

Sanctions Evasion 2.0: Unpacking the Role of Cryptocurrency in North Korea and Iran's External Trade Relations

AbdulMalik O., OLADIPUPO

Lead City University, Ibadan, Oyo State, Nigeria

oladipupo.abdulmalik@lcu.edu.ng

Abstract

This study delve into various ways through which cryptocurrency is being used for sanctions evasion, specifically in relation to the external trade relations of North Korea and Iran. The paper seeks to contribute to understanding the ways decentralized digital currencies support illicit financial activities via the use of a quantitative research methodology which involves an examination of official reports, policy documents, academic work and investigative journalism. The study is based on the intersectionality of state power, financial sovereignty and digital innovation in a multipolar world and based on the Theory of Realism and Constructivism. Analysis also shows that North Korea spends billions of cryptocurrencies every year stealing and laundering money with state-sponsored cybercrime, primarily through the Lazarus Group. At the same time, Iran is adopting a more institutionalized approach by legalizing crypto mining, guiding revenue towards the Central Bank and sanctioning entities taking advantage in trading with crypto exchanges and crypto mixers. Lastly, the study shows that the anonymity and border lessness of digital assets make them a problem to enforce globally and undermine traditional sanctions regimes. To further enhance the latter, it encourages international cooperation on crypto regulation, blockchain analytics capabilities, and addressed tailored sanctions on crypto service providers that aid in obfuscation. In order to solve the two challenges of technological innovation and illicit finance, a harmonized legal framework is needed.

Keywords: Cryptocurrency, sanctions evasion, North Korea, Iran, Digital economy.

Introduction

There is an enormous shift underway in the global financial system, powered by one thing in particular: digital, namely decentralized, cryptocurrencies. As a medium of exchange, cryptocurrencies that became the alternative to state-backed currencies in the beginning, Bitcoin, Ethereum, Monero, and other privacy-focused coins have in turn culminated as powerful tools for state actors seeking to circumvent international sanctions regimes. North Korea and Iran are two of the most prominent users of these digital currencies to evade sanctions, as the countries have endured decades of U.S., European Union, and United Nations Security Council economic restrictions, for their nuclear activities, sponsorship of terrorism and human rights abuses (UN Panel of Experts 2023; U.S. Department of the Treasury 2022). Cut off and heavily sanctioned, North Korea weaponized its elite cyber capabilities to raise money for its regime. The country has raised an estimated \$3 billion in cryptocurrency through cyberattacks, including the Axie Infinity hack in 2022, which is thought to have brought in a record-breaking \$620 million (Elliptic, 2022), is according to the United Nations Security

Council (UNSC) 2023 report. According to Chainalysis (2023), these stolen funds are redacted through mixers, privacy coins, and illicit exchanges to make it difficult to trace the origin before they are used to purchase dual-use technologies and luxury goods, contrary to international law.

On the contrary, Iran has adopted a more institutionalized approach. Despite sanctions being reintroduced following the U.S. withdrawal from the Joint Comprehensive Plan, or JCPOA in 2018, Iran has regulated, legalized and harnessed the opportunity of its vast and relatively cheap electricity resources to fuel cryptocurrency mining (Al Jazeera, 2022). Back in August, the Iranian Ministry of Industry, Mines and Trade announced it had purchased its first government import order (\$10 million) using cryptocurrency, which IMF Trade Fin and seven other news outlets reported upon, as a signal of a broader Iranian effort to circumvent U.S.-controlled financial systems like SWIFT (Reuters, 2022). Additionally, Iran has had, and continues to have, an ambition to build crypto based trade links with Russia, Venezuela, China and other nations similarly interested in developing alternative global payment networks.

This trend buckles against the increasing shift of both conventional and digital assets to circumvent sanctions, and represents a move beyond the original incarnation of ‘sanctions evasion 2.0’, as some analysts describe it: where state actors use the anonymity, speed and border lessness of blockchain built assets to fund their economies and promote political interest (Rosenberg & Dorfman, 2023). Repeatedly, the Financial Action Task Force (FATF) has warned that virtual asset risks “substantial” are made to be exploited by rogue countries, and encouraged broader implementation of the Travel Rule, which requires checking identity and reporting large currency transactions (CryptoFlight.co, 2023).

