. 46, No. 2, 1992, 398.
[52] Hopf, 193.

Constructivists argue that identity asserting policies are central to foreign policy choices.[53] This paper argues that this statement can be applicable to both foreign policy and regulatory policy. Norms often begin as practices, which are subsequently codified legally via international agreements (e.g. treaties and other agreements) or as domestic regulations (e.g. rulemakings and guidance) in administrative law. Additionally, sub-state institutions develop identities and norms that shape their respective cultures and the manner in which they carry out their legal mandates.

Next, the concepts of context and intersubjectivity are two critical terms in constructivist theory, which require definition for the purposes of this study. Context is defined as the circumstances in which an event, statement, or idea are perceived and in what terms it can be fully understood and assessed. Context is also formed by "precedents and shared symbolic materials—in order to impose interpretations upon events."[54] Cryptocurrency, in this case represents is a modern, documented social construction of a both a stored account of value and unit of account by a consensus among its adopters. Via the formation of transnational communities, cryptocurrencies have developed intersubjective meanings and contexts, which reinforced, or shifted by groupings of individuals. As these activities increasingly fall under the purview of sovereign state actors and sub-state agencies, individuals, and entities outside of these communities can also alter the understanding of and engagement with cryptocurrency.

So, why utilize constructivist theory as opposed to another school of international relations such as realist or liberal theory? Kowert writes that "realism and liberalism have been successful as theories of international politics not in spite of their normative content but precisely because people do, in fact, care about security and wealth."[55] Constructivism is just as well-equipped as these schools to address substantive problems, but also has the benefit of being able to assess individuals' identities as agents and confer those identities upon others.[56] A second critique of constructivist theory is that it often lacks specificity. Hopf concedes that constructivists for too long remained overly focused on the systemic level of analysis in world politics.[57] This case study aims to address both of these points. Though this case includes some systemic level analysis, the primary units of focus are sub-state actors, e.g. the DPRK's Intelligence Bureau General,[58] which is responsible for a great deal of theirs cyber activities, and the DOJ, Department of the Treasury, and the semi-independent financial services regulators under Treasury. Each of these entities operate within their own intersubjective contexts, which frame their understanding of themselves and each other.

---

[53] Paul A. Kowert, "The Peril and Promise of Constructivist Theory," *Ritsumeikan University Research Journal* 13-3, March 2001, 65.
[54] Hopf, 179.
[55] Kowert, 58.
[56] Kowert, 58.
[57] Hopf, 194.
[58] US Department of Justice, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe. Feb. 17, 2021. https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and. Hereafter referred to as DOJ 2021b.

Another critique that has been leveled against constructivism's methodological rigor is its use of "thick description."[59] However, rather than a shortcut, constructivism's "process and commitment to interpretivist thick description place extraordinary demands on the researcher to gather mountains of elaborate empirical data."[60] For this study in particular the use of "thick description" is essential to understand and explain the process by which broad objectives (e.g. the US imposing sanctions on the DPRK), are translated into enforceable, implemented policies. Specifically, this case requires a deep knowledge of the US regulatory rulemaking process, which covers the lifecycle of a law being implemented by a regulatory body.

COVID as an intervening variable

At the time of this writing, the global COVID-19 pandemic is ongoing. It is clear that COVID-19 is having severe impacts on the DPRK's economy, as the country has largely stopped the international movement of goods and people.[61] It's estimated that the DPRK's trade with China dropped 81% in 2020, resulting in a 10% contraction of their GDP.[62] While the long-term impacts of COVID-19 still unclear, it can be said with some confidence that the pandemic and the DPRK's response to it has done more damage to its economy than most of the sanctions previously imposed on it.[63]

SECTION 3: HOW HAS *CRYPTOCURRENCY* HAS CHANGED THE DPRK'S GENERATION AND MOVEMENT OF ILLICIT FUNDS

This section details how cryptocurrency caused a shift in the DPRK's ability and efforts to obtain revenue. First, there will be a brief history of their sanctions-evasion activities. Thereafter, this report will assess the increase in the frequency and scale of the DPRK cryptocurrency mining activities and cyberattacks on companies and other entities.

DPRK Sanctions Evasion Activities (Excluding Cryptocurrency and Cyber)

As the world economy integrated, the importance and efficacy of sanctions, particularly those imposed by the United States, has only grown in importance. Given the DPRK's defensive alliance with China and the obvious risks of war on the Korean Peninsula, the downsides of military options far outweigh potential benefits. This has incentivized indirect efforts to gain advantages vis-à-vis each other. The DPRK works to strengthen its position by acquiring missile and nuclear weapons capabilities as a deterrent against perceived US aggression. The

[59] Thick description utilizes requires the comprehensive dive into existing primary source materials.
[60] Hopf, 198.
[61] United Nations Security Council, "Report of the Panel of Experts Established Pursuant to Resolution 1874, S/2020/840," Aug. 28, 2020, https://www.undocs.org/en/S/2020/840
[62] Nikkei Asia, "North Korea's trade with China plunges 81% as lockdown bites," Jan. 19, 2021. https://asia.nikkei.com/Economy/North-Korea-s-trade-with-China-plunges-81-as-lockdown-bites.
[63] Sue Mi Terry. "South Korea Minimized the Damage from Covid-19. North Korea Maximized It." Center for Strategic and International Studies. https://www.csis.org/analysis/south-korea-minimized-damage-covid-19-north-korea-maximized-it, October 1, 2020.

United States seeks to cut off finances for these weapons programs via sanctions. Kim Jong Un depends on illicit funds in part to fund both the DPRK's military and to maintain domestic elite support for his rule. Please see the table below for a summary of ongoing DPRK sanctions evasion activities.

Table 2: Ongoing DPRK Sanctions Evasion Activities (Excluding Cryptocurrency)

1. Maritime 1.1. Reflagging of DPRK vessels 1.2. Prohibited fishing activities
2. Illegal Import and Export of Commodities and Other Goods 2.1. Imports of luxury goods 2.2. Ship to Ship transfers of refined petroleum products and coal 2.3. Export of sand totaling at least $22 million USD in 2019
3. Trade 3.1. Host biannual Pyongyang International Trade Fair
4. Financial Service / Operations of Designated Entities and Persons 4.1. DPRK bank representatives abroad 4.2. Financial operations of designated entities and DPRK diplomats
5. Conventional and Weapons of Mass Destruction (WMD) Sales and Materials Gathering 5.1. Use of diplomatic cover to transfer convention weapons and gather materials for WMD programs 5.2. Maintenance and sale of Soviet-legacy weapon systems
6. Counterfeiting / Illegal Goods 6.1. Counterfeit cigarettes and illegal drugs

Sources: United Nations Security Council,[64] Bechtol, Berlinger[65]

Separate from these activities are methods by which the DPRK obtained funds that have either largely ceased or declined in frequency or efficacy due to increased restrictions.

[64] See the following United Nations Security Council Reports: 1) Midterm of the Panel of Experts Pursuant to Resolution 2464, S/2019/691. Aug. 30, 2019. https://undocs.org/en/S/2019/691 (UNSC 2019); 2) Report of the Panel of Experts Established Pursuant to Resolution 1874, S/2020/151. March 2, 2020. https://undocs.org/S/2020/151 (UNSC 2020a); 3) Report of the Panel of Experts Established Pursuant to Resolution 1874, S/2020/840. August 28, 2020. https://www.undocs.org/en/S/2020/840 (UNSC 2020b).

