University of Tartu
Faculty of Social Sciences
Johan Skytte Institute of Political Studies

Brian Wiltse

CRYPTOCURRENCIES AS INSTRUMENTS OF SANCTIONS EVASION: THE CASE OF GARANTEX AND ITS ILLICIT NETWORK

MA Thesis

Supervisor: Shpend Kursani, PhD

Tartu 2025

Authorship Declaration

I have prepared this thesis independently. All the views of other authors, as well as data from literary sources and elsewhere, have been cited.

Word count of the thesis:

Brian Wiltse, (05.19.2025)

Non-exclusive licence to reproduce the thesis and make the thesis public

I, Brian Wiltse, grant the University of Tartu a free permit (non-exclusive licence) to reproduce, for the purpose of preservation, including for adding to the digital archives of the University of Tartu until the expiry of the term of copyright, my thesis *Cryptocurrencies as Instruments for Sanctions Evasion: The Case of Garantex and its Illicit Network,* supervised by Dr. Shpend Kursani; grant the University of Tartu a permit to make the thesis specified in point 1 available to the public via the web environment of the University of Tartu, including via the digital archives, under the Creative Commons licence CC BY NC ND 4.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright; am aware of the fact that the author retains the rights specified in points 1 and 2; confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Brian Wiltse
19/05/2025

Abstract

Cryptocurrencies are rapidly unraveling the effectiveness of economic coercion, allowing sanctioned actors to move value across borders with only fragments of an identity. This thesis examines that shift through a detailed case study of the cryptocurrency exchange Garantex, a platform that processed roughly US $96 billion in digital-asset trades, at least US $1.3 billion of which trace to ransomware crews, darknet vendors and sanctioned oligarchs. Framed by Disruptive Innovation, Transnational Organized Crime, Network and Sanctions-Busting theories, the research adopts a mixed-methods design using both qualitative and quantitative analysis. Results show that, following Russia's 2022 invasion of Ukraine, Garantex and it's over-the-counter brokers rerouted 82 percent of targeted entities' crypto through stablecoins, scripted address-rotation and continual re-branding, effectively sidestepping Western blacklists in real time. These findings demonstrate that sanctions architectures anchored in bank-centric choke points are becoming porous, and it highlights the urgent need for coordinated, near-real-time sharing of information and harmonized enforcement practices if economic sanctions are to retain credibility in an era of decentralized, programmable finance.

Table of Contents

1.0 Introduction

Since the early 21st century, economic sanctions have become a central tool of international statecraft. In response to Russia's actions in Ukraine (first in 2014 and again with the 2022 invasion), Western governments released a plethora of sanctions targeting Russia's financial and economic sectors. For example, by 2024 the United States had placed over 1,700 Russian individuals and entities on its Specially Designated Nationals (SDN) list (Hume & Rutter, 2025), while the EU had adopted 16 comprehensive sanction packages against Moscow to "maximise pressure" and curb the war effort (Council of the European Union, 2025). These measures included travel bans, asset freezes, export controls and financial restrictions all reflected a broader global trend. That being countries from the United States and EU to the United Nations have increasingly relied on sanctions to enforce international norms and punish aggression. In this environment, traditional financial controls like SWIFT exclusions, frozen reserves, and banking prohibitions all aim to sever sanctioned actors from the global economy.

At the same time, the digital revolution has produced a new class of financial instruments, in this case that being cryptocurrencies. Bitcoin's creation in 2009 ushered in tens of thousands of alternative tokens and blockchain-based networks over the following decade. Globally, hundreds of millions of people now hold cryptocurrency wallets, and the market capitalization of digital currencies has sometimes topped trillions of dollars. These systems operate on public ledgers and allow funds to move borderlessly, without central intermediaries. The intrinsic nature of pseudonymous public addresses, 24/7 global access, and independence from any single country's banking system is what gives the allure to cryptocurrencies being pseudonymous public addresses. Indeed, in 2019 roughly 42 million cryptocurrency wallets existed worldwide (Cavicchioli, 2020). However this number is fleeting because often a single person owns multiple wallets. But in five years that number exploded to over 400 million with Russia being ranked among the top countries in crypto adoption (Chainalysis, 2024). Meaning that wallets controlled by individuals (and private businesses) located in Russia generated enough activity to place the country high on Chainalysis's Global Crypto Adoption Index. Within Russia itself, despite bans on domestic crypto payments, interest had surged as of recent with institutions like Rosbank who have introduced cross-border crypto payment services, and President Putin has urged Russia "not to miss the moment" in regulating crypto as a tool to reduce reliance on the U.S. dollar (Bloomberg, 2024). Indicative of the broader theme of the Russian stance when it comes to crypto for this thesis.