While North Korea and Iran are different in their method and capability in their turn to cryptocurrency as a cornerstone in their external trade strategies under sanctions, this paper aims to unpack by what mechanisms and in what ways they have both turned to cryptocurrency in their efforts to break sanctions. It provides answers to three decisive questions:

- i. How is cryptocurrency being used to circumvent these restrictions by these states? Which tools and tactics are they using?
- ii. What are the implications for the world as a security issue?
- iii. How can the international community combat this emerging threat in the correct manner?

This study has a comparative analysis of crypto enabled sanctions evasion by comparing and contrasting their cases to the international relations theory.

Literature Review

Cryptocurrency as a Tool for Sanction Evasion

The rise of cryptocurrencies has radically changed the global financial world, giving increases and problems to states and non-state actors. This is one of the hottest on the same token as it is a matter of concern that in an increasingly digital world these digital currencies are being abused by sanctioned nations to circumvent the typical financial channels and regulatory mechanisms. One of the design specifications of cryptocurrencies such as blockchain technology powers decentralized networks that enable peer to peer transactions without the need for intermediaries, such as banks, or central authorities. While states use this feature to skirt international sanctions, this is also celebrated as a means for financial inclusion and soft

skill in the realms of tech and fin-tech. As Wright (2023) reminds us, however, this shift to a paradigm that is schematically decentralized, and with a lack of control held by state authorities, is a powder keg; cryptocurrency has found fertile soil for sanctioned countries, especially those that possess the capacity for sophisticated cyber weaponry, to monetize illicit cryptocurrency operations. North Korea is notorious in recent years for being on the brink of cybercrime for funding its state operations and its nuclear program, including ransomware attacks, phishing schemes and crypto thefts. However, these activities are carried out using obscure crypto wallets and crypto laundering mechanisms such as mixers and tumblers, which make the task almost impossible for international law enforcement agencies to detect and intervene.

Addressing this, Wronka (2022) explores in detail how digital currencies conduct anonymous international transactions. While Monero and Zcash are specifically crafted for privacy and let everyone obscure its origin and destination, Wronka says. Privacy-enhancing services and tools obfuscate even more mainstream cryptocurrencies like Bitcoin that only provide pseudo-anonymity. This anonymity makes such tracking orders impossible and also makes it almost impossible to find out who is standing behind the funds, as well as to enforce existing financial sanctions against those parties. Added to this is the nature of cryptocurrencies being borderless and transactions are performed across jurisdictions without regard to national financial laws or international sanctions frameworks. Such a strong reliance on institutions like SWIFT (Society for Worldwide Interbank Financial Telecommunication) in monitoring, controlling and reporting suspicious transactions is a traditional way for financial systems. Conversely, blockchain-based systems are untethered to these infrastructures and therefore, sanctioned states can continue to conduct trade and obtain hard currency through crypto exchanges, many of which reside in regulatory grey areas or non-cooperative jurisdictions, as well as convert digital assets to hard currency.

North Korea's Exploitation of Cryptocurrencies

Cryptocurrencies have become particularly popular for North Korea to exploit the technology to evade international sanctions and generate illicit revenue. North Korean linked entities accounted for \$1.3 billion (\$5.3 billion) worth of cryptocurrency theft in 2024, nearly two-thirds of all global cryptocurrency thefts that year (Chainalysis, 2025). The primary responsible clans for these cyber activities are overwhelmingly credited back to the Lazarus Group, an off haven hacking clan that is linked to Reconnaissance General Bureau, or as North Korea refers it to itself, the Reconnaissance General Bureau. The most recent cyber-attacks attributed to the Lazarus Group include some of the worst ever. In February 2025, it was reported that the group was behind the \$1.5 billion heist of the major Asian cryptocurrency exchange, ByBit, using complex phishing and social engineering techniques to bypass security systems (Elliptic, 2025). Not only is this a prime example of North Korea's scale and precision over cyber operations, but the involvement of digital currencies also suggests that the regime has adopted such financial instruments to sustain the regime and (to a large extent) their proliferation activities themselves.

