THE EVOLUTION OF SANCTIONS EVASION: HOW CRYPTOCURRENCY IS THE NEW GAME IN EVADING SANCTION AND HOW TO STOP IT

Summer Wright*

Abstract: When one country illegally invades another sovereign country, repeatedly, utilizing the mechanism of sanctions to try and curb the misconduct, has become a favored approach among democratic countries. Russia once again invaded Ukraine in the early part of 2022, defying all international pressure, to refrain from the illegal act. The rapid response from the international community was a litany of sanctions intended to cripple and deter Russia's actions. Sanctions evasions are not a new challenge for sanctioning countries and agencies. A United Nations (UN) report notes that low levels of governmental oversight in the cryptocurrency sector have enabled North Korea to generate income at an alarming rate. The efficacy of financial sanctions in this way is consistently undermined through illicit cryptocurrency transactions. As the cryptocurrency sphere exceeds forty-two million users worldwide, the question on those issuing sanctions remains: If cryptocurrency is left unregulated, will financial sanctions lose their power? This article will outline the use of sanctions as a preferred foreign policy tool and how they work. I look at the various sanctions the United States, European Union, United Nations have levied against the Russian Federation in response to repeated invasions of Ukraine's sovereign territory. I will also analyze cryptocurrency, defining what it is, how it works to lay the groundwork for the analysis of the current cryptocurrency regulations and how this relates to concerns of illicit activity within the cryptocurrency sphere, as a means for sanctions evasion. Several countries including The Russian Federation (Russia), The Bolivarian Republic of Venezuela (Venezuela), The Islamic Republic of Iran (Iran) and The Democratic People's Republic of North Korea (North Korea) are using innovative cybercrimes and other crypto-based efforts to evade economic and financial sanctions. This article will consider the pushback on regulation from the crypto industry as well as illuminating the loopholes that are causing increased concern and current incidences of illicit activity internationally. Finally, I propose a few areas of consideration for creating an international regulatory framework to help combat the evasion of financial sanctions, using cryptocurrencies.

Keywords: Sanctions; Russia; Ukraine; Cryptocurrency

* California Western School of Law, United States.

Table of Contents

Introduction 3

I. Understanding Sanctions 3

A. The Five Types of Sanctions Available 4

B. How do Economic Sanctions Work? 5

II. Sanctions against the Russian Federation 6

A. Sanctions in Response to the 2014 Annexation of Crimea by Russia 6

B. Current Sanctions against Russia 8

III. Understanding Cryptocurrency and Regulation 10

A. A Brief History of Cryptocurrency 10

B. Decentralized and Unregulated 12

IV. The Lack of Cryptocurrency Regulation Linked to Evasion of Sanctions 14

A. Illicit Cryptocurrency Activity 15

1. The Bolivarian Republic of Venezuela 15

2. The Russian Federation 15

3. The Democratic People's Republic of North Korea 16

4. The Islamic Republic of Iran 17

V. Pushback and Loopholes 18

VI. A Way Forward for Regulations 20

A. Three Considerations for International Regulation 21

B. International Coordination and Information Sharing 22

C. A Need for "Friendly Adversarialism" 23

Conclusion 24

INTRODUCTION

When one country illegally invades another sovereign country, repeatedly, utilizing the mechanism of sanctions to try and curb the misconduct, has become a favored approach among democratic countries. Russia once again invaded Ukraine in the early part of 2022, defying all international pressure, to refrain from the illegal act.[1] The rapid response from the international community was a litany of sanctions intended to cripple and deter Russia's actions.

Sanctions evasions are not a new challenge for sanctioning countries and agencies. A United Nations (UN) report notes that low levels of governmental oversight in the cryptocurrency sector have enabled North Korea to generate income at an alarming rate.[2] As of 2019, almost $ 2 billion had been acquired through the evasion of economic sanctions using cryptocurrencies.[3] North Korea is no lone wolf in the evasions of sanctions game. Russia[4] and Venezuela[5] have also leveraged the use of cryptocurrencies to evade international sanctions. The efficacy of financial sanctions in this way is consistently undermined through illicit cryptocurrency transactions.[6] As the cryptocurrency sphere exceeds forty-two million users worldwide,[7] the question on those issuing sanctions remains: If cryptocurrency is left unregulated, will financial sanctions lose their power?

In Part II of this paper, I will outline the use of sanctions as a preferred foreign policy tool and how they work. Part III will look at the various sanctions the United States, European Union, United Nations have levied against the Russian Federation in response to repeated invasions of Ukraine's sovereign territory. In Part IV I will analyze cryptocurrency, defining what it is, how it works to lay the groundwork for Part V. Part V, will consider the current cryptocurrency regulations and how this relates to concerns of illicit activity within the cryptocurrency sphere, as a means for sanctions evasion. I will highlight how several countries including The Russian Federation (Russia), The Bolivarian Republic of Venezuela (Venezuela), The Islamic Republic of Iran (Iran) and The Democratic People's Republic of North Korea (North Korea) are using innovative cybercrimes and other crypto-based efforts to evade economic and financial sanctions. Finally, in Part VI, I address pushback on regulation from the crypto industry as well as illuminating the loopholes that are causing increased concerns and current incidences of illicit activity internationally. I then propose a few areas of consideration for creating an international regulatory framework to help combat the evasion of financial sanctions, using cryptocurrencies.

I. UNDERSTANDING SANCTIONS

State and nonstate actors that threaten a government's interests or violate international norms, are often faced with restraints of their financial freedom by the one or multiple

---

[1] *Russian forces launch full-scale invasion of Ukraine*, ALJAZEERA (Feb. 24, 2022), https://www.aljazeera.com/news/2022/2/24/putin-orders-military-operations-in-eastern-ukraine-as-un-meets.
[2] Rep. of the S.C., at 4/142, U.N. Doc. S/2019/691 (2019).
[3] *Id.*
[4] Russian officials state that a primary motivation for the creation of a "crypto rouble" (a new type of cryptocurrency) was to "settle accounts with [Russia's] counterparties all over the world with no regard for sanctions." Cong. Rsch. Serv., IF10825, Digital Currencies: Sanctions Evasion Risks 2 (Feb. 8, 2018).
[5] Alexandra Ulmer & Deisy Buitrago, *Enter the 'Petro': Venezuela to Launch Oil-Backed Cryptocurrency*, REUTERS (Dec. 3, 2017), https://www.reuters.com/article/us-venezuela-economy/enter-the-petro-venezuela-to-launch-oil-backedcryptocurrency-idU.S.KBN1DX0SQ.
[6] *Id.*
[7] Lubomir Tassev, *The Number of Cryptocurrency Wallets is Growing Exponentially*, BITCOIN.COM (Sept. 26, 2019), https://news.bitcoin.com/the-number-of-cryptocurrency-wallets-is-growing-exponentially/.

countries. To strategically alter unwanted behavior, economic sanctions have been a defensive mechanism of choice used by governments and multinational bodies since 1966.[8] The United Nations Security Council (UNSC) established the first sanctions regime on Southern Rhodesia (modern day Zimbabwe) more than fifty years ago.[9] Since then, the global body has enacted over thirty sanctions regimes; of which fourteen of those are still active today. The United States has wielded this tool as a primary weapon of choice since the 1950s, and in recent years, the United States has expanded the use of sanctions applying them against roughly twenty-five countries including The Islamic Republic of Iran, North Korea, The Bolivarian Republic of Venezuela, and Russian Federation.[10] Economic sanctions are typically levied by states and supranational bodies such as the United Nations and the European Union.[11] Targets of sanctions can range from entire countries to individuals.[12]

In general, sanctions regimes aim to prevent escalation of or settle conflicts among countries, counter terrorism, bolster cybersecurity, deter, punish, shame human-rights violators and curtail nuclear proliferation.[13] Individuals and organizations engaging in illegal activities including, money laundering, terrorism or terrorist financing, drug trafficking, violation of international treaties and human-rights violations, can end up on sanctions lists as well.[14] Critics say sanctions are often poorly conceived and rarely successful in changing a target's conduct, while advocates for sanctions contend, they have in recent years become more effective and remained an essential foreign policy tool.[15]

A. The Five Types of Sanctions Available

In today's geopolitical landscape, states, and organizations alike must navigate the complex network of sanctions. Sanctions can impact not just states, banks, and financial institutions. Companies spanning a range of industries have been the target of these enforcement actions as well. Failing to comply with sanctions laws can result in significant legal, financial, and reputational ramifications.

The five categories that most sanctions fall under include: economic sanctions, diplomatic sanctions, military sanctions, sport sanctions and sanctions on individuals. Though some of these types of sanctions are inter-related, for the purpose of this Paper, the focus is on economic sanctions. Economic sanctions are defined as "the withdrawal of customary trade and financial relations for foreign- and security-policy purposes."[16] Sanctions take a variety of forms, to accomplish foreign policy ends. Sanctions can include arms embargoes, travel bans, foreign assistance reductions and cut-offs, export and import limitations, asset freezes, tariff increases, revocation of most favored nation (MFN)[17] trade status, negative votes in international financial institutions, withdrawal of diplomatic relations, visa denials,

[8] United Nations Security Council, Sanctions, https://www.un.org/securitycouncil/sanctions/information (last visited Dec. 10, 2022).
[9] S. C. Res. 232, 1 (Dec. 16, 1966).
[10] U.S. Dept. of Treasury, Sanctions Programs and Country Information (Nov. 16, 2022), https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information.
[11] *Id.*
[12] *Id.*
[13] *What is a Sanction?,* LEXISNEXIS https://internationalsales.lexisnexis.com/glossary/compliance/sanctions.
[14] *Id.*
[15] Jonathan Masters, *What are Economic Sanctions?*, COUNCIL OF FOR. RELATIONS (Aug. 12, 2019, 8:00 AM), https://www.cfr.org/backgrounder/what-are-economic-sanctions.
[16] Masters, *supra* note 15 .
[17] UNCTAD Series on International Investment Agreement II: Most-Favoured-Nation Treatment (2010).

cancellation of air links, and prohibitions on credit, financing, and investment.[18] They may be comprehensive, prohibiting commercial activity regarding an entire country, like the long-standing U.S. embargo on of Cuba[19], or they may be more targeted, blocking transactions by and with businesses, groups, or individuals.

B. How do Economic Sanctions Work?

Sanctions, while a form of intervention, are generally viewed as a lower-cost, lower-risk course of action between diplomacy and war. Between military intervention and imposing economic sanctions, often policymakers find the softer form of engagement, by way of sanctions to be more attractive and can even buy time when evaluating more punitive measures.[20] Each country abides by their own laws and regulations regarding how they unilaterally apply sanctions to states and nonstate actors. However, two international bodies, the United Nations and European Union have established methods of imposing and enforcing sanctions, whereby each member state must comply.