Thus, cryptocurrencies have become a pervasive feature of the modern financial landscape, offering new avenues for value exchange beyond the traditional banking system. This dual context being on one side rigorous Western sanction regimes and an ascendant cryptocurrency market distinctively gives rise to a pressing problem, sanctions evasion by non-state actors. This is not referencing state-sponsored schemes (e.g., North Korea's Lazarus

Group, which would be a state actor). It is highlighting how private individuals and networks like terror groups, criminal syndicates, sanctioned oligarchs, and smugglers are increasingly using the booming crypto ecosystem to duck under Western sanctions regimes. Even though the case being used in this thesis will be closely related to the Russian state itself, it is still best described as a non-state actor. In which the Cambridge Dictionary defines as, a person or an organization that is not part of a government, but is still involved in or important in politics, society, etc. in some way, because of their actions.

Western sanctions packages focus primarily on state institutions and politically connected elites, yet they are routinely mitigated by private and semi-private Russian networks. They are anywhere from oligarch-controlled firms and banks to privately owned media empires, pro-Kremlin militias such as Wagner, Gazprom-financed "volunteer" battalions, and even cryptocurrency exchanges like Garantex. One thing all of these networks have in common is that they sit just outside formal government structures and specialize in sanctions evasion (RUSI, 2024). These actors, while not constituting official government structures, may be aligned with Kremlin interests or act independently to preserve Russian economic power. Historically, similarly sanctioned countries (for instance Iran, North Korea, and Venezuela) have exploited cryptocurrencies by using mining or stablecoins to raise hard currency and circumvent restrictions (Fintegrity, 2024). U.S. congressional reports have warned that the pseudonymity of blockchains creates a risk that "Russian actors may use the 'pseudonymity' of cryptocurrency to evade sanctions" (Congressional Research Service, 2022). Also, keeping note that the congressional report was released three months after the initial invasion in 2022. To use a concrete case as an example, a Russian intermediary used the dollar-pegged stablecoin Tether (USDT) to purchase drone components from Hong Kong on behalf of the sanctioned arms manufacturer Kalashnikov (Berwick & Foldy, 2024). While considerable speculation and anecdotal evidence have emerged regarding the extent and practical use of cryptocurrencies within sanctioned Russian networks, comprehensive and empirically grounded analyses remain conspicuously sparse within academic and policy discourse.

Despite the implementation of stringent international sanctions designed to deter and penalize illicit activities, actors connected to Russia continue to access global financial systems and resources necessary for their operations. Evidence suggests that these sanctions have not significantly impeded Russia's strategic objectives or altered its behavior on the international stage (Connolly, 2018). For example, Russia has mitigated the impact of sanctions by diversifying its economic partnerships and utilizing alternative financial mechanisms (Weiss & Blanc, 2019). Moreover, Russian entities have been increasingly adopting cryptocurrencies to facilitate transactions, thereby circumventing traditional financial channels subject to sanctions (Fabrichnaya & Marrow, 2025). This persistence in accessing global financial resources despite sanctions reveals a critical gap in the effectiveness of current sanctions regimes.