While above high-profile cyber thefts, North Korea has developed a wider web of illicit financial manoeuvres to launder the money from these activities. For instance, the UN Panel of Experts (2024) has reported that North Korean-operated restaurants abroad, for example, the

'Sindat BBQ' operating out of Laos, not only generate revenue but also launder stolen digital assets. Proceeds from these establishments are channeled back to the regime as it also supports other, more general, covert operations like cryptocurrency mining and theft infrastructure. Combining cybercrime, cryptocurrencies, and covert state funding creates a challenge unique to the international community of both law enforcement and sanctions enforcement bodies. Without more effective coordinated international politics to combat North Korea's digital tactics, global financial security would remain compromised.

Iran's Institutional Approach to Cryptocurrency

As a way of circumventing the restrictions of international sanctions on the country, Iran has taken a more structured approach to integrating cryptocurrencies into its economy. In 2019, the Iranian government started legalizing certain terms of the cryptocurrency mining business to benefit from the budding crypto industry's potential to generate revenue (Coindesk, 2019). Nevertheless, this legalization came with strict regulations. One example is that miners were required to have official licenses, and they were ordered to sell its mined cryptocurrencies to Central Bank of Iran, consolidating the state control over the digital currency flows (Elliptic, 2021). However, according to reports, various Iranian state-linked entities had engaged in such illicit crypto activities. In 2022, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanction ten individuals and two companies that are affiliated with the Islamic Revolutionary Guard Corps (IRGC). Chainalysis (2022) further charged that these entities used ransomware attacks to extort cryptocurrency payments, laundered the obtained cryptocurrency, and rerouted the funds back into Iran's financial system by channelling it through their local exchanges. Iran has also been assisted by facilitators in other regions as part of its overall strategies concerning the domestic uses of cryptocurrency. In 2024, major money laundering networks were dismantled in the United Arab Emirates that used unlicensed cryptocurrency intermediaries (AGBI, 2024). Both China and the UAE promised to cooperate on fighting crypto-related crimes, including money laundering and fraud (Crypto Times, 2024). While there have been instances of crypto laundering in Malaysia, they have been low, and gaps that may be exploited by Iranian actors exist (The Star, 2024). This is why these developments are seen as crypto laundering on a globalized basis and prioritize the need for coordinated enforcement actions.

Regular Iranians have also outwitted domestic constraints by finding their own means of derogating them. The reason why many Iranians use virtual private network (VPN) is because they do not have access to international crypto platforms. The fact that it is an unregulated area, allows them to bypass local oversight and international restrictions, making it even more difficult to regulate them (Elliptic, 2021). While the country has created mechanisms to govern the crypto mining of the blockchains, sanctioned state actors as well as civilian continue to take advantage of loopholes. These are the obstacles of using conventional sanctions in an era of decentralized digital, and they require deeper international cooperation and containment.

Challenges in Enforcing Sanctions in the Crypto Ecosystem

Cryptocurrencies are a new type, particularly an asset backed by public, decentralized technology, and not controlled by any central authority: they present significant challenges in

terms of enforcement, for those trying to put in place and enforce effective sanctions. From targeting specific entities, some success has been achieved, but others still use digital assets to move funds through sanctioned addresses. Rapid exchange services, as well as decentralized finance (DeFi) platforms, are commonly used by these actors in order for the trail of illicit transactions to be as convoluted as possible. This trend has, in fact, come to the notice of the U.S. Department of the Treasury, which has raised serious concerns over this trend and has informed that terrorist organizations as well as hostile states like al Qaeda, Hamas, Russia, etc. are increasingly using virtual assets to camouflage their financial transactions and bypass international prohibitions (Reuters, 2024). During an April 2024 Senate testimony, Deputy Secretary Wally Adeyemo said that Congress needs to give law enforcement extra regulatory tools to deal with these growing threats.