[65] Joshua Berlinger, "North Korea might be making millions – and breaking sanctions – selling sand. Yes, sand," CNN Business, June 10, 2020, https://www.cnn.com/2020/06/09/business/north-korea-sand-intl-hnk/index.html

Table 3: DPRK Sanctions Evasion Activities (ceased and/or less frequent)

1.	Currency Counterfeiting of USD
2.	Human Trafficking / Overseas Labor
3.	Wildlife Trade
4.	Misuse of embassy properties and diplomatic staff
5.	Tourism

Sources: United Nations Security Council[66]

One example of this was the development of high-quality counterfeit $50 USD and $100 notes often called "supernotes." Following updates to the dollar's design, these supernotes were only being reported found three times between 2008-2016.[67]

Another revenue source for the DPRK comes from overseas labors whose earnings are largely repatriated to their government. DPRK overseas workers were still in Russia, Nigeria, and the Middle East as of 2018.[68] Following continued weapons tests and provocations, the UNSC passed Resolution 2397,[69] which required the repatriation of most DPRK nationals to the country by December 22, 2019. The reporting results of the resolution thus far seem mixed, with responses only submitted by 40 member states[70] and replies pending from some African and European nations.[71] Illegal wildlife trade has also been another revenue source for the DPRK, particularly in Africa, resulting in five nations expelling DPRK diplomats in sub-Saharan Africa.[72]

Finally, COVID-19 and the DPRK's response has also had a substantial impact on these revenue sources. The cross-border transportation of goods and people have been severely

[66] See the following United Nations Security Council Reports: 1) Midterm of the Panel of Experts Pursuant to Resolution 2464, S/2019/691. Aug. 30, 2019. https://undocs.org/en/S/2019/691 (UNSC 2019); 2) Report of the Panel of Experts Established Pursuant to Resolution 1874, S/2020/151. March 2, 2020. https://undocs.org/S/2020/151 (UNSC 2020a); 3) Report of the Panel of Experts Established Pursuant to Resolution 1874, S/2020/840. August 28, 2020. https://www.undocs.org/en/S/2020/840 (UNSC 2020b).
[67] Greg Walters, "North Korea's Counterfeit Benjamins Have Vanished," Vice News, March 16, 2016, https://www.vice.com/en/article/vb8pk9/north-koreas-counterfeit-benjamins-have-vanished.
[68] Mengqi Sun and Ian Talley. US Blacklists Two Companies It Says Exploits North Korean Workers. Wall Street Journal. Jan. 14, 2020. https://www.wsj.com/articles/u-s-blacklists-two-companies-it-says-exploits-north-korean-workers-11579033486.
[69] See United Nations Security Council, "Resolution 2397, S/RES/2397. Dec. 22, 2017. https://www.ncnk.org/sites/default/files/UNSCR_2397.pdf
[70] UNSC 2020b, 4.
[71] UNSC 2020a, 54-55.
[72] Rachel Nuwer, "North Korean Diplomats Accused of Smuggling Ivory and Rhino Horn," National Geographic. Oct. 16, 2017. https://www.nationalgeographic.com/news/2017/10/wildlife-watch-north-korea-illegal-wildlife-trade/.

restricted due to quarantine measures in response to COVID-19.[73] Although, drug trafficking by DPRK diplomats had largely ceased years ago,[74] COVID-19 further limited their ability to generate revenue.[75] A previous, related issue was the use of DPRK embassies for commercial activity,[76] which several European nations have cracked down on. Other than direct trade, perhaps the source of revenue most negatively impacted by COVID-19 has been tourism, especially from China.

How DPRK Sanctions Evasion Changed Due to Cryptocurrency

As US and international sanctions increased over the prior decade, the DPRK has responded by shifting its illicit economic activities to cyberattacks and other digital scams, with the goal of gaining cryptocurrency to convert into fiat currency.[77] This section will first provide definitions related to cyberattacks and cryptocurrency. Next, it will assess why the DPRK has become increasingly dependent on cryptocurrency. Finally, it will detail the tools available to the DPRK, as well as notable cyberattack incidents.

There are several methods through which one can generate revenue via cyberattacks. The first is malware, which cause other computers to not function or fail to carry out designated activities. In some cases, malware hijacks other computers' processing capability to mine cryptocurrency.[78] One prominent type of malware is called ransomware, which locks down a system's data and can be released through payment of a ransom to the attacker,[79] with convertible virtual currency (CVC)[80] being a preferred means of payment.[81] This has become an important enough issue that the Group of Seven (G7) and Treasury Department have issued statements on ransomware and the role of cryptocurrency in money laundering.[82]

So, how do individuals and sub-state actors money-launder via cryptocurrency? One way is to use a "mixer," which breaks the connection between addresses sending and receiving cryptocurrency, making transaction tracing difficult to nearly impossible.[83] Another method is called a "peel chain." Peel chains are a series of high-volume cryptocurrency transactions,

[73] UNSC 2020b, 4
[74] Sheena Greitens, "Illicit: North Korea's Evolving Operations to Earn Hard Currency," Committee for Human Rights in North Korea, Sept. 5, 2014, https://www.hrnk.org/uploads/pdfs/SCG-FINAL-FINAL.pdf.
[75] Todd Wiesel, "PacNet #13 – Keep an eye on North Korean cyber-crime as the Covid-19 spreads," *PacNet*, Pacific Forum, last accessed March 12, 2021, https://pacforum.org/publication/pacnet-13-keep-an-eye-on-north-korean-cyber-crime-as-the-covid-19-spreads
[76] UNSC 2020b, 29.
[77] Burgess; Priscilla Moriuchi, "North Korea's Ruling Elite Adapt Internet Behavior to Foreign Scrutiny," Recorded Future, April 25, 2018, https://www.recordedfuture.com/north-korea-internet-behavior/.
[78] Legitimate mining activities occur through the period release of new coins which are obtained through the solving of mathematical equations through the use of computers online.
[79] Irwin and Dawson.
[80] CVCs are more readily converted into fiat currencies such as the USD or Japanese Yen.
[81] US Financial Crimes Enforcement Network, "First Bitcoin "Mixer" Penalized by FinCEN for Violating Anti-Money Laundering Laws," Oct. 19, 2020, https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws. Hereafter referred to as FinCEN 2020b
[82] US Department of the Treasury, "Ransomware Annex to G7 Statement," Oct. 13, 2020, https://home.treasury.gov/system/files/136/G7-Ransomware-Annex-10132020_Final.pdf. Hereafter referred to as Treasury Department 2020a.
[83] FinCEN 2020b.

which are conducted in short period of time to obfuscate the origin of funds. A third method, "chain-hopping," is a type of peel chain where transactions are used to convert one type cryptocurrency into others before cashing out in a fiat currency (see Figure 4 and Figure 5 for visual representations).

For the DPRK, access to cryptocurrency provides several benefits. First, it replaces revenue sources lost to tightening sanctions. Second, blockchain and cryptocurrency technologies enable actors adversarial to the United States to increasingly operate outside of the US-led financial system.[84] In addition, obtaining cryptocurrency via malware and ransomware is seen as a relatively high-reward, low-risk option due to complex investigation and attribution processes.[85] It's estimated that the DPRK's Reconnaissance General Bureau has more than 6,000 full-time cyber-operatives and support staff involved in cybercrime.[86] Besides the practical necessity to obtain funds, the DPRK's cyber activities also reaffirm their national identity. First, their activities demonstrate asymmetrical capabilities against foreign adversaries, particularly the United States. Moreover, though not officially acknowledged, success in these efforts bolster domestic political support for Kim Jong Un's regime from the Workers' Party of Korea (WPK) and the DPRK military. In short, cyberattacks serve the regime's goals in several ways by 1) showing national strength, 2) obtaining funds for policy priorities, and 3) covertly thumbing their nose at the American-led international system.

A History of DPRK Cyber Activities

2014 seems to have been a turning point for the DPRK regarding cyberspace. The hacking of Sony Pictures was one of the first notable cyberattacks conducted by the DPRK. That same year, Mt. Gox, the world's large cryptocurrency exchange at the time, was attacked, resulting in the loss of $500 million worth of Bitcoin, causing their subsequent bankruptcy.[87] While the DPRK did not have a role in the attack, it can be assumed that they learned that cryptocurrency exchanges and traders were ripe targets.

