Exploring the role of cryptocurrencies in sanctions evasion: a systematic review

Orfeas Anastasios Koidis and Francesco Giumelli
International Relations and International Organization, Rijksuniversiteit Groningen, Groningen, The Netherlands, and

Oskar Josef Gstrein
Governance and Innovation, University of Groningen, Groningen, The Netherlands

Abstract

Purpose – There is a growing debate about the use of cryptocurrencies to evade sanctions. This paper aims to systematically collect and organize the available literature on cryptocurrencies and sanctions evasion. The aim is to map the debate, identify gaps and clarify the implications for global governance and the international order.

Design/methodology/approach – This research conducted a systematic literature review using a keyword-string search method across relevant databases. Due to limited peer-reviewed literature, additional "grey" literature was included to broaden the evidence base.

Findings – The mapping reveals a fragmented debate over a strong link between cryptocurrencies and sanctions evasion grounded in cryptocurrencies' design features. It identifies three main gaps concerning the scale of this form of evasion, the mechanisms through which it operates, and whether it represents a novel challenge or a reconfiguration of established practices under new technical infrastructure. Further research on these issues would contribute to an enhanced understanding of sovereignty, global governance and power.

Originality/value – While much of the literature on cryptocurrencies and illicit finance has centred on money laundering, their role in sanctions evasion remains underexplored. To the best of the authors' knowledge, this paper provides the first systematic consolidation of the dispersed academic and policy literature on the topic. It brings together peer-reviewed research and verified grey literature into a consolidated evidence base that can serve as a stepping stone for future debates and research on cryptocurrency-enabled sanctions evasion.

Keywords Cryptocurrencies, Digital currencies, Economic sanctions, Sanctions evasion

Paper type Literature review

1. Introduction

There is growing concern within both academic and policy circles that the emergence and widespread adoption of cryptocurrencies could undermine the effectiveness of financial regulations (Fanusie and Logan, 2019; Macfarlane, 2021). This concern arises from cryptocurrencies' decentralized architecture and inherent pseudonymity, which make them particularly appealing for illicit activities (Cozzi, 2020). Cryptocurrency transactions are verified through a decentralized network of computers, enabling them to operate with minimal dependence on traditional financial systems (Leuprecht *et al.*, 2023).

Journal of Financial Crime
Vol. 33 No. 4-5, 2026
pp. 216-232
Emerald Publishing Limited
1359-0790
DOI 10.1108/JFC-05-2025-0130

Simultaneously, the substantial degree of anonymity afforded to cryptocurrency users complicates the tracing and identification of transactions (Deepika and Kaur, 2017). These features create a range of security challenges (Leuprecht *et al.*, 2023), among which is the use of cryptocurrencies for sanctions evasion purposes (Wronka, 2022).

The design features of cryptocurrencies plausibly facilitate sanctions evasion (Wronka, 2022). Specifically, because identifiable information is concealed in cryptocurrency transactions, detecting transactions linked to sanctioned individuals and entities becomes more difficult (Macfarlane, 2021). At the same time, the decentralized nature of cryptocurrencies allows financial transactions to occur outside the oversight of traditional financial channels, complicating sanctions enforcement (Makhlouf and Selmi, 2022).

These concerns are reinforced by documented cases in which sanctioned actors, most prominently the Democratic People's Republic of Korea (hereinafter DPRK), have leveraged cryptocurrencies for sanctions evasion, through cyber theft, illicit laundering networks and obfuscation techniques to finance state activities (United Nations Security Council, 2024). Similarly, Russia and Iran have explored cryptocurrency-based mechanisms for circumventing sanctions (Cozzi, 2020; Ahari *et al.*, 2022), further demonstrating the broader risks these technologies pose to sanctions enforcement. According to industry estimates, in 2024, sanctioned jurisdictions and entities collectively received $15.8 billion in cryptocurrency, representing nearly 40% of all illicit cryptocurrency transactions (Chainalysis, 2025). At the same time, international sanctions have gained renewed prominence in the global financial system, particularly in the wake of Russia's invasion of Ukraine in February 2022. These developments have sharpened concerns about the resilience of sanctions amid the availability of cryptocurrencies as potential evasion tools.

Against this backdrop, this article systematically examines the existing literature to address the central research question:

RQ1. How has the literature addressed the concern that cryptocurrencies enable sanctions evasion, and what gaps and implications follow?

To address this question, we use a systematic literature review (SLR) that collects and organizes the academic and policy literature on cryptocurrencies and sanctions evasion.

Our review indicates that this concern is based on a strong link between cryptocurrencies and sanctions evasion grounded in their design features and supported by documented episodes of state use. However, the practical effects of these features are not absolute: pseudonymity remains, in principle, amenable to regulatory reach and despite the decentralized architecture, much activity ultimately routes through intermediaries that can be brought within supervisory frameworks. In this sense, scope remains for mitigating evasion, yet the fragmented regulatory landscape makes this a complex undertaking.

Even though a lot has been written on this alleged connection, the novelty and evolving nature of crypto-enabled sanctions evasion mean that a systematic assessment is still missing. Existing studies largely infer the scale and significance of the problem from a small number of cases, and they point to pathways without clearly specifying the conditions under which these become viable. Specifically, three gaps stand out. Firstly, the overall scale of cryptocurrency-enabled sanctions evasion remains unclear, both in absolute terms and relative to other evasion practices. Secondly, the mechanisms and conditions through which crypto-enabled sanctions evasion materializes are insufficiently specified. Thirdly, it remains contested whether the phenomenon reflects novel dynamics or rather a reconfiguration of existing evasion practices under new technical infrastructure. Beyond empirical uncertainties, resolving these gaps bears directly on whether states retain the capacity to assert authority, steer the key points through which sanctions are enforced, and leverage their

structural position within the international financial system to exert pressure. How these points resolve, therefore, carries different implications which, at the most worrying end, would suggest a material erosion of sovereign capacity and control.

Building on this, we begin by mapping the debate in three steps. Firstly, we trace how the literature links cryptocurrencies' technical features to sanctions enforcement and clarify their practical effects and limits for identification and oversight. Secondly, we illustrate how cryptocurrencies have been used to circumvent sanctions. Thirdly, we assess how the regulatory environment enables or constrains evasion. We then underline the main gaps and chart directions for future research. Finally, we draw implications for sovereignty, governance, and power, showing how the emerging uncertainties intersect with disputes over who exercises authority, how control is organized and where leverage resides.

2. Methodology

This study follows the SLR approach to synthesize and critically appraise the qualitative and quantitative evidence describing the intersection of cryptocurrencies and sanctions evasion. Its objective is to collect and organize the available literature, map the debate and identify key gaps to guide future research. Rather than producing new empirical data, this study provides a structured account that consolidates existing findings into one coherent narrative, clarifies the main concepts and identifies the analytical boundaries of this emerging research area. To reach this goal, we have developed a research protocol to ensure a rigorous sample selection process.