Tornado Cash, a cryptocurrency mixer which strives to second-hand anonymous digital currency transactions, is one of the most illustrative examples of the enforcement dilemma. Last year, not long after it emerged that Tornado Cash had been used to launder more than \$7 billion worth of cryptocurrency, including funds siphoned by North Korea's Lazarus Group, Tornado Cash was sanctioned by the U.S. Treasury's Office of Foreign Assets Control (OFAC) (U.S. Department of the Treasury, 2022). In October 2023, following Hamas attacks against Israel, the Financial Crimes Enforcement Network (FinCEN) suggested designating all foreign crypto mixers as national security threats because they are aiding money laundering, and all that more reason to regulate anonymizing tools in the digital economy (Wired, 2023). This is an indication of the whole debate of striking the right balance between safeguarding user privacy in the world of decentralized finance and taking measures to hinder illicit financial flows. In the process of these accelerating developments of cryptocurrencies, the international community needs to come up with an adaptive framework which account for enforcing challenges and the rights of the legitimate users.

Theoretical Framework

This paper uses a dual-theoretical lens – Realism and Constructivism, two influential theories in the International Relations (IR) field to understand how and why North Korea and Iran use cryptocurrencies for sanctions evasion. These perspectives enable us to also critically scrutinize both the strategic reasons and ideational bases for crypto enabled economic sporting by sanctioned states.

Realism: Survival and National Interest in Anarchic Systems

It is fueled by an assumption of a very anarchic international system and states orienting their actions mainly to the concern of survival and advancing their national interest (Mearsheimer, 2001; Waltz, 1979). Here, power (most notably economic and military) is currency in the realm of global politics. Comprehensive sanctions on countries like North Korea and Iran force states to innovate new channels of sowing for themselves economically. It therefore makes sense for them to use cryptocurrencies as there is no way globally to regulate them, which are decentralized (Gruszczak, 2022). These regimes are using crypto assets in order for national survival, for the maintenance of trade flows, and for the avoidance of financial asphyxiation. To name an example, North Korea's cyber unit the Lazarus Group has managed to launch major heists in the cryptocurrency field recouping huge revenue for the regime (Wright &

Moorthy, 2023). As such these acts can be interpreted as deliberate state action to reallocate global digital resources toward state national resilience, a central realist behavior.

Constructivism: Technology, Identity, and Norm Contestation

However, the view of constructivism also has its own complementary view, which emphasizes the role of social structure, identity, norms and ideational factors in shaping state behavior (Wendt, 1999). Rather than being material, power under Realism is seen as a symbolic and normative dimension including how actors interpret and respond to global norms, which Constructivism does.

It is not just a financial tool, as cryptocurrency in this framework is also a symbol of resistance against a drive for U.S. financial imperialism and the liberal international order. For instance, as Iran has rhetorically stated its digital currency strategy as an exercise of sovereignty and self-reliance, rigidly connected to its ideological anti-Western hegemony (Zarghami et al., 2023). Likewise, North Korea believes digital finance can be used to subvert US control of global trade and finance infrastructure, including SWIFT. Based on technological innovation these states reinterpret and redefine the legitimacy of internationally normative rules such as those in sanctions and global finance. However, constructivism makes a key contribution in helping us understand not only why they need to invest in alternative financial architecture, but also why they choose to invest in them as part of a normative contestation of Western dominated financial system. Cryptocurrencies are used strategically in a hostile international environment for tools of statecraft and survival, according to realism. On the other hand, crypto adoption is explained through constructivism in terms of how crypto fits into broader vocabularies of resistance, identity and alternative sovereignty. Consequently, they contribute to a more complete picture on how geopolitics, economy, and technology overlap to form crypto strategies of North Korea and Iran.