The United Nations Security Council (the principal crisis-management body of the Organization)[21] can opt to respond to global threats by imposing economic sanctions. Sanctions resolutions must garner a majority vote with the fifteen-member Council without a veto from any of the Permanent Members (P5): the United States, United Kingdom, China, France, Russia.[22] Any sanctions imposed by the UNSC, typically in the form of travel bans, arms embargoes, and asset freezes, are binding for all Member States.[23] UN sanctions are usually managed by a special committee or monitoring group. INTERPOL assists some of the sanction committees[24], but officially the UN has no independent means of enforcement and relies on member states for enforcement.[25]

The European Union (EU) (made up of twenty-eight member states), imposes sanctions or "restrictive measures" in accordance with its Common Foreign and Security Policy.[26] Unanimous consent from member states in the Council of the European Union,[27] is required for sanctions policies to be enacted. In addition to any UNSC imposed sanctions, along with EU imposed sanctions, individual EU states may also impose harsher sanctions independently within their national jurisdictions.[28]

---

[18] Richard N. Haass, Economic Sanctions: Too Much of a Bad Thing, Brookings Institute Report (June 1, 1998), https://www.brookings.edu/research/economic-sanctions-too-much-of-a-bad-thing/.
[19] Fact Sheet, U.S. Dept. of Treasury, Cuba Sanctions, https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1541 (last visited Dec. 8, 2022).
[20] The UN Security Council imposed comprehensive sanctions against Iraq just four days after Saddam Hussein's invasion of Kuwait in August 1990. The Security Council did not authorize the use of military force until months later. *See* S.C. Res. 665 (August 25, 1990).
[21] U.N. Charter art. 7.
[22] *Id.*, at para. 41
[23] *Id.*
[24] Particularly in cases involving al-Qaeda and the Taliban. *See* S. C. Res. 2178 ¶ 12 (Sept. 24, 2014).
[25] Many member states lack the political will or resources to engage in enforcement of UNSC sanctions or prosecute violations. This in effect makes the impact of sanctions weak.
[26] Common Foreign and Security Policy, Eur. Comm'n, https://fpi.ec.europa.eu/what-we-do/common-foreign-and-security-policy_en (last visited Dec. 8, 2022).
[27] Council of the European Union is the body that represents EU leaders. *see,* Council of the Eur. Union, Eur. Union https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/council-european-union_en, (last visited Dec. 8, 2022).
[28] EU council rules on sanctions for member states. *see, id.*

The United States leads the charge when it comes to the frequency and scope of sanctions imposed, more so than any other country. The process to levy sanctions on state and nonstate actors begins with either the executive or legislative branch. The President typically will draft an executive order (EO) that declares a national emergency in response to an "unusual and extraordinary" foreign threat.[29] An EO activates the president's special powers to regulate commerce regarding the identified threat for a period of one year, unless extended by the president or terminated by a joint resolution of Congress.[30]

Congress may pass legislation imposing new sanctions or modifying existing ones, which it has done many times.[31] Regardless, of whether the President or Congress initiates sanctions, US sanctions programs are administered by the Treasury Department's Office of Foreign Assets Control (OFAC), partnering often with other departments such as Homeland Security, Justice, Commerce and State departments for critical support.[32]

II. SANCTIONS AGAINST THE RUSSIAN FEDERATION

In March of 2014, Vladimir Putin invaded Crimea, part of the sovereign state of Ukraine. The West responded by imposing severe economic sanctions designed to force Russia to withdraw and punish the Russian government for breaching Ukraine's sovereignty.[33] In August of 2014, approximately 2,000 Russian troops, violating international law, invaded the Crimean Peninsula. This brazen act was the first European annexation since the Second World War.[34] In response, much of the West again imposed sanctions to provide protection to Ukraine's sovereign rights, prevent a war, and deter further aggression.[35]

A. Sanctions in Response to the 2014 Annexation of Crimea by Russia

The European Union and the United States imposed two types of sanctions on Russia: targeted and sectoral. Targeted sanctions are asset freezes and visa bans focused on individuals and industries with close ties to President Vladimir Putin and powerful Russian institutions such as the European Parliament Think Tank.[36] These individuals and companies were accused of undermining democracy, expropriating or seizing Ukrainian property, and violating human

[29] Exec. Order. 12938, 59 FR 58099 (declaring the proliferation of nuclear, biological, and chemical weapons); Exec. Or. 13661, 79 FR 15,535 (declaring the actions and policies of the Government of the Russian Federation with respect to Ukraine).
[30] *See*, 50 U.S.C. § 1705 (IEEPA "[C]odified presidential national emergency powers to investigate and impose controls on transactions as well as freeze foreign assets under the jurisdiction of the United States.").
[31] H.R. 5271 (Sept. 9, 1988) (A House passes a bill sanctioning Iraq for using chemical weapons to commit genocide against its citizens.).
[32] Masters, *supra* note 15.
[33] Exec. Order 13660, 13660, 13662, 31 C.F.R. part 589 (March 6, 2014). The Ukraine/Russia related sanctions program implemented by Office of Foreign Assets (OFAC) began on March 6, 2014. President Barack Obama initiated these sanctions through a series of Executive Orders, "[D]eclaring a national declared a national emergency to deal with the threat posed by the actions and policies of certain persons who had undermined democratic processes and institutions in Ukraine; threatened the peace, security, stability, sovereignty, and territorial integrity of Ukraine; and contributed to the misappropriation of Ukraine's assets."
[34] Laura Geiger, *2014 Sanctions Against Russia Failed, is the Second Time the Charm?,* COL. POL. REV. (Apr. 7, 2022), http://www.cpreview.org/blog/2022/4/2014-sanctions-against-russia-failed-is-the-second-time-the-charm.
[35] *Id.*
[36] Cong. Res. Serv. (CRS, 2019), U.S. Sanctions on Russia, 11 January, Washington DC.

rights.[37] Gradually both the US and the EU have expanded their sanctions to the people responsible for Russian policy on Crimea and enterprises operating there.[38]

The United States also sanctioned four of Putin's cronies, namely Yuri Kovalchuk, Arkady and Boris Rotenberg, and Gennady Timchenko, as well as their Bank Rossiya.[39]. These sanctions were based on the insight that Russia was a kleptocracy.[40] Similarly, sanctions were imposed on enterprises owned by the Russian state or President Putin's cronies, and only exceptionally on private enterprises.

Economic sanctions were widened by the EU and the U.S. after Russian proxies gunned down the Malaysian Airlines passenger jet flying over Eastern Ukraine in July 2014.[41] This widely condemned incident instigated the second round of sanctions known as sectoral sanctions, aimed primarily at Russia's energy firms and state-owned corporations in the defense and financial sectors.[42] The July 2014 sanctions went much further than the Crimea sanctions. The financial sanctions prohibited lending to the sanctioned state banks and companies for 30 days or more, and the European Bank for Reconstruction and Development was blocked from offering new financing in Russia.[43] The energy sanctions were limited to three kinds of oil development: deep offshore drilling, arctic offshore, and tight oil. They did not harm production in the short term, but in the long term. The EU insisted that gas must not be subject to any sanctions because of its great dependence on Russian gas.[44]

President Barack Obama imposed the Ukraine related US sanctions through presidential executive orders, which meant that they could be modified at any time.[45] During the presidential election campaign in 2016, then candidate Donald Trump repeatedly criticized the US sanctions on Russia, arousing fear that he would abolish them.[46] In response, Congress codified these sanctions into law in the Combating America's Adversaries through Sanctions Act (CAATSA),[47] which President Trump signed into law on August 2, so that the President no longer could alter the Russia sanctions without the consent of Congress.

In April 2018, the US Treasury issued its first Ukraine-related sanctions based on CAATSA and the authority therein.[48] They were so severe, they were unprecedented. The Treasury sanctioned 24 people and 14 enterprises. Most of the people sanctioned were quite close to Putin, including his former son-in-law Kirill Shamalov. Several big oligarchs were sanctioned, notably Oleg Deripaska. These were designations, meaning that no US person was allowed to do any business with these people or enterprises. Finally, these sanctions hit some

---

[37] Anders Aslund, Western Sanctions on Russia over Ukraine 2014-2019, 20 CESifo Forum 14 (December 2014). [hereinafter Aslund, Western Sanctions].
[38] *Id.*
[39] The EU sanctioned Kovalchuk and Arkady Rotenberg as well, and a fifth crony Nikolai Shamalov. *see, id.,* at 14.
[40] A government by people who use their power to steal their country's resources, *Kleptocracy*, OXFORD DICTIONARY (7th ed. 2013).
[41] *Collateral damage*, THE ECONOMIST (Jul. 24, 2014), https://www.economist.com/briefing/2014/07/24/collateral-damage.
[42] Aslund, Western Sanctions, *supra* note 37.
[43] *Id.*
[44] CRS 2019, *supra* note 36.
[45] Exec. Orders, *supra* note 33.
[46] OFAC: CAATSA: Ukraine/Russia-Related Sanctions Program (2017), https://home.treasury.gov/system/files/126/eo13662_directive4_20171031.pdf.
[47] Countering America's Adversaries Through Sanctions Act of 2017, *see,* H.R. 3364, 115th Cong. (Jan. 3, 2017) (CAATSA) (enacted).
[48] OFAC: CAATSA, *supra* note 46.

very big enterprises, notably Deripaska's company Rusal, which was a listed company and accounted for 6 percent of global aluminum production.

Though sanctions were broad and severe, they were largely considered to have failed in deterring Russian advancement in Ukraine because the Russian economy was not sufficiently impacted to change the Kremlin's foreign policy.[49] The Russian government skillfully mitigated the damage of the 2014 and subsequent sanctions, through banking policies and purposefully devaluating the Russian currency.[50]

B. Current Sanctions against Russia

On February 24, 2022, Vladimir V. Putin ordered Russian forces to invade Ukraine.[51] The repercussions were immediate, and far-reaching. Now, following the launch of Russia's full-scale invasion, the largest mobilization of forces Europe has seen since 1945 is underway. So far, Moscow has struggled to secure a dominant victory failing to capture major cities across the country, including Kyiv, the capital. It has been weighed down by an ill-prepared military and has faced tenacious resistance from Ukrainian soldiers and civilian resistance fighters.[52] Still, Russia has superior military might, and President Putin has indicated that his goal is to capture Kyiv, take down Ukraine's democratically elected government, and retain Ukraine again as Russia's sovereign land.[53]

The invasion threatens to destabilize the already volatile post-Soviet region, with serious consequences for the security structure that has governed Europe since the 1990s. Mr. Putin has long lamented the loss of Ukraine and other republics when the Soviet Union broke apart. Before invading, Russia made a list of far-reaching demands[54] to reshape that structure — positions NATO and the United States rejected.[55]

The response from Western countries globally, has been swift and fierce. Within days of Russia's initial invasion into Ukraine, the EU and US levied sweeping economic sanctions against the aggressor. The difference between the current sanctions and the 2014 sanctions is that there has been a unified front from the West to cripple Russia's economy. Australia, Canada, the European Union, Japan, Great Britain, and the United States, have all collaborated

---

[49] After the initial round of sanctions, the Kremlin's aggression grew. Russia formally absorbed Crimea and upped its financial and military support for pro-Russian rebels in eastern Ukraine (including those who allegedly shot down the Malaysia Airlines flight.) It is speculated that the sanctions may have deterred Russia from even greater aggression in Ukraine at the time, but based on Russia's current, ongoing invasion of Ukraine, it seems all Russia really was intending with the annexation of Crimea was a "slow-burning insurgency.", *see*, Emma Ashford, *Not-So-Smart Sanctions: The Failure of Western Restrictions Against Russia*, 95 FOREIGN AFFAIRS 114, 116 (Council on Foreign Rel. ed., Jan./Feb. 2016), https://www.jstor.org/stable/43946631.