Over the past few years, the DRPK launched enough cyberattacks on the Republic of Korea's (ROK) business, government, and non-profits to the point where the ROK had to increase their own counter cyber capabilities to deal with it.[88] In 2016, the DPRK also conducted a series of attacks referred to as the "FASTCash Campaign," stealing millions from ATMs in Asia and Africa.[89] The following year, they stole $81 million from the Central Bank of Bangladesh via the SWIFT money transfer system.[90] Also in 2017, the DPRK launched a

[84] Fanusie and Logan, 6
[85] UNSC, 2019, 27, see footnote 30.
[86] Eun DuBois, "Building Resilience to the North Korean Cyber Threat: Experts Discuss," Brookings, December 23, 2020, https://www.brookings.edu/blog/order-from-chaos/2020/12/23/building-resilience-to-the-north-korean-cyber-threat-experts-discuss/.
[87] McBride and Gold, 12.
[88] Bechtol, 39.
[89] US Cybersecurity & Infrastructure Security Agency, "Alert (AA20-106A) Guidance on the North Korean Cyber Threat," April 15, 2020, 4, https://us-cert.cisa.gov/ncas/alerts/aa20-106a.
[90] Bechtol, 41

series of cyberattacks on public and private institutions, including the United Kingdom's National Institute of Health's hospital system.[91]

Over time, the DPRK shifted to attacks on cryptocurrency exchanges as other targets bolstered their defenses. According to a 2020 UNSC panel of experts' report:

> One Member State reported that attacks against virtual currency exchange houses have produced more illicit proceeds than attacks against financial institutions, whose information technology infrastructure is typically less susceptible to cyberintrusion.[92]

The most frequent initial targets were ROK-based cryptocurrency exchanges. An attack in April 2017, cost the Youbit exchange $4.7 million USD and resulted in its closure. Bithumb, another ROK-based exchange was attacked at least four times between February 2017-March 2019 with loses totaling around $51 million.[93] In April 2018, the DPRK hacked the Digital Currency Exchange.[94] As of August 2019, the UNSC panel of experts were undertaking investigations of at least 35 suspected DPRK attacks on financial institutions, cryptocurrency exchanges, and mining activities by the DPRK.[95] There is even evidence that the DPRK created fake cryptocurrency exchanges targeting investors and traders. One of these, Marine Chain Platform Limited, was registered in April 2018 in Hong Kong to trade digital tokens for partial ownership of maritime vessels as a DPRK front company.[96] JPMT Trader and Celas Trade Pro also posed as trading platforms intended to infect users' computers with malware linked to the Lazarus group.[97]

Another means by which the DPRK obtains cryptocurrency is through mining activities. According to a 2018 study, the DPRK continued mining Bitcoin and started mining Monero,[98] a type of AEC, which is extremely difficult to trace.[99] The UNSC panel of experts confirmed that the DPRK military also has a branch engaged in mining Bitcoin and Monero,[100] with Monero mining activity growing significantly.[101] Once obtained, the DPRK moves their cryptocurrency and other illicit digital assets through numerous banks and front companies[102] and exploits "over the counter" brokering services to convert illicit digital assets into fiat currency.[103] As this section has demonstrated, the DPRK's strategy of revenue generation has changed significantly over time to include a large and increasing cyber component in order to obtain cryptocurrency. Besides the material gains, these activities also serve to tacitly reaffirm the DPRK's national self-identity.

---

[91] Keith B. Alexander and Jamil N. Jaffer. Enduring US Dominance in Cyberspace in a World of Significant Peer and Near-Peer Competition. *Georgetown Journal of International Affairs* 19, no. 1 (Fall 2018): 51-66.
[92] UNSC 2020b, 43.
[93] UNSC 2019, 27-28.
[94] US Cybersecurity & Infrastructure Security Agency, 4.
[95] See UNSC 2019, 26 & 109-112 for a full list of suspected attacks.
[96] UNSC 2019, 28.
[97] UNSC 2019, 213-214, See Annex 53.
[98] Moriuchi.
[99] UNSC 2019.
[100] UNSC 2019, 28.
[101] UNSC 2020b, 43, footnote 93.
[102] Bechtol, 44.
[103] UNSC 2020b, 44.

SECTION 4: US POLICY SHIFTS TO ADDRESS DPRK CYBERATTACKS AND MONEY LAUNDERING VIA CRYPTOCURRENCY

This section will look at how US policy has sought to address the DPRK's new cryptocurrency money laundering activities. First, a brief history of US sanctions on the DPRK looking at legislation, regulatory guidance, rulemakings, and actions by financial services and law enforcement authorities will be detailed. Then, recent actions taken to regulate cryptocurrency activities and prevent money-laundering will be explained and contextualized in relation to the DPRK's activities. The primary scope of coverage for this section is the second Obama term of the administration (2013-2017) and the Trump administrations (2017-2021). Finally, there will be an assessment of the shift in US policy on cryptocurrency, particularly as it relates to cybersecurity issues.

Obama Administration: From 'Strategic Patience' to Strategic Sanctions

While President Obama's approach towards the DPRK was referred to as "strategic patience," patience began to run out towards the end of his first term. This led to the development of a comprehensive sanctions regime on the DPRK utilizing tools developed and implemented following the 2001 -9/11 terrorist attacks. In 2011, President Obama issued Executive Order (EO) 13570, which prohibited the direct or indirect import of any goods, services, or technology from the DPRK.[104] Financial transactions with the DPRK also began to be explicitly targeted when the Treasury Department issued an advisory in 2014.[105] In 2015, this was further expanded by EO13687 which,

> [b]locks transfer, payment, export, withdrawal or otherwise dealings with property and interests in property that are in the United States by the DPRK government, the Workers' Party of Korea [WPK]. Additionally covered are those who materially assisted or provided support to the DPRK government, or acted on their behalf.[106]

The following year, the Treasury Department designated the DPRK a jurisdiction of primary money laundering concern under Section 311 of the USA PATRIOT Act,[107] imposing further barriers on private entities that conducted financial transactions or other business with the DPRK.

In 2016, EO13722 was issued, further expanding EO13687's provisions to include larger sectors of the DPRK economy such as the export of workers for revenue generating

---

[104] Executive Office of the President, "Executive Order 13570 of April 20, 2011. Prohibiting Certain Transactions with Respect to North Korea," Federal Register, Vol. 76, No. 26, https://www.federalregister.gov/documents/2011/04/20/2011-9739/prohibiting-certain-transactions-with-respect-to-north-korea.
[105] Bechtol, 61.
[106] Executive Office of the President of the United States, "Executive Order 13687 of Jan. 6, 2015: Imposing Additional Sanctions with Respect to North Korea," Federal Register, Vol. 80, No. 3. https://www.federalregister.gov/documents/2015/01/06/2015-00058/imposing-additional-sanctions-with-respect-to-north-korea.
[107] Bechtol, 64.

activities.[108] It also significantly sanctioned entities who "have engaged in significant activities undermining cybersecurity through the use of computer networks or systems against targets outside of North Korea on behalf of the Government of North Korea or the Workers' Party of Korea."[109] This represented a clear acknowledgement of the fact that overseas workers and cyberattacks constituted a significant source of revenue for the DPRK. In addition to executive action, Congress passed the *North Korea Sanctions and Policy Enforcement Act of 2016*,[110] which greatly broadened the authority of the executive branch to sanction DPRK actors. Please see Table 4 below detailing the range of restricted activities.

Table 4: Mandatory Designations Under the North Korea Sanctions and Policy Enforcement Act of 2016

1.	Direct and indirect involvement with the import, export or reexport of goods, services or technologies controlled for export by the United States with the DRPK
2.	Direct or indirect training, technical assistant or financial contribution to manufacture, maintenance or use of a WMD (table) with the DPRK
3.	Import, export or reexport of luxury goods
4.	Engages in, responsible for or facilitating censorship by the DPRK government
5.	Engages in, responsible for or facilitating human rights abuses by the DPRK
6.	Engages in money laundering, counterfeiting, cash smuggling or narcotics trafficking that support the DPRK or persons acting for or on their behalf
7.	Engage in activities that undermine cybersecurity on behalf of the DPRK government (or any person acting on their behalf)
8.	Selling, supplying, or transferring to the DPRK materials for use by or in industrial processes related to WMDs or other proliferation activities

Source: 22 USC 9201. North Korea Sanctions and Policy Enforcement Act of 2016.