Research Methodology

Qualitative, comparative case study is used as methodology of this study based on North Korea and Iran which are paradigmatic examples of states employing cryptocurrency to evade international sanctions. The research mainly relies on secondary data sources, both from credible materials such as United Nations Panel of Experts reports, Financial Action Task Force (FATF) assessments, blockchain analytics of firms such as Chainalysis, as well as scholarly publications and policy briefs from global think tanks. In the study such recurring theme, strategy and pattern of these states to use digital currencies for the external trade, is identified by the content analysis. The step-by-step coding of data helps uncover the key trend in the state backed crypto operations, illicit financial flows, and the role of decentralized finance in the case of sanctions evasion. The methodology allows one to qualitatively investigate how cryptocurrencies are remodeling the terrain of economic statecraft and geopolitical resistance by comparing divergent and complementary strategy of North Korean and Iranian.

Findings and Discussions

North Korea: Cyber-Enabled Cryptocurrency Exploitation

According to United Nations experts in 2024, North Korea-linked cyber actors stole digital assets valued between \$630 million and over \$1 billion, a record high in terms of the amount involved (Associated Press, 2024). Believed to fund the regime's strategic weapons program, some say cybercrime accounts for up to 40 per cent of its nuclear and ballistic missile development budget (The Times, 2024). To obscure the tracks of stolen cryptocurrency, North Korea has a suite of advanced laundering tools. One method that is quite interesting is the introduction of cryptocurrency mixers, services which obscure transaction history. Al Arabiya (2024) reported in March 2024 that North Korea had used a Tornado Cash mixer to wash \$147.5 million in funds linked to a tumbling of the HTX exchange in the country. Further, the regime deploys the so-called chain hopping, which is the ability to quickly connect assets across all the blockchain networks, resulting in greater untrace ability (Lawfare, 2024).

There are over two hundred front companies and international shell entities through which North Korea leverages to process cryptocurrency-to-fiat conversions. The U.S. Department of the Treasury (U.S. Department of the Treasury, 2024) sanctioned at least several people and entities associated in the United Arab Emirates that were used to launder crypto proceeds on behalf of North Korea's weapons programs in 2024. They have a very important role in exchanging digital assets for the hard currency to pay for the illicit procurement.

One of the new trends in North Korea's crypto operations is sending highly skilled IT professionals abroad. These operatives often pose as freelancers working for legitimate foreign companies, earning crypto-based wages that are partially funneled back to the state. The UN investigated at least 11 cryptocurrency thefts in 2024, totaling \$54.7 million, suspected to involve North Korean IT workers (Al Arabiya, 2024).

Iran and North Korea have also increasingly used cryptocurrencies to access international markets for illicit goods such as weapons, oil and rare materials in addition to domestic strategies. Such covert trade operations (Elliptic, 2023) are facilitated by cryptocurrencies that allow transactions to bypass formal banking channels. Because peer-to-peer (P2P) exchanges have become particularly important since perpetrators can exchange crypto directly without centralized oversight, detection has been particularly tricky (Chainalysis, 2024). Offshore platforms conducting such trades also have additional paths available for laundering proceeds using loosely regulated jurisdictions to combine crypto-to-crypto swaps and mixing services to obscure transaction origins (TRM Labs, 2024). They are decentralized and offshore; and they undercut traditional sanctions regimes and threaten efforts by the international community to restrict access to the global markets.

Iran: Institutionalized Use of Cryptocurrency in Trade

Merely by contrast to North Korea clandestine cyber activities, Iran is relatively open. It approved the use of cryptocurrency mining in 2019 as a strategic economic activity. Wikipedia (2024) Reported, the Central Bank of Iran (CBI) allows the proceeds of licensed miners' earnings to fund sanctioned imports. Although regulated, high energy tariffs have nearly driven these mining operations underground, giving rise to a parallel unregulated market. Iran announced in August 2022 that it had placed the first official import order using cryptocurrency for about \$10 million (Middle East Institute, 2024). It was an important move for digitizing

digital assets for international trade, especially with countries that quarrel with the West and that are also under sanctions, like Venezuela and Russia.