[50] Corey Flintoff, *Russia Marks Crimea Annexation with A Banknote Rapidly Losing Value*, NPR (Dec. 23, 2015, 2:18 PM), https://www.npr.org/sections/parallels/2015/12/23/460831232/russia-marks-crimea-annexation-with-a-banknote-rapidly-losing-value.

[51] ALJAZEERA, *supra* note 1.

[52] Dan Bilefsky, et. al, *The Roots of the Ukraine War: How the Crisis Developed*, N.Y. TIMES (Oct. 12, 2022), https://www.nytimes.com/article/russia-ukraine-nato-europe.html.

[53] *Id.*

[54] Andrew E. Kramer & Steven Erlanger, *Russia Lays Out Demands for a Sweeping New Security Deal With NATO*, N.Y. TIMES (Dec. 17, 2021), https://www.nytimes.com/2021/12/17/world/europe/russia-nato-security-deal.html.

[55] Bilefsky, *supra* note 52.

in imposing sanctions against Russia.[56] The aim is to limit Russia's access to money. To do this, the US has barred Russia from making debt payments using foreign currency held in US banks. Major Russian banks have been removed from the international financial messaging system, Society for Worldwide Interbank Financial Telecommunication (SWIFT).[57] Cutting certain Russian banks from accessing SWIFT was a striking and previously unconsidered move to harm and isolate Russian financial markets. This has delayed payments to Russia for its oil and gas exports.[58]

The United Kingdom (UK) has excluded key Russian banks from the UK financial system, frozen the assets of all Russian banks, barred Russian firms from borrowing money and placed limits on deposits Russians can make at UK banks.[59] In addition to the financial measures, Western countries, specifically the UK and US are working to end their reliance on Russian gas, by imposing additional sanctions including: the European Union's ban on imports of Russian oil brought in by sea from December, and a ban on all new imports of refined oil products from Russia.[60] The U.K. will phase out Russian oil by the end of 2022 and no longer imports Russian gas.[61] In another astounding move, Germany cancelled the licensing of Nord Stream 2 ,an already completed gas line between Germany and Russia, signaling to Russia that the EU will no longer prioritize its economic relations over a humanitarian crisis.[62] Germany has already reduced their imports of Russian gas from 55% to 35% with the goal of eventually importing no gas from Russia.[63] The US has followed suit introducing strict sanctions, including a ban on all Russian oil and gas imports.[64]

The US, EU, UK and other countries have also sanctioned more than 1,000 Russian individuals and businesses - including so-called oligarchs.[65] Most recently, the US is imposing sanctions on 278 members of Russia's parliament, for enabling the supposed referendums to

---

[56] *How much pain will the West's sanctions cause Vladimir Putin?,* THE ECONOMIST, (Feb. 23, 2022), https://www.economist.com/the-economist-explains/2022/02/23/how-much-pain-will-the-wests-sanctions-cause-vladimir-putin.

[57] Russell Holten, *Ukraine conflict: What is Swift and why is banning Russia so significant?*, BBC NEWS SERV. (May 4, 2022), https://www.bbc.com/news/business-60521822.

[58] *What are the sanctions on Russia and are they hurting its economy?,* BBC NEWS SERV. (Sept. 30, 2022), https://www.bbc.com/news/world-europe-60125659.

[59] *Id.*

[60] *Id.*

[61] *Id.*

[62] *Nord Stream 1: How Russia is cutting gas supplies in Europe*, BBC NEWS SERV (Sept. 29, 2022), https://www.bbc.com/news/world-europe-60131520.

[63] *Id.*

[64] Ashford, *supra* note 49.

[65] Press Release, Treasury Sanctions Kremlin Elites, Leaders, Oligarchs, and Family for Enabling Putin's War Against Ukraine, U.S. Dept. of Treasury, (March 11, 2022); *see also*, Daniel Sanford, *Russia oligarchs: The mega-rich men facing global sanctions*, BBC NEWS SERV (March 15, 2022), https://www.bbc.com/news/uk-60593022, (Defining that [o]ligarchs are wealthy business leaders, Russian elites who are thought to be close the Kremlin, such as former Chelsea Football Club owner Roman Abromovich.). Assets belonging to President Putin and Foreign Minister Sergei Lavrov have been frozen in the US, EU, UK and Canada.; *see also*, Press Release, $300 Million Yacht of Sanctioned Russian Oligarch Sulemian Kerimov Seized by Fiji at Request of United States, D.O.J. (May 5, 2022), https://www.justice.gov/opa/pr/300-million-yacht-sanctioned-russian-oligarch-suleiman-kerimov-seized-fiji-request-united#:~:text=May%205%2C%202022-,%24300%20Million%20Yacht%20of%20Sanctioned%20Russian%20Oligarch%20Suleiman%20Kerimov%20Seized,sanctioned%20Russian%20oligarch%20Suleiman%20Kerimov (Superyachts linked to sanctioned Russians have been seized); *see also,* Tier 1 Investor Visa route closes over security concerns, Home Office, The Rt Hon Priti Patel MP, Gov.UK, (Feb. 17, 2022), https://www.gov.uk/government/news/tier-1-investor-visa-route-closes-over-security-concerns, (The UK has stopped the sale of "golden visas", which allowed wealthy Russians to get British residency rights).

annex four regions in Ukraine.[66] It is also targeting 14 people connected with its defense industries.[67] The US says it will also target organizations outside Russia which provide support for its military, or its annexation of Ukrainian territory.[68] A new round of sanctions, drawn up by the European Commission, proposes a further ban on Russian imports. It would also ban more hi-tech goods from being exported.[69] These economic efforts will isolate Russia more than any sanctions have previously done, but they can still be further escalated to send a message to the Kremlin.

III. UNDERSTANDING CRYPTOCURRENCY AND REGULATION

A. A Brief History of Cryptocurrency

Cryptocurrency, in the simplest definition is a digital or virtual currency that uses cryptography for security, meaning it can be virtually impossible to counterfeit or double-spend.[70] Many cryptocurrencies are decentralized systems based on blockchain technology, a ledger distributed and enforced across a large network of computers. [71] The use of cryptocurrency has revolutionized international commerce unlike any other financial mechanism or institution.[72]

The first digital currency and still the most widely traded, Bitcoin, was developed in 2009.[73] As of 2019, an estimated forty-two million users have access to over 2000 digital currencies.[74] The gain in popularity of digital currencies[75], including cryptocurrencies among private and state actors, hinges on two key aspects.[76] One distinct feature of cryptocurrencies, is that they are typically decentralized, meaning they are organic in nature; generally not issued by any central authority, "rendering it theoretically immune to governmental interference or manipulation."[77] In practice, this means that transactions can be completed without the use of intermediaries such as banks.[78] Decentralization is attractive because, it in essence removes the middle men who serve as gatekeepers to the intersections of economies and charge a fee for entrance in the process.[79]

---

[66] Press release, Treasury Imposes Swift and Severe Costs on Russia for Putin's Purported Annexation of Regions of Ukraine, U.S. Dept. of Treas. (Sept. 30, 2022), https://home.treasury.gov/news/press-releases/jy0981.
[67] *Id.*
[68] *Id.*
[69] Ashford, *supra* note 49.
[70] *See* Jake Frankenfield, Cryptocurrency Currency Explained with Pros and Cons for Investment, INVESTOPEDIA (Sept. 26, 2022), https://www.investopedia.com/terms/c/cryptocurrency.asp
[71] *Id.*
[72] Ilker Koksal, *The Rise of Crypto as Payment Currency*, FORBES (Aug. 23, 2019 10:28AM), https://www.forbes.com/sites/ilkerkoksal/2019/08/23/the-rise-of-crypto-as-payment-currency/#42d0901b26e9.
[73] Frankenfield, *supra* note 70.
[74] *Id.*
[75] *See generally,* Tommaso Mancini-Griffoli et al., *Casting Light on Central Bank Digital Currencies*, INT'L MONETARY FUND (Nov. 12, 2018) (Describing that [t]here are distinctions between digital currencies and cryptocurrencies. Digital currencies are the "overall superset" that includes cryptocurrency. Some digital currencies, such as Central Bank Digital Currencies ("CBDCs") have the potential for mass centralization. However, cryptocurrencies rely on cryptography (unlike, for example CBDCs), which lends itself to decentralization.
[76] *Id.*
[77] Frankenfield, *supra* note 70.
[78] Koksal, *supra* note 72.
[79] *Id.*

Secondly, cryptocurrencies are mostly "pseudo-anonymous." They are pseudonymous, versus strictly anonymous because each user has a public address (or public key) that theoretically could be traced back to an IP address or exchange account (and by proxy, an actual identity) through proper network analysis.[80]

Cryptocurrency, like Bitcoin depends on a distributed ledger system (that tracks transactions made with these public keys) known as the blockchain.[81] The essential power of blockchain technology is its ability to distribute information. Because it is distributed across all the nodes, or individual computers, that make up the system, the term "blockchain technology" is often swapped with "distributed ledger technology."[82] A blockchain's database is not held in a single location, which could be infiltrated or controlled by a single party, but rather it is hosted by numerous (typically thousands) computers all at once.[83]

The blockchain system employs encryption, allowing users to key in special passwords to send digital money directly to each other without disclosing those passwords to any person or institution.[84] Equally important, it lays out the steps that computers in the network must perform to reach a consensus on the validity of each transaction. Once that consensus or verification has been reached, a payee knows that the payer has sufficient funds - that the payer isn't sending counterfeit digital money.[85] Put simply, cryptocurrency is an asset existing virtually rather than in physical (or fiat) form and blockchain is the technology making that happen.[86]

---

[80] To understand how this pseudo-anonymity works, one must first understand an aspect of blockchain technology that underlies all cryptocurrencies. This technology is called "public key cryptography." Public key cryptography is a cryptographic system that uses a pair of digital keys. Each cryptocurrency user has two keys. One is a public key, and one is private. The private key is a randomly generated hexadecimal number. As the name suggests, the user must always keep their private key private. Public keys are another hexadecimal number; they are derived from (and mathematically related to) the private key. *See generally, Is Bitcoin Anonymous?,* BITCOIN MAG. (Aug. 17, 2020), https://bitcoinmagazine.com/guides/is-bitcoin-anonymous. For more on pseudo-anonymity and public key cryptography, *see Public and Private Keys*, BLOCKCHAIN.COM (Mar. 29, 2020), https://support.blockchain.com/hc/en-us/articles/360000951966-Public-and-private-keys; *see also, Surveillance Defense*, SURVEILLANCE SELF-DEFENSE (Nov. 29, 2018), https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work.

