Social Sciences & Humanities Open 13 (2026) 102550

Contents lists available at ScienceDirect

Social Sciences & Humanities Open

journal homepage: www.sciencedirect.com/journal/social-sciences-and-humanities-open

Regular Article

Ramifications of cryptocurrency proliferation on national security

Karthik Iyer

Jindal School of International Affairs, O.P. Jindal Global University, Sonipat, Haryana, India

ARTICLE INFO

Keywords:
Cryptocurrencies
National security
Bitcoin
Ethereum
Stablecoins
Great power competition

ABSTRACT

Cryptocurrencies constitute a fast-evolving, disruptive technological development. Their proliferation and mainstreaming are undermining national security in several ways. By exploring emblematic cases, this paper examines how decentralised digital assets challenge sovereign functions, complicate law enforcement efforts, and give rise to security challenges. It explores different state-level responses to these developments by drawing on policy documents, reports, and guidance from multilateral regulatory authorities, alongside literature from finance, security studies, international relations, and technology governance. Strategic considerations spanning areas of illicit finance, sanctions evasion, great power rivalry, and state co-option by means of issuing Central Bank Digital Currencies and establishing cryptocurrency strategic reserves are delineated. A comprehensive mapping of the actual impact of cryptocurrencies across several strategic domains is carried out, synthesising insights from previously siloed technical, legal, and international relations literatures into an integrative national-security analytical lens. Specific recommendations are provided for policymakers and planners to navigate this fast-evolving threat landscape.

1. Introduction

The close link between economic security and national security has long been articulated, with recent scholarship emphasising *risk vectors* through which economic factors and national security intersect (Retter et al., 2020). A clear example of risk transmission was the global financial crisis from mid-2007 to early 2009, which shook confidence in the international financial system and eventually created fertile ground for cryptocurrencies to flourish (Roth, 2009).

What started as a protest by a small group of tech-savvy users sceptical of government-controlled systems soon evolved into a mainstream financial instrument, characterised by attributes such as greater accessibility and lower barriers to entry (Jaiswal & Chaudhari, 2023). This evolution also generated significant concerns for governments and policy planners, given the expanding avenues for criminal activity, terror financing, money laundering, tax evasion, cybercrime, and the circumvention of capital controls (Alfieri, 2022; Foley et al., 2019). Regulatory gaps at the international level enabled regulatory arbitrage and created vulnerabilities that malign actors could exploit. Ransomware attacks demanding Bitcoin, sanctioned regimes stealing or mining cryptocurrency to fund weapons programmes, and the broader erosion of sanctions regimes all point to mounting strategic stakes (Akartuna & Madelin, 2023; Chitsungo, 2024; Dimovski, 2024).

Rising great-power competition has spilled over into technology, finance, and trade, narrowing the space for multilateral cooperation (Wong, 2025). Domestically, when governments have attempted to act, these efforts have been complicated by the inherent design of cryptocurrencies–resistant to central control, borderless, and functioning without an underwriting authority (Ukwueze, 2021). Some states, such as China, have chosen to co-opt the technology and launch their own central bank digital currencies (CBDCs) (Caudevilla & Kim, 2023; Ferreira, 2020). Others, such as the United States and El Salvador have moved in the opposite direction—declaring Bitcoin legal tender or evaluating it as a strategic reserve.

The evolution and proliferation of cryptocurrencies have created opportunities as well as risks for governments. Scholars of international relations have pointed out that states derive their authority from their ability to supervise flows—whether financial, informational, or territorial—and that disruptions to this capacity can unsettle how states pursue security and economic stability (Keohane, 1984; Krasner, 1988; Strange, 1986). This is particularly relevant for countries of the Global South, many of which lack the resources to shape global crypto governance but will nonetheless bear the consequences of its trajectory.

This paper addresses the important question: What ramifications does the proliferation of cryptocurrencies have on national security? Its objective is to highlight emblematic cases, analyse the associated challenges, and offer recommendations for policymakers. These emblematic cases were chosen based on (i) governmental approaches to

E-mail address: kiyer@jgu.edu.in.

https://doi.org/10.1016/j.ssaho.2026.102550
Received 30 June 2025; Received in revised form 26 January 2026; Accepted 5 February 2026
Available online 10 February 2026

cryptocurrencies—including adoption, banning, and accumulation; (ii) national-security relevance, sanctions evasion, monetary sovereignty, illicit finance; (iii) availability of credible substantiating evidence from peer-reviewed journals, multilateral agency reports and reputable institutions; and (iv) geographic and developmental diversity among the countries selected. A central argument developed in this paper is that the decentralised design of cryptocurrencies directly challenges the financial and security functions that modern states rely upon, and that this shift necessitates regulatory adaptation domestically and internationally.

In addition to peer-reviewed scholarship, the analysis draws on publicly available policy documents, official guidance, and reports issued by multilateral organisations and national authorities. These sources were identified through targeted, issue-specific searches of institutional repositories and official websites, including those of the United Nations Office on Drugs and Crime (UNODC), the Financial Action Task Force (FATF), the International Monetary Fund (IMF), the World Bank, and the European Union Agency for Law Enforcement Cooperation (Europol), as well as national treasury and law-enforcement bodies, with deliberate reliance on multilateral organisations to mitigate jurisdiction-specific or national reporting bias and to ensure cross-regional comparability in security-relevant assessments.

Building on insights from security studies and international political economy, this article conceptualises cryptocurrencies as a challenge to core state capacities: the ability to monitor value flows, enforce rules, and maintain authority over monetary and security architectures. Rather than offering a technical treatment of protocols or a narrow legal analysis, it adopts an exploratory, integrative approach that connects technological evolution, market practices, and institutional responses across financial, security, regulatory, and technological domains of national security. While there is a growing body of work on blockchain design, price volatility, monetary policy, and regulatory classification, the implications of cryptocurrencies for national security remain fragmented across literatures on crime, terrorism finance, sanctions evasion, cyber risk, and strategic competition. By mapping these strands together and situating them in a common analytical frame, the paper addresses this gap and clarifies how cryptocurrencies intersect with—and in some cases reconfigure—established tools of state power and security governance.

The paper is structured as follows: Section 2 outlines the evolutionary arc of cryptocurrencies. Section 3 examines the national security impacts in detail across different dimensions. Section 4 offers policy recommendations, Section 5 outlines limitations and future research directions, and Section 6 concludes the paper. While the paper draws on selected technical features where relevant, the analysis is grounded primarily in international-relations and national-security frameworks rather than computer-science perspectives.

2. Evolutionary arc of cryptocurrencies

Notwithstanding sporadic earlier attempts at digital payments, the era of cryptocurrencies in their present form began when the pseudonymous Satoshi Nakamoto released the 2008 white paper *Bitcoin: A Peer-to-Peer Electronic Cash System* (Nakamoto, 2008), proposing a system for transferring value directly between parties without intermediary institutions. The key innovation lay in the introduction of blockchain technology—a distributed, cryptographically secured ledger—designed to provide trust and transparency within a decentralised network. This was followed on January 3, 2009, by the mining of the Genesis Block.

By the early 2010s, altcoins began to appear, seeking to refine Bitcoin's design or to target new applications. Namecoin and Litecoin experimented with parameters such as faster confirmation times and alternative hashing algorithms (Gandal & Halaburda, 2015). A major shift occurred with the 2015 launch of Ethereum, which extended blockchain functionality by incorporating smart contracts—self-executing code deployed on-chain—thereby allowing decentralised applications and enabling token issuance (Buterin, 2013). This moved the narrative beyond Bitcoin as merely an alternative form of money towards blockchain as a programmable infrastructure. The 2017 ICO boom, largely built on Ethereum, demonstrated both the promise and excesses of this innovation, illustrating that blockchain technology could support diverse assets and applications (Momtaz, 2020).

The limitations of volatile cryptocurrencies for everyday payments prompted experiments with 'stablecoins'—tokens engineered to maintain stable value, often pegged 1:1 to the US dollar. Tether, originally branded Realcoin, was the first to achieve major significance, offering a dollar-denominated safe harbour within the crypto ecosystem and rapidly becoming central to trading, liquidity management, and cross-exchange arbitrage (Griffin & Shams, 2020; Lyons & Viswanath-Natraj, 2023). Stablecoins reduced on-ramp frictions and later served as a foundational collateral layer for decentralised finance (DeFi) protocols, although doubts about reserve transparency and counterparty risk drew regulatory scrutiny (Aramonte et al., 2021). The relevance of these shifts lies less in their technical design and more in the new policy dilemmas they created for regulators, central banks and security agencies, which were suddenly confronted with financial activity taking place outside established institutional channels.

From 2020 onward, DeFi protocols, largely on Ethereum, created decentralised alternatives to traditional financial services; non-fungible tokens (NFTs) gained mainstream attention; and new blockchains such as Solana attracted users by offering higher throughput and lower fees. However, the sector's growing maturity also exposed systemic risks. In May 2022, the collapse of TerraUSD wiped out tens of billions in value, and later that year, the FTX exchange imploded amid allegations of fraud, triggering a crisis of confidence and prompting governments and central banks to intensify efforts to craft regulatory frameworks and, in some cases, to develop their own digital currencies (Vidal-Tomás et al., 2023).

Driven by motivations such as efficiency, sovereignty, and technological modernisation, central banks increasingly explored CBDCs. Early pilots included Uruguay's e-Peso, Sweden's e-krona, and the Bahamas' Sand Dollar, which achieved national rollout in 2020 (Central Bank of The Bahamas, 2020; Sarmiento, 2022; Sveriges Riksbank, 2018). The most notable example was China's e-CNY, which was piloted in Shenzhen in 2020 following years of research, and had already reached more than 225 million wallets and processed around US$2 trillion in cumulative transactions by September 2025, with features such as controllable anonymity and smart-contract-style programmability (Knoerich, 2021; People's Bank of China, 2025). Notably, CBDCs are not mere regulatory responses to private cryptocurrencies, but represent a parallel evolutionary branch of digital money with the potential to transform retail and wholesale payment systems. The following figure provides a concise timeline of these developments (see Fig. 1).

Contemporary scholarship increasingly situates cryptocurrencies within national-security discourse. Decentralised and pseudonymous value networks challenge state monopolies over money issuance, complicate surveillance architectures underpinning counterterrorism and sanctions regimes, and blunt the effectiveness of coercive economic tools (Alfieri, 2022; Financial Action Task Force [FATF], 2019; US Department of the Treasury, 2023). As a result, the evolution of digital money now intersects with broader concerns of power projection, geopolitical rivalry, and the future architecture of the international order. These themes form the foundation for the national-security analysis that follows.