Iranian crypto exchanges like Nobitex have helped digital trade by allowing it to take place. Even though Iran bans cryptocurrencies originating from foreign mines and anti-cryptocurrency laws are instilled, Iranians seeking to avoid restrictions use VPNs and access offshore platforms (Wikipedia, 2024). This shows the semi-permissive regulatory environment, where the state goals (sanctions circumvention) and decentralized crypto are coexistent. From 2018 to 2022, entities working with the Islamic Revolutionary Guard Corps (IRGC) transacted almost \$8 billion in crypto transactions using global exchanges like Binance (Middle East Institute, 2024). This evidence points to how far state-linked institutions are spreading within the global crypto ecosystems for strategic reasons.

Comparative Analysis: North Korea vs. Iran

Aspect	North Korea	Iran
Core Strategy	Cyber theft, laundering, hacking	Legal mining, state-regulated crypto trade
Scale of Operations	Over \$1 billion in crypto theft (2022)	\$8 billion in processed transactions (2018–2022)
Laundering Mechanisms	Mixers (e.g., Tornado Cash), chain-hopping, shell companies	VPNs, semi-legal exchanges, fiat conversion through trade
Key Actors	Lazarus Group, state-sponsored hackers	IRGC-linked firms, Central Bank of Iran
External Trade Targets	Raw materials, tech parts, weapons components	Imports of sanctioned goods (e.g., machinery, medical equipment)

North Korea exemplifies a *cyber-mercenary model* of crypto exploitation, while Iran follows an *institutionalized pathway* aimed at long-term integration of cryptocurrency into its sanctioned economy. Despite their differing approaches, both nations reveal how state actors can subvert global financial controls using blockchain-based technologies.

Conclusion and Recommendations

The integration of cryptocurrency into the external trade practices of those sanctioned states, like North Korea and Iran, represents little other than a seismic change to the geo-political and financial tables. Two of these are cases that show how digital currencies are reinventing the paradigm of state compliance, economic isolation and international law enforcement.

Yet it is now crypto-enabled rogue actor, North Korea, using its elite cyber units alongside international hacker networks, to step up a notch further with its capabilities. The digital assets are not only used to make money, but as a weapon of asymmetrical warfare to disrupt the global systems while the regime gets rich. On the other hand, Iran's strategy proves the less structured, more institutional one. Rather than relying on covert operations, it has attempted to legitimize and embed crypto into its domestic economic policy, recruiting crypto as a sanctioned option when performing international payments, even with allies who are sympathetic or strategic.

Neither model points to a fatal flaw in the former sanction's framework: that conventional crypto monitoring tools do not completely trace, close, or penalize crypto enabled transactions that happen in the Byzantine space of borderless economies.

The implications are profound. A rapidly evolving global regulatory environment will be necessary to keep up with the interests of more and more sanctioned and economically isolated states who are exploring the realms of blockchain-based finance. Decentralized finance (DeFi) systems can operate as them when there is no coordinated action, can be used as safe havens not only for sanctions evasion, but also for terrorism financing, proliferation procurement, and other illicit activity.

Recommendations

1. **Strengthen Blockchain Surveillance:** International collaboration should be enhanced to monitor suspicious flows using advanced analytics from firms like Chainalysis and CipherTrace.
2. **Regulate Crypto Mining and Exchanges:** Multilateral sanctions regimes must include crypto-specific clauses that target mining operations and exchanges facilitating illicit state trade.
3. **Develop Sanction-Resilient Monitoring Frameworks:** Existing frameworks like FATF's Travel Rule must evolve to include decentralized finance (DeFi) protocols and privacy coins.
4. **Public-Private Partnership:** Governments should cooperate with crypto exchanges, financial institutions, and blockchain firms to ensure compliance and intelligence sharing.