[81] *What is a Blockchain?,* BITCOIN MAG. (Aug. 17, 2020), https://bitcoinmagazine.com/guides/what-is-blockchain.

[82] *Id.*

[83] The blockchain network automatically verifies itself at certain intervals, creating a self-auditing system that guarantees the accuracy of the data it holds. Groups of this data are known as "blocks," and as these blocks are cryptographically chained together, the pieces of data get buried and harder to manipulate. Altering any piece of data on the blockchain would require a huge amount of computing power. *see, id.*

[84] PAUL VIGNA & MICHAEL J. CASEY, THE AGE OF CRYPTOCURRENCY: HOW BITCOIN AND DIGITAL MONEY ARE CHALLENGING THE GLOBAL ECONOMIC ORDER 9 (2015).

[85] VIGNA & CASEY, *supra* note 84.

[86] Of the digital currencies, Bitcoin is generally considered the first completely decentralized currency and is by far the most widely used cryptocurrency., *see* Nathan Reiff, *What Was the First Cryptocurrency?*, INVESTOPEDIA (July 23, 2022), https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/; Broken down to its simplest form, Bitcoin is made up of "the digital units of value that are used by people in exchange for goods and services or other currencies, and whose price tends to swing wildly against traditional government issued currencies." Because of this, many laws and regulations fashioned by governmental institutions to regulate cryptocurrencies often refer to these currencies as bitcoin(s), utilized as a catch-all term to refer to cryptocurrencies more broadly., *see* Mancini-Griffoli, *supra* note 75., *see also*, Bernard Marr, *A Short History of Bitcoin and Cryptocurrency Everyone Should Read*, FORBES (Dec. 6, 2017), https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#70edd3813f27.

Finally, crypto exchanges are platforms that allow investors and consumers to "buy, sell, and trade cryptocurrencies through fiat currencies" such as US dollars or other cryptocurrencies.[87] Exchanges reflect current market prices of the cryptocurrencies they offer. You can also convert cryptocurrencies back into the U.S. Dollar or another currency on an exchange, to leave as cash within your account (if you want to trade back into crypto later) or withdraw to your regular bank account.[88]

Millions of people globally, including 16 percent of adult Americans, have purchased digital assets—which reached a market capitalization of $3 Trillion globally last November. Digital assets present potential opportunities to reinforce U.S. leadership in the global financial system and remain at the technological frontier. But they also pose real risks as evidenced by recent events in crypto markets. The May crash of a so-called stable coin and the subsequent wave of insolvencies wiped out over $600 billions of investor and consumer funds. Cryptocurrency may be still evolving but it is doing so exponentially.

B. Decentralized and Unregulated

One of the unique qualities of cryptocurrency, equally attractive to some and concerning for governments, is the unregulated, decentralized nature of the infrastructure. At their core, cryptocurrencies are built around the principle of a universal, inviolable ledger, one that is made fully public and is constantly being verified by these high-powered computers, each essentially acting independently of the other, creating inherent self-regulation.[89] The digital ledger (in most cases, blockchain) works as a stand-in for the middlemen since it can just as effectively identify whether a party to a transaction is good for his or her money.[90] The remarkable thing about this technology is that while cutting out the middleman it still provides an infrastructure inside of which strangers can exchange currency with one another globally.[91]

However, governments, institutions and banks alike point to cryptocurrencies novelty and what supporters opine, as its best feature (being decentralized), as a significant threat to the stability of our global financial institutions, creating an environment ripe for individuals and states seeking to evade taxes and or sanctions to have a work around.[92] In addition to concerns about users' risks associated with a decentralized, unregulated currency[93], the concern

---

[87] Kendall Little, *Want to Buy Crypto? Here's What to Look for In a Crypto Exchange?,* TIME (May 3, 2022), https://time.com/nextadvisor/investing/cryptocurrency/what-are-cryptocurrency-exchanges/.
[88] *Id.*
[89] Marr, supra note 86.
[90] *Id.*
[91] *Id.*
[92] The Digital Asset Sanctions 5 Compliance Enhancement Act of 2022 has yet to pass, but Senator Elizabeth Warren continues to press for robust regulatory system of the digital finance and cryptocurrency sector. *See*, S. 912, 117th Cong. (2022). *See also*, Elizabeth Warren, Regulate Crypto or It'll Take Down the Economy, WALL ST. J.: OP-ED (Nov. 22, 2022, 11:57 AM), https://www.wsj.com/articles/regulate-crypto-or-itll-take-down-the-economy-fraud-reporting-know-your-customer-loophole-energy-disclosure-ftx-bankman-fried-ftx-11669123750?mod=opinion_lead_pos5. Unlike with fiat currency, all cryptocurrency transactions are recorded. That makes them perfectly traceable, so it's easy to monitor dealings between legitimate businesses. However, the problem is that ownership of virtual cash is not necessarily attributable to specific people or businesses. And digital currency units can be anonymized by putting them through what's known as a tumbler or 'mixer', "a service that changes the owner's identity by exchanging the tokens with ones belonging to other users also seeking anonymity.", *see generally*, Owen Matthews, *Bitcoin and Blockchain: A Russian Money Laundering Bonanza?*, NEWSWEEK (September 18, 2017, 1:16 PM), https://www.newsweek.com/russia-finally-embracing-virtual-currencies-666794.
[93] For more on risks associated with investing in cryptocurrency, *see* Frankenfield, *supra* note 70. Unlike traditional finance, there is no way to reverse or cancel a cryptocurrency transaction after it has already been

for nefarious and illicit activity continues to rise. The evolution of cryptocurrency appears to be happening at a pace faster than any revelation of what kind of a regulatory counterpart fits the industry. One of the fundamental challenges for regulation has been determining how to quantify and categorize what, cryptocurrency is thus being able to identify who and how it should be regulated; is it a commodity, currency, a security to be governed by the U.S. Securities and Exchange Commission (SEC)[94]?

Cryptocurrencies globally are regulated differently on a country-to-country basis.[95] Despite the global, borderless nature of cryptocurrency, there is yet to form an international regulatory body or system. In the United States, there is increased regulatory uncertainty around cryptocurrency, but the Federal government is taking small steps toward solutions.[96] Though domestic tax compliance may seem unrelated to preventing foreign state and non-state actors from evading sanctions, but cryptocurrency by nature is transnational, it is easy for US citizens to engage in aiding or at the very least, being complicit in helping Russian's evade sanctions through the exchange of cryptocurrency.[97]

Federally, the Biden administration has worked to develop and define cryptocurrency regulations, however the U.S. government "finds itself caught between two extremes".[98] On

---

sent. By some estimates, about a fifth of all bitcoins are now inaccessible due to lost passwords or incorrect sending addresses. Also, there are counterparty risks; many investors and merchants rely on exchanges or other custodians to store their cryptocurrency. Theft or loss by one of these third parties could result in the loss of one's entire investment. As seen in the recent FTX scandal. *See* Kelsey Piper, *Sam Bankman-Fried tries to explain himself*, VOX (Nov. 16, 2022, 3:20 PM), https://www.vox.com/future-perfect/23462333/sam-bankman-fried-ftx-cryptocurrency-effective-altruism-crypto-bahamas-philanthropy?campaign_id=9&emc=edit_nn_20221117&instance_id=77783&nl=the-morning&regi_id=72351920&segment_id=113408&te=1&user_id=7e8ea228414c430288453c1748fdc9f6.

[94]*See* J. Riley Key *et. al*, *Cryptocurrencies: Currency, Commodity, Security, or Something Else?*, FIN. SERV. PERSPECTIVE (Feb. 5, 2019), https://www.financialservicesperspectives.com/2019/02/crytpocurrencies-currency-commodity-security-or-something-else/ ([A]ssessing a few American legal decisions regarding how cryptocurrencies should be defined, and how these definitions conflict amongst the various US regulatory agencies: "While the SEC appears to take a broad view of what constitutes a security in the cryptocurrency space, not all regulators and courts agree"). *See also*, SEC v. Ripple Labs Inc, U.S. District Court, Southern District of New York, No. 20-CV-10832. (Ripple's founders created XRP in 2012. XRP is the world's seventh largest cryptocurrency. The SEC sued the San Francisco-based company and its current and former chief executives in December 2020, alleging they have been conducting a $1.3 billion unregistered securities offering since the token's creation.). The ruling in this case will no doubt have major implications on the SEC's ability to regulate in the crypto space. *See generally*, Jody Godoy, Ripple, *SEC make final bids for a quick win in XRP lawsuit*, REUTERS (Dec. 5, 2022, 9:49 AM), https://www.reuters.com/legal/transactional/ripple-sec-make-final-bids-quick-win-xrp-lawsuit-2022-12-05/.

[95] *See*, Global Legal Research Center, Regulation of Cryptocurrency Around the World, L. Libr. Cong. 9-9 (June 2018), https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf.

[96] U.S. DEPT. OF TREAS., THE AMERICAN FAMILY PLAN TAX COMPLIANCE AGENDA (May 2021) (Showing [a]n amended version of President Biden's American Family Plan, including a new rule for businesses and crypto exchanges, requiring them to report any cryptocurrency transactions with a fair market value of $10,000 or more to the IRS.).

[97] Press Release, U.S. Dept. of Just., Two European Citizens charged for Conspiracy with a U.S. Citizen to Assist Korea in Evading U.S. Sanctions (April 25, 2022), https://www.justice.gov/opa/pr/two-european-citizens-charged-conspiring-us-citizen-assist-north-korea-evading-us-sanctions. (U.S. citizen Virgil Griffith pleaded guilty to conspiring to assist North Korea in evading sanctions in violation of the International Emergency Economic Powers Act (IEEPA), and was sentenced on April 12 to 63 months in prison and a $100,000 fine by U.S. District Judge P. Kevin Castel).