Firstly, a keyword-string search method was used to delimit the corpus of sources. The keywords included were "cryptocurrencies", "sanctions" and "evasion", as well as synonyms to ensure comprehensive coverage. Regarding the keyword "cryptocurrencies", we included the terms "digital currencies", "distributed ledger technologies" and "virtual currencies". Even though they are conceptually distinct, they are often used interchangeably in practice, and therefore, we assume they contribute to the debate. The terms "Bitcoin" and "Ethereum" were also included as the two most popular and most established cryptocurrencies. Regarding the term "sanctions", we also included "restrictive measures" as the equivalent term for sanctions in European Law terminology. Finally, synonyms for "evasion" included "circumvention", "bypass" and "sanctions-busting". These terms were adapted to the specific search formats of each database. Boolean indicators and truncation tools were used to refine the results.

This search strategy was applied to online academic databases such as Scopus, Web of Science and Emerald Insight. The search yielded 170 articles. Their titles and abstracts were screened for relevance to the review question. Full texts were reviewed where relevance remained unclear. An additional search was conducted on Google Scholar to capture relevant yet potentially overlooked sources. Furthermore, a snowballing technique was used, wherein the reference lists of selected papers were reviewed to identify pertinent contributions. The final sample of included peer-reviewed studies and their main characteristics are presented in Table 1.

Given the limited peer-reviewed output during our search window, we supplemented academic sources with select grey literature. Methodological guidance on systematic reviews supports the inclusion of grey literature to broaden the evidence base (Petticrew and Roberts, 2006; Rothstein and Hopewell, 2009). In our context, this is an emerging field characterized by rapidly evolving practices and time-sensitive evidence that often appears first outside academic journals. Technical analyses in this field often rely on proprietary databases and tools not typically available to academic researchers. Accordingly, we applied pragmatic inclusion criteria considering institutional credibility, methodological transparency and

Table 1. Characteristics of included studies in this systematic review

Author and year	Research design	Key findings and relevance for RQ
Ahari *et al.*, 2022	Mixed-method policy analysis	Shows that around Russia's 24 Feb 2022 invasion, RUB–crypto trading and Bitcoin volumes briefly spiked before normalizing; attributes this mainly to individual wealth protection and small-scale transfers, noting that overall market liquidity remains far too limited to sustain large-scale sanctions evasion
Clautice (2019)	Qualitative policy, case-based analysis	Sanctioned states use cryptocurrency primarily to evade restrictions on access to international finance and to generate foreign exchange. Highlights North Korea's state-sponsored crypto thefts and the emergence of state-backed coins (e.g. Iran's PayMon, Venezuela's Petro). Identifies regulatory lag in Office of Foreign Assets Control/FinCEN frameworks and the decentralized affordances of crypto as key enablers of evasion
Cozzi (2020)	Qualitative legal and policy analysis	Argues that blockchain can both aid and hinder sanctions enforcement: pseudonymity enables evasion, but transparency and automation could enhance compliance. Highlights how technological affordances shape both evasion and enforcement dynamics in sanctions governance
Fantacci and Gobbi (2021)	Qualitative policy analysis	Argues that stablecoins and CBDCs can be used to bypass US sanctions by creating alternative payment networks outside SWIFT. Links this to broader challenges to US monetary hegemony and sanctions enforcement. Shows how technological innovation enables states to evade sanctions and weaken US control over global payments
Kirkpatrick *et al.*, 2019	Qualitative legal and policy analysis	Examines how Iran, Russia and Venezuela explore cryptocurrencies to bypass SWIFT and US sanctions. Notes OFAC's position that crypto transactions remain sanctionable and highlights compliance gaps for exchanges. Shows how sanctioned states exploit crypto to evade US financial controls, while weak compliance frameworks enable persistent enforcement challenges
Konowicz (2018)	Qualitative policy analysis	Identifies five strategies (crypto theft, mining, national coins, joint coins, public adoption) used by sanctioned states to bypass US sanctions. Urges US interagency action and blockchain tracking as countermeasures. Demonstrates how state and societal crypto use undermines sanctions, reinforcing the need for coordinated enforcement and technological monitoring
Macfarlane (2021)	Qualitative doctrinal and policy analysis	Argues that pseudo-anonymity and weak cross-border regulation enable crypto-based sanctions evasion by states like North Korea and Iran. Proposes a multilateral treaty to harmonize international oversight. Highlights how fragmented enforcement environments and crypto's affordances sustain state-level sanctions evasion, reinforcing need for coordinated global regulation

(*continued*)

Table 1. Continued

Author and year	Research design	Key findings and relevance for RQ
Makhlouf and Selmi (2022)	Mixed-method policy analysis	Finds that sanctions on Russian banks and removal from SWIFT sharply reduce formal remittances. Notes limited potential for crypto to offset sanctions due to liquidity and traceability constraints. Shows that while crypto offers theoretical evasion pathways, structural limits reduce its utility, reinforcing sanctions' short-term financial impact
Theiri *et al.*, 2022	Quantitative empirical event study	Finds that the Russia–Ukraine invasion triggered only short-lived BTC/ETH liquidity spikes; medium-term spreads unchanged – limiting capacity for large-scale Russian sanctions evasion via crypto markets. Indicates insufficient, non-persistent crypto market depth to support sustained Russia sanctions circumvention
Wronka (2022)	Qualitative case-based policy analysis	Shows that digital currencies heighten sanctions-evasion risk through pseudonymity and fragmented, cross-jurisdictional regulation; discusses Russia's push for a state-run "cryptorouble" and non-SWIFT rails to bypass dollar constraints; argues stronger KYC/monitoring are needed to curb such workarounds
Wright, 2023	Qualitative legal and policy analysis	Shows that weak/uneven crypto regulation enables sanctions evasion; surveys Russia's 2014–2022 cases alongside Venezuela, Iran and DPRK. Proposes international coordination and stronger KYC requirements to curb crypto-enabled sanctions evasion. Links Russia-focused evasion pathways to regulatory gaps, clarifying how technological affordances and enforcement capacity shape sanctions effectiveness
Zhao and Miao, 2023	Quantitative empirical study	Shows that Russia's 24 Feb 2022 invasion did not sustain increases in Bitcoin-Russian Ruble/Bitcoin-US Dollar trading pair volumes; Bitcoin co-moves with risk assets, and Bitcoin volume only weakly tracks Russian oil exports – indicating insufficient depth for large-scale Russian sanctions evasion

recency. Grey literature was not given probative weight over peer-reviewed or official sources and, where deemed appropriate, was used to fill empirical gaps and provide technical context that the academic literature has yet to cover. This approach maintains methodological transparency while ensuring a comprehensive synthesis of the available evidence.