Moreover, the act explicitly codified restrictions on financial transactions with the DPRK. Under Title II, Sec. 201 of the law, the DPRK was determined to be a jurisdiction of primary money laundering concern.[111] This designation requires US financial institutions and foreign institutions with a US presence (e.g. representative offices or foreign bank branches) to take additional measures regarding to prevent money laundering by the DPRK. Given the size

[108] Executive Office of the President of the United States, "Executive Order 13722 of March 15, 2016: Blocking Property of the Government of North Korea and the Workers' Party of Korea, and Prohibiting Certain Transactions With Respect to North Korea," Federal Register, Vol. 81, No. 53, https://www.federalregister.gov/documents/2016/03/18/2016-06355/blocking-property-of-the-government-of-north-korea-and-the-workers-party-of-korea-and-prohibiting.
[109] Executive Office of the President of the United States, 2016.
[110] See 22 United States Code 9201, "North Korea Sanctions and Policy Enforcement Act of 2016," https://www.congress.gov/114/plaws/publ122/PLAW-114publ122.pdf. Hereafter referred to as North Korea Sanctions and Policy Enforcement Act of 2016.
[111] North Korea Sanctions and Policy Enforcement Act of 2016, 101.

and influence of the US economy, this has a large extraterritorial effect requiring financial institutions to apply the US standards internationally. Sec. 202 of the act set conditions for ensuring the consistent enforcement of UNSC resolutions and financial restrictions on the DPRK. [112] Finally, Sec. 210 codified sanctions on DPRK activities undermining cybersecurity.[113] This created a comprehensive framework for applying US and UN sanctions against a broad swath of the DPRK's economy Overall, the Obama administration saw a codification and scaling up of sanctions on the DPRK, which was subsequently expanded upon under President Trump.

Trump Administration: From Fire and Fury to Face-to-Face Diplomacy

While President Trump's administration often broke sharply from his predecessor's policies. However, regarding the DPRK, the Trump administration largely continued Obama-era policies of expanding sanctions against them. EO13810 broadened US sanctions to include individuals and entities with commercial or economic ties with the DPRK.[114] The intent behind this was to utilize "secondary sanctions"[115] to target entities and individuals trading with DPRK and the banks which moved their money.[116] The most notable application of this was the imposition of sanctions by the United States against the Chinese Bank of Dandong.[117] Additionally, in June and August 2017, three civil forfeiture cases were filed against shell companies that laundered money towards DPRK weapons programs.[118]

Along with continued executive action against the DPRK, several pieces of significant legislation were also passed during the Trump administration. The first was in response to an American citizen who was imprisoned, beaten into a coma in the DPRK, and died in 2017. The Otto Warmbier Act[119] expanded upon Title II of the *North Korea Sanctions and Policy Enhancement Act of 2016* to allow for the imposition of secondary sanctions on foreign financial entities, which perform significant financial services to any DPRK citizens as designated by:

> (1) subsection (a), (b), or (g) of section 104 [of the North Korea Sanctions and Policy Enforcement Act of 2016]; (2) an applicable Executive order; or (3) an applicable United Nations Security Council resolution.[120]

The law blocks access to assets, financial accounts, and services for designated individuals. In March and August 2020, the DOJ announced complaints seeking civil forfeiture of virtual

---

[112] North Korea Sanctions and Policy Enforcement Act of 2016, 104.
[113] North Korea Sanctions and Policy Enforcement Act of 2016, 111.
[114] Executive Office of the President, "Executive Order 13810 of September 20, 2017; Imposing Additional Sanctions with Respect to North Korea," September 20, 2017, Federal Register, Vol. 82, No. 184, https://www.federalregister.gov/documents/2017/09/25/2017-20647/imposing-additional-sanctions-with-respect-to-north-korea.
[115] Sanctions imposed against individuals or entities who do business with a designated person or entity.
[116] Bechtol, 65.
[117] Bechtol, 66.
[118] Bechtol, 77.
[119] See 22 United States Code 9201 "Otto Warmbier North Korea Nuclear Sanctions and Enforcement Act of 2019," December 20, 2019, https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf. Hereafter referred to as the Otto Warmbier Act.
[120] Otto Warmbier Act, 1048.

currency accounts associated with DPRK cyber hacks and money laundering[121] under the authority provided by the law.

At the end of 2020, two additional laws were passed as part of the *2021 National Defense Appropriations Act*: 1) the *Anti-Money Laundering Act of 2020* (AML Act) and; 2) the *Corporate Transparency Act* (CTA).[122] The AML Act of 2020 broadened the range of provisions that could increase enforcement penalties against cryptocurrency firms for AML violations.[123] It also expanded the definition of financial institutions and MSBs to include the exchange or transmission of "value that substitutes for currency" and reinforces the US government's assertion that the BSA applies to cryptocurrency.[124] The CTA closed a loophole related to the reporting of "beneficial ownership,"[125] which previously allowed a large number of shell companies to hide and move illicit assets and to exist under the radar in the United States. While these two laws don't directly target the DPRK, they could be applied against them, and they do seek to set standards which other nations may emulate to close off some avenues of money laundering.

Integrating Cryptocurrency into the US Financial Services Framework

Rhetoric aside, perhaps one of the most important differences between the Obama and Trump administration's policies towards countering the DPRK's illicit revenue generation was an increased focus on cryptocurrency. This was due to several factors. First, cryptocurrency theft and cybersecurity issues only reached wider notoriety towards the end of President Obama's second term. Also, it became clear around the transition to the Trump administration how much money the DPRK was able to obtain via cryptocurrency. Finally, the tracking, regulatory, and enforcement infrastructures around cryptocurrency were and still are maturing

Rulemakings

Significant implementation of comprehensive US regulations regarding cryptocurrency has taken place, particularly since 2019. This section will look at rulemakings, guidance, and enforcement actions taken in the last three years by US financial service agencies to rationalize market activities involving cryptocurrency consistent with conventional regulations.

---

[121] DOJ 2020a, 28.

[122] Public Law No. 116-283, "H.R.6395 - National Defense Authorization Act for Fiscal Year 2021," 116th Congress of the United States, https://www.congress.gov/bill/116th-congress/house-bill/6395/text/pl. See Division F, Sec. 6003-6314 for details on the AML Act of 2020 and Sec. 6401-6403 for the Corporate Transparency Act respectively. Hereafter referred to as the National Defense Authorization Act for Fiscal Year 2021.

[123] Stark.

[124] Stark.

[125] Beneficial ownership refers to exceeding a certain ownership threshold, or having some other contractual obligations that demonstrate some degree of control over a company. In this case, National Defense Authorization Act for Fiscal Year 2021, Title LXIV, Sec. 6403 requires much more substantial reporting of beneficial ownership directly from companies within a year of creation or modification to FinCEN.