[98] Exec. Order 14067, 87 FR 40881 (Mar. 9, 2022); *see,* FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets, White House (Sept. 16, 2022) (outlining the six key priorities identified in the EO: consumer and investor protection; promoting financial stability; countering illicit finance; U.S. leadership in the global financial system and economic competitiveness; financial inclusion; and responsible innovation).

one hand, the government is unwilling to actively block cryptocurrency transactions as it does not want to hamstring or restrain a growing and potentially lucrative, and critical industry for engaging in the global financial market. However, with the rise of cryptocurrency-based cybercrimes, the government cannot remain uninvolved in policing illicit and criminal activity in this sphere.[99]

The Biden administration remains committed to supporting the growth of the cryptocurrency industry while simultaneously searching for ways to restrict illegal uses.[100] The emphasis seems to be on information sharing, within federal agencies, including the Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC), Consumer Financial Protection Bureau (CFPB) and Federal Trade Commission (FTC), but also across international lines.[101] Federal agencies are scrambling to keep up and adapt their practices to fit the world of cryptocurrency.[102]

The Department of Justice also established a 'crypto enforcement' arm in 2019. The Market Integrity and Major Frauds Unit (MIMF) works to prosecute those who commit fraud and market manipulation involving cryptocurrency.[103] The MIMF unit often works in collaboration or parallel to the U.S. SEC and the CFTC.[104] In just under three years prosecutors have charged, crypto CEOs, Traders, Founders, Executives, etc. with over $2 billion in intended financial losses to investors.[105]

IV. THE LACK OF CRYPTOCURRENCY REGULATION LINKED TO EVASION OF SANCTIONS

Sanctions are intended to exert pressure on the targeted party, through economic isolation measures. The more severe and more prolonged the sanctions, however, the greater incentive there is for individuals and governments, restrained by the sanctions to pursue creative new avenues to continue to participate in financial transactions globally. In recent years, digital and cryptocurrency have emerged as an attractive tool for individuals and regimes seeking to evade sanctions. Barred from traditional cross-border payment networks, parties

---

[99] Josephine Wolff, The competing priorities facing U.S. crypto regulations, Brookings Inst.: TECH STREAM (Oct. 17, 2022), https://www.brookings.edu/techstream/the-competing-priorities-facing-u-s-crypto-regulations-bitcoin-ethereum/.

[100] Exec. Order 14067, *supra* note 98.

[101] *Id.*

[102] OFAC's recent guidance confirmed that "sanctions compliance obligations apply equally to transactions involving virtual currencies and those involving traditional fiat currencies." *see* OFAC, Sanctions Compliance Guidance for Virtual Currency ("OFAC Guidance"), at 1 (Oct. 2021)

[103] Using traditional law enforcement strategies coupled with blockchain data analytics, prosecutors aim to identify and prosecute a variety of cryptocurrency-based cybercrimes. "Since 2019, the Unit has charged cryptocurrency fraud cases involving over $2 billion in intended financial losses to investors from around the world. Prosecutors use blockchain data analytics and traditional law enforcement techniques to identify and prosecute complex cryptocurrency investment schemes; price and market manipulation involving cryptocurrencies; unregistered cryptocurrency exchanges involved in fraud schemes; and insider trading schemes affecting cryptocurrency markets." *See* U.S. Dept. of Just., Crypto Enforcement (Sept. 26, 2022), https://www.justice.gov/criminal-fraud/crypto-enforcement.

[104] *Id.*

105 *See e.g.,* United States v. Satish Kurjibhai KUMBHANI, aka "Vindee," aka "VND," aka "vndbcc,", Defendant., 2022 WL 609822 (S.D.Cal.).; *see also,* Kristina Davis, *Founder of cryptocurrency company BitConnect charged in $2.4-billion fraud*, LA TIMES (Feb. 26, 2022), https://www.latimes.com/california/story/2022-02-26/cryptocurrency-founder-charged-in-2-4-billion-fraud (Where [p]rosecutors consider the kind of alleged price manipulation conspiracy committed by BitConnect, to be commodities fraud, which is believed to be the first time cryptocurrency has been alleged to function as a commodity, the U.S. attorney's office said).

targeted by sanctions — and even some nonsanctioned, nefarious parties — have zeroed in on borderless digital alternatives to escape the scrutiny of government regulators.[106]

A. Illicit Cryptocurrency Activity

When pressed to be innovative, sanctioned governments and individuals have found ways to continue to move money around, outside of the traditional methods, i.e., setting up a shell company in the Cayman Islands. Several different strategies using digital currencies and cryptocurrencies have been employed to commit criminal acts or specifically to evade sanctions.

1. The Bolivarian Republic of Venezuela

In 2017, the U.S. imposed broad new sanctions prohibiting the Venezuelan government from accessing U.S. financial markets. In response, shortly thereafter, Venezuela attempted to create its own oil-backed cryptocurrency, the Petro.[107] Venezuelan President Nicolas Maduro was brazened and transparent in his promotion of the Petro, describing his regime's focus on cryptocurrency as one aspect of Venezuela's efforts to "circumvent the financial blockade created by the U.S. government".[108] Despite its launch in 2018[109],Venezuelan citizens do not appear to actively use the Petro. However, Venezuelans do trade an estimated $8 million worth of bitcoin each week, and Maduro recently announced plans for the Venezuelan government to move to a fully digitalized economy.[110]

2. The Russian Federation

The sanctions imposed upon Russia by the United States in 2014, in response to the invasion of Crimea, hit the country's economy hard. Economists estimated that the sanctions imposed by Western countries in 2014 cost Russia $50 billion.[111] Russia announced plans in 2017 for a state-run cryptocurrency called the Crypto ruble. Russia's approach to digital currency was slightly different than Venezuela's, however. Crypto rubles would be issued by the Russian government rather than mined — i.e., verified through cryptographic algorithms, like the bitcoins of the world — and would thus resemble a digital fiat currency, equal in value to a regular ruble.[112] Importantly, however, the Russian government would have the ability to provide anonymity to crypto ruble users. The Russian government stated the purpose of the crypto ruble — which is still under development — in no uncertain terms: The digital currency will help Russia "settle accounts with [its] counterparties all over the world with no regard for sanctions."[113] In line with their propensity for hacking and ransomware attacks, Russia has

---

[106] *See infra* Part IV (A-C).
[107] Ulmer & Buitrago, *supra* note 5.
[108] *Id.*
[109] Nicolle Yapur, *Venezuela's Maduro Plans to Shift to Fully Digitalized Economy*, BLOOMBERG (Jan. 2, 2021, 10:47 AM), https://www.bloomberg.com/news/articles/2021-01-02/venezuela-s-maduro-plans-shift-to-a-fully-digitalizedeconomy.
[110] *See,* Jeffrey Gogo, *Venezuela to Start Using Cryptocurrency in Global Trade in Efforts to Fend Off U.S. Sanctions*, BITCOIN (Oct. 1, 2020), https://news.bitcoin.com/venezuela-to-start-using-bitcoin-in-global-trade-in-efforts-to-fend-offu-s-sanctions; *See also,* Yapur, s*upra* note 109.
[111] Emily Flitter & David Yaffe-Bellany, *Russia Could Use Cryptocurrency to Blunt the Force of U.S. Sanctions*, N.Y. TIMES, (Feb. 24, 2022), https://www.nytimes.com/2022/02/23/business/russia-sanctions-cryptocurrency.html.
[112] Jake Rudnitsky, Vladimir Putin aide eyes cryptocurrencies to beat sanctions, Russia newswire says. THE SYDNEY MORNING HERALD (December 13, 2017, 7:04 AM), http://www.smh.com.au/world/vladimir-putin-aide-eyes-cryptocurrencies-to-beat-sanctionsrussian-newswire-says-20171212-h03jju.html.
[113] *Id.*

also developed a software called Hydra, that can mask the origin of the transaction on blockchain, allowing Russian businesses to trade without detection.[114]

3. The Democratic People's Republic of North Korea

North Korea is perhaps the starkest example of a country that has sought to exploit digital currencies to circumvent sanctions restrictions. [115] Sanctioned in some capacity since the 1950s in response to their prolific nuclear program[116], North Korea, an already isolated,[117] totalitarian state, turned to using talented skillful,[118] homegrown, hackers to evade sanctions.[119] North Korea openly employs state sponsored cybercriminals like the infamous Lazarus Group, in an effort to hack and steal their way around sanctions.[120] The crypto sector is their latest sanctions evasion route of choice.[121] Compared to the more traditional fiat currency-generating crimes such as narcotics trafficking and arms trade,[122] cybercrimes offer criminals greater protection from investigation through layers of anonymity.

---

[114] At present, Hydra cannot handle the volume of transactions that would be required to evade sanctions, but other money laundering techniques could be deployed. *see*, Thorston J. Gorny, *Russia Sanctions and Sanctions Evasion with Cryptocurrencies,* SANCTIONS.IO (June 14, 2022), https://www.sanctions.io/blog/russia-sanctions-and-sanctions-evasion-with-cryptocurrencies#:~:text=Last%20year%2C%2074%25%20of%20global,the%20US%20and%20other%20nations. *See id.*, Last year, 74% of global ransomware profits ($400 million of cryptocurrency) went to entities affiliated with Russia.

[115] *See generally*, KING MALLORY, NORTH KOREAN SANCTIONS EVASION TECHNIQUES 15 (RAND Corp. 2021).; *See also*, Andrew W. Lehren & Dan De Luce, *Secret Documents Show How North Korea Launders Money Through U.S. Banks*, NBC NEWS (Sept. 20, 2020), https://www.nbcnews.com/news/world/secret-documents-show-how-north-korea-launders-money-through-u-n1240329.

[116] *See* Kelsey Davenport & Elizabeth Philipp, *UN Security Council Resolutions on North Korea*, ARMS CONTROL ASS'N (Apr. 2018), https://www.armscontrol.org/factsheets/UN-Security-Council-Resolutions-on-North-Korea.; *see also,* Eleanor Albert, *What to Know About Sanctions on North Korea*, COUNCIL ON FOR. REL. (July 16, 2019, 8:00 AM), https://www.cfr.org/backgrounder/what-know-about-sanctions-north-korea. *See North Korea Overview*, NUCLEAR THREAT INITIATIVE (Oct. 19, 2021), https://www.nti.org/analysis/articles/north-korea-overview/.

[117] *See generally*, Charlotte Alfred, *How North Korea Became So Isolated*, HUFFPOST (Oct. 17, 2014, 05:42 PM), https://www.huffpost.com/entry/north-korea-history-isolation_n_5991000.

[118] See, U.S. DEP'T HEALTH & HUM. SERV.., OFF. INFO. SEC., NORTH KOREAN CYBER ACTIVITY 3 (2021), https://www.hhs.gov/sites/default/files/dprk-cyber-espionage.pdf.; *See also*, Morten Soendergaard Larsen, *While North Korean Missiles Sit in Storage, Their Hackers Go Rampant*, FOREIGN POLICY (Mar. 15, 2021), https://foreignpolicy.com/2021/03/15/north-korea-missiles-cyberattack-hacker-armies-crime/ (quoting Bruce Klingner--a former CIA deputy division chief and current Heritage Foundation senior research fellow).

[119] North Korea conspired with a cryptocurrency expert to teach and advise members of the North Korean government on cutting-edge cryptocurrency and blockchain technology, all for the purpose of evading U.S. sanctions meant to stop North Korea's hostile nuclear ambition. *See* Press Release, U.S. Dept. of Just., Two European Citizens charged, *supra* note 91. See also, U.S. DEP'T TREASURY, National Strategy for Combating Terrorist and Other Illicit Financing 21 (2020).

[120] North Korea harbors a massive army of cyber operatives as part of its strategy for conducting cyber-based financial crimes as part of its sanction's evasion strategy. Most of the commercial hackers that focus on financial crimes operate under the command of the Reconnaissance General Bureau, North Korea's key military-intelligence division, and its subunits of hackers like the Lazarus Group. *See*, Ed Caesar, *The Incredible Rise of North Korea's Hacking Army*, NEW YORKER (Apr. 19, 2021), https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army.