3. Analysis of impact on national security

The technical aspects of cryptocurrencies that make them versatile are important. However, this paper deliberately chooses to view cryptocurrencies not through the prism of their technical architecture but through the institutional and geopolitical pressures they introduce. In

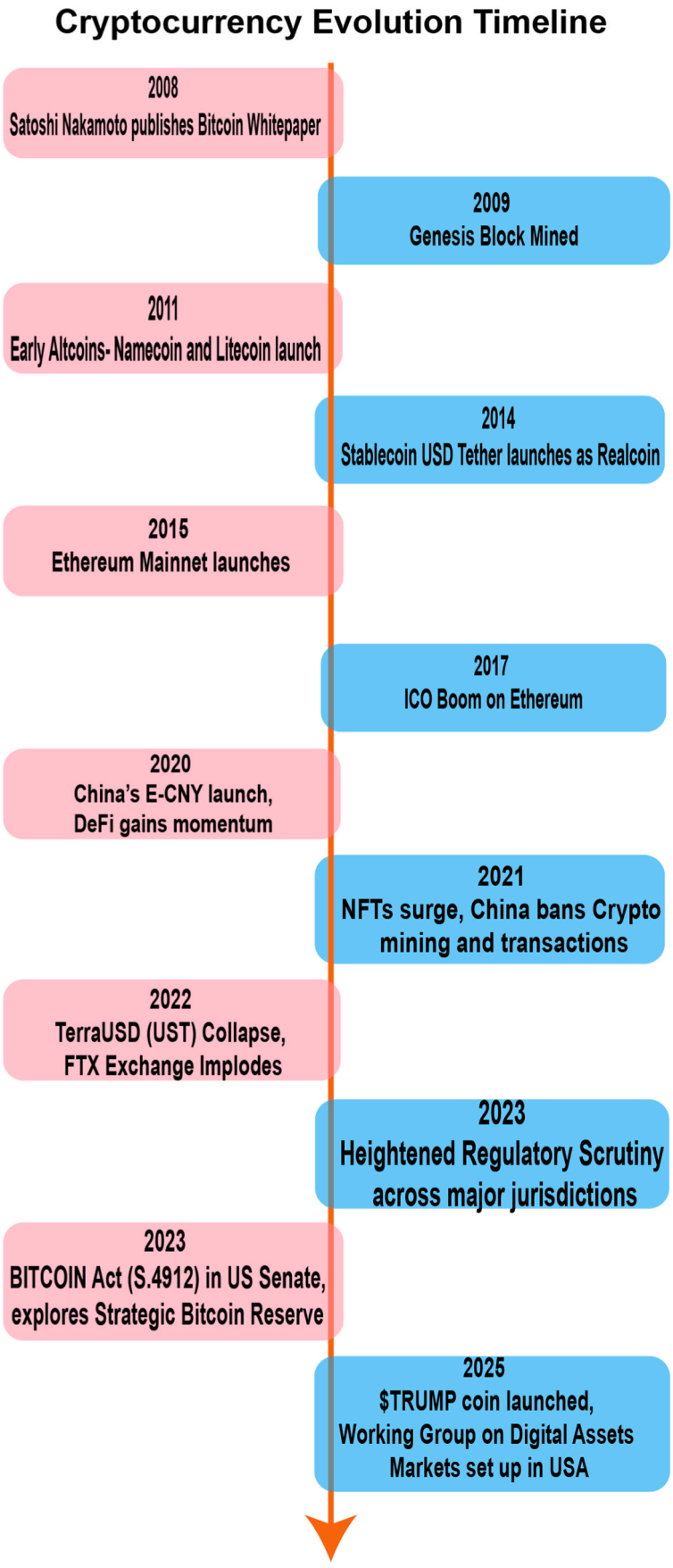

Fig. 1. Cryptocurrency evolution timeline.

national-security terms, cryptocurrencies challenge what scholars describe as the state's core functions: controlling value flows, enforcing rules, and maintaining internal and external security. When financial activity migrates to decentralised systems that lie partly outside state reach, the instruments through which states exercise authority—surveillance, regulation, taxation, and deterrence—all come under strain. Scholars contend that core state functions—surveillance, extraction, and enforcement—are not incidental features but the foundation upon which national security rests (Buzan, 1991; Levi, 1988; Tilly, 1990). When new technologies create spaces that lie partially outside these mechanisms, their effects are felt across multiple security domains. The following sections examine how these pressures manifest across specific areas of national security.

3.1. Financial stability

Cryptocurrencies transcend national, geographic, and legal boundaries. Deutsche Bank Research (2019) has noted that the future of the traditional financial system will be significantly affected by decentralised digital currencies. Poskart (2022) emphasises that cryptocurrencies have enabled the creation of a private, denationalised, independent and largely uncontrollable global value-transfer system as an alternative to the current monetary system, becoming a competitor not only to fiat currencies, but also to incumbent transaction networks. Manjula et al. (2022) argue that cryptocurrencies could change the way internet-connected markets interact by removing impediments posed by exchange rates and national currencies and by revolutionising digital trade markets by creating a free-flowing trading system without fees.

Pacelli et al. (2025) demonstrate a notable spillover between cryptocurrency and traditional financial markets, with risk factors interacting across borders. They conclude that the sensitivity of the crypto market to traditional markets reflects increasing integration. Saleem et al. (2024) similarly find that indicators such as the Consumer Price Index and the Dow Jones Industrial Average show a strong positive correlation with cryptocurrency market capitalisation, leading them to recommend vigilance as integration deepens. Donoiu and Iacob (2023) likewise regard the crypto market as a potential amplifier of risks originating in traditional finance, thereby posing risks to financial stability. Joebges et al. (2025) point out that the partial money-like nature of cryptocurrencies promotes "toxicity" in the financial system, with instability arising from the introduction of banking-type functions within an unregulated DeFi sector that can affect the real economy. Highlighting their unbacked and volatile nature, World Bank research notes that cryptocurrencies may threaten financial and fiscal stability (Feyen et al., 2024). Shahzad et al. (2024) warn of the possibility of the crypto market becoming a "Wild West" in the absence of clear regulatory guidelines, with attendant risks for users.

3.2. Digital crime

Cryptocurrencies evolved partly in response to perceived flaws in the traditional financial system and, by design, did not incorporate many features intrinsic to traditional finance, such as robust customer identity verification. This allowed a degree of anonymity for users, even though every transaction is recorded on a public ledger. Malefactors have exploited this anonymity for illicit trade and smuggling, money laundering, tax evasion, and more serious offences such as terrorist financing. Chitsungo (2024) notes that characteristics such as lack of oversight, anonymity, and ease of transfer that make cryptocurrencies appealing to some users also make them well suited to criminal activities. Leuprecht et al. (2023) point out the tendency of malicious actors to exploit under-regulated technological innovations.

Dimovski (2024) identifies five factors that attract criminals to cryptocurrencies: (i) anonymity, (ii) lack of intermediaries, (iii) ease and speed of transactions, (iv) ease of storage and transfer, and (v) their transnational nature, which blunts the threat of seizure by national authorities. Foley et al. (2019) estimate that around 25% of Bitcoin users are involved in illegal activity, with approximately US$76 billion in illegal activity per year, amounting to about 46% of all Bitcoin transactions. The UNODC Global Cybercrime Assessment (2023) notes that virtual assets have become a standard tool in transnational fraud and ransomware ecosystems, particularly in Southeast Asia (United Nations Office on Drugs and Crime [UNODC], 2023a). Europol's IOCTA 2023 similarly highlights that cryptocurrencies now routinely feature in investigations across organised crime, with stablecoins increasingly preferred for laundering (Europol, 2023). Blockchain analysis platforms document a steady rise in the value of illicit funds routed through mixers, DeFi exploits, and ransomware groups, underscoring that misuse has diversified even as its share relative to overall transaction volume has declined (Chainalysis, 2024). Taken together, these more recent findings confirm the broad direction of Foley et al.'s concerns, while offering a firmer empirical basis for understanding how crypto-related crime manifests today.

By blending the anonymity of cash with the ease of digitisation and cross-border reach, cryptocurrencies have the potential to change how black markets operate. The technical features of these assets are relevant only to the extent that they alter the institutional landscape within which law-enforcement and regulatory authorities operate. In practical terms, the difficulty is not the cryptography itself but the way in which decentralisation weakens established mechanisms of surveillance, compliance, and cross-border cooperation. These developments expose the limits of existing governance arrangements, which were built around identifiable intermediaries and jurisdictional control—two features that decentralised systems deliberately minimise. Cumming et al. (2019) highlight several concerns that necessitate urgent action including.

a. **Non-existent assets:** unsecuritised assets that are not registered with any regulatory authority.
b. **Fraudulent funds and advisers:** crypto funds and advisers luring investors with unsubstantiated promises of high returns, often involving multi-level participation.
c. **Market manipulation:** minimal regulation, digital-only assets and AI-enabled trading bots create ripe conditions for manipulation.
d. **Theft of computing power:** "cryptojacking", in which devices are infected with malware to mine cryptocurrencies without consent. Agencies including European Union Agency for Cybersecurity (ENISA) and INTERPOL have all emphasised a clear upward trend in cryptojacking, indicating that cryptojacking now constitutes a persistent and evolving security challenge (Cybersecurity and Infrastructure Security Agency, 2023; European Union Agency for Cybersecurity, 2023; INTERPOL, 2022).
e. **Sanctions evasion:** sanctions—used by multilateral organisations and governments, notably the United States, to penalise foreign entities by exploiting dominance over the international financial architecture and SWIFT—can be undermined when cryptocurrencies allow transactions outside these systems (Galant M., 2025).

Arnold (2019) notes that cryptocurrencies can be used to bypass both national and international financial systems, with important ramifications for governments relying on sanctions to deter unwanted behaviour. Gutmann et al. (2023) point out that the merits of sanctions as a deterrent require re-examination considering potential crypto-enabled evasion. Zola et al. (2024) find that cryptocurrencies enable entities to evade sanctions and continue operations, with freezing or blocking digital assets proving difficult and, in the case of Bitcoin, often unfeasible.

Existing International Relations literature on economic statecraft positions sanctions as tools of coercive diplomacy whose effectiveness depends on the degree to which states can restrict financial channels and enforce compliance (Baldwin, 1985; Drezner, 2011). When alternative pathways for settlement begin to emerge, even at the margins, the strategic value of sanctions becomes harder to sustain. Sanctions depend

on a state's ability to control the channels through which international payments are cleared. As cryptocurrencies create parallel rails for settlement, even if at the margins, sanctioned actors gain room to manoeuvre. The issue is not that digital assets can fully replace established global networks, but that they can blunt the immediacy and bite of coercive measures. Over time, even a partial weakening of sanctions efficacy alters the strategic calculus for both imposing and targeted states. This is consistent with established findings in the sanctions literature, which show that the credibility and impact of sanctions depend not only on political intent but on the ability to restrict alternative channels of settlement (Drezner, 2015; Pape, 1997). Parallel crypto-based pathways, even if marginal, complicate this calculus.

f. **Tax evasion:** IMF estimates that US$500-600 billion is lost due to corporate tax avoidance, with Fortune 500 companies reportedly parking trillions overseas (Shaxson, 2019). Developing countries are particularly hard hit. The United Nations (2024) has proposed a new tax accord to curb avoidance by high-net-worth individuals and ensure multinationals are taxed fairly. Nawaz et al. (2023) observe that cryptocurrencies have been implicated in tax-evasion accusations, complicating oversight. Marinova et al. (2024) note that lack of jurisdiction, decentralisation and anonymity enable tax evasion, imposing high costs on states. Specific concerns include firms accepting part payment in cryptocurrencies, enabling under-reporting. de Carvalho et al. (2024) find that stablecoin transaction intensity is a potential indicator of tax evasion among younger and mid-sized service firms.

g. **Exchange hacks:** although cryptocurrencies are decentralised, exchanges concentrate assets and are often unregulated and uninsured, making them frequent targets. Major hacks have affected platforms such as Mt. Gox, Wormhole, DMM Bitcoin, Mixin, Euler Finance, Bitmart, Nomad Bridge, Beanstalk, Wintermute and Multichain, resulting in cumulative losses of billions of dollars (Makarov & Tschiatschek, 2025). The following figures help to illustrate the scale of these developments (see Figs. 2 and 3):

h. **Ransomware attacks:** while extortion is not new, demanding payment in cryptocurrencies that are instantly transferable, non-reversible and difficult to trace—especially when mixers are used—poses a new challenge. The risk escalates when state-backed actors are involved. A US Senate Homeland Security Committee staff report claimed that in 2021 around 74% of global ransomware revenue was transferred to Russian entities, highlighting the geopolitical dimensions involved (US Senate Committee on Homeland Security & Governmental Affairs, 2022).