References

AGBI. (2024, December). *Dubai busts global money laundering gangs*. Retrieved from <https://www.agbi.com/finance/2024/12/dubai-busts-global-money-laundering-gangs/>

Al Jazeera. (2022, August 10). *Iran's use of crypto to skirt sanctions prompts global concern*. Retrieved from: <https://www.aljazeera.com/news/2022/8/10/irans-use-of-crypto-to-skirt-sanctions-prompts-global-concern>

Boston University Review of Banking and Financial Law. (2023, May 17). *The use of cryptocurrency to evade OFAC sanctions*. <https://www.bu.edu/rbfl/2023/05/17/the-use-of-cryptocurrency-to-evade-ofac-sanctions/>

Chainalysis. (2022). *OFAC Sanctions Iranian Nationals Tied to Ransomware Scheme*. Retrieved from <https://www.chainalysis.com/blog/ofac-sanctions-iran-september-2022>

Chainalysis. (2023). *Crypto Crime Report*. Retrieved from: <https://www.chainalysis.com/resources/reports/2023-crypto-crime-report/>

Chainalysis. (2024). *The 2024 Crypto Crime Report*. Retrieved from <https://www.chainalysis.com/reports/2024-crypto-crime-report>

- Chainalysis. (2025). *2025 Crypto Crime Report*. Retrieved from <https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/Chainalysis>
- Coindesk. (2019, July 22). *Iran Legalizes Crypto Mining*. Retrieved from <https://www.coindesk.com/markets/2019/07/22/iran-legalizes-crypto-mining>
- Crypto Times. (2024, June 3). *China, UAE pledge joint crackdown on cryptocurrency crimes*. Retrieved from <https://cryptootimes.com/2024/06/03/china-uae-pledge-joint-crackdown-on-cryptocurrency-crimes/>
- Elliptic. (2021, May 21). *How Iran Uses Bitcoin Mining to Evade Sanctions*. Retrieved from <https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions>
- Elliptic. (2022). *The Lazarus Heist and the \$620M Axie Infinity Hack*. Retrieved from: <https://www.elliptic.co/blog/tracing-the-ether-the-latest-axie-infinity-hack-update>
- Elliptic. (2023, October 17). *North Korea's Lazarus Group Launders \$900 Million via Crypto*. Retrieved from <https://www.elliptic.co/blog/north-korea-lazarus-group-crypto-laundering>
- Financial Action Task Force (FATF). (2022). *Virtual assets: Red flag indicators of money laundering and terrorist financing*. <https://www.fatf-gafi.org>
- Financial Action Task Force (FATF). (2023). *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*. Retrieved from: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-Update-VA-VASPs.html>
- Gruszczak, A. (2022). Cybersecurity and international relations: Realist perspectives in digital age conflict. *Journal of Strategic Security*, 15(2), 33–47. <https://doi.org/10.5038/1944-0472.15.2.1970>
- Hufbauer, G. C., Schott, J. J., Elliott, K. A., & Oegg, B. (2007). *Economic sanctions reconsidered* (3rd ed.). Peterson Institute for International Economics.
- Mearsheimer, J. J. (2001). *The tragedy of great power politics*. W.W. Norton & Company.
- Miller, B. (2021). The Lazarus heist: How North Korea uses crypto to evade sanctions. *Carnegie Endowment for International Peace*. <https://carnegieendowment.org>
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.
- Portela, C. (2010). *European Union sanctions and foreign policy: When and why do they work?* Routledge.

Reuters. (2022, August 9). *Iran makes first official import order using cryptocurrency*. Retrieved from: <https://www.reuters.com/technology/iran-makes-first-official-import-order-using-cryptocurrency-2022-08-09/>

Reuters. (2024, April 9). *US Treasury's Adeyemo warns 'malign' actors are using virtual assets*. Retrieved from <https://www.reuters.com/markets/us/us-treasurys-adeyemo-warns-malign-actors-are-using-virtual-assets-2024-04-09/>

Rosenberg, E., & Dorfman, J. (2023). *Crypto's Role in Sanctions Evasion: Emerging Threats to U.S. National Security*. Center for a New American Security (CNAS). Retrieved from: <https://www.cnas.org/publications/reports/cryptos-role-in-sanctions-evasion>