In April 2020, the Office of Foreign Assets Control (OFAC) implemented amendments based on the *2020 National Defense Authorization Act* by "incorporating blocking and correspondent account sanctions provisions, adding a new prohibition that is applicable for entities that are owned or controlled by a US financial institution and established or maintained outside the United States," which would include cryptocurrency.[126] In December 2020, the Treasury Department proposed a rule which would require financial institutions to record and sometimes report significant cryptocurrency transactions involving unhosted wallets,[127] in order to help quickly and accurately track money laundering by terrorists, drug and human traffickers, and cyber criminals. Additionally, it clarified the definition of "money" to consistently apply rules related to domestic and cross-border transactions involving cryptocurrency in a manner similar to legal tender.[128] Effectively this would require the collection, verification, and retention of personal identifiers by financial institutions of the transmitters and beneficiaries of transactions.[129] Additionally, it lowers the required reporting threshold from $3,000 USD to $250 USD for fund transfers and transmission of funds that begin or end outside of the United States.[130] This could also be applied to tracking information on illicit funds being transferred to or from state actors such as the DPRK.[131] That same month, FinCEN issued a related rulemaking…

> to require banks and money service businesses ("MSBs") to submit reports, keep records, and verify the identity of customers in relation to transactions involving convertible virtual currency ("CVC") or digital assets with legal tender status ("legal tender digital assets" or "LTDA") held in unhosted wallets . . . or held in wallets hosted in a jurisdiction identified by FinCEN.[132]

One of the reasons for the rulemaking cited in the document was as a response to ransomware attacks.[133] US authorities have found the use of CVCs to among other things, "facilitate . . . sanctions evasion, and transnational money laundering . . . malware and other computer hacking tools . . ."[134] Additionally, FinCEN seeks to deal with challenges posed by

---

[126] US Office of Foreign Assets Control, "North Korea Sanctions Program Regulations," April 10, 2020, https://www.federalregister.gov/documents/2020/04/10/2020-07497/north-korea-sanctions-regulations. Hereafter referred to as OFAC 2020b.
[127] US Department of the Treasury, "Frequently Asked Questions: Requirements for Certain Transactions Involving Certain Convertible Virtual Currency or Digital Assets," Dec. 18, 2020, https://home.treasury.gov/system/files/136/2020-12-18-FAQs.pdf. Hereafter referred to as Treasury 2020b.
[128] US Financial Crimes Enforcement Network, "Proposed Rulemaking: Threshold for the Requirement to Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement to Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets with Legal Tender Status," Dec. 30, 2020, 1. https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201023a.pdf. Hereafter referred to as FinCEN 2020d.
[129] FinCEN 2020d, 6-7.
[130] FinCEN 2020d, 8.
[131] DOJ 2020a, 16, citation 39.
[132] FinCEN 2020c, 1.
[133] FinCEN 2020c, 1-2.
[134] FinCEN 2020c, 7.

AECs, which have been tied to the WannaCry attack and use on various "darknet"[135] marketplaces.[136] This is also compounded by concerns about the targeting of critical infrastructure by malign actors seeking illicit payment during the COVID-19 pandemic.[137] These sentiments were echoed by both OFAC and the US Federal Bureau of Investigations.[138]

Though not explicitly a rulemaking, the SEC issued a statement on Custody of Digital Assets by Special Purpose Broker Dealers, which will be valid for five years while market participants develop best practices and processes for security control over digital asset securities.[139] The statement is premised on the idea that broker dealers trading in digital asset securities limit themselves to just this activity to minimize risk and have policies in place to access the tools to transfer the asset (such as DLT and private keys).[140] The SEC is seeking to address cybersecurity risks associated with cryptocurrency as financial securities. Finally, in January 2021 an interagency rule was proposed requiring financial institutions to report computer-security incidents within 36 hours to their primary prudential federal regulator.[141] This should help provide federal agencies a quicker heads up of cyber breaches of critical financial infrastructure, such as ransomware attacks.

Guidance

Though not the same as rulemakings, agency guidance serves as an indicator of the direction of future potential regulatory actions. In April 2020, several agencies released interdepartmental guidance on how to protect governments, civil society, and individuals from DPRK cyber threats.[142] The DPRK was cited as conducting cyber-enabled financial theft and money laundering, extortion campaigns, and cryptojacking.[143] In October 2020, FinCEN published guidance assessing trends and indicators of ransomware and related money laundering activities, including the use of convertible virtual currency.[144] Notably, the guidance indicated that the "facilitat[ion of] ransomware payments to cybercriminals . . . could

[135] Darren Guccione, "What is the dark web? How to access it and what you'll find," CSO, https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html. The darknet (also commonly referred to as the dark web), is a subset of unindexed websites, which are only accessible via the use of specialized web browsers and search engines. Some, but not all sites on the dark web are used for illicit purposes.
[136] FinCEN 2020c, 8.
[137] FinCEN 2020c, 2.
[138] US Office of Foreign Assets Control. Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. Oct. 1, 2020. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf, 1 Hereafter referred to ask OFAC 2020d.
[139] US Securities and Exchange Commission, "Statement: Custody of Digital Asset Securities by Special Purpose Broker Dealers," Dec. 23, 2020, 4, https://www.sec.gov/rules/policy/2020/34-90788.pdf.
[140] SEC 2020, 2-3.
[141] US Department of the Treasury, "Proposed Rulemaking: Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers," Jan. 12, 2021, 1, https://www.federalregister.gov/documents/2021/01/12/2020-28498/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank.
[142] US Cybersecurity & Infrastructure Security Agency, 5-7.
[143] US Cybersecurity & Infrastructure Security Agency, 2.
[144] FinCEN 2020b.

constitute money transmission."[145] OFAC issued similar guidance stating that the payment of ransomware could also constitute a sanctions breach.[146] In short, FinCEN and OFAC's policy postures could significantly raise the negative opportunity costs for individuals, companies, and other entities who choose to pay ransomware. The purpose of this is to make it more costly to pay ransomware than it is to either: a) address the cybersecurity deficiencies that allowed the breach in the first place or b) replace the lost or stolen data. Building on this, the Treasury Department published the National Strategy for Combatting Terrorist and Other Illicit Financing at the end of June 2021, which among other things seeks to "[c]larify or update our regulatory framework to expand coverage of digital assets."[147]

Enforcement Actions

DPRK-affiliated individuals and groups along with cryptocurrency have come into the crosshairs of US regulators and law enforcement. In the past few years, a number of enforcement actions and prosecutions have been undertaken. One example of this is the sanctioning of three North Korean state-sponsored groups ("Lazarus Group," "Bluenoroff," and "Andariel") responsible for cyberattacks on critical infrastructure, including the 2017 WannaCry 2.0 attack by OFAC in 2019.[148] At the beginning of 2021, the DOJ filed charges against three DPRK computer programmers in the Reconnaissance General Bureau with conducting the 2014 Sony Pictures attack, the 2016 Bank of Bangladesh heist, and the 2017 WannaCry Attacks.[149] Soon thereafter, there was the first extradition of a DPRK citizen from Malaysia to the United States on charges of money laundering through the US financial system.[150]

Separate from direct prosecutions of DPRK citizens, US agencies also targeted others who have helped the DPRK money launder..[151] Additionally, OFAC reached a $500,000 settlement with BitPay, Inc., a cryptocurrency exchange, for violations of DPRK and other sanctions programs while processing cryptocurrency transactions from 2013-2018.[152] One of the most prominent sanctions enforcement cases was the prosecution of Virgil Griffith, an American citizen, on conspiracy to violate the *International Emergency Economic Powers Act*. Griffith was accused of providing services to the DPRK without approval from OFAC

[145] FinCEN 2020b.
[146] OFAC 2020d, 1
[147] US Department of the Treasury, "National Strategy for Combatting Terrorist and Other Illicit Financing," June 30, 2021. https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf, 4.
[148] US Department of the Treasury, "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups," September 13, 2019, https://home.treasury.gov/news/press-releases/sm774.
[149] US Department of the Treasury, "Assistant Attorney General John C. Demers Delivers Remarks on the National Security Cyber Investigation into North Korean Operatives," Feb. 17, 2021, https://www.justice.gov/opa/pr/assistant-attorney-general-john-c-demers-delivers-remarks-national-security-cyber. Hereafter referred to as DOJ 2021c.
[150] US Department of Justice, "First North Korean National Brought to the United States to Stand Trial for Money Laundering Offenses," March 22, 2021, https://www.justice.gov/opa/pr/first-north-korean-national-brought-united-states-stand-trial-money-laundering-offenses. Hereafter referred to DOJ 2021d.
[151] DOJ 2021b.
[152] US Office of Foreign Assets Control, "OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions," Feb. 18, 2021, https://home.treasury.gov/system/files/126/20210218_bp.pdf.