The central puzzle of this research is understanding how these actors exploit cryptocurrencies to bypass traditional sanctions mechanisms and why current sanctions are ineffective in preventing this. By examining the role of cryptocurrencies, this thesis seeks to uncover the methods employed by Garantex actors to evade financial restrictions, contributing to the broader understanding of sanctions effectiveness in the digital age. Based on this puzzle, the primary research question is: How are Garantex actors utilizing cryptocurrencies to evade international sanctions, and what does this imply for the effectiveness of current sanctions regimes? Then by advancing a critical argument that Russia's intentional integration of cryptocurrency into its sanctions-evasion tactics represents the creation and evolution of an intricate, multi-dimensional, and adaptive financial ecosystem. This ecosystem stretches farther than simple opportunism. It's instead a systematic and coordinated response that seamlessly integrates numerous actors across the public and private sectors. The cryptocurrency landscape within Russia involves diverse methodologies, including stablecoin transactions, decentralized exchanges, peer-to-peer (P2P) crypto markets, sophisticated crypto mixers designed to obscure transaction trails, decentralized finance (DeFi) protocols, and even explicit state-endorsed initiatives such as the development of the Digital Ruble. Collectively, these digital financial avenues interact dynamically, continually evolving in response to global regulatory measures, technological advancements, and shifts in enforcement tactics.

Furthermore, the Russian state itself has demonstrably shifted its stance from initial skepticism and cautious observation toward strategic endorsement and active facilitation of cryptocurrency adoption. For example, the head of the Duma's financial market committee Anatoly Aksakov said, "previously, there were fears that the legalization of cryptocurrency could create problems for the development of the domestic market. While cryptocurrencies may help Russia to bypass Western sanctions, their use is an objective phenomenon and cannot be ignored" (Bitcoinist, 2024). Recent legislative measures and regulatory shifts explicitly promote the use of cryptocurrencies to reinforce economic resilience and mitigate the adverse impacts of sanctions. This official state endorsement has significantly empowered private enterprises and financial networks, leading to the rapid development of advanced infrastructures tailored explicitly to meet Russia's strategic economic and geopolitical objectives amid stringent financial isolation. These developments represent a profound conceptual transformation because cryptocurrencies are no longer peripheral or experimental financial tools but integral and strategic components of contemporary economic statecraft.

By systematically exploring both theoretical frameworks and empirical data related to cryptocurrency-facilitated sanctions evasion, this thesis provides critical insights into how Russia's comprehensive network of digital asset utilization effectively undermines traditional sanctions regimes. This research rigorously challenges prevailing assumptions regarding the continuing effectiveness of financial sanctions within the context of rapidly advancing digital technologies. In doing so, it questions whether current international regulatory frameworks

possess sufficient adaptability, agility, and technological sophistication to counter these sophisticated and continuously evolving evasion strategies effectively.

Ultimately, the evidence and analyses presented within this research argue compellingly for a fundamental reassessment and strategic evolution of sanctions enforcement practices. In an era increasingly dominated by decentralized digital financial platforms and technologies, conventional enforcement mechanisms including blacklisting entities, restricting banking access, and freezing traditional financial assets must urgently adapt or risk becoming obsolete. The detailed case analysis vividly demonstrates how sanctioned entities can and do increasingly employ innovative, digital-centric financial methodologies to evade international regulatory frameworks. Thus, comprehending and addressing this emergent phenomenon is imperative, extending beyond mere economic considerations to encompass broader dimensions of global security and international cooperation.

2. Theoretical Framework

Modern sanctions regimes, which traditionally depend on centralized financial institutions to enforce asset freezes and blockades, are encountering heightened challenges in a global economy increasingly shaped by decentralized digital assets. In their study on economic coercion, Hufbauer et al. observed that a central premise of sanctions has been the ability to leverage major banks and international clearing systems as critical choke points, compelling targeted entities to comply with external demands (Hufbauer et al., 2007). Yet once cryptocurrencies entered the financial landscape, that premise began to weaken in ways that reshaped the conversation around sanctions efficacy. Later, the blockchain concept began to take shape with Casey and Vigna, emphasizing that digital assets operate on distributed, cryptographically secured networks, circumventing the reliance on traditional banking infrastructure (Casey and Vigna, 2018). Consequently, actors under sanctions and especially those facing significant Western penalties find cryptocurrencies a pathway to sustain cross-border financial operations.