Ruggie, J. G. (2022). *Continuity and Transformation in the World Polity: Toward a Neo-Constructivist Synthesis*. *International Organization*, 76(S1), 1–29. <https://doi.org/10.1017/S0020818321000397>

The Guardian. (2025, February 27). *FBI accuses North Korea of \$1.5bn crypto hack*. <https://www.theguardian.com/world/2025/feb/27/north-korea-bybit-crypto-exchange-hack-fbi>

The Star. (2024, December 18). *MOF: Low instances of using cryptocurrency in money laundering*. Retrieved from <https://www.thestar.com.my/business/business-news/2024/12/18/mof-low-instances-of-using-cryptocurrency-in-money-laundering>

The Times UK. (2024, October 15). *How Kim Jong Un's regime launders money via noodle bars*. <https://www.thetimes.co.uk/article/how-kim-jong-uns-regime-launders-money-via-noodle-bars-9vfvwnh88>

TRM Labs. (2024, February). *Illicit Crypto Ecosystem: Laundering Trends and Typologies*. Retrieved from <https://www.trmlabs.com/reports/illicit-crypto-ecosystem-2024>

U.S. Department of the Treasury. (2022). *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*. Retrieved from <https://home.treasury.gov/news/press-releases/jy0916>

U.S. Department of the Treasury. (2022, April 14). *Treasury Targets North Korean Lazarus Group Involved in Cryptocurrency Theft*. Retrieved from: <https://home.treasury.gov/news/press-releases/jy0706>

UN Panel of Experts. (2024). *Report on Democratic People's Republic of Korea Sanctions Implementation*. Retrieved from https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports

United Nations Security Council (UNSC) Panel of Experts. (2023). *Final report submitted pursuant to resolution 2627 (2022)*. Retrieved from: <https://www.undocs.org/Home/Mobile?FinalSymbol=S%2F2023%2F167&Language=E&DeviceType=Desktop>

Waltz, K. N. (1979). *Theory of international politics*. Addison-Wesley.

Wendt, A. (1999). *Social theory of international politics*. Cambridge University Press.

Wikipedia contributors. (2024). *Cryptocurrency in Iran*. Wikipedia. https://en.wikipedia.org/wiki/Cryptocurrency_in_Iran

Wikipedia contributors. (2024). *Economic activities of the Iranian Revolutionary Guard Corps*. Wikipedia. https://en.wikipedia.org/wiki/Economic_activities_of_the_Iranian_Revolutionary_Guard_Corps

Wired. (2023, October 19). *Citing Hamas, the US Wants to Officially Treat Crypto Anonymity Services as Suspected Money Launderers*. Retrieved from <https://www.wired.com/story/us-treasury-crypto-mixer-hamas>

Wright, D. (2023). North Korea's crypto crimes: Cyber-theft, laundering, and sanctions evasion. *International Journal of Law and Emerging Technologies*, 1(1), 25–38. <https://www.ijlet.org/2023-1-1-25>

Wright, T., & Moorthy, N. (2023). *Crypto, Coercion and the State: The North Korean Paradigm*. *International Affairs*, 99(1), 113–134. <https://doi.org/10.1093/ia/iac265>

Wronka, J. (2022). Cryptocurrencies and financial crime: A growing threat to sanctions enforcement. *Journal of Financial Crime*, 30(1), 95–110. <https://doi.org/10.1108/JFC-07-2021-0158>

Zarghami, A., Ghassemi, R., & Noori, M. (2023). *Cryptocurrency and Iran's Economic Diplomacy: Between Sanctions Evasion and Sovereign Digital Strategy*. *Global Policy*, 14(1), 121–134. <https://doi.org/10.1111/1758-5899.13123>

Zola, E., Gu, X., Hu, Y., & Ma, R. (2024). *Analyzing sanctioned entities on Ethereum*. arXiv. <https://arxiv.org/abs/2409.10031>