between August 2018-November 2019.[153] The charges stemmed from Griffith travelling to the DPRK and attending the Pyongyang Blockchain and Cryptocurrency Conference where he "provided the DPRK with valuable information on blockchain and cryptocurrency technologies, and participated in discussions regarding using cryptocurrency technologies to evade sanctions and launder money."[154] The DOJ stated that Griffith knowingly provided provision of services and a transfer of technical knowledge to the DPRK, which they would probably use to avoid US sanctions. Griffith subsequently plead guilty to the charges on September 27, 2021.[155]

This has also coincided with a general increase in enforcement against cryptocurrency-related money laundering. FinCEN fined an operator of two companies operated virtual currency "mixers" for violations of the BSA,[156] by obfuscating the origins or original holders of the CVC in October 2020. The following month, the US government seized $24 million in connection with a large cryptocurrency fraud scheme called "Operation Egypto" at the request of the Brazilian government.[157]

Overall US Policy Orientation

The shift in regulatory rulemakings, guidance, and enforcement actions indicate several points. First, the US is stepping up efforts to address cyberattacks and money laundering by the DPRK including cryptocurrency. Next, enforcement actions against individuals and companies involved with cryptocurrency exchanges and businesses are on the rise, but prosecutions specific to the DPRK are still somewhat limited on that issue. The US government sees "ransomware payments made to sanctioned persons or to comprehensively sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States."[158] Finally, in a report by the Attorney General's cyber digital taskforce in October 2020, they categorized the illicit use of cryptocurrency into three categories:

> 1) financial transactions associated with the commission of crimes;
> 2) money laundering and the shielding of legitimate activity from tax, reporting, or other legal requirements; or
> 3) crimes, such as theft, directly implicating the cryptocurrency marketplace itself.[159]

Overall, there has been a significant shift in US policy regarding both sanctions vis-a-vis the DPRK and regulation towards cryptocurrency.

---

[153] US Southern District of New York Federal Court, 1.
[154] US Southern District of New York Federal Court, 2-3.
[155] US Department of Justice, "United States Citizen Pleads Guilty To Conspiring To Assist North Korea In Evading Sanctions," September 27, 2021, https://www.justice.gov/usao-sdny/pr/united-states-citizen-pleads-guilty-conspiring-assist-north-korea-evading-sanctions.
[156] FinCEN 2020b.
[157] US Department of Justice, "US Seizes Virtual Currencies Valued at $24 Million Assisting Brazil in Major Internet Fraud Investigation," Nov. 4, 2020, https://www.justice.gov/opa/pr/us-seizes-virtual-currencies-valued-24-million-assisting-brazil-major-internet-fraud. Hereafter referred to as DOJ 2020d.
[158] OFAC 2020d, 3.
[159] DOJ 2020a, viii.

SECTION 5: CONCLUSION

Assessment of Analytical Structure Applied to this Case Study

The social constructivist theory structure detailed in this paper held up well relative to the information presented in the case study. The DPRK governments saw new opportunities to fund policy goals while reaffirming their national identity via cryptocurrency, while projecting strength, striking at adversaries, and affirming the elite domestic legitimacy of Kim Jong Un's leadership.

This change in DPRK behavior caused a response from the United States. Given the large, bureaucratic structure of the US federal government, federal and state agencies have developed separate, sometimes disjointed approaches to the regulation of cryptocurrency based on their authorities, mandates, and institutional cultures. Consequently, while long-term policy is moving towards a "prudential regulation" regime for cryptocurrency, the fragmentation of the regulatory rulemaking process has considerably slowed down accomplishing this goal. If the United States is able to create and enforce a consistent rules regime, it could have a significant impact on reducing the DPRK's access to illicit funds and undermining confidence in Kim Jong Un's leadership as well as their foreign policy goals.

Finally, the COVID-19 pandemic has amplified existing trends in both the DPRK and US. With the DPRK's border closures, there is a strong perceived need to recoup lost funds. In the United States, the pandemic significantly increased the importance of cyber infrastructure. This increased threat perception extends to attacks on public and private cyber infrastructure as losses from malware and ransomware attacks on private businesses mount.

Policy Implications of this Study

There are a number of implications that can be drawn from this study. First, the emergence and maturation of cryptocurrency as a technology and tool of economic exchange has at least temporarily reduced the capabilities of the United States and the international community to effectively sanction the DPRK. This is because of the DPRK's ability to acquire and transmit funds via cryptocurrency, which didn't exist even 15 years ago. Despite the expansion of US and international sanctions since 2015, their effectiveness has been blunted. COVID-19 at least in the short-term makes cryptocurrency an even more critical source of funds for the DPRK.

For the United States to take effective countermeasures against the DPRK, a new comprehensive framework around the economics, politics, and regulation of cryptocurrency must be developed. Many pieces of this framework already exist but need to be put together by US executive and semi-independent financial services regulatory agencies. The current situation is akin to trying to understand what an elephant is and how it works when you can only know about one part of the whole animal. Finally, in terms of theory, the value of social constructivism as an interdisciplinary analytical tool has been bolstered. It is particularly

useful for analysis related to cryptocurrency, which crosses many disciplinary boundaries in social science.

Policy Recommendations

This study makes a few policy recommendations quite clear. First, the US government needs to come to a legal and regulatory consensus regarding cryptocurrency. This could take several, non-mutually exclusive forms: 1) legislation[160], 2) an interagency task force, and/or 3) an executive order on the subject. Of these, a hybrid approach would be recommended. That is, it would be advisable to create an interagency task force composed of federal (and perhaps some state) agencies including law enforcement, financial services regulators, and broker dealer regulatory agencies. Given the size and varied jurisdictions of states, an interstate body such as the Conference of State Bank Supervisors[161] might be able to credibly fulfill this role on behalf of US state regulators. The group could draft legislative and regulatory proposals to create consistent standards for cryptocurrency usage in the United States. Given the high degree of technical knowledge required, the risks of cryptocurrency being the subject of domestic political contention are relatively low.

Such an approach is advisable as the United States should be taking a leading role in defining the global legal and regulatory framework of cryptocurrencies to ensure US competitiveness.[162] Moreover the success of such an endeavor would be greatly aided by coordination with US allies and other strategic partners. Japan, the ROK, and the European Union[163] are all notable market players in the cryptocurrency space in terms of existing activities and government regulation. In the absence of a US-led group setting the rules, there is a risk of nations adversarial to US interests doing so and undercutting the US and further mitigating the effectiveness of economic sanctions against the DPRK going forward. Additionally, Japan, and the ROK[164] would make natural partners for such an effort, given the frequently with which they are targeted by the DPRK.

There are a number of essential policies that should be included in whatever policy consensus is reached. First, cryptocurrency exchanges must apply the same or substantially similar standards as financial institutions with regards to money laundering, freezing assets, blocking transactions, monitoring suspicious transactions, and cyberattack information sharing practices.[165] This will assist law enforcement and other officials to respond more promptly to attacks and improve odds of attribution. Second, all cryptocurrencies should implement a "Customer Identification Program" (CIP) for cryptocurrencies and exchanges, a bedrock

[160] At the time of this paper's publication, H.R.3684 passed by both houses of the U.S. Congress, but not yet signed by President Biden. Sec. 80603 of this legislation seeks to clarify the definition of digital assets (including cryptocurrency) as a security and adds reporting requirements beginning in 2023. This should help somewhat to clarify the fragmented regulatory environment but will depend on how it is implemented administratively. See https://www.congress.gov/bill/117th-congress/house-bill/3684/text for details.
[161] https://www.csbs.org/.
[162] Fanusie and Logan, 20.
[163] See, Pirya Dailani, "A Rundown of Cryptocurrency Regulations Across the World, Analytics Insight, June 14, 2021, https://www.analyticsinsight.net/a-rundown-of-cryptocurrency-regulations-across-the-world/. Additional potential partners of note include: Australia, Canada, Singapore, Germany and Mexico.
[164] Ha and Maxwell, 29.
[165] UNSC 2019, 30.