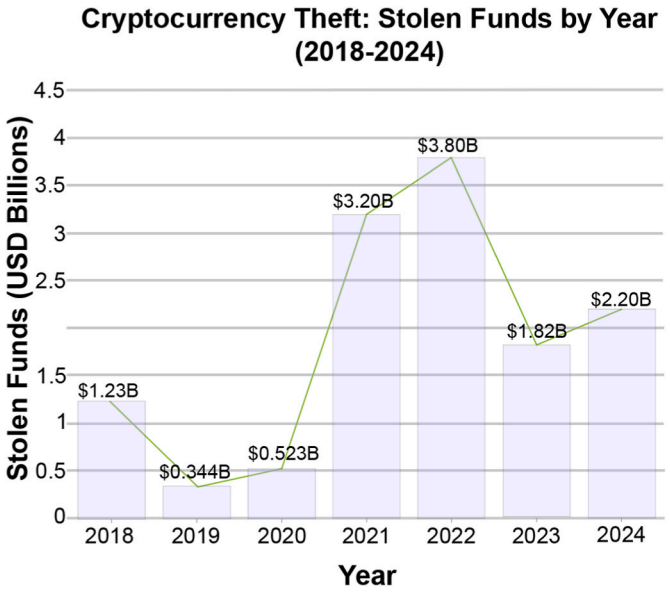

Fig. 2. Cumulative amount of funds stolen by year (2018-24).
Source: Chainalysis Data

3.2.1. *Illicit finance*

Monitoring authorities now offer a clearer indication of the intersection between cryptocurrencies and illicit finance. UNODC documents how transnational organised crime groups have increasingly converged cyber fraud, trafficking, and money laundering through cryptocurrencies, with notable rises in mixer usage to obscure illicit flows (UNODC, 2024). The Egmont Group of Financial Intelligence Units notes that crypto-related suspicious transaction reports more than doubled between 2019 and 2022 (Egmont Group of Financial Intelligence Units, 2023). Europol has also documented similar cross-border laundering structures, with its investigations showing how criminal groups recruit individuals in multiple countries to move illicit proceeds through a chain of wallets, exchanges, and cash-out points (Tolbaru, 2023, pp. 152–156).

These cases underline how virtual assets are being incorporated into older laundering techniques, but with far greater speed and geographic reach. The UK's National Crime Agency, under *Operation Destabilise*, disrupted a multi-billion-dollar laundering network that swapped crypto for cash across the UK, the Middle East, Russia, and South America (National Crime Agency, 2024; United Nations Office on Drugs and Crime, 2023a) regional assessments note that large fraud compounds operating across Southeast Asia have begun routing victim proceeds through layered crypto wallet structures, involving perpetrators and victims of multiple nationalities (UNODC, 2023). Thus, there is clear evidence that virtual assets are no longer peripheral to illicit finance but now constitute a material and evolving component of cross-border financial crime risk.

3.2.2. *Privacy-oriented coins*

Law enforcement agencies now face significant challenges stemming from the cryptographic methods used by privacy-oriented coins, which contain features that weaken attribution, complicate jurisdictional cooperation, and shrink the informational space on which state authority depends. For example, Monero uses a technique called *ring signatures,* which mix a user's key with a group of decoy keys. This helps hide the identity of the real signer of a transaction, making them untraceable. Monero also utilises stealth addresses—one-time-use destination addresses that break the link between receiver and sender (Noether & Mackenzie, 2016). Zcash uses even more advanced technology with zero-knowledge proofs (zk-SNARKs), which make it possible to validate transactions without revealing the address or amount in a transaction (Hopwood et al., 2018). These tools are intended to give users strong guarantees of privacy. However, they also have the unintended effect of erasing the audit trails that regulators and enforcement agencies use to trace illicit finance. In simpler terms, once funds move from transparent blockchains to these privacy-oriented coins, attribution becomes difficult, the deterrent value of surveillance weakens, and cross-border investigations become more challenging.

The technical proposals differ in design, but they reflect a broader policy question rather than a purely cryptographic one: can privacy and regulatory visibility be reconciled in ways that preserve state capacity? Several recent studies have tried to answer this question. Elfadul et al. (2024a) combine ring signatures, stealth addresses and a Merkle Tree to ensure government supervision and enforcement of regulations in their Privacy and Compliance in Regulated Anonymous Payment System Based on Blockchain (PCRAP). Another attempt was made by Elfadul et al. (2024b) to use RSA accumulators in conjunction with Schnorr protocol to enable compliance with government regulations while maintaining privacy in their Secure and Compliant Cryptocurrency Transactions in a Decentralised Anonymous Regulated System (SCCT DARS). Jia et al. (2024) describe a multi-level regulatory model that

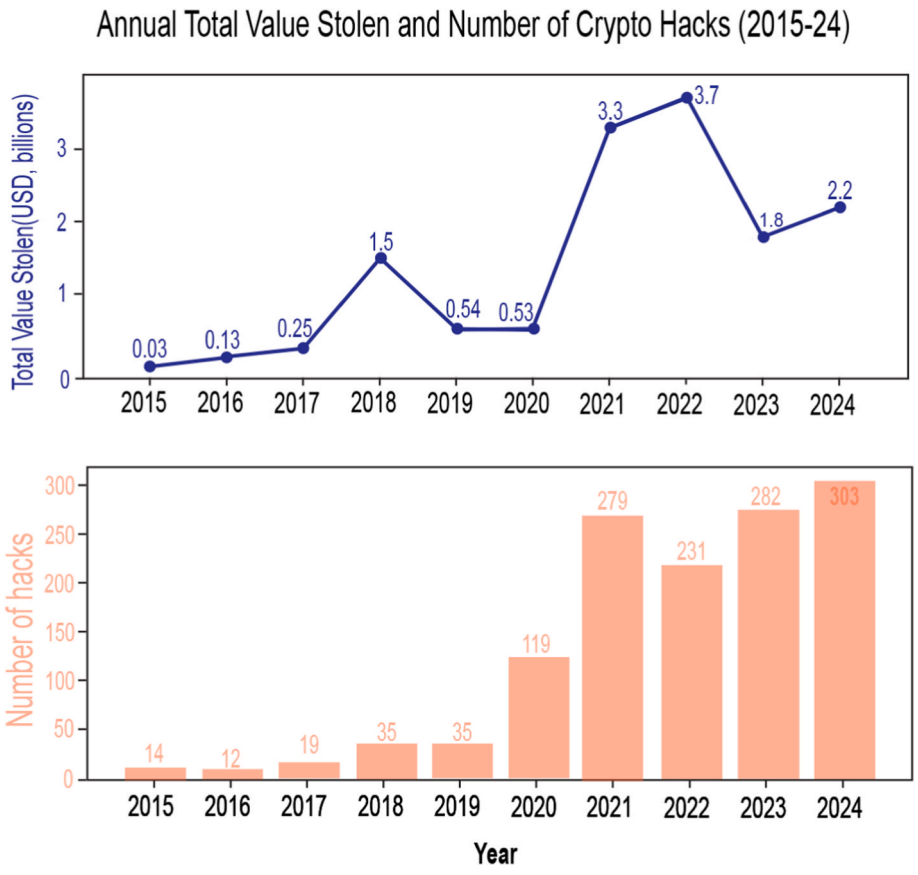

Fig. 3. Total value stolen in Crypto Hacks and Number of Hacks.
Source: Chainalysis Data

relies on zk-SNARKs and attribute-based encryption (ABE) to keep some transaction details concealed but still allows regulators to have selective oversight. Chaudhary and Ivey-Law (2023) attempt to leverage a Selective De-Anonymization (SeDE) framework that lets investigators examine inter-connected transactions that are indicative of illegal activity, while leaving privacy features for other transactions intact. Zhaolu et al. (2024) discuss splitting oversight across different actors under their decentralised anonymous payment scheme with collaborative regulation (DAPCR) so that no single agency holds complete control to abuse privacy. Xiong et al. (2025) propose an Attribute Based Access Control (ABAC) Framework called 'RegKYC' that attempts to balance privacy with external AML and KYC compliance requirements. Xue et al. (2023) introduce a Decentralised Anonymous Payment (DAP) scheme that introduces regulators who define policies for anonymous payments, which are subsequently enforced by means of commitments and non-interactive zero-knowledge proofs. Technological details aside, the common thread across these efforts is that privacy does not have to imply a regulatory vacuum; much depends on how the system is designed, and who is allowed to see what, and under what conditions.

These developments raise uncomfortable questions about state capacity in the digital age. A significant part of modern statecraft rests on the ability to monitor value flows, enforce tax obligations, protect the integrity of financial institutions and, when required, trace illicit transfers. Cryptocurrencies introduce blind spots in each of these domains. Even where transactions are visible on-chain, attribution remains difficult, and the rapid movement of funds across exchanges, mixers and decentralised platforms makes enforcement reactive rather than preventative. For countries with limited institutional capacity, the problem is even more acute. Thus, cryptocurrencies now shape the operational space in which law-enforcement agencies function. Their role, however, is not confined to criminal activity alone, and the implications become even sharper when these systems are used by designated terrorist organisations, as the next section shows.

3.3. Terror financing

Terrorist organisations are adept at leveraging cryptocurrencies for terror financing, as the unfortunate October 2023 attack on Israel and the March 2024 attack in Moscow indicate (Seibt, 2023; Ukrainska Pravda, 2024). Anggriawan and Susila (2024) highlight that decentralisation, anonymity, and the absence of centralised oversight over wallet ownership enable a nexus between cryptocurrency and terrorism financing. Akcinaroglu and Shi (2023) argue that cryptocurrencies provide terrorist organisations with new avenues for covert fundraising and subtly enhance their operational dynamics. Ahmad et al. (2024) note that terrorist organisations are increasingly preferring cryptocurrencies to finance operations, underscoring the need to disrupt this nexus. Researchers at The Soufan Center find that groups such as Islamic State Khorasan (ISK), Palestinian Islamic Jihad (PIJ), Hamas, and Hezbollah are increasingly using cryptocurrencies to evade counter-terrorism financing efforts (The Soufan Center, 2024). They observe a shift away from Bitcoin towards privacy coins such as Monero, posing additional challenges for law-enforcement authorities.

Recent counter-terrorism assessments highlight these challenges. The United Nations Counter-Terrorism Committee Executive Directorate has been reported as estimating that one in five recent terror incidents have some cryptocurrency link, with more than forty designated organisations having attempted to use digital assets in some capacity (Bloomberg News, 2022; United Nations Security Council Counter-Terrorism Committee Executive Directorate, 2024) FATF's 2025 update similarly notes that close to 69% of jurisdictions continue to face gaps in core terrorist-financing enforcement functions. This

places all countries, especially those already affected by terrorism, on high alert (FATF, 2025). FATF emphasises that without proper regulation, cryptocurrencies risk becoming a safe haven for terrorists and criminals (Financial Action Task Force, n.d). It has urged countries to understand the risks and (i) implement its binding standards, (ii) supervise the crypto sector as rigorously as other financial institutions, and (iii) license virtual-asset service providers.

The intersection of cryptocurrency and terror is not just a law-enforcement problem but a strain on the wider counter-terrorism governance architecture. Existing regimes rely on shared reporting systems, cooperative surveillance, and harmonised enforcement—precisely the areas where decentralised assets create friction. However, cryptocurrencies are beginning to have an impact at a much deeper strategic level, as the next section indicates.