[121] *See, Lazarus Group Pulled Off 2020's Biggest Exchange Hack and Appears to be Exploring New Money Laundering Options,* CHAINALYSIS: BLOG (Feb. 9, 2021), https://blog.chainalysis.com/reports/lazarus-group-kucoin-exchange-hack.

[122] MALLORY, *supra* note 115, at 19.

To strategically overcome economic sanctions, North Korea has increasingly employed advanced cyber capabilities to conduct ransomware attacks, [123] digital bank heists, cryptocurrency theft, crypto-based cyber scams,[124] and crypto jacking schemes[125]--all of which include money laundering aspects. The cyber-based nature of these financial crimes, especially in a constantly evolving arena of cryptocurrency, leaves the U.S. and international community strained in their attempts to curb North Korea's continued sanctions evasion and money laundering activities that are often assisted by individuals and organizations across the globe.[126]

According to the United States Department of Justice (DOJ), the three North Koreans named in the February indictment acted on behalf of the North Korean government as part of a North Korean military intelligence agency.[127] And a more recently the Lazarus group have been linked with the theft of over $600M in crypto by hacking Axie Infinity Video game.[128] Since the attack in March, the hackers are still laundering the stolen money via Blender, a cryptocurrency mixer. Cryptocurrency-based financial crimes are likely to remain North Korea's primary sanctions evasion and money laundering operations in cyberspace.[129] North Korea has shown remarkable willingness and ability to utilize blockchain technology and possesses sophisticated levels of adaptability and maturity in deploying its schemes. Members of the international community, therefore, need to respond with urgency.

4. The Islamic Republic of Iran

Iran's long history of economic isolation from U.S. sanctions began in 1979, when President Jimmy Carter's administration banned Iranian imports and froze $12 billion in assets over the storming of the U.S. Embassy in Tehran.[130] With few other options, Iran has turned to

---

[123] Ransomware attack generally involves infecting a victim's computer with an access-denying malware and then demanding payments in cryptocurrency in return for granting the victim access to his or her computer. S*ee* Thomas Brewster, *Microsoft Just Took a Swipe at NSA Over the WannaCry Ransomware Nightmare*, FORBES (May 14, 2017), https://www.forbes.com/sites/thomasbrewster/2017/05/14/microsoft-just-took-a-swipe-at-nsa-over-wannacry-ransomware-nightmare/?sh=7fec72133585 [https://perma.cc/6UMS-N93R].; *See* Alex Hern & Samuel Gibbs, *What is WannaCry Ransomware and Why is it Attacking Global Computers?*, GUARDIAN (May 12, 2017), https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20 [https://perma.cc/942S-6SUU].

[124] *See* North Korea's alleged attempt to lure investors to its dubious Marine Chain Vessel Token Offering represents this type of cyber scam. *See* Cristina Rotaru, *The Curious Case of Marine Chain: The DPRK Cyberscam Behind a Blockchain-Powered Maritime Investment Marketplace*, VERTIC (Apr. 24, 2019), https://www.vertic.org/2019/04/the-curious-case-of-marine-chain-the-dprk-cyberscam-behind-a-blockchain-powered-maritime-investment-marketplace/.

[125] Cryptojacking refers to the act of using malware-infected computers' computing power to mine cryptocurrency. *See* U.S. DEP'T JUST. ET AL., DPRK CYBER THREAT ADVISORY: GUIDANCE ON THE NORTH KOREAN CYBER THREAT 2 (Apr. 15, 2020) [hereinafter DPRK CYBER THREAT ADVISORY].

[126] *See* Arjun Kharpal, *Hackers Have Found a Way to Mine Cryptocurrency and Send It to North Korea*, CNBC (Jan. 9, 2018), https://www.cnbc.com/2018/01/09/north-korea-hackers-create-malware-to-mine-monero.html.

[127] Supra note 118.

[128] Carly Page, *US officials link North Korean Lazarus hackers to $625M Axie Infinity crypto theft*, TECHCRUNCH, (April 15, 2022), https://techcrunch.com/2022/04/15/us-officials-link-north-korean-lazarus-hackers-to-625m-axie-infinity-crypto-theft/.

[129] While its hackers roam cyberspace launching illicit attacks, North Korea runs little risk of being targeted itself because most of the country is offline. "For North Korea, it's a low-cost, low-risk but high-return criminal enterprise," said Yoo Dong-ryul, a former chief antiterrorism analyst at the South Korean national police agency. *See*, Choe Sang-Hun & David Yaffe-Bellany, *How North Kora Used Crypto to Hack Its Way Through the Pandemic*, NY TIMES (June 30, 2022), https://www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html.

[130] *See generally*, Patrick Clawson, *Iran Primer: U.S. Sanctions*, PBS: FRONTLINE (Oct. 21, 2010), https://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/10/iran-primer-us-sanctions.html.

digital currencies to alleviate the crippling impact of sanctions in recent years.[131] Cheap, heavily subsidized energy sources have fueled a robust, fast growing crypto mining industry and encouraged foreign crypto mining operations to move their energy-intensive computer farms to Iran.[132] In 2019, Iran was one of the first countries to officially recognize crypto mining as a legitimate industry, and since then the Iranian government continues to focus on deriving much-needed income through crypto mining industry regulation.[133] Effectively, Iran is selling its energy reserves on the global markets, using Bitcoin mining to bypass trade embargoes. Miners based in Iran are paid directly in cryptocurrency which can in turn be used to pay for imports, circumventing financial sanctions.[134] The government has adopted crypto mining officially as an effective tool for evading sanctions.[135]

V. PUSHBACK AND LOOPHOLES

A big debate is underway on whether sanctions evasion with crypto is a realistic possibility. Insiders and practitioners of the cryptocurrency industry deny the possibility. Their main arguments include: 1) issues with liquidity, the crypto industry is just too small, with the entire market cap at approximately $2 trillion, 2) SWIFT processes 42 million financial messages on average every day. The current decentralized financial technology is not robust enough to efficiently handle that kind of scale, 3) the use of blockchain, a publicly accessible, highly traceable ledger, does not, some crypto experts think, make it an effective tool for illicit activity, especially on a grand scale and 4) they further argue that the idea that some cryptocurrency can be used to evade sanctions is highly dependent on that particular asset being purchased for widespread use, which is not the case at the moment.

Cryptocurrencies are created and exchanged through blockchain networks, which store "tamper-resistant" records of transactions.[136] Most cryptocurrency transactions between parties are recorded directly on public blockchains meaning anyone can view the records.[137] Cryptocurrency supporters argue that sanctions evasion is impossible because transactions are publicly viewable on blockchains, which law enforcement may trace using analytics software and user's public key addresses. However, it is not that simple. There are ways sanction evaders may attempt to obscure their blockchain transactions and evade any measures imposed by exchanges.

---

[131] *See, e.g.*, Thomas Erdbrink, *How Bitcoin Could Help Iran Undermine U.S. Sanctions*, N.Y. TIMES (Jan. 29, 2019), https://www.nytimes.com/2019/01/29/world/middleeast/bitcoin-iran-sanctions.html.

[132] Bitcoin and other crypto asset networks run on electricity, a lot of it. "Bitcoin miners run power-hungry computers, which process new transactions and add them to the blockchain." In return, the miners are rewarded with bitcoins - both from transaction fees as well as the minting of new bitcoins. The mining process effectively converts energy into cryptocurrency. Iran has seized upon Bitcoin mining as an attractive opportunity for their heavily sanctioned economy suffering from a shortage of liquid cash, but with a surplus of oil and natural gas. See Tim Robinson, *How Iran Uses Bitcoin Mining to Evade Sanctions and "Export" Millions of Barrels of Oil*, ELLIPTIC: BLOG (May 21, 2021), https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions.

[133] *See id.*, (Showing that Iran charges a tariff, thought cheaper than most, for their electricity sources for the purpose of crypto mining).

[134] *Id. See also,* Sebastian Sinclair, *Iran Central Bank to Allow Money Changers, Banks to Pay for Imports Using Mined Crypto*, COINDESK (Sept. 14, 2021, 5:46 AM), https://www.coindesk.com/markets/2021/04/27/iran-central-bank-to-allow-money-changers-banks-to-pay-for-imports-using-mined-crypto/.

[135] *See* Behnam Gholipour, *Official Report: Iran Could Use Cryptocurrencies to Avoid Sanctions*, Iran Wire (March 2, 2021), https://iranwire.com/en/features/69084/.

[136] *See* supra Part III (A).

[137] *Id.*

One method is called chain-hopping. This is a process of converting one cryptocurrency into another to hide illicit funds.[138] Another way to increase the difficulty of determining the source of illicit funds is to use mixers or tumbling services.[139] Users pay a fee to send cryptocurrency to a mixer account, which combines cryptocurrencies from various customers, before sending to the end recipient.[140] One of the more publicly discussed concerns and areas of new sanctions on Russia are in relation to the use of un-hosted wallets.[141] A wallet is digital software or hardware for storing private keys corresponding to cryptocurrency and other blockchain based assets.[142] Exchanges may provide 'hosted" wallets but are not required to monitor transactions with un-hosted wallets. If law enforcement agencies are aware of a sanctioned individual's un-hosted wallet, they may be unable to access and recover the cryptocurrency without the wallet's private keys.

Nevertheless, un-hosted wallets still require an exchange as an "off-ramp" for users to convert to fiat currency. Individuals may use un-hosted wallets to shift funds to exchanges in jurisdictions with fewer anti-money laundering (AML) or Know Your Customer (KYC) requirements. The Office of Foreign Assets Control (OFAC) has sanctioned certain Russian-linked cryptocurrency exchanges to eliminate certain pathways for potential sanctions evasion.[143] The Financial Crimes Enforcement Network (FinCEN) has a proposed rulemaking extending reporting requirements to un-hosted wallets.[144] If enacted, crypto exchanges would be required to collect names and home addresses, among other personal details, from anyone hoping to transfer cryptocurrencies to their own private wallets.[145]

Another area of vulnerability could be Peer-to-Peer (P2P) exchanges.[146] These are cryptocurrency exchanges that operate without any central intermediary or authority to transmit assets or collect customer information. This increases the difficulty of tracing illicit activity or complying with the Bank Secrecy Act (BSA), which requires U.S. financial institutions to assist the government in detecting and preventing money laundering. Though concern exists that illicit activity could be more easily hidden via P2P exchanges, FinCEN considers P2P

---

[138] *What is blockchain?, supra* note 81.
[139] Gareth Jenkinson, Into the storm: The murky world of cryptocurrency mixers, COIN TELEGRAPH (Dec. 7, 2022), https://cointelegraph.com/news/into-the-storm-the-murky-world-of-cryptocurrency-mixers.
[140] *Id.*
[141] Helen Partz, *Blockchain.com closes crypto custody for Russians amid EU sanctions*, COIN TELEGRAPH (Oct. 14, 2022), https://cointelegraph.com/news/blockchain-com-closes-crypto-custody-for-russians-amid-eu-sanctions.
[142] *Id.*
[143] Press Release, U.S. Dept. of the Treasury, Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex (April 5, 2022) (on file with the author).
[144] "FinCEN is proposing to amend the regulations implementing the Bank Secrecy Act (BSA) to require banks and money service businesses (MSB) 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 un-hosted wallets, or held in wallets hosted in a jurisdiction identified by FinCEN." Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 85 Fed. Reg. 83840 (Dec. 23, 2020) (to be codified 31 CFR pts. 1010, 1020, 1022).
[145] *Id.*, However, crypto advocates said they were concerned the rules might be impossible for certain wallets to comply with because they are not controlled by people and therefore are not tied to this personal information. There is also concern the compliance requirement might be overly burdensome for individuals. *see*, Nikhilesh De, *The Unhosted Crypto Wallet Rule is Back*, COINDESK (Jan. 31, 2022, 7:13 AM), https://www.coindesk.com/policy/2022/01/29/the-unhosted-crypto-wallet-rule-is-back/.
[146]Darren Kleine, *Crypto Regulation is Coming to Europe: Are Exchanges Ready for New Rules?*, COINTELEGRAPH (Dec. 18, 2019), https://cointelegraph.com/news/crypto-regulation-is-coming-to-europe-are-exchanges-ready-for-new-rules.

exchanges and mixers to be money service businesses and are therefore already under regulation.