In the specific case of Garantex, Connolly notes that a series of sanctions introduced after the annexation of Crimea in 2014 generated a concerted search for alternative instruments to resist Western pressure (Connolly, 2018). This search included diversifying trade partners, reinforcing domestic production, and strengthening ties with non-Western financial allies. Cryptocurrencies emerged as a novel and potentially transformative element within these broader strategies. Researchers such as Galeotti, who focuses on Russia's intersection of organized crime and state structures, argue that the country's financial elite, along with semi-criminal networks, naturally gravitate toward any mechanism that promises to undercut reliance on established global banking circuits (Galeotti, 2018). Building on top of this suggests that once technical

barriers to adopting digital assets recede, sanctioned entities can swiftly incorporate them into a pre-existing set of evasive tactics, thereby strengthening their overall resilience.

When Pape examines why sanctions frequently fail to shift the policies of targeted regimes, he reinforces that the ineffectiveness often stems from the adaptability of sanctionees, who find avenues to sustain core economic functions (Pape, 1997). Cryptocurrencies, by offering pseudonymous and sometimes privacy-enhanced transaction methods, effectively grant these avenues a global scale. These methods allow for near-instantaneous transfer of wealth, often beyond the scope of conventional AML (Anti-Money Laundering) systems. This evolution not only challenges the assumption of Western-led sanctions having universal reach but also introduces a paradigm in which the cost of enforcement escalates quickly. A critical crux of the regulation is regulators must keep pace with a technology that was not designed with government oversight in mind and that thrives in a borderless online environment. Yet, Bureaucracies are inherently slow, not by intention but more of an unintended consequence of the system.

Drezner, in his exploration of international financial statecraft, suggests that successful sanctions typically rely on international coalitions that can collectively police financial inflows and outflows (Drezner, 2011). This becomes problematic if sanctioned actors rely on decentralized networks rather than centralized bank accounts. Building on Drezner's viewpoint, it's important to note how cryptocurrencies accelerate the fragmentation of financial oversight, making it more likely that at least one jurisdiction, exchange, or decentralized protocol remains accessible to sanctioned users. These users, in turn, exploit the technology to move funds across multiple wallets, often layering transactions through mixing services to obscure origin and destination. Mixing services are systems for deliberately severing the on-chain link between the sender and the eventual recipient of a crypto-asset. They pool many users' coins together, reshuffle them through algorithmic randomness, and pay each participant back an equivalent value and usually to a brand-new address so that outside observers can no longer tell whose money became whose. As a result, the regulated points of contact that once could be coerced such as correspondent banks are no longer the only vital links in the financial chain.

All of these shifts highlight the need for a theoretical framework that blends insights from international political economy, criminology, technological innovation studies, and historical analyses of sanctions evasion. Examining only the macro-level policy environment would fail to capture how specific crypto protocols facilitate cross-border transfers, just as focusing solely on the technical details of blockchain transactions would overlook the strategic motivations driving adoption among sanctioned actors. This study's integrated approach therefore draws on four theoretical pillars: Disruptive Innovation Theory, Transnational Organized Crime Theory, Network Theory, and Sanctions Busting Theory to illuminate distinct dimensions of Russian crypto-based sanctions evasion. While each theory brings its own lineage and focus, they collectively address why cryptocurrencies hold a particular allure for sanctioned entities, how

criminal and state-aligned networks cooperate across borders, which structural features of decentralized ledgers enable rapid adaptation to enforcement, and why efforts to tighten sanctions appear to spur new phases of illicit innovation rather than definitive compliance.

Through this blended lens, the subsequent sections will articulate in detail how disruptive financial technologies degrade the coercive strength of sanctions, how Russia's complex nexus of criminal and political interests co-opts such innovations, how network structures enhance or limit the reach of enforcement, and how sanctioned actors perpetually adjust to novel restrictions. The essential tension lies in whether sanctioning powers can modify their policies and the international financial architecture can act fast enough to keep pace with a technology that thrives on decentralization and a target that has historically demonstrated resilience in evading external pressures.

2.1 Disruptive Innovation Theory

Disruptive Innovation Theory, primarily associated with Christensen's research on how nascent technologies unexpectedly undermine entrenched market leaders, provides a vital lens through which to interpret the transformative impact of cryptocurrencies on global financial oversight. When Christensen (1997) first delineated the concept, he described how novel products or services, initially perceived as too niche or lacking in mainstream appeal, could refine their capabilities until they threatened or even displaced well-established incumbents. In the current financial environment, cryptocurrencies epitomize that disruptive trajectory because they bypass conventional banking systems and the centralized authorities that typically enable effective sanctions enforcement.