3. Mapping the debate: conceptual claims, empirical manifestations and regulatory conditions

There is an active debate across academic and policy circles about the role of cryptocurrencies in sanctions evasion (Cozzi, 2020; Macfarlane, 2021; Wronka, 2022, Wright, 2023). This section maps this debate by organizing the literature into three linked dimensions. Firstly, it explains the link between cryptocurrencies' design features and sanctions evasion and clarifies their practical effects and limits. Secondly, it examines how these dynamics manifest empirically through selected cases of sanctioned states. Thirdly, it assesses how the regulatory environment shapes these dynamics. Taken together, this mapping reveals that assessments of cryptocurrency-enabled sanctions evasion vary with underlying assumptions about technical design, state capacity and regulatory coordination.

(i) Disentangling the link between cryptocurrencies and sanctions evasion

This section illustrates how existing research has documented the link between cryptocurrencies and sanctions evasion. It first offers a concise account of how cryptocurrencies operate, isolating the technical features that ground the proposed link to sanctions evasion. It then disentangles the baseline claim that cryptocurrencies' decentralized and pseudonymous design enables sanctions evasion by making two clarifications about how these features operate, clarifying their limits.

Cryptocurrencies facilitate peer-to-peer transactions within decentralized payment systems that operate largely outside traditional financial institutions (Macfarlane, 2021). These systems rely on encryption to verify and secure transactions (Macfarlane, 2021). Public key cryptography underpins this technology, enabling users to transact in ways often characterized as anonymous, which complicates identification and tracing (Deepika and Kaur, 2017; Leuprecht *et al.*, 2023). Cryptocurrency transactions are publicly validated through a distributed network of computers, allowing them to function with minimal reliance on traditional financial systems (Leuprecht *et al.*, 2023). These features pose significant security challenges (Leuprecht *et al.*, 2023) and make cryptocurrencies appealing for illicit activities such as money laundering (Dupuis and Gleason, 2020), tax evasion (Meling *et al.*, 2024) and terrorist financing (Kapsis, 2023).

Across the literature, a recurring view is that cryptocurrencies' design features, particularly decentralization and anonymity, create opportunities for sanctions evasion (Wronka, 2022; Cozzi, 2020; Macfarlane, 2021). Targeted sanctions function by restricting the access of designated entities or individuals to their financial assets and excluding them from the broader financial system (Cortright and Lopez, 2002). Their effectiveness rests on two conditions: the accurate identification of the targets and the effective enforcement by trusted intermediaries. Both conditions may be affected by these features (Cozzi, 2020:12), though not necessarily in the way that a surface reading of "anonymity" and "decentralization" would suggest.

With respect to identification, cryptocurrency transactions conceal most of the identifiable user information (Macfarlane, 2021:201–202). This hampers the identification of designated individuals and entities (Cozzi, 2020:12). Although scholars agree that the concealment of user identity provides leeway for sanctions circumvention, they emphasize that cryptocurrencies are essentially enabling pseudonymous rather than anonymous transactions (Macfarlane, 2021:210–211, Cozzi, 2020). The reason is that cryptocurrency users are tied to

an alias, represented by a unique identifier such as a wallet address. As a transaction is verified, it is immutably inscribed in the blockchain and can be traced back to that alias (Government Blockchain Association, 2019). Although the unique identifier itself does not immediately reveal the user's real-world identity, once linked to a person, all transactions associated with it can be traced back to them. This duality is crucial: pseudonymity conceals users' identities and facilitates sanctions evasion, yet it also allows for traceability once an alias is connected to an individual. Recognizing that claims of anonymity often refer to pseudonymity clarifies why it constrains enforcement while providing limited opportunities for detection and mitigation.

With respect to enforcement, cryptocurrencies operate through decentralized networks, whereby transactions are verified and recorded on a "blockchain" by a network of autonomous computers rather than by a central authority (Makhlouf and Selmi, 2022:3). Sanctioned actors can use the peer-to-peer nature of cryptocurrencies to move funds across borders (Ahari *et al.*, 2022:10–11). In this setting, the absence of centralized trusted intermediaries limits the ability to exclude sanctioned actors from transactions.

Yet in practice, much activity ultimately routes through intermediaries, most notably exchanges and related service providers. This is because cryptocurrency holdings often require conversion into fiat currency to be widely usable. Cryptocurrencies are not legal tender and do not reliably function as a medium of exchange or store of value, primarily due to their low adoption and high volatility (Ammous, 2017). As a result, actors seeking to evade sanctions are typically dependent on liquidating their assets, as they are exposed to a significant degree of risk by preserving their wealth in the form of cryptocurrencies. In this sense, cryptocurrency exchanges constitute a necessary passage point. Regulated exchanges can serve as transit portals that enable monitoring and blocking, for example, through direct oversight (Clautice, 2019:13–16), weakening the disintermediation inherent in cryptocurrencies. At the same time though, cryptocurrency exchanges are private entities that operate under a cost-benefit calculus, with their primary source of revenue being fees from transactions (Kim *et al.*, 2021). Where suspicious activity reporting threatens transaction volumes and, by extension, fee income, incentives to prevent illicit transactions can be minimal and some exchanges may even be motivated to facilitate transactions for users in sanctioned jurisdictions (Macfarlane, 2021:221). Together, these clarifications sharpen rather than dissolve the debate over whether cryptocurrencies' design features materially weaken sanctions, suggesting that the central issue is not the possibility of cryptocurrency-enabled evasion in the abstract but the specific conditions and mechanisms through which it occurs.

(ii) Empirical evidence

The shift from mere concern to observable pattern is evident in documented cases of sanctioned states leveraging cryptocurrencies for sanctions evasion. The cases of the DPRK, Russia and Iran are illustrative. Although these cases vary in political context and technical capacity, they reveal recurring patterns in how cryptocurrencies are used – particularly the ways in which the technology facilitates evasion, the role of the intermediaries and the regulatory environments. This tripartite framework allows for comparative insights across cases.