principle of AML regulation. Requiring CIP information raises negative opportunity costs for individuals and entities associated with money laundering. Serendipitously, blockchain technology can also contribute to promoting transparency and accountability as well through its distributed open ledger as transactions are publicly visible. In fact, FinCEN noted in a 2020 rulemaking "investigators may be able to use blockchain data to identify illicit activity."[166]

Finally, this study opens up a policy discussion on how to approach cryptocurrency regulation going forward. As this study has demonstrated, continuing a "liberalized," hands-off approach to cryptocurrency is inadvisable given its frequent usage in activities which undermine US foreign policy goals, particularly towards the DPRK. It can be argued that there should be continued movement towards "prudential enthusiasm,"[167] which would aid US efforts to prevent illicit finance by adversarial actors. The debate on how to proceed next can be framed by three potential options: 1) public-private cooperation via a standards settings organization of some kind; 2) the exercise of sovereign authority by the government to more closely regulate cryptocurrency; or 3) the outright banning of cryptocurrency. The first model would be to develop some kind of cooperation between government regulators and cryptocurrency market players, directly or through trade associations, to develop comprehensive standards that address illegal activities which utilize cryptocurrency via exchanges. The US Federal Deposit Insurance Corporation is exploring the feasibility of such a model with regards to third-party technology service providers for financial institutions,[168] which could serve as a future template to emulate. An additional, complementary option which has been explored in a number of states is to create "regulatory sandboxes" in which new technologies are tested in the market under the close observation of regulators and consumers are advised regarding the higher degree of risk and uncertainty.

Alternatively, the US government could exercise its sovereign authority to further regulate cryptocurrency under current or new laws. This is currently being done to some degree by FinCEN and OFAC with regards to money transmission and sanctions. As previously discussed, one such model for applying this to cryptocurrency markets is "Access Theory,"[169] which puts additional onus for preventing illegal activities on gatekeepers. This could be applied to cryptocurrency exchanges and kiosks by treating them as money-service businesses. While these two approaches are largely mutually exclusive, there could be an opportunity for markets to step up, lest the government have to step in. If both options were to fail or seems infeasible the US government could move to ban cryptocurrency activities, but this would be a quite radical step as it would likely meet hostile resistance from private companies and individuals.

Limitations of this Study and Future Inquiries

[166] FinCEN 2020c, 12.
[167] Rodima-Taylor and Grimes, 91.
[168] US Federal Deposit Insurance Corporation, "Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services," Federal Register, Vol. 85, No. 143, July 24, 2020, https://www.federalregister.gov/documents/2020/07/24/2020-16058/request-for-information-on-standard-setting-and-voluntary-certification-for-models-and-third-party.
[169] Freedman and Sporkin, 786.

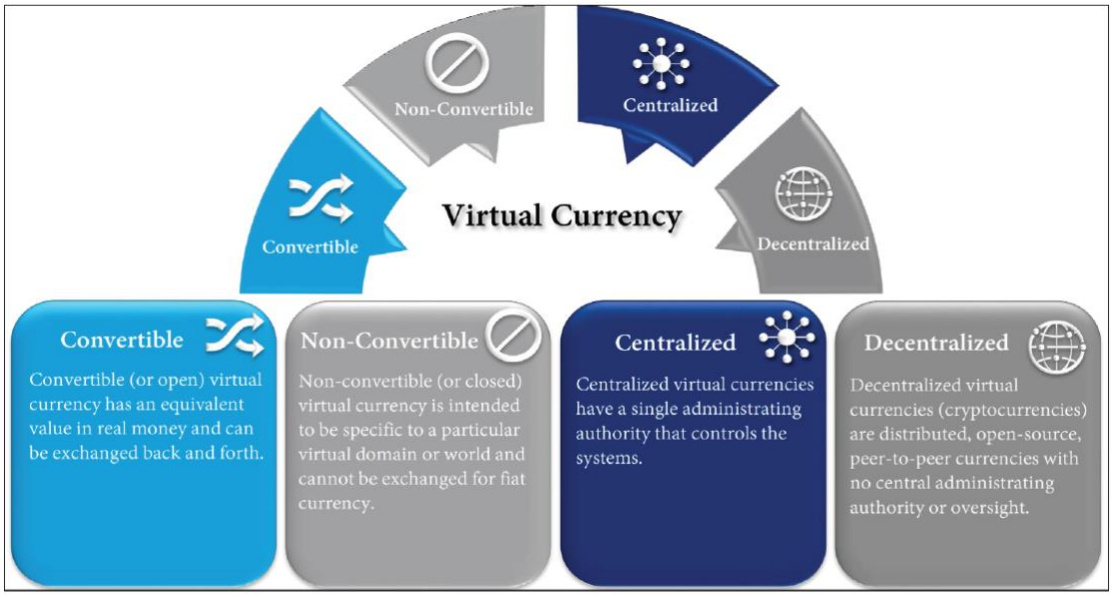
While this study breaks new ground on the political-economic effects of cryptocurrency on US-DPRK interactions over the past few years, there are limitations on what can be covered. International cooperation on the prevention of illicit finance via cryptocurrency is worth further scholarly research as its own stand-alone topic. Another potential future inquiry for a quantitative analysis would be to look at cryptocurrency transactional data in aggregate to look for patterns related to the DPRK and other non-state actors' efforts at money laundering. Such a study would require technical knowledge of both quantitate data analytical methods and of how blockchains work.

Of final note is the influence of COVID-19 on this study. With the pandemic it's difficult to effectively assess its enduring effects on both the DPRK and United States. However, it can be said with certainty is that COVID-19 has had a significant negative impact on the DPRK's economy in the short-term and increased global reliance on cyberspace to sustain the global economy. What is not yet understood and is beyond the scope of this study are the long-term sustained impacts of COVID-19 on the DPRK's activities in terms of weapons development, illicit finance, etc. which will persist beyond the end of the pandemic.