Casey and Vigna (2018) emphasize that blockchain-based assets negate the conventional reliance on interbank settlement processes, forging peer-to-peer mechanisms where validation occurs collectively through cryptographic protocols rather than through banks or governmental clearinghouses. By removing these once-crucial institutional mediators, cryptocurrencies open channels of value transfer that prove inherently resistant to standard forms of regulatory control. This resistance holds significant consequences for sanctions regimes that have traditionally hinged on blocking adversarial actors' access to dollar-clearing services or mainstream financial channels. Extending Christensen's original thesis, the critical point of a disruptive technology is that incumbents, including regulatory bodies, are often slow to recognize or react to its potential. This lag gives early adopters and including those under sanctions an unanticipated advantage, enabling them to craft and refine evasion tactics before the broader system adapts to the new threat.

Regulatory hesitance or uncertainty, which Christensen (1997) saw as a frequent response to emerging market interlopers, is particularly evident in the realm of decentralized finance.

Many central bankers initially dismissed digital currencies as speculative curiosities, and it was only after major exchanges began processing billions in trading volume that policymakers began exploring tighter oversight (Casey and Vigna, 2018). Consequently, illicit actors discovered ample room to exploit crypto platforms that operated in regulatory gray zones, often in countries lacking stringent know-your-customer rules. This mismatch between crypto's global growth and inconsistent regulatory frameworks exemplifies the "early-stage advantage" identified by Christensen (1997), where new market entrants face limited competition or pushback from incumbents and here, the incumbents being national treasuries and transnational financial monitoring bodies.

The intrinsic disruptive essence of cryptocurrencies does not end with their capacity to relocate transactions beyond bank-based gatekeepers which are primarily just traditional banks that play a role in mediating or controlling financial transactions. It extends to how they enable entirely new organizational models, such as decentralized autonomous organizations (DAOs) and decentralized exchanges (DEXs), that subvert the hierarchical logic of traditional finance. In a sanctions context, sanctioned entities that were once forced to rely on complicit banks or shell companies can now tap into DEX liquidity pools or launch pseudo-anonymous ICOs. This possibility reflects Christensen's (1997) description of disruption as a fundamental reconfiguration of how industries or in this case, global financial flows are structured.

The Russian embrace of crypto channels, particularly after the Crimean sanctions, illustrates how quickly disruptive technologies can be woven into state strategies, even if initially adopted by fringe or experimental users. Where Drezner (2011) notes that effective sanctions depend on a shared alignment of major financial powers, cryptocurrencies drive a wedge into this alignment by allowing sanctioned parties to eschew traditional gatekeeping altogether. Because they review, approve, or sometimes deny transactions based on regulatory requirements and compliance with external laws (such as sanctions). This dynamic further validates Christensen's insight that once disruptive tools gather enough momentum and user adoption, attempts at containment often prove reactive and insufficient. For instance, while some Western jurisdictions introduced stronger AML requirements for crypto businesses, many smaller nations, or those seeking to court investment without Western interference, remain amenable to lightly regulated platforms that willingly serve Russian clientele under sanction. This patchwork enforcement environment stands as a textbook case of what happens when incumbents as global regulators have to face a technology that can so easily operate across borders and in partial secrecy.

Another critical piece of Christensen's theory is that disruptive innovations do not merely compete on price or scale, but on entirely new value propositions. Cryptocurrencies offer an unprecedented blend of pseudonymity and global reach, features that sanction-evading actors prize above everything else. They also confer autonomy from existing financial norms because

once an individual or institution acquires crypto holdings, they can transact or hold those funds without requiring the continued cooperation of banks subject to Western regulations. This independence is precisely what Christensen flags as a key element of disruption, since it redefines users' needs and sets new performance metrics (1997). For sanctioned Russian entities, the new metric is ensuring undisrupted capital mobility despite external pressure. This becomes attainable in a system that is not only decentralized but also inherently border-agnostic.