However, many do not register with FinCEN which is required. It comes back to the question of enforcement both of compliance with registering and tracking down violators.[147] As it stands, Cryptocurrency transfers on digital financial exchanges, that are not yet fully regulated for anti-money laundering and counter-terrorist financing. Tokens can be used to bypass steep economic sanctions in cases where exchanges don't comply with rules, if companies have inadequate compliance procedures, or when technologies that increase anonymity are used.[148] Though mass, country-wide evasions of sanctions may not be a current reality, the preverbal crypto-train has left the station and as described above, there is illicit activity and money laundering taking place via cryptocurrency channels.[149]

VI. A WAY FORWARD FOR REGULATIONS

Looking at recent litigation offers some insights into possible options for crypto regulation, but the cases still do not offer bright line rules, rather how best to enforce and rule on sanctions evasions through crypto-based crimes, still seems to be fact and case sensitive. Earlier this year the DOJ charged, for the first time, an unnamed U.S. citizen for using cryptocurrency to evade sanctions against Russia.[150] This citizen allegedly opened two digital currency accounts, one in the U.S. and one in the sanctioned country, with which the citizen transmitted over $10 million worth of bitcoin between the U.S. and the sanctioned country, using a U.S.-based IP address.[151] Civil and criminal liability for evading sanctions has been around for decades. The International Emergency Economic Powers Act (IEEPA) which authorizes the president to levy sanctions, has long made it unlawful to "violate, ... conspire to violate, or cause a violation of" levied sanctions.[152] Most sanction regimes "prohibit the direct and indirect importation, exportation, and re-exportation of goods, services, and technology, without a license from OFAC."[153] Services include "any transfer of funds, directly or indirectly."[154] What appears to be new, if not surprising, is guidance affirming that

---

[147] The Department of Justice (DOJ) has prosecuted P2P exchangers for money and laundering and BSA violations. *See*, Press Release, U.S. Dept. of Just., Operator of Unlawful Bitcoin Exchange Sentenced to More Than 5 Years in Prison For Leading Multimillion-Dollar Money Laundering And Fraud Scheme (June 27, 2017), https://www.justice.gov/usao-sdny/pr/operator-unlawful-bitcoin-exchange-sentenced-more-5-years-prison-leading-multimillion#:~:text=MURGIO%20was%20sentenced%20today%20by,million%20in%20illegal%20Bitcoin%20transactions.

[148] Kleine, *supra* note 146.

[149] *See supra* Part IV(A).

[150] In May 2022, DOJ filed an application for a criminal complaint with Judge Faruqui charging a U.S. person ("Defendant") with conspiring to violate the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. § 1705, and defrauding the United States, in violation of 18 U.S.C. § 371. The docket in this case is under seal. For that reason, the court redacted facts and identifying information about the witnesses and defendant and declined to mention the specific country to which the U.S. citizen allegedly transferred the cryptocurrency. Possible countries include Cuba, Iran, North Korea, Syria or Russia.; *see also*, In re: Criminal Complaint, No. 22-mj-067-ZMF at 1–3 (D.D.C. May 13, 2022). IEEPA makes it illegal to violate comprehensive trade-based sanctions programs (*e.g.*, Iran, North Korea, and Russia) administered by the Treasury's Office of Foreign Assets Control ("OFAC") and carries a stiff maximum penalty – 20 years' imprisonment and a $1,000,000 fine. Most sanction regimes "prohibit the direct and indirect importation, exportation, and re-exportation of goods, services, and technology, without a license from OFAC."

[151] *Id.*

[152] IEEPA, *supra* note 30.

[153] In re: Criminal Complaint, *supra* note 150, at 3.

[154] *Id.*

cryptocurrency transactions fall within the IEEPA's reach.[155] The U.S., like other countries are independently searching for and testing out methods of regulation and enforcement by using existing regulatory mechanisms.[156] However, the cryptocurrency arena is transnational, fast moving and ever changing and actors seeking to evade international sanctions in this space, thus fall under multi-national jurisdictions. Therefore, the need for an internationally coordinated approach to cryptocurrency regulation, will be critical to curtailing sanctions evasions.

A. Three Considerations for International Regulation

There are a few areas worth considering when looking at how best to stem the flow of sanction evasions by way of cryptocurrency. A successful international regulatory framework of cryptocurrency should include two aspects. First, it should provide governments with the identities of their countries' cryptocurrency users. This should preserve a level of "pseudo-anonymity" and permit the implementation of regulatory functions: users' identities will remain anonymous to all but certain governmental actors.[157] This is important as a frequent concern raised in response to the prospect of an international regulatory regime is the erasure of cryptocurrency users' anonymity.[158]

Exposing parts of a user's identity should be viewed as a shift on the spectrum of anonymity instead of an erasure of user anonymity altogether, as it pertains to regulations. The European Union recently implemented Know Your Customer ("KYC") laws modeling one way this shift might be accomplished.[159] These KYC regulations require European financial institutions to identify and verify their clients' identities.[160] Cryptocurrency exchanges throughout Europe have been impacted, as they are now required to peel back layers of anonymity to uncover their users' identities.[161] This system possesses still, several

---

[155] That guidance came last October when the U.S. Department of the Treasury's Office of Foreign Assets Control which administers the IEEPA, issued guidance stating that: OFAC sanctions compliance obligations apply equally to transactions involving virtual currencies and those involving traditional fiat currencies. *See* U.S. Dep't of the Treasury, Sanctions Programs and Country Information, https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information (last visited Nov. 18, 2022); *See also*, Off. Foreign Assets Control, Sanctions Compliance Guidance for the Virtual Currency Industry 1 (Oct. 2021), https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.

[156] *See supra* Part III.

[157] This is a key component of why cryptocurrency works. *See, supra* note 72.

[158] Rakesh Sharma, *What Does Government Regulation Mean for Privacy-Focused Cryptocurrencies?*, INVESTOPEDIA (June 25, 2019), https://www.investopedia.com/news/what-does-increased-government-regulation-mean-privacyfocused-coins (quoting the CEO of Digital Dash, an open source alternative cryptocurrency: "Privacy is important for many practical reasons including user safety, so we believe it is an important aspect to incorporate into our solutions."); *see also*, Jerry Brito, *China intends to launch a national digital currency that will let the government easily surveil spending. Following in their footsteps would be a mistake*, COINCENTER (Oct. 21, 2019), https://www.coincenter.org/china-intends-to-launch-a-national-digital-currency-that-will-let-the-government-easily-surveil-spending-following-in-their-footsteps-would-be-a-mistake/ ("Any ... American-led effort [to regulate cryptocurrencies] must ... mak[e] anonymity and censorship-resistance core network features.").

[159] S*ee The Impact of Rising KYC & AML Regulations in Europe*, Know Your Customer, https://knowyourcustomer.com/impact-rising-kyc-aml-regulations-europe (last visited Oct. 11, 2020).

[160] Fedor Poskriakov et al., *Cryptocurrency Compliance and Risks: A European KYC/AML Perspective*, BLOCKCHAIN & CRYPTOCURRENCY REGULATION (Josias N. Dewey ed., 2nd ed. 2020), https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/11-cryptocurrency-compliance-and-risks-a-european-kyc-aml-perspective.

[161] Importantly, KYC laws do not reveal crypto users' identities to the public at large. Rather, users' identities are mandatorily disclosed to a select sphere of institutional actors as identified in the KYC regulations. *See generally* Craig Adeyanju, *What Crypto Exchanges Do to Comply with KYC, AML and CFT Regulations*,

vulnerabilities as untrustworthy third-party intermediaries still act as gatekeepers to sensitive data.[162] However, the European KYC laws illustrate that cryptocurrency regulations can exist without handicapping users' pseudo-anonymity altogether. Financial institutions, moreover, can learn by putting in practice traditional approaches to financial regulation, in an adaptable way and still maintain cryptocurrency's structural integrity.[163]

B. International Coordination and Information Sharing

Secondly, when considering how to make the sharing of sensitive information streamlined, secure and easy to monitor both at the international and state level, we can look at an existing framework for guidance. One such organization is the International Civil Aviation Organization ("ICAO"), a specialized agency of the United Nations.[164] ICAO develops recommended aviation practices followed by signatories of the Convention on Civil Aviation (the "Chicago Convention").[165] One program many are familiar with and participants of already, is the Traveller Identification Programme ("TRIP").[166] The objective of TRIP is for all U.N. Member States to have the ability to "uniquely identify individuals," i.e., that all citizens who wish to travel internationally, will have a unique identifying number, colloquially, your passport number.[167] The program outlined in TRIP allows countries autonomy and flexibility in meeting these goals.[168] Crucially, the TRIP program simultaneously maintains a global network in which passports--and thereby individuals--can be identified at any international juncture.[169] The multilateral nature of ICAO allows for evolution and the continuous adaptation of travel protocols.[170] For these reasons, a coordinated "public key directory" could be a streamlined way to track and share information as part of a regulatory

---

COINTELEGRAPH (May 17, 2019), https://cointelegraph.com/news/what-crypto-exchanges-do-to-comply-with-kyc-aml-and-cft-regulations; Darren Kleine, *Crypto Regulation is Coming to Europe: Are Exchanges Ready for New Rules?*, OINTELEGRAPH (Dec. 18, 2019), https://cointelegraph.com/news/crypto-regulation-is-coming-to-europe-are-exchanges-ready-for-new-rules.

[162] *See supra* Part IV.

[163] Adeyanju, *supra* note 162.

[164] *See Convention on International Civil Aviation--Doc 7300*, ICAO, https://www.icao.int/publications/pages/doc7300.aspx (last visited Oct. 11, 2020).