3.4. Strategic and geopolitical implications

International relations scholars have long held that systemic behaviour can shift when the underlying structure of international finance shifts. Whether framed through Waltz's structural lens or through analyses of monetary power such as Helleiner's, the central point is that financial architectures shape how states exercise influence beyond their borders (Helleiner, 1994; Waltz, 1979). Technologies that weaken financial control or dilute monetary sovereignty can impact how states position themselves in the international order, how they respond to external pressure, and how they exercise influence. Digital assets contribute to a gradual reconfiguration of security architectures, where informational control, payment infrastructure, and monetary tools increasingly function as instruments of state power and diplomatic leverage.

Cryptocurrencies have been linked with state-driven espionage-related activity. Olalekan (2024) notes that the ability to move funds outside traditional banking systems adds a new dimension to counter-intelligence challenges, enabling state actors to move resources with minimal infrastructure and lower risk of immediate detection. The Lazarus Group, reportedly tied to North Korean military intelligence, has specialised in high-profile crypto hacks, allegedly helping to fund weapons programmes and sanctions evasion (Hacken, 2024). The following table gives a snapshot of their activity (see Table 1).

Chainalysis (2025) estimates that North Korean hackers stole about US$660.5 million in 2023 across 20 incidents, with activity intensifying to around US$1.34 billion across 47 incidents in 2024—an increase of over 100 %. These estimates have also shown up in the work of different security agencies. A joint advisory by the National Security Agency and the Cybersecurity and Infrastructure Security Agency described how North Korean units move stolen cryptocurrency through mixers and informal brokers (Cybersecurity and Infrastructure Security Agency, National Security Agency, Federal Bureau of Investigation and Defense Cyber Crime Center, 2024). The same modus operandi was flagged by the Center for Strategic and International Studies (Bae, 2025), which emphasised the use of virtual assets by DPRK for evading sanctions. Europol's analysis notes that virtual assets now appear regularly in difficult, multi-country cybercrime cases, especially those involving state-linked actors or groups operating with some degree of state tolerance (Europol, 2024). This indicates that cryptocurrencies are now part of the wider security landscape, rather than being a mere technical challenge for countries. The following figure brings out the intensity of hacking activity attributed to DPRK (see Fig. 4).

Table 1
Biggest crypto currency hacks by lazarus group.

S. No.	Attack Name/ Incident	Losses (Estimated)	Techniques Used
1.	Bithumb Exchange Hack	$7 million	Phishing, Social Engineering, Malware
2.	Coincheck Hack	$534 million	Spear Phishing, Exploitation of Poor Security Practices
3.	Youbit Exchange Hack	Unknown	Spear Phishing, Malware, Insider Compromise
4.	Upbit Exchange Hack	$49 million	Phishing, Unauthorized Access, API Exploitation
5.	KuCoin Exchange Hack	$275 million	Social Engineering, Unauthorized Access, Exploitation of Hot Wallets
6.	Eterbase Hack	$5.4 million	Phishing, Credential Stuffing, Exploitation of Hot Wallets
7.	Liquid Exchange Hack	$97 million	Phishing, Credential Theft, Social Engineering
8.	Ronin Network Hack	$600 million	Exploitation of Validator Nodes, Social Engineering
9.	Harmony Bridge Hack	$100 million	Exploitation of Multisig Wallet Vulnerabilities, Social Engineering
10.	Horizon Bridge Hack	$100 million	Exploitation of Smart Contract Vulnerabilities, Phishing
11.	WazirX Incident	$235 million	Phishing, Social Engineering, API Exploitation

Data Source: Hacken. io

Concerns regarding sanctions evasion have already been discussed previously. Crespo (2020) reminds us that traditional currency warfare is now augmented by cyber capabilities that enable states to target the increasingly digital architecture of currency and finance. As countries move towards CBDCs and maintain crypto-asset stockpiles, responding to hacks or offensive cyber actions—particularly from non-state actors—acquires greater strategic salience. The growing integration of blockchain technologies with transport, communications, and energy grids introduces fresh vulnerabilities, with cyber-attacks having the potential for cascading failures (Bangui & Buhnova, 2022).

Strategic implications now extend into the broader geopolitical landscape. Countries are attempting to leverage cryptocurrencies to challenge the existing international architecture anchored by the US dollar and the petrodollar system. For instance, amid hyperinflation and domestic economic challenges, the Venezuelan government announced the introduction of a new cryptocurrency called the *Petro*. This was to be backed by Venezuelan oil resources, with one Petro equalling one barrel of oil (Brown et al., 2022; Valero, 2018). Although the Petro struggled to gain traction, Akyildirim et al. (2020) note that the speed with which a sanctioned, crisis-ridden state attempted a sovereign-backed crypto-currency raised concerns about how such actions might reshape geopolitical financial relationships.

Iran offers another compelling example. According to data from the Cambridge Centre for Alternative Finance, Iran's share of the global Bitcoin hashrate reached around 6.9% in June 2021, before registering a sharp decline in subsequent months as regulatory crackdowns and electricity-supply interventions took effect (Cambridge Centre for Alternative Finance, 2021). Although Iran temporarily banned mining in

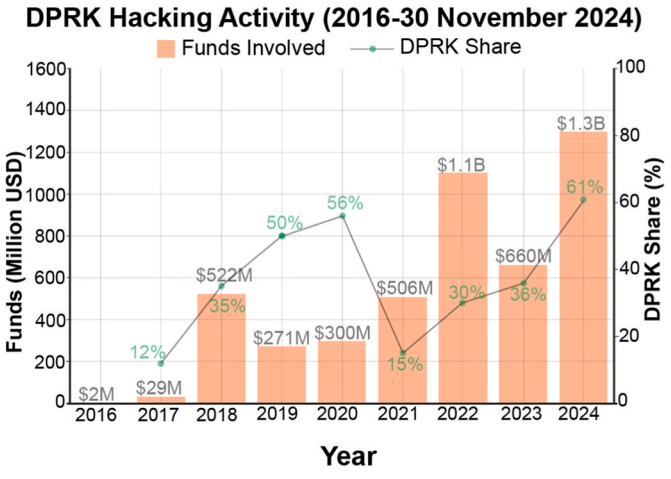

Fig. 4. Dprk hacking activity (**2016- Nov 2024**).
Source: Chainalysis Data

2021 due to power strain, it soon placed its first official import order of US$10 million using cryptocurrency in 2022 (BBC News, 2021; Reuters, 2022). Reports indicate that Iran has pursued crypto cooperation with Russia and other countries, signalling efforts to bypass sanctions (Lob, 2022). Such developments suggest that alternative crypto-denominated payment channels may weaken US dominance over global financial flows, as also noted by scholars such as Fantacci and Gobbi (2021), who warn that widespread use of privately created or algorithmic digital assets could erode the dollar's international role and fragment the monetary system.

While the preceding discussion demonstrates the use of crypto-currencies by state-linked actors, the same structural vulnerabilities manifest at the societal level under different institutional conditions. Where state capacity is eroded not by external sanctions but by domestic macroeconomic instability, currency controls, or financial exclusion, similar incentives drive civilian actors towards decentralised digital assets. In this sense, citizen-driven remittance and hedging behaviours observed in some developing countries represent a parallel response to institutional stress within the global monetary system.

For instance, reporting by Chainalysis (2024) indicates that when the naira witnessed significant fluctuations in pricing in 2023-2024, many Nigerians diversified into USDT stablecoin on peer-to-peer networks. Specifically, this phenomenon was observed coinciding with periods of high volatility in Naira's price. A similar trend was recorded in Argentina, where inflation and strict controls on the access to foreign currency led households to shift small savings and day-to-day payments to dollar-denominated stablecoins instead. These examples may point to a behavioural tendency among citizens in developing countries to explore cryptocurrency systems outside the purview of the traditional financial architecture when confronted with uncertainty or volatility, undermining governments' ability to enforce foreign-currency limits and capital controls.

Remittance flows are vital for developing countries. World Bank estimates that 184 million migrants sent remittances totalling US$656 billion in 2023 (World Bank, 2024). If this activity shifts to crypto-currency channels, receiving countries will be denied valuable foreign currency and associated tax revenues. El Salvador's experience, where its diaspora used the Chivo wallet to remit more than US$52 million while avoiding fees, is illustrative (Jenkinson, 2022).

These incidents are a timely reminder to policymakers that the emergence of privately issued digital assets can shrink the space for monetary policy actions, especially when grappling with difficult

Table 2
– Comparative national approaches to cryptocurrency.

Country	Domestic Context	Adoption Behaviour	Motivation/Drivers	Regulatory Stance	Implications for Monetary Sovereignty	Geopolitical Implications
Venezuela	Hyperinflation; USD sanctions	Launched Petro (2018); limited usage	Create sanction-proof payment; project autonomy	Highly centralised sovereign crypto	Attempt at re-asserting monetary sovereignty; limited success	Showed possible sovereign use of crypto for sanctions evasion
Iran	Longstanding sanctions; inexpensive power available	Mined ~6.9% of global BTC at peak (2021); Explored crypto-based trade	Monetise energy; find alternative to dollar channels	Fragmented oversight; mining stops/resumes	Weakens Iranian reliance on SWIFT and USD channels	Sanctions Evasion; De-dollarisation
China	Capital controls; proven digital capability	Expansive e-CNY rollout; prohibition on domestic mining and use of crypto	Control unauthorized transactions; internationalise RMB	Banned crypto trading/mining; CBDC pilot	Strong assertion monetary sovereignty; e-CNY aids RMB internationalisation	Framed as digital financial sovereignty; strong push to De-dollarisation
El Salvador	High remittance dependence; dollarised economy	Bitcoin made legal tender; Chivo wallet introduced; geothermal mining explored	Lower remittance costs; attract investment	BTC coexists with USD; minimal CGT	Creates parallel monetary rails; Co-option of cryptocurrency in governance framework	Positions itself as crypto-first nation; defies warnings by multilateral regulatory body on risks
DPRK	Longstanding sanctions; proven cyber capabilities	Reported involvement of entities in Hacks and laundering	Diversion towards weapons programme; evade sanctions	No framework; active cyber exploitation	Enables off-ledger funding which cannot be supervised by external actors	Undermines AML and sanctions frameworks. Crypto firms and customers in other countries at risk of theft/hacks
Bhutan	State-led modernisation; abundant hydro power	Piloting CBDC; Mining Bitcoin, has ~13,000 BTC sovereign holdings	Economic Diversification and Revenue; Utilise surplus power	CBDC pilot w/ Ripple; state BTC holdings	Bitcoin reserves diversify assets and increase resilience	Relatively opaque sovereign BTC accumulation
Kazakhstan	Stable and inexpensive Energy available; re-location post-China mining ban	Crypto mining hub; CBDC pilot	Monetise energy; formalise sector	Licensing regime; sell via local exchanges	Balances innovation with control	State-regulated crypto hub model
Uruguay	Fintech-oriented approach; financial consumer protection	Early e-Peso pilot (2017); formal regulation already in place since 2024	Test retail CBDC; formalise crypto; AML compliance; alignment with international standards.	Legal recognition; central bank oversight	Legal clarity; tax revenue from crypto; insights from pilot	Positioned as regulatory leader in Latin America.
Nigeria	High crypto use; financial exclusion	eNaira (2021); past banking ban on Crypto; underground adoption	Financial inclusion; currency stability	CBDC supported; regulation implemented in 2025 treats digital assets as securities	Limited eNaira uptake; underground crypto persists	Illustrates control–adoption trade-off
Russia	Sanctions; post-2022 isolation	Digital Ruble pilot; restricted crypto use domestically	Sanctions resilience; payment independence	Legal asset status; banned for domestic payment; CBDC trial	Payment channel diversification; re	CBDC used in bilateral trade, actively promotes de-dollarisation
The Bahamas	Island geography; access gaps	Sand Dollar (2020); crypto-friendly DARE Act	Boost inclusion; modernise payments	Mandated CBDC support; updated regulation (DARE 2024)	Low adoption; strong compliance	Early example of a live CBDC in place

Source: Authors Compilation

economic conditions. Governments have responded to these developments using myriad approaches-from passing legislation attempting to regulate digital assets, to co-opting the technology to roll out their own CBDCs, and, in some cases, quietly accumulating assets in a reserve. The following table compares the different national approaches to cryptocurrencies (see Table 2).