In addition, Casey and Vigna (2018) point out that as blockchains mature, they incorporate additional layers of functionality, such as smart contracts and interoperability between chains, which expand the array of evasion tactics. These functionalities enable cross-chain swaps and complex structuring maneuvers that can confound even the most tech-savvy enforcement agencies. Drawing on Christensen's framework, it is evident that incremental improvements in the crypto ecosystem such as better user interfaces, faster transaction speeds, and more private channels raise the overall disruption quotient, giving sanctioned users an even bigger edge. In short, disruptive innovation not only revolutionizes how transactions are validated but also continuously spawns offshoots and enhancements that challenge regulators to stay updated.

To interpret this iterative process as a contributing factor to the cyclical nature of sanctions evasion: with each new wave of enforcement, sanctioned parties find slightly upgraded or novel crypto tools to circumvent restrictions. Regulators, in turn, scramble to incorporate these emergent methods into compliance requirements, but they often trail behind the pace of development. Casey and Vigna (2018) call this gap the "innovation void," referring to the period during which criminals or sanctioned actors exploit the features of a new system while the incumbent structures remain partially blind to it. The result is a scenario in which Russia or any similarly sanctioned entity effectively harnesses the ongoing disruption in blockchain finance to remain a step ahead of the most widely used enforcement tactics.

Alternative innovation theories (such as general technological diffusion or routine innovation models) do not capture this dynamic as sharply. For instance, one might explain crypto adoption by sanctioned Russians purely in terms of rational choice or necessity. However, Disruptive Innovation Theory provides a richer insight by framing it as part of a broader pattern of incumbent-entrant competition. It highlights how the global banking regime (incumbent system) was structurally unprepared for a technology that operates outside its governance. Much like phone companies initially were unprepared for the internet. This theory thus prevails in explaining why crypto was able to gain a foothold. As traditional financial institutions over-served the average user with heavy regulations and monitoring (which for sanctioned actors is a barrier), creating an opening for a simpler alternative. Other frameworks, such as diffusion of innovations (Rogers, 1962) or general fintech adoption models, might describe how new tech spreads, but they lack the explicit emphasis on the incumbency dilemma that is central to

understanding sanctions evasion. The disruptive lens captures the cat-and-mouse innovation race between regulators and sanctioned actors. A race very evident since 2014 when initial sanctions on Russia drove exploration of Bitcoin, and accelerating after 2022.

Ultimately, Disruptive Innovation Theory reveals why cryptocurrencies pose such a formidable challenge to the sanctions architecture: they represent not just a minor extension of digital payment systems, but a radical shift in the locus of financial control. Christensen (1997) asserts that disruptive technologies often empower new players who were previously relegated to the margins. In the sanctions context, these new players include Russian crypto exchanges, private wallet providers, peer-to-peer trading networks, and decentralized finance protocols, all of which operate beyond the immediate jurisdiction of Western-led institutions. That freedom erodes the effectiveness of blacklists and asset freezes, leaving the sanctioning coalitions with fewer pressure levers to force behavioral changes in the targeted actors. It seems that this transition exemplifies a double disruption phenomenon where not only do cryptocurrencies challenge the incumbent global banking system, but they simultaneously erode the viability of economic coercion, a fundamental instrument of international statecraft.

2.2 Transnational Organized Crime Theory

Transnational Organized Crime (TOC)theory asks how illicit entrepreneurs manufacture, move, and safeguard value beyond the reach of any single sovereign. Since the late 1980s the field has evolved into a genuinely interdisciplinary field, integrating a plethora of criminology, economic sociology, critical geography, international political economy, and, more recently, digital‑platform studies. This resulted in what Levi (2002), called a global “security quilt” of legislation, regulations and institutions aimed at dealing with illegal money flows. Because the thesis traces how Russian non‑state actors launder cryptocurrency to elude sanctions, TOC is less a distant theory than the interpretive frame that clarifies why crypto flows circumvent policy intent whenever regulators lag behind technical innovation.