The DPRK is a notable example of a sanctioned state that has used cryptocurrencies to circumvent sanctions. Its exploitation of the cryptocurrency market is yet another progression in its long-standing history of sanctions evasion (Zellers, 2024:283). The DPRK has invested in developing cyber capabilities to support the hacking and exploitation of digital infrastructures (Park, 2022). In 2023, it accounted for nearly one-third of crypto funds stolen via cyberattacks on multiple exchanges. According to a UN Security Council Report,

the DPRK is allegedly involved in cyberattacks that reportedly resulted in losses of roughly $3 billion (United Nations Security Council, 2024). For comparison, the DPRK – subject to heavy sanctions – earned $89 million in official exports in 2022. At the same time, its trade volumes in 2023 exceeded those of 2022, potentially indicating ongoing sanctions evasion that can be attributed to cryptocurrencies (United Nations Security Council, 2024). This case illustrates a technologically intensive model of evasion that relies on cybertheft and obfuscation tools rather than market integration or regulatory manipulation. Its approach highlights how technical capacity can compensate for limited access to global financial intermediaries.

These obfuscation methods include the use of "mixers", which pool funds of different users to obscure transaction trails. The Office of Foreign Assets Control's (hereinafter OFAC) sanctioning of Tornado Cash, a mixer service that facilitated the laundering of over $7 billion worth of cryptocurrencies, including illicitly acquired cryptocurrencies by the DPRK, illustrates the scale of such operations (Zellers, 2024:287). In addition, attackers use a digital form of layering to conceal their activity by creating thousands of transactions, using single-use cryptocurrency wallets in real time (United Nations Security Council, 2024).

Russia provides another example of a sanctioned state exploiting cryptocurrencies in the context of sanctions pressure. As a highly active participant in the cryptocurrency market, Russia accounts for approximately $16.8 billion in annual cryptocurrency transaction volume (Ahari *et al.*, 2022:1) and ranks among the top five countries in cryptocurrency mining, reflecting high domestic adoption. The possibility of circumventing sanctions is considered a major driver of Russia's engagement with cryptocurrencies (Ahari *et al.*, 2022:8). In addition, Russia has a well-established presence in the realm of cybercrime, with industry data indicating that 74% of global ransomware revenues have been funneled into the country, further illustrating its integration into illicit digital financial activities (Chainalysis, 2022a).

The invasion of Ukraine provides a context in which the role of cryptocurrencies in sanctions evasion became more visible. In the period leading up to and immediately following the invasion, ruble-denominated cryptocurrency transactions increased significantly. From February 19–24, 2022, trading volume in ruble-denominated crypto transactions surged by over 900%, exceeding $70 million (Ahari *et al.*, 2022:4). This increase suggests that actors within Russia sought to exploit cryptocurrencies during a period of heightened geopolitical and economic uncertainty. While some analysts, such as Chainalysis, suggest that much of the increased trading activity may have been driven by individuals seeking to protect their savings rather than large-scale sanctions evasion (Chainalysis, 2022b), the timing of these fluctuations underscores how cryptocurrencies can function as a potential buffer against sanctions pressure.

Liquidity constraints and price volatility in cryptocurrency markets are frequently cited as limitations to large-scale evasion, with estimates suggesting that attempts to liquidate substantial holdings could trigger significant price declines (Chainalysis, 2022a; Theiri *et al.*, 2022; Clautice, 2019:24, Makhlouf and Selmi, 2022:5; Zhao and Miao, 2023). However, these structural limits do not preclude sanctions evasion strategies, particularly through intermediaries and jurisdictions that remain outside the sanction framework. Overall, the available evidence indicates that while full-scale sanctions evasion through cryptocurrencies remains constrained by market dynamics (Ahari *et al.*, 2022; Chainalysis, 2022b; Theiri *et al.*, 2022, Zhao and Miao, 2023), Russia has actively explored and used cryptocurrencies in response to sanctions (Wright, 2023). Russia's strategy is shaped less by technological innovation than by its established presence in global cryptocurrency markets and cyber-enabled financial infrastructure. This case

reflects a market-integrated model of evasion, mainly leveraging financial infrastructure and jurisdictional asymmetries.

Finally, Iran provides a further example of a sanctioned state using cryptocurrencies to evade sanctions. Estimates suggest that Iran accounts for approximately 3.1% to 4.5% of global cryptocurrency mining activity. Iranians exploit the abundance of natural gas reserves and subsidized electricity prices to enhance cryptocurrency mining (Ahari *et al.*, 2022:10). Chainalysis estimates that Iran's mining activity generated more than $160 million between 2015 and 2021. (Chainalysis, 2022a). Reports also suggest that actors linked to Iran have relied on intermediaries in jurisdictions such as Turkey, Lebanon and the UAE to act as middlemen for moving funds, and have been linked to ransomware cyber-attacks demanding cryptocurrency payments ultimately laundered through exchanges into Iranian riyals (Cozzi, 2020:15). Chainalysis reports that in 2024, outflows from Iranian cryptocurrency exchanges reached $4.18 billion, a 70% increase compared to the previous year, with Iranian services taking a significantly larger share of sanctions-related cryptocurrency activity (Chainalysis, 2025). Iran's reliance on energy resources and state-sanctioned mining activity exemplifies a resource-conversion model of evasion, where domestic comparative advantages substitute for financial connectivity. Viewed together, the DPRK, Russia and Iran cases demonstrate that cryptocurrency-enabled sanctions evasion operates through distinct pathways, each shaped by different interactions between state capacity, intermediary dependence and regulatory context.

(iii) Regulation and the space for crypto-enabled evasion

The empirical cases outlined above shift the focus towards the mechanisms and conditions that enable evasion. Although these mechanisms vary across cases, the literature consistently shows that regulation shapes the space in which evasion occurs. This can happen through lax requirements, misaligned rules across jurisdictions or intermediaries that fall outside effective oversight (Macfarlane, 2021; Cozzi, 2020; Konowicz, 2018; Wronka, 2022).

The proliferation of cryptocurrencies has prompted regulatory responses at national and international levels. However, these remain fragmented, leaving space for illicit use, such as sanctions evasion (Wronka, 2022; Cozzi, 2020:12, Macfarlane, 2021). This fragmentation reflects the novelty and rapidly evolving nature of this technology (Clautice, 2019:13). Against this background, nation-by-nation regulation results in under-inclusivity, creating jurisdictional loopholes that actors can exploit to avoid detection (Macfarlane, 2021).

While harmonization is a central debate in the literature (Konowicz, 2018; Wronka, 2022; Macfarlane, 2021:203–209), a broad multilateral framework is widely considered as unrealistic. This limitation is evident in how sanctioned states, such as Russia and Iran, have adapted their positions on cryptocurrencies in response to intensifying sanctions (Fantacci and Gobbi, 2021:18, Kirkpatrick *et al.*, 2019; Ahari *et al.*, 2022). For example, following the exclusion of Iranian banks from SWIFT, Iran signed a trilateral blockchain cooperation agreement with Russia and Armenia (Kirkpatrick *et al.*, 2019). Similarly, following the invasion of Ukraine, Russia shifted its approach by allowing greater flexibility in digital investing, mining and cryptocurrency-based payments, while simultaneously tightening monitoring and oversight (Ahari *et al.*, 2022:2).