3.4.1. CBDCs, monetary sovereignty and de-dollarisation

Not all governments favour privately issued cryptocurrencies. Features such as immutability, programmability, speed, and low cost also appeal to states seeking efficiency and greater control. This has driven the development of state-issued CBDCs and discussions on shared digital currencies within groupings such as BRICS (TASS, 2024). In the future, interoperable CBDCs could reduce dependence on the US dollar and contribute to de-dollarisation.

There are domestic considerations too, with CBDCs potentially altering monetary policy transmission. Several studies indicate that a carefully designed CBDC can strengthen the channels through which policy signals reach households and firms, reducing frictions (Meaning et al., 2021). Evidence from early pilots, including China's e-CNY, also shows that digital currencies can make intermediate targets more controllable and improve the precision with which structural tools are implemented (Li & Jiang, 2022). However, concerns abound. Fantacci and Gobbi (2021) note that CBDCs could affect traditional banking by competing with private deposits, influencing capitalisation and financial stability. Adalid et al. (2024) caution that if a shift from deposits into CBDCs is poorly managed, banks could face tighter funding conditions, which in turn may restrict credit supply. Infante and Rungcharoenkitkul (2022) caution about the risk of disintermediation during periods of stress.

Design choices are therefore important to strike a balance. The import of this discussion is institutional rather than technical. What matters for policymakers is how CBDCs redistribute monetary authority between central banks, commercial banks and citizens, and how this, in turn, affects the state's capacity to steer economic outcomes during periods of volatility or coercive pressure. Davlatov et al. (2025) argue that a well-structured CBDC—one that uses tiered remuneration or holding limits—can widen the reach of monetary policy and support financial inclusion, while avoiding the inflationary or destabilising effects that might follow from an unrestrained or overly attractive CBDC design. While scholarship is still emerging, there appears to be an indication that CBDCs can enhance state capacity in monetary management, but only with careful design and calibration.

Major power rivalry amplifies these dynamics. China-now the largest trading partner of more than 120 countries, has launched the e-CNY (Green, 2023). Caudevilla and Kim (2023) highlight China's attempts to internationalise the e-CNY via its participation in RCEP, the PBOC-SWIFT joint venture, and pilot projects in Hong Kong. This has prompted concerns among Western policymakers about Chinese visibility over global financial activity. Aysan and Kayani (2022) argue that while China enjoys first-mover advantage, widespread internationalisation still depends on global confidence in its financial system. They also contend that the United States retains the option to catch up by developing its own CBDC and mobilising allies.

The United States' own posture towards cryptocurrencies has shifted significantly. President Trump stated in 2019 that he was *not a fan* of Bitcoin and viewed it as volatile and *based on thin air* (Trump, 2019). Yet an early action in his second term was the formation of a Working Group on Digital Asset Markets, which also examined whether the US should accumulate a strategic stockpile of cryptocurrencies, particularly Bitcoin (Executive Order No. 141473 C.F.R., 2025). In public comments and on social media, President Trump has indicated that he could impose tariffs of up to 100% on BRICS countries, should their de-dollarisation initiatives materially threaten the role of the US dollar (Nitzberg, 2025). While not a formal policy announcement, this development illustrates how major powers increasingly view digital-asset developments and alternative settlement systems through a strategic lens rather than as purely financial innovations.

Parallel developments in the US Congress emphasise this shift. The BITCOIN Act, introduced in July 2024 by Senator Cynthia Lummis, proposes that the US Treasury build a Strategic Bitcoin Reserve by purchasing one million bitcoins over five years—around 5% of global supply (US Senate, 2025). Publicly available blockchain-tracking data has led some analysts to suggest that addresses attributed to US law-enforcement agencies may collectively hold digital assets worth more than US$21 billion (Bitbo.io, 2025). While this figure is not formally disclosed by the US government, it offers a sense of the scale of assets that have accumulated through seizure activity in recent years, which could be incorporated into such a reserve. The anticipated appreciation of Bitcoin is cited as a means of offsetting deficits and bolstering the dollar (US Senate, 2025).

The contest today extends beyond technology to the deeper question of who sets the standards for global value transfer in the decades ahead. These debates echo long-standing IR arguments that monetary power is exercised not only through currency strength but through control over the infrastructure of global payments (Cohen, 1998; Kirshner, 1995; Strange, 1988). CBDCs sit at the intersection of technical design, monetary sovereignty and geopolitical influence. Control over payment architecture has historically underpinned reserve-currency status and, by extension, the geopolitical heft. If CBDCs or widely held digital assets begin to shift settlement away from dollar-centric systems, even incrementally, the strategic implications for US influence are significant. Conversely, countries that feel constrained by the present system view digital currencies as an opportunity to insulate themselves from external pressure. These are not abstract possibilities but could presage a broader geo-economic realignment already under way. Thus, debates around digital assets can no longer be confined only to technology circles. They now complicate long-standing questions regarding monetary power, institutional authority, and the diplomatic tools states rely upon to shape international behaviour.

Strategic implications extend to citizen safety abroad and for labour mobility. Enforcement agencies in several regions have reported complex cryptocurrency-linked fraud networks that recruit or target individuals across borders. INTERPOL's assessment of technology-enabled scam compounds notes that many such operations rely on crypto-denominated payments and involve victims, recruiters and operators dispersed across multiple jurisdictions (INTERPOL, 2023). The US State Department's *Trafficking in Persons* Report adds a further layer of concern by highlighting instances in Southeast Asia where foreign nationals have been coerced into working in cyber-fraud operations that use cryptocurrency as the primary medium of payment and laundering (US Department of State, 2024). Taken together, these patterns underscore the strain that crypto-enabled crime can place on existing mechanisms of legal cooperation and the challenges governments face in safeguarding their citizens overseas.

Preceding sections and the table below indicate that cryptocurrencies have broad strategic and geopolitical implications, intersecting with terrorism financing, sanctions evasion, espionage, great-power rivalry, reserve-currency politics, labour mobility and domestic governance. Policymakers therefore need to recognise that cryptocurrencies—-whether private, state-issued or hybrid—are now embedded within the fabric of international politics and will continue to shape national-security calculations in the years ahead. A snapshot of the national security dimensions of cryptocurrency use and a consolidated mapping of their ramifications can be seen below.

The categories presented in Fig. 5 were derived through an iterative analytical process that combines inductive insights from the emblematic cases with concepts and state-capacity perspectives already introduced in the security studies and international political economy literature discussed in the paper. The mapping is intended as a conceptual consolidation of recurring vulnerabilities and strategic pressures identified across the analysis, rather than as an exhaustive or predictive

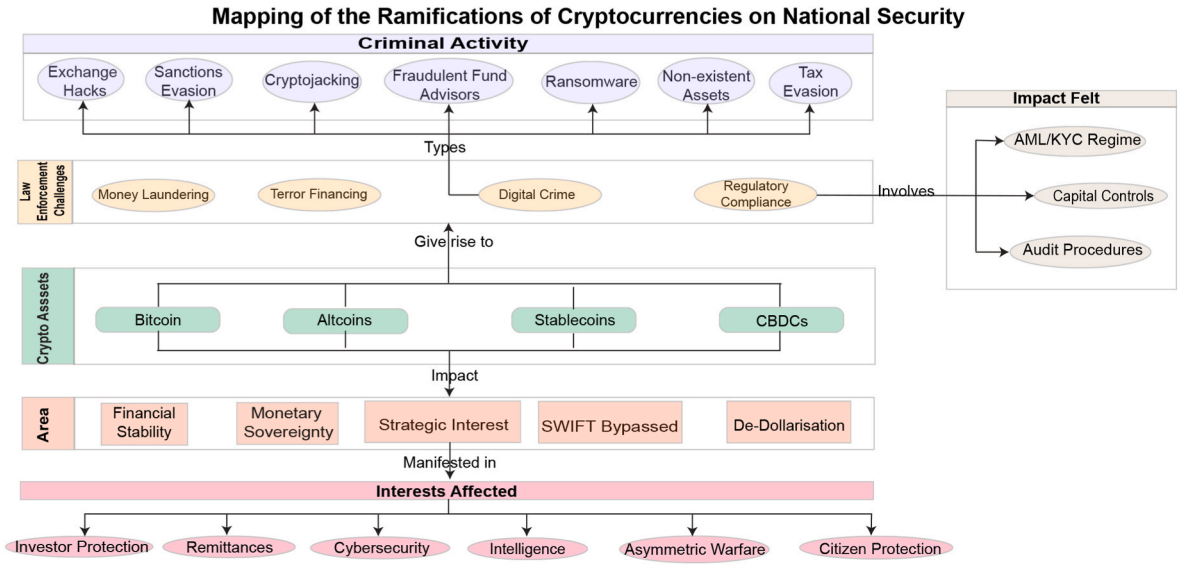

Fig. 5. Mapping of the ramifications of cryptocurrencies on national security.
Source: Author's Conceptualization

model (see Table 3, Fig. 5).

4. Recommendations for policy makers

The preceding analysis makes it evident that cryptocurrencies are now a challenge that policymakers must navigate. They give rise to national security concerns that cannot be wished away. While crafting a policy response, governments may consider the following.

4.1. Prioritising a comprehensive regulatory framework that prioritises national security

To address the enforcement blind spots and jurisdictional arbitrage identified in Sections 3.2 and 3.2.1, where decentralised platforms and uneven regulatory oversight complicate anti-money laundering, sanctions enforcement, and financial intelligence functions, there is a need to formulate national regulatory frameworks that keep national security considerations paramount, rather than treating them as an afterthought while regulating digital assets. This would require the following measures.

i. Compulsory registration of cryptocurrency exchanges, wallets, and other service providers with government regulators.
ii. Frequent audits to ensure that anti-money laundering/know your customer (AML/KYC) norms are enforced in line with FATF requirements.
iii. Mandatory real-time reporting by virtual asset service providers (VASPs)
iv. Incorporating cryptocurrency risk assessments into national financial intelligence unit (FIU) mandates.

4.2. Strengthening cybersecurity measures for crypto-exposed infrastructure

Governments should designate cryptocurrency infrastructure—such as exchanges, custodial wallets, mining operations, and CBDC platforms—as part of critical national infrastructure. They should include crypto-specialist units in the national Computer Emergency Response Teams. There should be mandatory cybersecurity audits for VASPs and exchanges at regular intervals. Standard operating procedures need to be developed for ensuring a coordinated response to hacking attempts targeting crypto infrastructure in the country. These measures respond to the patterns of exchange vulnerabilities and state-linked cyber activity discussed in Sections 3.2 and 3.4, where concentrated crypto infrastructure has emerged as a repeated target for large-scale theft and strategic exploitation.

4.3. Investing in capacity building

Given the technical, jurisdictional, and evidentiary constraints in addressing crypto-enabled crime and terrorism financing brought out in Sections 3.2.1 and 3.3, it is recommended that policymakers incorporate cryptocurrency-related modules within national security, intelligence, law enforcement, judiciary, tax enforcement, and election-monitoring agencies. Care must be taken to ensure that judicial academies offer training on crypto-crime prosecution and asset recovery, electoral commissions update campaign finance regulations to include cryptocurrency donations, and tax authorities provide clarity on crypto tax treatment, enforcement, and penalties.