APPENDICES

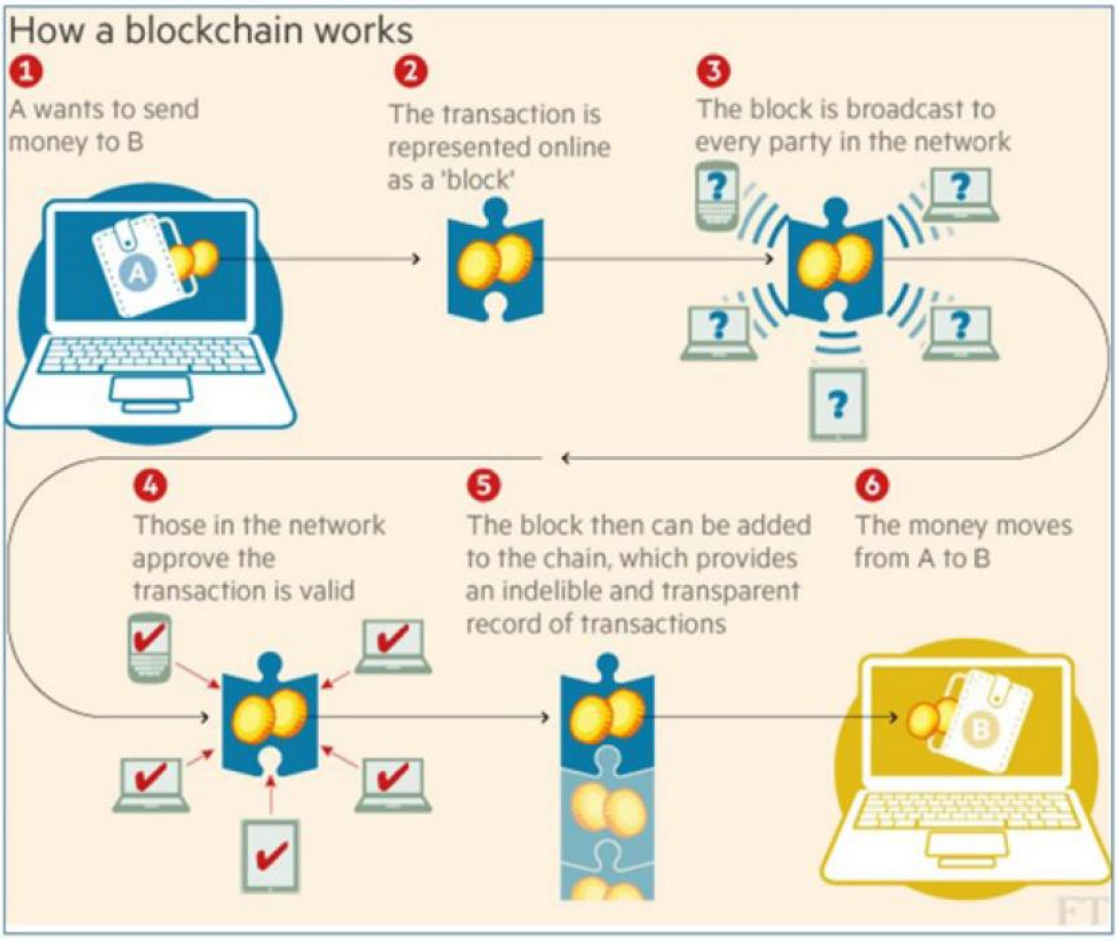
Appendix A: Figures

Figure 1: Defining Cryptocurrency



Source: Department of Justice, Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework (2020)

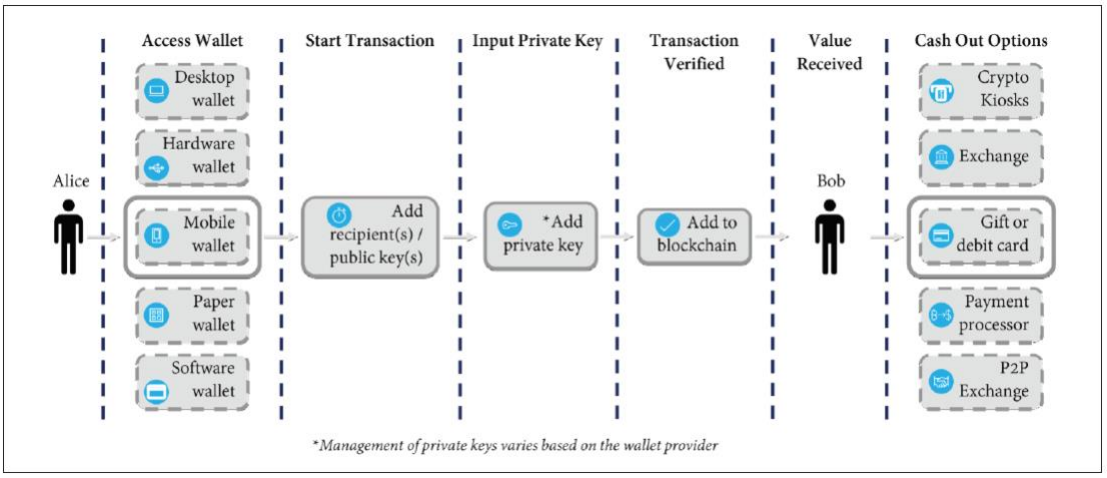
Figure 2: How a Blockchain Works



Source: World Economic Forum[170]

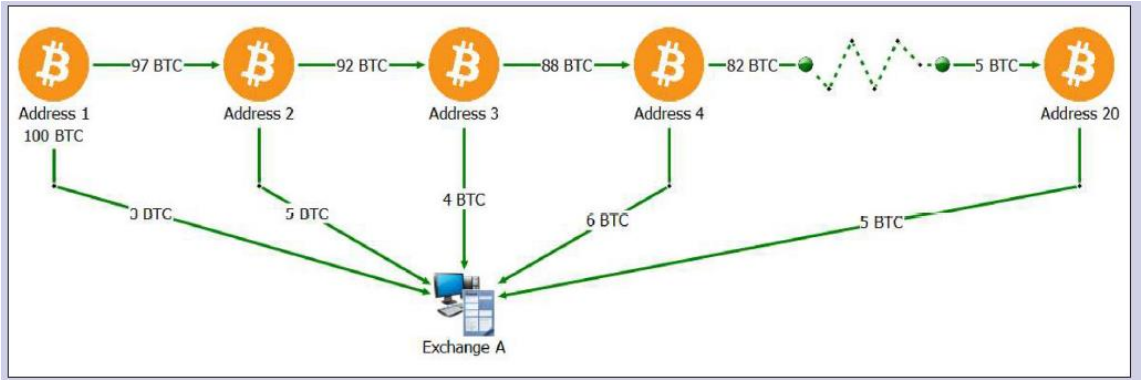
[170] Rosamond Hutt, "All you need to know about blockchain, explained simply," World Economic Forum, June 17, 2016. https://www.weforum.org/agenda/2016/06/blockchain-explained-simply/.

Figure 3: The process of transmitting and receiving a cryptocurrency transaction



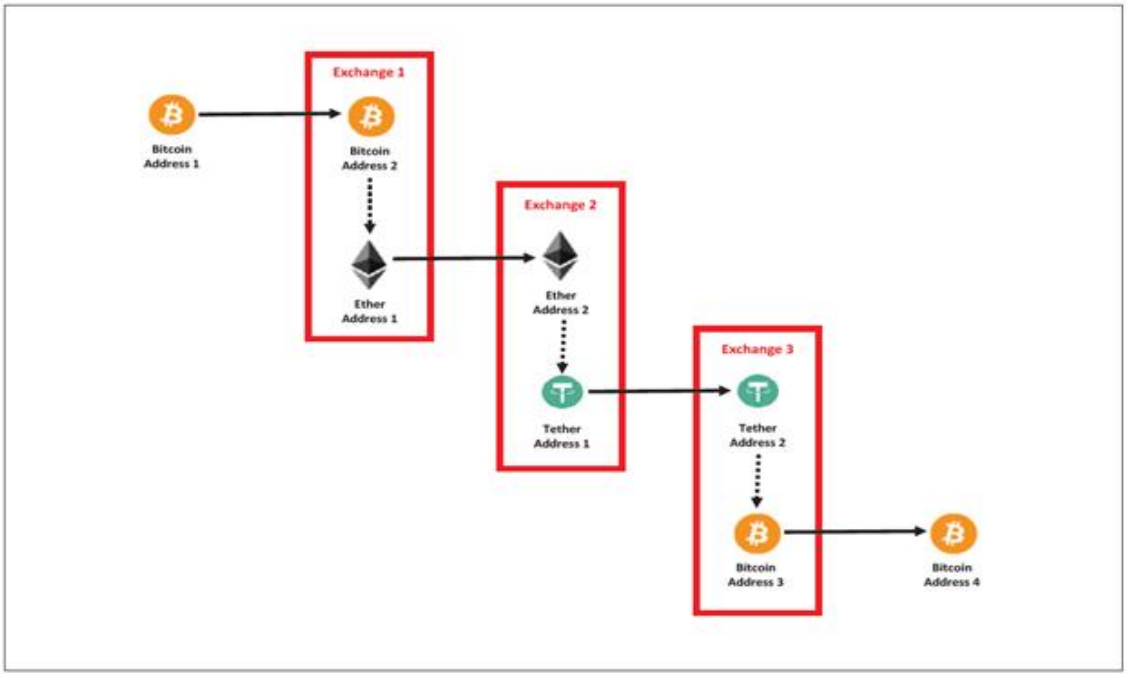
Source: Department of Justice, Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework (2020)

Figure 4: Depiction of a "Peel Chain" / Cryptocurrency laundering



Source: Department of Justice, Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework (2020)

Figure 5: "Chain-Hopping"



Source: Department of Justice, Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework (2020)

ABOUT THE AUTHOR

Michael Buckalew (michaelbuckalew84@gmail.com)is an executive legal assistant at Davis, Wright, Tremaine, where the conducts financial services legislative and regulatory research. He received his MA at Korea University's Graduate School of International Studies and his BA at Arcadia University.