Within this context, a second debate concerns both whom and how to regulate. With respect to who, regulatory efforts have increasingly focused on actors that fall within regulatory reach, notably intermediaries such as cryptocurrency exchanges (Cozzi, 2020:19). These regulatory initiatives vary not only in scope but also in orientation. Some, such as actions by OFAC, are deterrence-driven and punitive, while others, such as the European Union's Markets in Crypto-Assets Regulation (MiCA), emphasize preventive oversight and

institutional compliance, reflecting a shift towards more robust oversight of cryptocurrency intermediaries. Enforcement has expanded in line with this focus on intermediaries. For example, OFAC reached a $24 million settlement with Bittrex for processing transactions for users in sanctioned countries (e.g. Iran, Cuba), and designated mixers Blender.io and Sinbad.io for facilitating laundering linked to sanctioned jurisdictions (U.S. Department of the Treasury, 2022a, 2022b).

With respect to how to regulate, efforts have primarily focused on extending Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements to cryptocurrency intermediaries (Clautice, 2019:13–16, Kirkpatrick *et al.*, 2019), thereby restoring identification *ex* ante and reintroducing enforcement leverage *ex post*, limiting the scope for pseudonymity and decentralization. Taken together, these measures impose practical constraints on cryptocurrency-enabled sanctions evasion. However, where regulation remains fragmented or uneven, it continues to create openings, leaving a transnational issue largely governed by national jurisdictions.

4. Between concern and evidence: Gaps in the crypto-sanctions literature

Despite growing attention and documented cases, important aspects of cryptocurrency-enabled sanctions evasion remain unclear. The literature leaves three main gaps. Firstly, there is no systematic assessment of how widespread cryptocurrency-enabled evasion is both in absolute terms and relative to other evasion practices. Secondly, the relative importance of different pathways and the regulatory and market conditions that enable them remain underspecified. Thirdly, it is unclear whether these practices represent a genuinely novel challenge that exceeds the reach of existing regulatory tools, or a reconfiguration of familiar evasion strategies under new technical infrastructure. The remainder of this section elaborates on these points.

While the literature documents instances of cryptocurrency use by sanctioned states, the available evidence is insufficient for a systematic assessment of its scale or significance. Most accounts rely on single-case studies, focused on a small number of jurisdictions and even in those cases, the interpretation of the evidence remains contested. Russia – the most recent empirical focus – illustrates this ambiguity. Some analyses contend that Russia used cryptocurrencies, particularly around the invasion of Ukraine, to circumvent sanctions (Ahari *et al.*, 2022). Others argue that market depth and volatility limit the feasibility of large-scale evasion, suggesting that observed trading patterns primarily reflect household wealth preservation rather than state-directed sanctions circumvention (Theiri *et al.*, 2022; Chainalysis, 2022b). As a result, it remains unclear whether cryptocurrency-enabled sanctions evasion constitutes a marginal supplement to existing evasion practices or a meaningful shift in their scale or nature.

Beyond questions of scale, existing work identifies several mechanisms through which evasion occurs, but offers limited insight into their prevalence and enabling conditions. The literature describes multiple pathways – cybertheft and subsequent laundering, mining and conversion, cross-border routing through permissive or weakly supervised intermediaries – yet provides little evidence on how frequently these pathways are used, which regulatory and market settings make them viable, or how they are combined in practice. Within this landscape, cryptocurrency exchanges play a pivotal role in sanctions compliance. Under robust supervision, exchanges and related service providers can function as chokepoints; however, where incentives are weak or regulatory standards are unevenly enforced, they may operate as conduits (Clautice, 2019; Macfarlane, 2021). The central task is to explain when and why particular pathways are selected, and how regulatory and market conditions shape their use in concrete episodes of evasion.

A further gap concerns whether cryptocurrency-enabled sanctions evasion is genuinely novel or a reconfiguration of longstanding practices under new technical infrastructure. The literature often treats cryptocurrencies as disruptive because of their design features (Cozzi, 2020; Wronka, 2022), yet it remains contested whether this amounts to a structural break with earlier evasion techniques or a functional analogue that differs mainly in form rather than logic. Even where design features are foregrounded, much of the literature ultimately treats regulation as the proximate enabler shaping when and where these practices occur (Macfarlane, 2021). Notwithstanding the novelty of these design features, several of the mechanisms cited are in fact old problems in a new guise. Regulatory arbitrage, the use of third-country middlemen for routing, and layering to obscure transaction trails all have predecessors in earlier sanctions evasion and AML contexts (Draganidis, 2023; Schneider and Windischbauer, 2008; Early, 2015). Without comparative work linking crypto-enabled pathways to historical evasion techniques, it is difficult to determine whether the underlying dynamics are genuinely distinct or continuous with past patterns.

The question of whether crypto-enabled evasion is truly novel also extends to the regulatory domain, particularly regarding the effectiveness and scope of regulatory responses. Empirically, it remains unclear whether recent enforcement measures result in suppression, displacement or adaptation, and under which conditions each outcome occurs. While discussions on the harmonization of regulation (Konowicz, 2018; Wronka, 2022) and the potential for a multilateral framework have dominated the literature (Macfarlane, 2021:215–228, Cozzi, 2020:18–22), there is limited evidence about the outcomes or durability of such efforts. In that regard, the EU's MiCA regime provides a recent example of a comprehensive regulatory rollout where such effects can be traced. Conceptually, it is unresolved whether the challenges faced by regulators are unique to cryptocurrencies or reflect recurring governance problems associated with earlier financial or technological transformations. Current approaches largely transpose AML/KYC logics onto cryptocurrency, reaffirming an intermediary-centric model of control (Clautice, 2019:13–16, Kirkpatrick *et al.*, 2019), raising the question of whether the unique features of cryptocurrencies exceed what AML/KYC-based tools can manage, or whether the difficulties observed reflect familiar challenges of fragmented governance. Without systematic cross-jurisdictional assessment and comparative analysis linking crypto-era dilemmas to historical precedents, it remains difficult to determine whether recent measures deter evasion, rearrange it or do both in shifting proportions.

Taken together, these gaps point to several questions: how much cryptocurrency-enabled evasion contributes relative to established forms of evasion in particular contexts; under which regulatory and market conditions particular pathways are selected; and when and why intermediaries function as conduits rather than as chokepoints. Addressing these questions would clarify the role of cryptocurrencies in sanctions contexts and the scale and drivers of cryptocurrency-enabled evasion, thereby situating cryptocurrencies within broader theoretical debates on global governance and power.