4.4. Public-education and awareness efforts

Investor enthusiasm in cryptocurrencies remains high, often fuelled by hopes of extraordinary returns. However, customers may not be fully aware of the associated risks and legal complications involved. This creates openings for scams, hacks and rug pulls. A focused public-awareness effort—carried out through both public and private channels—would help consumers become more aware and reduce the chances of avoidable harm. Given the inherent technical complexity involved, this outreach is important for responsible and sustainable adoption.

4.5. Enhancing international cooperation on crypto-related security threats

The cross-border money laundering structures, sanctions evasion pathways, and regulatory fragmentation documented in Sections 3.2, 3.2.1, and 3.4 attest that the decentralised nature of cryptocurrencies challenges state control over finance and security, requiring a global policy shift. For this purpose, countries should.

i. Utilise available frameworks such as the United Nations to set up a global regulatory framework for cryptocurrencies.

Table 3
National-security dimensions of cryptocurrency use.

S. No.	Domain	Use Case	Primary National Security Concern	Implications
1	Strategic & Geopolitical Competition	CBDCs, sovereign crypto experiments, proposals for pooled digital currencies, and strategic reserves.	Potential reshaping of reserve-currency order and global payment architecture.	Accelerates geo-economic realignment; fuels contestation over standards and financial governance norms.
2	Digital & Organised Crime	Moving fraud proceeds, ransomware payments, cross-border scams, and laundering through mixers or privacy coins.	Loss of investigative visibility; faster illicit flows; weak attribution.	Places heavy pressure on law-enforcement cooperation; strengthens the reach of transnational criminal groups.
3	Terror Financing	Small-value fundraising, covert transfers, and routing donations through privacy-enhancing assets.	Undermines CFT systems and enables bypassing of surveillance and sanctions.	Dilutes collective counter-terror norms and increases uneven compliance across jurisdictions.
4	Sanctions Evasion	Mining, peer-to-peer routing, offshore settlement channels and crypto-denominated imports/exports.	Reduces the impact of coercive economic tools and obscures procurement efforts.	Reduces salience of dollar-centric networks; alters coercive diplomacy.
5	Espionage & State-Linked Cyber Activity	Funding cyber-units, paying operatives, and moving stolen digital assets with fewer conventional traces.	Difficult attribution; reduced transparency over hostile intelligence activity.	Blurs boundary between criminal and state-sponsored actions; complicates strategic cyber-response frameworks.
6	Financial Stability	Speculative flows, rapid cross-border movements, stablecoin runs, bank and exchange collapses.	Contagion risk; runs on exchanges; spillover into banking/FX markets during stress.	Limits central-bank capacity to manage volatility; forces regulators to expand macro-prudential tools beyond banks.
7	Monetary Sovereignty	Citizens shifting into Bitcoin or stablecoins during inflation, foreign currency restrictions or political uncertainty.	Erosion of seigniorage; diminished control over capital flows and currency management.	Shrinks policy space during crises; creates parallel monetary circuits outside sovereign oversight.
8	Remittances & Cross-Border Payments	Migrant workers using stablecoins or P2P rails to avoid fees or bypass foreign currency controls.	Loss of foreign-currency inflows; tax revenue lost; reduced visibility of financial flows into households.	Alters balance-of-payments management; weakens fiscal projections in countries dependent on remittances.
9	Investor & Citizen Protection	Retail participation in volatile assets; exposure to scams, unregulated exchanges, and fraudulent schemes.	Consumer losses; political pressure on regulators; reduced trust in institutions.	Forces governments to strengthen oversight frameworks and modernise investor-protection regimes.

Source: Authors Conceptualization

ii. Aim to finalize recommended protocols to govern cryptocurrency exchange licensing, asset freezing, and admissibility of digital evidence.
iii. Set up regulatory sandboxes under the World Bank or IMF to harmonise compliance and eventual integration of CBDCs.
iv. Establish arrangements for cross-border data exchange and real-time wallet tracking.

5. Limitations and further scope of research

Given the nascent stage of development and rapidly evolving nature of cryptocurrencies, and the absence of a consolidated body of work mapping their implications for national security, the principal contribution of this paper lies in elucidating the wide-ranging impact of cryptocurrencies across multiple strategic domains in a manner accessible to policymakers. To achieve this, a deliberate prioritisation of analytical breadth over technical depth was adopted, allowing for a clearer synthesis of institutional, regulatory, and security implications without excessive technical detail. Because of this approach, certain specialised areas—such as the detailed mechanics and security implications of privacy-oriented cryptocurrencies like Monero and Zcash—are acknowledged but not examined exhaustively in the present analysis.

The mapping presented here is exploratory and intended to demonstrate that national security is indeed impacted by cryptocurrencies. Each strand identified in this paper would benefit from a deeper, case-by-case investigation in future work. In other words, this paper suffices to answer the question of whether national security is impacted by cryptocurrencies, but for a detailed examination of the extent, underlying mechanisms, and how these dynamics differ vis-à-vis fiat currency require further research.

Two additional limitations warrant emphasis. First, while the paper deliberately relies on reports from multilateral organisations to enhance cross-regional comparability, much of the publicly available monitoring and enforcement data on cryptocurrency-related risks is produced by Western-based agencies and private analytics firms. This may introduce a degree of detection or reporting bias, particularly in regions with less transparent financial infrastructures. Second, although the selected emblematic cases are analytically instructive, the strategic outcomes observed in specific contexts—such as heavily sanctioned states or small economies with distinctive monetary conditions—may not be fully generalisable to countries with different institutional capacities or political-economic structures.

The paper does not attempt any econometric analysis linking crypto-market volatility to traditional financial indicators, nor does it offer comparative figures on criminal activity across crypto and fiat channels. These issues merit separate, detailed examination beyond this paper's scope. Future work could, for example, systematically compare the effectiveness of different regulatory models in constraining crypto-enabled sanctions evasion, or construct panel-data analyses linking crypto-market indicators to financial-stability metrics and terrorism-financing incidents across jurisdictions. Such studies would complement the broad mapping presented here with finer-grained evidence on causal mechanisms and policy outcomes.

Finally, as CBDC pilots mature, detailed studies of implementation

will be essential for understanding design choices, public acceptance and the wider strategic implications for different countries and the global financial architecture.

6. Conclusion

The broader developmental trajectory of the cryptocurrency ecosystem remains uncertain. Competition will almost certainly lead to winners and losers, and certain digital assets may take on roles that are difficult to anticipate at this stage. Some policymakers are already contemplating treating cryptocurrencies like Bitcoin as a reserve-style asset. Should that occur, governments that have taken early steps to understand the technology and its impact, encourage domestic expertise, and examine how these systems may be aligned with their own objectives, may find themselves in an advantageous position.

At a time of great uncertainty in geopolitics, governments are having to respond to the challenge posed by cryptocurrencies. The steps they take and how quickly institutions adapt will determine the balance between vulnerability and strategic advantage. Ultimately, the cryptocurrency challenge is institutional rather than technical: states will need to rework elements of their domestic governance, cross-border cooperation, and diplomatic engagement to retain authority over financial flows in a decentralised environment.

Declaration of the use of AI

The author declares that no AI assisted technologies were used during any stage in the preparation of this article.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author.

Ethical statement

Ethical approval is not applicable to this manuscript.

Funding statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The author would like to thank Prof. (Dr.) Krishan K Pandey, Dean, Office of Doctoral Studies, O.P. Jindal Global University and Prof. (Dr.) Rajni Goel, Professor and Associate Provost of Faculty Affairs at Howard University for their constant guidance and encouragement.

References

Adalid, R., Burlon, L., & Dimou, M. (2024). Central bank digital currency: Impact on monetary policy transmission via banks. *National Institute Economic Review, 269*, 4–15. https://doi.org/10.1017/nie.2024.25

Ahmad, M., Idrees, M., & Qazi, M. S. (2024). Digital currency financing terrorists in Pakistan: The way forward. *Bulletin of Business and Economics (BBE), 13*(1), 177–181. https://doi.org/10.61506/01.00176

Akartuna, E. A., & Madelin, T. (2023). *The state of cross–chain crime*. Elliptic. Retrieved December 5, 2025, from https://www.elliptic.co/resources/state-of-cross-chain-crime-2023.

Akcinaroglu, S., & Shi, M. (2023). Exploring the impact of cryptocurrency on terrorism. *Terrorism and Political Violence, 37*(1), 111–135. https://doi.org/10.1080/09546553.2023.2275057

Akyildirim, E., Corbet, S., Sensoy, A., & Yarovaya, L. (2020). Riding the wave of crypto–exuberance: The potential misusage of corporate blockchain announcements. *Technological Forecasting and Social Change, 159*. https://doi.org/10.1016/j.techfore.2020.120191. Article 120191.

Alfieri, C. (2022). Cryptocurrency and national security. *International Journal on Criminology, 9*(1), 1–12. https://doi.org/10.18278/ijc.9.1.3

Anggriawan, R., & Susila, M. E. (2024). Cryptocurrency and its nexus with money laundering and terrorism financing within the framework of FATF recommendations. *Novum Jus, 18*(2), 249–277. https://doi.org/10.14718/novumjus.2024.18.2.10

Aramonte, S., Huang, W., & Schrimpf, A. (2021). DeFi risks and the decentralisation illusion. *BIS Quarterly Review*. December 2021, 21–36. Bank for International Settlements. Retrieved December 9, 2025, from https://www.bis.org/publ/qtrpdf/r_qt2112b.htm.

Arnold, A. (2019). A financial sanctions dilemma. *The Washington Quarterly, 42*(4), 57–71. https://doi.org/10.1080/0163660X.2019.1693098

Aysan, A. F., & Kayani, F. N. (2022). China's transition to a digital currency: Does it threaten dollarization? *Asia and the Global Economy, 2*(1). https://doi.org/10.1016/j.aglobe.2021.100023. Article 100023.

Bae, S. (2025). *Deterrence under pressure: Sustaining US-ROK cyber cooperation against North Korea*. Center for Strategic and International Studies. Retrieved December 10, 2025, from https://www.csis.org/analysis/deterrence-under-pressure-sustaining-us-rok-cyber-cooperation-against-north-korea.

Baldwin, D. A. (1985). *Economic statecraft*. Princeton University Press.

Bangui, H., & Buhnova, B. (2022). Blockchain patterns in critical infrastructures: Limitations and recommendations. In *Proceedings of the 17th international conference on software technologies (ICSOFT 2022)* (pp. 457–468). SCITEPRESS. https://doi.org/10.5220/0011278500003266.

BBC News. (2021). Iran bans cryptocurrency mining for four months after blackouts. Retrieved December 6, 2025, from https://www.bbc.com/news/world-middle-east-57260829.

Bitbo.io. (2025). US government bitcoin holdings. Retrieved December 9, 2025, from https://bitbo.io/treasuries/usa/.

Bloomberg News. (2022). *UN says crypto use in terror financing likely soaring*. Bloomberg. Retrieved December 5, 2025, from https://www.bloomberg.com/news/articles/2022-10-31/un-finding-more-cases-where-crypto-involved-in-terror-financing.

Brown, P., Margesson, R., Nelson, R. M., & Seelke, C. R. (2022). Venezuela: Background and US relations. https://www.congress.gov/crs-product/R44841. (Accessed 10 December 2025).

Buterin, V. (2013). Ethereum: A next-generation smart contract and decentralized application platform. https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. (Accessed 28 November 2025).

Buzan, B. (1991). *People, states and fear: An agenda for international security studies in the post-cold War era*. Harvester Wheatsheaf.