[165] *See* Convention on International Civil Aviation, Dec. 7, 1944, 15 U.N.T.S 295.

[166] *Traveller Identification Programme,* ICAO, https://www.icao.int/security/FAL/TRIP/Pages/default.aspx, (last visited Dec. 8, 2022).

[167] Id. To facilitate the TRIP objective, the ICAO issues recommendations that help countries develop databases to store and process credible evidence of identification. The ICAO also facilitates the creation of globally connected systems which link passports to their holders.

[168] For example, TRIP permits nations flexibility in the identifying information held in each national passport database. Some nations such as Argentina maintain biometric data accessible by a wide variety of Argentinian governmental agencies; others, such as Canada, are in the process of eliminating the development of centralized databases containing biometric information. *Biometric Data Retention for Passport Applicants and Holders*, L. LIBR. CONG. (Mar. 2014), https://www.loc.gov/law/help/biometric-data-retention/biometric-passport-data-retention.pdf [hereinafter *Biometric Data Retention*]. TRIP also provides recommendations for Machine Readable Travel Documents ("MRTD" or passports) which allows for flexibility in their form and substance. *See Machine Readable Travel Documents (Doc 9303)*, ICAO (7th ed. 2015), https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf.

[169] *Id.*

[170] For example, ICAO has recently begun to engage with the United Nations' sustainable development goals ("SDGs") and has linked its strategic objectives to these goals. It continuously monitors the effects of these goals and develops its framework as appropriate. *Aviation Development*, ICAO, https://www.icao.int/about-icao/aviation-development/Pages/default.aspx (last visited Oct. 11, 2020); *ICAO and the United Nations Sustainable Development Goals*, ICAO, https://www.icao.int/about-icao/aviation-development/pages/sdg.aspx (last visited Oct. 11, 2020).

scheme of cryptocurrency. Cryptocurrencies are a fast-developing market[171] which national governments and inter-government agencies struggle to fully understand.[172] For an industry that is constantly changing, flexibility and agility will be crucial especially in the beginning stages of an international regulatory structure.[173]

C. A Need for "Friendly Adversarialism"

Finally, when seeking to regulate a volatile, non-traditional financial mechanism such as open-source cryptocurrency, one that resembles the wild west more than an organized institution, we must consider equally non-traditional, and sometimes riskier, means of regulation. One way that companies and governments could aim to safeguard themselves from sanction evaders, particularly those who use ransomware, malware or spyware to steal and launder money through cryptocurrency, [174] is to consider utilizing White Hat Hackers (WHH).[175] The use of WHHs (i.e., ethical hackers), is a controversial approach yet one that puts companies and governments in an offensive, empowered position to better regulate, monitor and potentially curtail theft, and catch bad actors.[176] A WHH's main goal is to find and expose vulnerabilities in codes, the same way cybercriminals do. The difference is, WHHs give the money back, expose the threat, and sometimes aid in correcting the flawed systems.[177] WHHs operate in a presumed grey area, both ethically and legally.[178]

Decentralized finance continues to be a vulnerable industry with anonymous founders, open-source code and billions of dollars looking to take on risk. The enormous amount of capital in this space has created an incentive system aligned with teams that build fast and

---

[171] There are over 2000 different cryptocurrencies available on the market. *See generally,* Lubomir Tassev, *The Number of Cryptocurrency Wallets is Growing Exponentially*, BITCOIN.COM (Sept. 26, 2019), https://news.bitcoin.com/the-number-of-cryptocurrency-wallets-is-growing-exponentially/.

[172] *See supra* Part V.

[173] Timothy Massad, *It's Time to Strengthen the Regulation of Crypto-Assets*, BROOKINGS UNIV. 21, 42 (Mar. 2019).

[174] *See supra* Part V (North Korea).

[175] The terms "white hat" and "black hat" come from the golden age of Hollywood Westerns, when the good guy and the bad guy were easily identifiable to the audience by the color of their hats. Black hats are no-gooders who will steal anything and everything from anyone. White hats, by contrast, work to protect companies, projects and individuals., *see* Andrew Froehlich, What is a white hat hacker?, TECHTARGET, https://www.techtarget.com/searchsecurity/definition/white-hat#:~:text=The%20terms%20come%20from%20old,legally%20permitted%20to%20do%20so. (last visited Dec.10, 2022).

[176] *See* Edward Oosterbaan, *Why White Hat Hackers are Vital to the Crypto Ecosystem*, COINDESK (Dec. 10, 2022), https://www.coindesk.com/layer2/2022/02/23/why-white-hat-hackers-are-vital-to-the-crypto-ecosystem/, (Stating that Jay Freeman (a WHH) stopped a potential $750 million vulnerability from being exploited on three of Ethereum's layer 2 networks.)

[177] Freeman has also contemplated where the middle ground between "Code is Law" and third-party trust falls. "Bug bounties are essential in incentivizing good actors to seek out and find vulnerabilities. By setting the reward for being a good actor on a similar scale as the payout for being a bad actor, that scale suddenly tilts the incentives toward white hatting." As Freedman put it, this sort of "friendly adversarialism" can encourage ecosystem participants to be more open, honest and even pessimistic about new ideas. *see id.*

[178] While the open nature of blockchain technology means that most protocols and smart contracts are accessible without breaking into a corporate network to look for weaknesses, even testing that a vulnerability exists can be something the law frowns upon. *See id.*

release tokens.[179] This can be a lucrative, exciting profession for talented hackers, and a means to expose and secure vulnerabilities on a regular basis.[180]

Of course, another important part of crypto security, specifically relating to how actors might be evading sanctions, is being able to protect against and track hacked funds, whether going out or coming in.[181] This however, requires a more coordinated effort than solely employing, often rouge white hats that traditionally work for themselves and are more motivated by the chase and bug bounties than working on an internal team to monitor particular companies.[182] WHHs should be viewed as tool in the hands of a more coordinated multi-agency (both current and potentially new) regulation scheme. There is a growing presence of analytics platforms[183] that may fill the gap where traditional compliance officers or companies lack the skill, expertise to combat crypto-based crimes and sanctions evasions.[184] These platforms can build and monitor risk management systems, monitor potential compliance problems, and investigate and track digital assets.[185] Just as traditional financial institutions employ skilled compliance officers and general counsel to ensure regulatory compliance and asses risk for traditional methods of doing business, businesses in the financial sector and businesses that deal in cryptocurrency, will need to be proactive to enhance their due diligence.[186] The ways in which the government and international agencies regulate this space by nature has and will continually evolve and adapt, since cryptocurrency is still evolving. Now more than ever businesses must arm themselves with cyrpto-saavy compliance and legal teams and expert advisors to guard against current and possible risks.[187]

CONCLUSION

Russia invaded Ukraine earlier this year. Ever since people from all over the world have donated tens of millions of dollars' worth of cryptocurrency directly to the Ukrainian

---

[179] In Praise of White Hat Hackers, CRYSTAL BLOCKCHAIN (Sept. 15, 2021), https://crystalblockchain.com/articles/in-praise-of-white-hat-hackers/.

[180] White hats have many motivations, beginning with making a living by doing something they love and showing off their skills while doing good. Others are largely doing it for fun or for rewards — the "bug bounties" many tech companies offer for bringing security flaws to their attention. "Bug bounties" can range from $500 to $500,000 depending on the amount of the breach. *See id.*

[181] CRYSTAL BLOCKCHAIN, *supra* note 179.

[182] *In Praise of White Hat Hackers*, *supra* note 181.

[183] *See e.g.,* Press Release, Chainalysis Launces Sanctions Screening Tools Free of Charge for Cryptocurrency Industry, CISION PR NEWSWIRE (Mar. 10, 2022), https://www.prnewswire.com/news-releases/chainalysis-launches-sanctions-screening-tools-free-of-charge-for-cryptocurrency-industry-301500350.html.

[184] There is a growing number of advisors filling the space to educate and guide best practices for companies. *See generally*, Che Sidanius, *How are digital assets used to evade sanctions?*, REFINITIV: REGULATIONS (Aug. 8, 2022), https://www.refinitiv.com/perspectives/regulation-risk-compliance/how-are-digital-assets-used-to-evade-sanctions/.; *See id.*, A coalition to fight financial crime, established The Digital Asset Task Force (DATF) an expert committee comprising a range of industry leaders concentrating on the relationship between digital assets and financial crime.

[185]*See generally*, Crypto assets and Sanctions Compliance Report, Global Blockchain Business Council (GBBC) Digital Finance, (2022), https://www.gdf.io/wp-content/uploads/2022/07/Cryptoassets-and-Sanctions-Compliance-Report-Final-1.pdf. [hereinafter GBBC Report].

[186] Because U.S. individuals and companies, broadly are prohibited from engaging in transactions with sanctioned parties, and as sanctions are "strict liability," sanctions evasion not only presents designation risks for evaders and facilitators, but also creates risks of enforcement action (financial penalties), as well as practical and reputational risks to unwitting parties that process such payments. *See generally*, Winston & Strawn, LLP, Russia-Ukraine Conflict Increases Regulatory Risks for Sanctions Evasion Through Crypto-Based Transaction (Jul. 27, 2022), https://www.winston.com/en/global-trade-and-foreign-policy-insights/russiaukraine-conflict-increases-regulatory-risks-for-sanctions-evasion-through-crypto-based-transactions.html#!/closed_state.

[187] GBBC Report, *supra* note 186, at 8-9.

government,[188] some of which has already used the funds to help purchase military equipment.[189] This is an inspiring demonstration of how cryptocurrency enables people to easily engage in financial transactions, across borders at the speed of the worldwide web and serves as a powerful example of what this relatively new financial ecosystem can do. The possibilities for financial inclusion as the cryptocurrency space matures, seem to be boundless.

As highlighted in this Paper, these innovations are available to both good and bad actors. While those in favor of democracy and the sovereignty of countries, celebrate the Ukrainian government's successful fundraising initiative, the very real concerns, and incidences where cryptocurrency is being used by sanctioned entities and individuals in Russia to evade sanctions, continues to beckon an international regulatory response. As independent countries work to bolster existing agencies,[190] an international regulatory initiative, rooted in coordination, innovation, and modification of existing laws, are important next best steps on the journey to pay sheriff in the wild west of cryptocurrency.

[188] Magenzie Sigalos, *Ukraine has raised more than $54 million as bitcoin doations pour in to support the war against Russia*, CNBC (Mar. 24, 2022), https://www.cnbc.com/2022/03/03/ukraine-raises-54-million-as-bitcoin-donations-surge-amid-russian-war.html.
[189] Olga Kharif, *Ukraine Buys Military Gear With Donated Cryptocurrencies*, BLOOMBERG (Mar. 5, 2022 7:21 AM), https://www.bloomberg.com/news/articles/2022-03-04/ukraine-spends-15-million-of-crypto-donations-on-military-gear?sref=tHYYdqx0#xj4y7vzkg.
[190] See supra section on US regulation