5. Expanding the frame: Cryptocurrency-enabled sanctions evasion in a wider context

Addressing these gaps informs broader debates in international relations and law on sovereignty, global governance and power. Sanctions evasion through cryptocurrencies raises questions about how national sovereignty operates in an increasingly de-territorialized manner (Atzori, 2017). These dynamics reflect how new technologies reshape existing power structures in the international system. The case of cryptocurrencies exemplifies the broader debate on the long-standing relationship between technology and International

Relations (Der Derian, 2003). Technology has been understood both as a capabilities-enhancing instrument allowing states to gain power *vis-à-vis* others (Leese and Hoijtink, 2019:5) and as a connective medium reorganizing relations among actors (Burton, 2020:14). More generally, technological change can shift where authority lies, how control is exercised, and reshape the meaning and practice of governance and sovereignty (Drezner, 2019; Weiss, 2005; Skolnikoff, 1993). This section assesses the identified gaps through these lenses to show what the implications for these concepts are.

Historically, sovereignty has adapted to political and technological change (Krasner, 2001; Pohle and Thiel, 2020; MacCormick, 1999). Yet, the digital revolution loosened the state's grip over data flows and capital (Weiss, 2005:302), prompting calls for "digital sovereignty" as states seek to reassert authority over digital infrastructures (Pohle and Thiel, 2020; Madiega, 2020). Cryptocurrencies intensify this tension, raising questions about where and on what basis sovereign authority can be exercised. The push for digital sovereignty reflects broader concerns over control in the digital age. In contrast, an alternative framing emphasizes data autonomy, centred on informational self-determination over digital infrastructures and, in this context, financial flows (Gstrein, 2023:391–393). Operationally and ideologically, cryptocurrencies often sit closer to this autonomy paradigm. Read through this lens, the question is not only whether states can reassert control, but whether state control should remain the primary benchmark for assessing the implications of technological change for political authority. The case of sanctions evasion through cryptocurrencies serves as a novel case study for understanding how transformations in the exercise of state sovereignty may materialize in practice. International sanctions are an expression of sovereignty, as they represent the state's ability to impose economic or political pressure to enforce its policies and uphold its norms (Baldwin, 2020). Within the broader sovereignty debate, one interpretation holds that digital architectures shift activity onto infrastructures beyond effective state supervision, thereby constraining enforcement and regulatory control (DeNardis, 2014). Under this reading, some argue that cryptocurrencies mark a fundamental reconfiguration of sovereignty (Manski and Manski, 2018). Another interpretation sees sovereignty as adaptive rather than diminished, as states reassert control through intermediaries and standards to bring these infrastructures within regulatory reach (Pohle and Thiel, 2020; Madiega, 2020). A third perspective sees sovereignty redistributed across networks, where public, private and technical actors share or contest control, rather than the state simply losing it (Castells, 2009). Yet, through the data autonomy lens, the same shifts might not register as a loss of sovereignty at all but rather as a redistribution of control away from state supervision towards user empowerment. Which view holds depends on whether control remains within the state's reach.

Accordingly, the focus shifts to global governance, understood as the exercise of authority in the absence of a central controller (Rosenau, 1992; Held and McGrew, 2002). The key question is how sanctioning states manage declining enforcement capacity. Cryptocurrency intermediaries can function either as chokepoints or as conduits (Clautice, 2019; Macfarlane, 2021) and governance depends on whether enforcement continues to operate through actors that states can steer. Where this is the case, governance persists through delegation and coordination (Abbott and Snidal, 2009). Where it is not, control shifts beyond effective supervision, displacing governance from established mechanisms of authority.

Such dynamics would not be unprecedented. Digital technologies have long enabled social, economic and political coordination through networks not confined to physical locations, elevating non-state actors as central managers of cross-border activity (Castells, 2009:442–446; Nye, 2011). Whether these dynamics are novel or continuous with past

patterns shapes how governance failures are interpreted. Such failures may reflect coordination and delegation problems or, alternatively, they may point to limits rooted in technical infrastructures that do not map cleanly onto territorial jurisdiction. If failures resemble earlier coordination and delegation problems, they may be addressed through strengthening compliance incentives and supervisory capacity. By contrast, if evasion depends primarily on technical infrastructures and services outside effective supervisory reach, governance problems shift from coordination to the limits of territorial jurisdiction. In either case, how these dynamics are understood carries implications beyond sanctions, informing, more generally, how digitally mediated illicit activities are governed.

Finally, this technological shift may have disruptive effects on the power dynamics of the international system. As much as sanctions are an expression of sovereignty, they also represent an exercise of power (Baldwin, 1971; Giumelli, 2011). In networked financial systems, this power derives from control over chokepoints and the ability to restrict access. Farrell and Newman describe this as weaponized interdependence, whereby states leverage their strategic position over key infrastructures to cut adversaries off from network flows (Farrell and Newman, 2021).

Against this backdrop, the unresolved governance questions identified above bear directly on the distribution of power. Whether coercive leverage can be sustained in sanctions enforcement depends on whether control over critical enforcement infrastructures remains within reach of public authority. Where chokepoints can be supervised, states retain leverage because they can still control access to the systems on which others depend (Farrell and Newman, 2021). Where control instead migrates to technical systems or to actors that the state cannot supervise, the capacity to translate insights into coercive force is weakened. Hence, losing control over these infrastructures may create openings for resistance, making the study of crypto-enabled sanctions evasion relevant not only for understanding potential reconfiguration of power but also for tracing new forms of contestation.

Until the empirical gaps on the scale and mechanisms of cryptocurrency-enabled sanctions evasion are resolved, it remains unclear whether cryptocurrencies redistribute power outward or primarily complicate its exercise through existing enforcement channels. If evasion continues to run through actors that states can supervise and compel, governance remains delegated and sovereignty can still be enacted through those channels. Otherwise, the power of states to act in this domain is likely to erode.

6. Conclusion

This article examines how the literature addresses the concern that cryptocurrencies enable sanctions evasion, as well as which uncertainties and implications follow. It offers a structured synthesis of the academic and policy literature at the intersection of cryptocurrencies and sanctions evasion, assembling dispersed contributions into a coherent map of the field. This, in turn, allows for the identification of key gaps and directions for future research.

Several patterns emerge across the literature. Firstly, the design features of cryptocurrencies – such as decentralization and anonymity – are widely viewed as creating opportunities for sanctions evasion. Documented state practice introduces multiple pathways, including cybertheft with subsequent laundering, state-sanctioned mining and cross-border routing via permissive venues. Secondly, assessments of the scale and significance of such activities diverge. Some sources interpret the use as extensive, while others argue that market dynamics – such as liquidity and volatility – limit large-scale evasion. The latter view attributes most of the observed activity to individual wealth preservation rather than state-directed schemes. Thirdly, the fragmented regulatory

landscape creates a strong dependence on intermediaries – such as exchanges and related service providers – which can function either as enforcement-enabling chokepoints or as conduits.