Cambridge Centre for Alternative Finance. (2021). *Cambridge Bitcoin Electricity Consumption Index (CBECI): Mining map*. Cambridge Judge Business School, University of Cambridge. Retrieved November 28, 2025, from https://ccaf.io/cbeci/mining_map.

Caudevilla, O., & Kim, H. M. (2023). The Digital Yuan and cross-border payments: China's rollout of its central bank digital currency. *SSRN*. https://doi.org/10.2139/ssrn.4371414

Central Bank of The Bahamas. (2020). The sand dollar is on schedule for gradual national release to The Bahamas in mid-October 2020. *Central Bank of The Bahamas*. Retrieved December 8, 2025, from https://www.centralbankbahamas.com/news/public-notices/the-sand-dollar-is-on-schedule-for-gradual-national-release-to-the-bahamas-in-mid-october-2020.

Chainalysis. (2024). The 2024 geography of cryptocurrency report. https://go.chainalysis.com/2024-geography-of-cryptocurrency-report.html.

Chainalysis. (2025). $2.2 billion stolen in crypto in 2024 but hacked volumes stagnate. https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/. (Accessed 6 December 2025).

Chaudhary, A., & Ivey-Law, H. (2023). SeDe: Balancing blockchain privacy and regulatory compliance by selective de-anonymization [Preprint]. *arXiv*. https://doi.org/10.48550/arXiv.2311.08167

Chitsungo, C. (2024). Harnessing digital strategies to combat cryptocurrency-enabled crimes: Addressing money laundering, illicit trade, and cyber threats. *American Journal of International Relations, 9*(7), 77–106. https://doi.org/10.47672/ajir.2523

Cohen, B. J. (1998). *The geography of money*. Cornell University Press.

Crespo, R. A. (2020). *Currency warfare: The weaponization and targeting of currency from the American Revolution to the war against ISIS*. University of California, Riverside]. eScholarship. Doctoral dissertation https://escholarship.org/uc/item/6r56g9hm.

Cumming, D. J., Johan, S., & Pant, A. (2019). Regulation of the crypto-economy: Managing risks, challenges, and regulatory uncertainty. *Journal of Risk and Financial Management, 12*(3). https://doi.org/10.3390/jrfm12030126. Article 126.

Cybersecurity and Infrastructure Security Agency, National Security Agency, Federal Bureau of Investigation, Defense Cyber Crime Center. (2024). *North Korea cyber group conducts global espionage campaign to advance regime's military and nuclear programs (Joint Cybersecurity Advisory AA24-207A)*. Cybersecurity and Infrastructure Security Agency. Retrieved December 10, 2025, from https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a.

Davlatov, E., & Sági, J. (2025). The transmission mechanism of monetary policy and central bank digital currency: A new monetary order? *Journal of Central Banking Theory and Practice, 14*(1), 95–119. https://doi.org/10.2478/jcbtp-2025-0006

de Carvalho, R. M., Inácio, H. C., & Marques, R. P. (2024). An empirical analysis of tax evasion among companies engaged in stablecoin transactions. *Journal of Risk and Financial Management, 17*(9). https://doi.org/10.3390/jrfm17090400. Article 400.

Deutsche Bank Research. (2019). Cryptocurrencies: The 21st century cash. In *Imagine 2030* (pp. 24–28). Deutsche Bank Research. Retrieved November 25, 2025, from https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000503196/Imagine_2030.pdf.

Dimovski, D. (2024). Cryptocurrencies and crime. *Teme, 48*(4), 975–990. https://doi.org/10.22190/TEME220701060D

Donoiu, P. C., & Iacob, D. (2023). The cryptocurrency market and financial stability. *Proceedings of the International Conference on Business Excellence, 17*(1), 1769–1778. https://doi.org/10.2478/picbe-2023-0157

Drezner, D. W. (2011). Sanctions sometimes smart: Targeted sanctions in theory and practice. *International Studies Review, 13*(1), 96–108. https://doi.org/10.1111/j.1468-2486.2010.01001.x

Drezner, D. W. (2015). Targeted sanctions in a world of global finance. *International Interactions, 41*(4), 755–764. https://doi.org/10.1080/03050629.2015.1041297

Egmont Group of Financial Intelligence Units. (2023). Annual report 2021/2022. *Egmont Group of Financial Intelligence Units*. Retrieved December 5, 2025, from https://egmontgroup.org/wp-content/uploads/2023/07/Egmont-Group_AnnualReport_2021-22_FINAL_07-31-23_SINGLE-PGS_WEB.pdf.

Elfadul, I., Wu, L., Elhabob, R., & Elkhalil, A. (2024a). A privacy and compliance in regulated anonymous payment system based on blockchain. *Journal of Ambient Intelligence and Humanized Computing, 15*, 3141–3157. https://doi.org/10.1007/s12652-024-04801-2

Elfadul, I., Wu, L., Elhabob, R., & Elkhalil, A. (2024b). SCCT-DARS: Secure and compliant cryptocurrency transactions in a decentralized anonymous regulated system. In H. Yang, & R. Lu (Eds.), *Frontiers in cyber security: 6th international conference, FCS 2023, Chengdu, China, August 21–23, 2023, revised selected papers (communications in computer and information science, 1992* pp. 34–54). Singapore: Springer Nature. https://doi.org/10.1007/978-981-99-9331-4_3.

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023: July 2022 to June 2023* (Publication No. 10.2824/782573). European Union Agency for Cybersecurity. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf.

Europol. (2023). Internet organised crime threat assessment (IOCTA) 2023. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023.

Europol. (2024). Internet organised crime threat assessment (IOCTA) 2024. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024.

Executive Order No. 14147, 3 C.F.R.. (2025). Executive office of the President. *Strengthening American leadership in digital financial technology*. Retrieved December 9, 2025, from https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/.

Fantacci, L., & Gobbi, L. (2021). Stablecoins, central bank digital currencies and US dollar hegemony: The geopolitical stake of innovations in money and payments. *Accounting, Economics, and Law: Convivium, 11*(1), 1–28. https://doi.org/10.1515/ael-2020-0053

Ferreira, A. (2020). Emerging regulatory approaches to blockchain based token economy. *The Journal of The British Blockchain Association*. https://doi.org/10.31585/jbba-3-1-(6)2020

Feyen, E., Klingebiel, D., & Ruiz, M. (2024). *Crypto-assets: Unfit for central bank reserves today*. World Bank Blogs. Retrieved December 8, 2025, from https://blogs.worldbank.org/allaboutfinance/crypto-assets–unfit-for-central-bank-reserves-today.

Financial Action Task Force. (n.d.). *Virtual assets*. FATF. Retrieved December 10, 2025, from https://www.fatf-gafi.org/en/topics/virtual-assets.html.

Financial Action Task Force. (2019). Guidance for a risk-based approach to virtual assets and VASPs. *FATF*. Retrieved December 10, 2025, from https://www.fatf-gafi.org/en/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html.

Financial Action Task Force. (2025). Comprehensive update on terrorist financing risks. https://www.fatf-gafi.org/en/publications/Methodsandtrends/comprehensive-update-terrorist-financing-risks-2025.html.

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies? *Review of Financial Studies, 32*(5), 1798–1853. https://doi.org/10.1093/rfs/hhz015

Galant, M. (2025). US sanctions policy: Frequently asked questions. Center for Economic and Policy research. https://cepr.net/publications/us-sanctions-policy-frequently-asked-questions/.

Gandal, N., & Halaburda, H. (2015). Competition in the cryptocurrency market. In D. Lee Kuo Chuen (Ed.), *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data* (pp. 439–457). Academic Press.

Green, M. A. (2023). *China is the top trading partner to more than 120 countries*. Wilson Center. Retrieved December 8, 2025, from https://www.wilsoncenter.org/blog-post/china-top-trading-partner-more-120-countries.

Griffin, J. M., & Shams, A. (2020). Is bitcoin really untethered? *The Journal of Finance, 75*(4), 1913–1964. https://doi.org/10.1111/jofi.12903

Gutmann, J., Neuenkirch, M., & Neumeier, F. (2023). The economic effects of international sanctions: An event study. *Journal of Comparative Economics, 51*(4), 1214–1231. https://doi.org/10.1016/j.jce.2023.05.005

Hacken. (2024). Inside lazarus group: Analyzing north Korea's Most infamous crypto hacks. https://hacken.io/discover/lazarus-group/. (Accessed 9 December 2025).

Helleiner, E. (1994). *States and the reemergence of global finance: From Bretton Woods to the 1990s*. Cornell University Press.

Hopwood, D., Bowe, S., Hornby, T., & Wilcox, N. (2018). *Zcash protocol specification (Version 2018.0-beta-15)*. Zcash Project. Retrieved December 2, 2025, from https://cryptopapers.info/assets/pdf/zcash_protocol.pdf.

Infante, S., & Rungcharoenkitkul, P. (2022). CBDCs: Implications for bank intermediation and stability. https://doi.org/10.2139/ssrn.4055978.

INTERPOL. (2022). Global crime trend summary report. https://www.interpol.int/en/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf.

INTERPOL. (2023). Annual report 2023. https://www.interpol.int/content/download/22267/file/INTERPOL%20Annual%20Report%202023%20EN.pdf.

Jaiswal, V. K., & Chaudhari, A. K. (2023). The economic implications of cryptocurrency adoption: A comparative analysis of traditional financial systems and decentralized alternatives. *IOSR Journal of Economics and Finance, 14*(4, Ser. I), 56–64. Retrieved December 9, 2025, from https://www.iosrjournals.org/iosr-jef/papers/Vol14-Issue4/Ser-1/I1404015664.pdf.

Jenkinson, G. (2022). *El Salvador's bitcoin wallet Chivo scores $52M in remittances in 2022*. Cointelegraph. https://cointelegraph.com/news/el-salvador-s-bitcoin-wallet-chivo-scores-52m-in-remittances-in-2022.

Jia, W., Xie, T., & Wang, B. (2024). A privacy-preserving scheme with multi-level regulation compliance for blockchain. *Scientific Reports, 14*(1). https://doi.org/10.1038/s41598-023-50209-x. Article 438.

Joebges, H., Herr, H., & Kellermann, C. (2025). Crypto assets as a threat to financial market stability. *Eurasian Economic Review, 15*, 473–502. https://doi.org/10.1007/s40822-025-00311-4, 2025.

Keohane, R. O. (1984). *After hegemony: Cooperation and Discord in the world political economy*. Princeton University Press.

Kirshner, J. (1995). *Currency and coercion: The political economy of international monetary power*. Princeton University Press.

Knoerich, J. (2021). China's new digital currency: Implications for renminbi internationalization and the US dollar. In N. Bilotta, & F. Botti (Eds.), *The (near) future of central bank digital currencies* (pp. 145–166). Peter Lang. https://doi.org/10.3726/b18087.

Krasner, S. D. (1988). Sovereignty: An institutional perspective. *Comparative Political Studies, 21*(1), 66–94. https://doi.org/10.1177/0010414088021001004

Leuprecht, C., Jenkins, C., & Hamilton, R. (2023). Virtual money laundering: Policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime, 30*(4), 1036–1054. https://doi.org/10.1108/JFC-07-2022-0161

Levi, M. (1988). *Of rule and revenue*. University of California Press.

Li, Y., & Jiang, Z. (2022). A study on the influence mechanism of CBDC on monetary policy: An analysis based on e-CNY. *PLoS One, 17*(7). https://doi.org/10.1371/journal.pone.0268471. Article e0268471.

Lob, E. (2022). *Iran and cryptocurrency: Opportunities and obstacles for the regime*. Middle East Institute. Retrieved November 28, 2025, from https://www.mei.edu/publications/iran-and-cryptocurrency-opportunities-and-obstacles-regime.