Given the evolving nature of this issue, the available evidence remains thin and case-specific, leaving several questions unanswered. These include the overall scale of cryptocurrency-enabled evasion relative to established evasion; the prevalence, sequencing and enabling conditions of distinct mechanisms; and the effectiveness and durability of regulatory responses across jurisdictions. More broadly, it remains unclear whether cryptocurrency-enabled evasion constitutes a substantive departure from earlier forms of evasion or a reconfiguration of longstanding practices with new technical infrastructure.

The importance of resolving these questions extends beyond the immediate policy domain. Depending on how these dynamics unfold, cryptocurrencies may leave sovereign capacity largely intact, with governance exercised through regulated intermediaries. Alternatively, if mitigation efforts prove insufficient, cryptocurrencies may contribute to a redistribution of power away from states and towards networks and technical systems. To the extent outlined in this article, such shifts may carry not only operational but also normative implications, as cryptocurrencies embrace an autonomy-first approach, making attempts to reassert control – along a traditional understanding of sovereignty – harder. Ultimately, whether cryptocurrencies remain a marginal complication in sanctions enforcement or become a catalyst for broader transformations in sovereignty, governance and power depends on how these dynamics evolve.

References

Abbott, K.W. and Snidal, D. (2009), "The governance triangle: regulatory standards institutions and the shadow of the state", *International Organization*, Vol. 63 No. 3, pp. 501-537.

Ahari, A., Duong, J., Hanz, J., Lichtenegger, E.M., Lobnik, L. and Timel, A. (2022), "Is it easy to hide money in the crypto economy? The case of Russia", *Focus on European Integration, Oestereichische Nationalbank*, Vol. 4, pp. 71-89.

Ammous, S.H. (2017), "Can cryptocurrencies fulfill the functions of money?", *The Quarterly Review of Economics and Finance*, Vol. 70, pp. 38-51, doi: 10.1016/j.qref.2018.05.010.

Atzori, M. (2017), "Blockchain technology and decentralized governance: is the state still necessary?", *Journal of Governance and Regulation*, Vol. 6 No. 1, pp. 45-62.

Baldwin, D.A. (1971), "The power of positive sanctions", *World Politics*, Vol. 24 No. 1, pp. 19-38, doi: 10.2307/2009705.

Baldwin, D.A. (2020), *Economic Statecraft*, 2nd ed., Princeton University Press, Princeton, NJ.

Burton, J. (2020), "Histories of technologies", *Emerging Technologies and International Security, Routledge*, New York, NY, pp. 12-26, doi: 10.5281/zenodo.6138571.

Castells, M. (2009), *The Rise of the Network Society*, 2nd ed., Wiley-Blackwell, Chichester.

Chainalysis (2022a), "Cryptocurrency brings millions in aid to Ukraine, but could it also Be used for Russian sanctions evasion?", available at: www.chainalysis.com/blog/cryptocurrency-ukraine-russia-sanctions/ (accessed 23 February 2024).

Chainalysis (2022b), "Cryptocurrency markets aren't liquid enough for mass Russian sanctions evasion", available at: www.chainalysis.com/blog/cryptocurrency-liquidity-russia-sanctions/ (accessed 23 February 2024).

Chainalysis (2025), "The 2025 crypto crime report", available at: https://go.chainalysis.com/2025-Crypto-Crime-Report.html (accessed 3 March 2025).

Clautice, T. (2019), "Nation state involvement in cryptocurrency and the impact to economic sanctions", *Economic Crime Forensics Capstones*, La Salle University Digital Commons.

Cortright, D. and Lopez, G.A. (2002), *Smart Sanctions: Targeting Economic Statecraft*, Rowman and Littlefield Publishers, Lanham, MD.

Cozzi, F. (2020), "Will blockchain technologies strengthen or undermine the effectiveness of global trade control regulations and financial sanctions?", *Global Jurist*, Vol. 20 No. 2, pp. 1-18, doi: 10.1515/gj-2019-0047.

Deepika, P. and Kaur, E.R. (2017), "Cryptocurrency: trends, perspectives, and challenges", *International Journal of Trend in Research and Development*, Vol. 4 No. 4.

DeNardis, L. (2014), *The Global War for Internet Governance*, Yale University Press, New Haven, CT.

Der Derian, J. (2003), "The question of information technology in international relations", *Millennium: Journal of International Studies*, Vol. 32 No. 3, pp. 441-456.

Draganidis, S. (2023), "Jurisdictional arbitrage: combatting an inevitable by-product of cryptoasset regulation", *Journal of Financial Regulation and Compliance*, Vol. 31 No. 2, pp. 170-185.

Drezner, D.W. (2019), "Technological change and international relations", *International Relations*, Vol. 33 No. 2, pp. 286-303, doi: 10.1177/0047117819834629.

Dupuis, D. and Gleason, K. (2020), "Money laundering with cryptocurrency: open doors and the regulatory dialectic", *Journal of Financial Crime*, Vol. 28 No. 1, pp. 60-74, doi: 10.1108/jfc-06-2020-0113.

Early, B.R. (2015), *Busted Sanctions: Explaining Why Economic Sanctions Fail*, Stanford University Press, Stanford, CA.

Fantacci, L. and Gobbi, L. (2021), "Stablecoins, Central bank digital currencies and US dollar hegemon", *Accounting, Economics, and Law: A Convivium*, Vol. 14 No. 2, pp. 173-200, doi: 10.1515/ael-2020-0053.

Fanusie, Y.J. and Logan, T. (2019), "Crypto rogues. U.S. State adversaries seeking blockchain sanctions resistance", Foundation for Defense of Democracies, available at: www.fdd.org/wp-content/uploads/2019/07/fdd-report-crypto-rogues.pdf

Farrell, H. and Newman, A.L. (2021), "How global economic networks shape state coercion", *The Uses and Abuses of Weaponized Interdependence*, Brookings Institution Press, Washington, DC.

Giumelli, F. (2011), *Coercing, Constraining and Signalling: explaining UN and EU Sanctions after the Cold War*, Routledge, London and New York, NY.

Government Blockchain Association (2019), "Enforcing sanctions in the age of cryptocurrency", available at: https://gbaglobal.org/blog/2019/06/27/enforcing-sanctions-in-the-age-of-cryptocurrency/ (accessed 19 March 2024).

Gstrein, O.J. (2023), "Data autonomy: recalibrating strategic autonomy and digital sovereignty", *European Foreign Affairs Review*, Vol. 28 No. 4, pp. 379-396, doi: 10.54648/eerr2023028.

Held, D. and McGrew, A. (2002), *Governing Globalization: power, Authority and Global Governance*, Polity Press, Cambridge, UK.

Kapsis, I. (2023), "Crypto-assets and criminality", in Jasinski, D., Phillips, A. and Johnston, E. (Eds), *Organized Crime, Financial Crime, and Criminal Justice*, Routledge, New York, NY, pp. 122-141, doi: 10.4324/9781003020813-8.

Kim, D., Bilgin, M.H. and Ryu, D. (2021), "Are suspicious activity reporting requirements for cryptocurrency exchanges effective?", *Financial Innovation*, Vol. 7 No. 1, doi: 10.1186/s40854-021-00294-6.

Kirkpatrick, C., Savage, C., Johnston, R. and Hanson, R. (2019), "Virtual currency in sanctioned jurisdictions: stepping outside of SWIFT", *Journal of Investment Compliance*, Vol. 20 No. 2, pp. 39-44, doi: 10.1108/JOIC-04-2019-0019.

Konowicz, D. R. (2018), *The New Game: Cryptocurrency Challenges US Economic Sanctions.* Naval War College, Newport, United States.

Krasner, S.D. (2001), "Sovereignty", *Foreign Policy*, No. 122, pp. 20-29.

Leese, M. and Hoijtink, M. (2019), "How (not) to talk about technology", in Hoijtink, M. and Leese, M. (Eds), *Technology and Agency in International Relations*, Routledge, New York, NY, pp. 1-23, doi: 10.4324/9780429463143-1.

Leuprecht, L., Jenkins, C. and Hamilton, R. (2023), "Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency", *Journal of Financial Crime*, Vol. 30 No. 4, pp. 1036-1054, doi: 10.1108/JFC-07-2022-0161.

MacCormick, N. (1999), *Questioning Sovereignty: Law, State and Nation in the European Commonwealth*, Oxford University Press, Oxford, United Kingdom, UK.

Macfarlane, E. (2021), "Strengthening sanctions: solutions to curtail the evasion of international economic sanctions through the use of cryptocurrency", *Michigan Journal of International Law*, Vol. 42 No. 1, pp. 199-229, doi: 10.36642/mjil.42.1.strengthening.

Madiega, T. (2020), "Digital sovereignty for Europe", European Parliamentary Research Service (EPRS), available at: www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

Makhlouf, F. and Selmi, R. (2022), "Do sanctions work in a crypto world? The impact of the removal of Russian banks from SWIFT on remittances", *HAL*, doi: 10.48550/arXiv.2203.02956.

Manski, S.G. and Manski, B.R. (2018), "No gods, No masters, No coders? The future of sovereignty in a blockchain world", *Law and Critique*, Vol. 29 No. 2, pp. 151-162.

Meling, T.G., Mogstad, M. and Vestre, A. (2024), *Crypto Tax Evasion*, National Bureau of Economic Research, doi: 10.3386/w32865.

Nye, J.S. Jr (2011), *The Future of Power*, Public Affairs, New York, NY.

Park, J. (2022), "The art of evasion in the cyber economy", in Charron, A. and Portela, C. (Eds), "*Multilateral Sanctions Revisited: Lessons Learned from Margaret Doxey,* ", McGill-Queen's University Press, pp. 193-206.

Petticrew, M. and Roberts, H. (2006), *Systematic Reviews in the Social Sciences: A Practical Guide*, Blackwell Publishing, Malden, MA.

Pohle, J. and Thiel, T. (2020), "Digital sovereignty", *Practicing Sovereignty: Digital Involvement in Times of Crises*, Transcript Verlag, Bielefeld, Germany, doi: 10.14763/2020.4.1532.

Rosenau, J.N. (1992), "Governance, order, and change in world politics", in Rosenau, J.N. and Czempiel, E-O. (Eds), *Governance without Government: Order and Change in World Politics*, Cambridge University Press, Cambridge, pp. 1-29.

Rothstein, H.R. and Hopewell, S. (2009), "Grey literature", In Cooper, H., Hedges, L. V. and Valentine, J. C. (Eds), *The Handbook of Research Synthesis and Meta-Analysis*, Russel Sage Foundation, New York, NY. New York, NY.

Schneider, F. and Windischbauer, U. (2008), "Money laundering: some facts", *European Journal of Law and Economics*, Vol. 26 No. 3, pp. 387-404.

Skolnikoff, E. (1993), *The Elusive Transformation: science, Technology, and the Evolution of International Politics*, Princeton University Press, Princeton, NJ.

Theiri, S., Nekhili, R. and Sultan, J. (2022), "Cryptocurrency liquidity during the Russia–Ukraine war: the case of bitcoin and ethereum", *The Journal of Risk Finance*, Vol. 24 No. 1, pp. 59-71, doi: 10.1108/JRF-05-2022-0103.

United Nations Security Council (2024), *Final Report of the Panel of Experts Established Pursuant to Security Council Resolution 1718(2006), S/2024/215*, United Nations, New York, NY.

U.S. Department of the Treasury (2022a), "Treasury announces two enforcement actions for over $24M and $29M against virtual currency exchange bittrex, inc", available at: https://home.treasury.gov/news/press-releases/jy1006 (accessed 25 March 2024).

U.S. Department of the Treasury (2022b), "U.S. Treasury issues First-Ever sanctions on a virtual currency mixer, targets DPRK cyber threats", available at: https://home.treasury.gov/news/press-releases/jy0768 (accessed 27 March 2024).

Weiss, C. (2005), "Science, technology, and international relations", *Technology in Society*, Vol. 27 No. 3, pp. 295-313, doi: 10.1016/j.techsoc.2005.04.004.

Wright, S. (2023), "The evolution of sanctions evasion: how cryptocurrency is the new game in evading sanction and how to stop it", *International Journal of Law Ethics and Technology*, pp. 1-25.

Wronka, C. (2022), "Digital currencies and economic sanctions: the increasing risk of sanction evasion", *Journal of Financial Crime*, Vol. 29 No. 4, pp. 1269-1282, doi: 10.1108/JFC-07-2021-0158.

Zellers, K. (2024), "Hacked! North Korea's Billion-Dollar crypto heisting scheme", *Penn State Journal of Law and International Affairs*, Vol. 12 No. 2, pp. 261-302, doi: 10.15405/epsbs.2021.09.02.85.

Zhao, J. and Miao, J. (2023), "Is bitcoin used to evade financial sanction?", *Finance Research Letters*, Vol. 55, p. 104005, doi: 10.1016/j.frl.2023.104005.

Corresponding author
Orfeas Anastasios Koidis can be contacted at: o.a.koidis@rug.nl