Lyons, R. K., & Viswanath-Natraj, G. (2023). What keeps stablecoins stable? *Journal of International Money and Finance, 131*. https://doi.org/10.1016/j.jimonfin.2022.102777. Article 102777.

Makarov, I., & Tschiatschek, B. (2025). Cybersecurity crimes in cryptocurrency exchanges (2009–2024) and their economic impact. *Frontiers in Blockchain, 8*. https://doi.org/10.3389/fbloc.2025.1713637. Article 1713637.

Manjula, B. C., Shilpa, B. S., & Sundaresh, M. (2022). Analysis of cryptocurrency, Bitcoin and the future. *East Asian Journal of Multidisciplinary Research, 1*(7), 1293–1302. https://doi.org/10.55927/eajmr.v1i7.803

Marinova, T., Goldman, S., Boulanguer, C., & Jandah, M. (2024). Unbacked cryptomoney, fiscal evasion and environmental tax: Some policy recommendations in Europe. *Bulgarian Journal of International Economics and Politics, 4*(1), 3–22. https://bjiep.unwe.bg/en/journalissues/article/40991.

Meaning, J., Dyson, B., Barker, J., & Clayton, E. (2021). Broadening narrow money: Monetary policy with a central bank digital currency. *International Journal of Central Banking, 17*(2), 175–204. from https://www.ijcb.org/journal/ijcb21q2a1.htm. (Accessed 25 November 2025).

Momtaz, P. P. (2020). Initial coin offerings. *PLoS One, 15*(5), Article e0233018. https://doi.org/10.1371/journal.pone.0233018

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. (Accessed 8 December 2025).

National Crime Agency. (2024). Operation Destabilise: NCA disrupts multi-billion Russian money laundering networks with links to drugs, ransomware and espionage resulting in 84 arrests. https://www.nationalcrimeagency.gov.uk/news/operation-destabilise-nca-disrupts-multi-billion-russian-money-laundering-networks-with-links-to-drugs-ransomware-and-espionage-resulting-in-84-arrests. (Accessed 10 December 2025).

Nawaz, A. D., Bhutto, N. A., & Khan, S. (2023). Cryptocurrencies-tax evasion nexus: Does economic performance matter? The case of G-7 countries. *Research Square*. https://doi.org/10.21203/rs.3.rs-3287399/v1 [Preprint].

Nitzberg, A. (2025). *Trump reasserts towering 100% tariff threat against BRICS countries*. Fox Business. https://www.foxbusiness.com/politics/trump-reasserts-towering-100-tariff-threat-against-brics-countries.

Noether, S., Mackenzie, A., & Monero Core Team. (2016). *Ring confidential transactions (Monero Research Lab Report No. MRL-0005)*. Monero Research Lab. Retrieved December 8, 2025, from https://www.getmonero.org/resources/research-lab/pubs/MRL-0005.pdf.

Olalekan, O. A. (2024). Crypto-enabled espionage: The growing threat to national security. *African Journal of Social Sciences and Humanities Research, 7*(4), 235–246. https://doi.org/10.52589/AJSSHR-Z73T57O2

Pacelli, V., Di Tommaso, C., Foglia, M., & Ingannamorte, S. (2025). Cryptocurrencies and systemic risk: Spillover effects between cryptocurrency and financial markets. In V. Pacelli (Ed.), *Systemic risk and complex networks in modern financial systems* (pp. 343–358). Springer. https://doi.org/10.1007/978-3-031-64916-5_18.

Pape, R. A. (1997). Why economic sanctions do not work. *International Security, 22*(2), 90–136. https://doi.org/10.1162/isec.22.2.90

People's Bank of China. (2025). *China's digital RMB transactions top 14.2 trillion yuan*. State Council Information Office. http://english.www.gov.cn/archive/statistics/2025 10/29/content_WS6901a9c9c6d00ca5f9a0726a.html.

Poskart, R. (2022). The emergence and development of the cryptocurrency as a sign of global financial markets financialisation. *Central European Review of Economics & Finance, 36*(1), 53–66. https://doi.org/10.24136/ceref.2022.004

Retter, L., Frinking, E., Hoorens, S., Lynch, A., Nederveen, F., & Phillips, W. (2020). *Relationships between the economy and national security: Analysis and considerations for economic security policy in the Netherlands (RR-4287)*. RAND Corporation. Retrieved December 1, 2025, from https://www.rand.org/content/dam/rand/pubs/research_reports/RR4200/RR4287/RAND_RR4287.pdf.

Reuters. (2022). Iran makes first import order using cryptocurrency - Report. https://www.reuters.com/business/finance/iran-makes-first-import-order-using-cryptocurrency-tasnim-2022-08-09.

Roth, F. (2009). The effect of the financial crisis on systemic trust. *Intereconomics, 44*, 203–208. https://doi.org/10.1007/s10272-009-0296-9

Saleem, M. N., Doumenis, Y., Katsikas, E., Izadi, J., & Koufopoulos, D. (2024). Decrypting cryptocurrencies: An exploration of the impact on financial stability. *Journal of Risk and Financial Management, 17*(5). https://doi.org/10.3390/jrfm17050186. Article 186.

Sarmiento, A. (2022). Seven lessons from the e-Peso pilot plan: The possibility of a central bank digital currency. *Latin American Journal of Central Banking, 3*(2), Article 100062. https://doi.org/10.1016/j.latcb.2022.100062

Seibt, S. (2023). Is cryptocurrency helping hamas fund terrorism? France 24. https://www.france24.com/en/middle-east/20231022-is-cryptocurrency-helping-hamas-fund-terrorism.

Shahzad, M. F., Xu, S., Lim, W. M., Hasnain, M. F., & Nusrat, S. (2024). Cryptocurrency awareness, acceptance, and adoption: The role of trust as a cornerstone. *Humanities and Social Sciences Communications, 11*(1). https://doi.org/10.1057/s41599-023-02528-7. Article 4.

Shaxson, N. (2019). *Tackling tax havens*. IMF Finance & Development. http://www.imf.org/en/Publications/fandd/issues/2019/09/tackling-global-tax-havens-shaxon.

Strange, S. (1986). *Casino capitalism*. Basil Blackwell.

Strange, S. (1988). *States and markets*. Basil Blackwell.

Sveriges Riksbank. (2018). *The Riksbank's e-krona project: Report 2*. Sveriges Riksbank. from https://www.riksbank.se/globalassets/media/rapporter/e-krona/2018/the-riksbanks-e-krona-project-report-2.pdf. (Accessed 10 December 2025).

TASS. (2024). Kremlin announces creation of blockchain-based payment system in BRICS. https://tass.com/politics/1755521.

The Soufan Center. (2024). Blockchain and bloodshed: The role of cryptocurrencies in terrorist financing. https://thesoufancenter.org/intelbrief-2024-october-16/. (Accessed 27 November 2025).

Tilly, C. (1990). *Coercion, capital, and European states, AD 990–1990*. Blackwell.

Tolbaru, C.-E. (2023). Considerations on combating money laundry in the field of crypto assets, at european union level. *RAIS Conference Proceedings 2023*. Retrieved December 8, 2025, from https://rais.education/wp-content/uploads/2023/09/0312.pdf.

Trump, D. J. (2019). I am not a fan of Bitcoin and other cryptocurrencies, which are not money, and whose value is highly volatile and based on thin air [@realDonaldTrump] https://twitter.com/realDonaldTrump/status/1149472282584072192.

Ukrainska Pravda. (2024). Media outlets find crypto wallet of ISIS Tajikistan wing used to transfer payment for terrorist attack in Moscow oblast. https://www.pravda.com.ua/eng/news/2024/03/29/7448665/.

Ukwueze, F. (2021). Cryptocurrency: Towards regulating the unruly enigma of fintech in Nigeria and South Africa. *Potchefstroom Electronic Law Journal, 24*, 1–38. https://doi.org/10.17159/1727-3781/2021/v24i0a10743

United Nations. (2024). Why the world needs a UN global tax convention. *UN News*. https://news.un.org/en/story/2024/08/1153301. (Accessed 7 December 2025).

United Nations Office on Drugs and Crime. (2023a). *Global cybercrime assessment 2023: Illicit digital economies and cross-border crime*. United Nations Office on Drugs and Crime. Retrieved December 7, 2025, from https://www.unodc.org/unodc/en/cybercrime/index.html.

United Nations Office on Drugs and Crime. (2024). Transnational organized crime and the convergence of cyber-enabled fraud. *Underground banking and technological innovation*. Retrieved December 7, 2025, from https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

United Nations Security Council Counter-Terrorism Committee Executive Directorate. (2024). CTED trends tracker. *Evolving trends in the financing of foreign terrorist fighters' activity: 2014–2024*. Retrieved December 7, 2025, from https://www.un.org/securitycouncil/ctc/content/cted-trends-tracker-evolving-trends-financing-foreign-terrorist-fighters%E2%80%99-activity-2014-%E2%80%93-0.

US Department of State. (2024). *2024 trafficking in persons* report. https://www.state.gov/reports/2024-trafficking-in-persons-report/.

US Department of the Treasury. (2023). Treasury releases 2023 DeFi illicit finance risk assessment. https://home.treasury.gov/news/press-releases/jy1391.

US Senate. (2025). *BITCOIN act of 2025*, S.954, 119th congress. https://www.congress.gov/bill/119th-congress/senate-bill/954.

US Senate Committee on Homeland Security & Governmental Affairs. (2022). Use of cryptocurrency in ransomware attacks. https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report.pdf.

Valero, P. (2018). *Special report: In Venezuela, new cryptocurrency is nowhere to be found*. Reuters. https://www.reuters.com/article/business/special-report-in-venezuela-new-cryptocurrency-is-nowhere-to-be-found-idUSKCN1LF18F/.

Vidal-Tomás, D., Briola, A., & Aste, T. (2023). FTX's downfall and Binance's consolidation: The fragility of centralised cryptocurrency exchanges. *Physica A: Statistical Mechanics and Its Applications, 625*, Article 129044. https://doi.org/10.1016/j.physa.2023.129044

Waltz, K. N. (1979). *Theory of international politics*. McGraw-Hill.

Wong, L. (2025). *S Rajaratnam Lecture 2025: A safe harbour in a turbulent world [Speech]*. Singapore: Ministry of Foreign Affairs. Retrieved November 27, 2025, from http://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2025/04/S-Rajaratnam-Lecture-PM-Wong-2025.

World Bank. (2024). *Remittances (KNOMAD brief)*. World Bank. Retrieved November 27, 2025, from https://www.worldbank.org/en/topic/migration/brief/remittances-knomad.

Xiong, X., Huth, M., & Knottenbelt, W. J. (2025). RegKYC: Supporting privacy and compliance enforcement for KYC in blockchains. In *Proceedings of the 2025 IEEE international conference on blockchain and cryptocurrency (ICBC)* (pp. 1–5). IEEE. https://doi.org/10.1109/ICBC64466.2025.11114514.

Xue, L., Liu, D., Ni, J., Lin, X., & Shen, X. S. (2023). Enabling regulatory compliance and enforcement in decentralized anonymous payment. *IEEE Transactions on Dependable and Secure Computing, 20*(2), 931–943. https://doi.org/10.1109/TDSC.2022.3144991

Zhaolu, Z., Zhang, Y., & Li, X. (2024). Collaborative regulation for privacy-preserving blockchains. *IEEE Transactions on Information Forensics and Security, 19*, 1234–1245. https://doi.org/10.1109/TIFS.2023.3348268

Zola, F., Medina, J. A., & Orduna, R. (2024). Assessing the impact of sanctions in the crypto ecosystem: Effective measures or ineffective deterrents? *arXiv*. https://doi.org/10.48550/arXiv.2409.10031 [Preprint].