Early work replaced Mafia folklore with market reasoning. As an early example, Reuter’s case using ethnography of Los Angeles cocaine wholesalers demonstrated that traffickers fine‑tune bulk‑pricing formulas in response to fluctuating seizure rates, signalling that illicit entrepreneurs use the same risk‑return calculus as commodity traders (Reuter, 1983).
Nikos Passas extended this insight with regulatory asymmetry, observing that shipment routes shift dynamically toward jurisdictions where compliance costs dip below projected profits (Passas, 2003). In sanctions‑evasion space, the logic appears in Garantex’s decision to move servers to Moscow’s Federation Tower after Estonian regulators tightened licensing. A relocation that preserved customer liquidity while sheltering the exchange behind opaque Russian corporate shells.

Geographical literature sharpens the causal chain. Peter Andreas conceptualises borders as both barriers and funnels, stressing that enforcement surges often reroute rather than halt contraband (Andreas, 2000). Blockchain data exhibit an identical pattern because when OFAC blacklisted Suex in September 2021, ransomware payments detoured through Garantex in less than forty-eight hours, a migration captured in Chainalysis heat maps that depict address clusters hopping between exchanges like commuters changing subway lines (Chainalysis, 2025). Empirical confirmation also arrives in U.S. Customs and Border Protection's analysis of rail-export manifests, which warns that "the lack of detailed electronic manifest data … impedes CBP's enforcement efforts on rail exports" (U.S. Customs and Border Protection, 2025). FATF's 2023 report echoes the point, noting that only ten G-20 jurisdictions fully implement Travel-Rule metadata transfers, leaving hop-scotch corridors open for crypto mixers (FATF, 2023). For policymakers, the lesson is plain, harmonization glitches amplify systemic risk far beyond their apparent administrative triviality.

TOC theory then shifts the lens from where opportunities lie to who brokers them. Carlo Morselli's network analyses reveal that actors positioned in structural holes enable illicit systems to reconfigure after enforcement shocks (Morselli, 2009). This explains why secondary Russian brokers on Telegram could pivot to OTC trades denominated in Tether within days of the Hydra takedown. Extending the argument, Edwards and Gill's nodal governance model depicts crime control as a choreography of interdependent nodes each possessing partial authority over access to markets (Edwards & Gill 2003). In the crypto realm, a Latvia-based payment processor that ignores enhanced due-diligence flags becomes as crucial a node as any physical port, because it anchors the fiat off-ramp stage of laundering. Analytically, the thesis therefore treats Garantex not as a stand-alone entity but as one hub embedded in a wider aray.

Digitalization magnifies both reach and vulnerability, making TOC's arbitrage and adaptation visible in real time. The U.S. Department of Justice recounts that access to German hosting infrastructure enabled the seizure of Hydra's $25 million Bitcoin reserve in April 2022, providing insight that jurisdictional chokepoints still bite even in cyberspace (DOJ, 2022). Yet Hydra's demise did not deflate laundering volumes; Chainalysis records $448 million in ransomware proceeds rerouted to smaller Russian-language mixers in 2023, illustrating crime's capacity to rebound through modular substitution (Chainalysis 2025). Soska and Christin's study of online anonymous marketplaces clarifies the mechanism, "reputation systems and multisignature escrow contracts provide powerful, code-based enforcement that allows even novice vendors to transact at scale without resorting to violence" (Soska & Christin, 2015). In sanctions-evasion terms, the implication is glaring because regulatory blacklists disrupt centralized exchanges but leave the long tail of algorithm-mediated OTC desks largely intact until coding standards embed compliance by design.

Adaptive-systems modelling adds another layer as to why piecemeal crackdowns can backfire. Manzi and Calderoni's agent-based MADTOR simulations show that "surviving organizations face increasing recovery difficulties as more members are arrested," revealing a non-linear, diminishing-returns pattern that forces networks to re-route logistics and restructure roles. Essentially a hydra effect that multiplies complexity rather than reducing capacity (Manzi & Calderoni, 2024). This mirrors the post-Suex landscape, where ransomware affiliates shifted from Bitcoin to Monero to sidestep traceability, a chain-hop documented in Chainalysis typology charts. The adaptive-systems lens therefore supports the thesis recommendation that enforcement focus on chokepoint harmonization and shared KYC rule-sets, interoperable sanctions lists, and smart-contract auditing, rather than headline-grabbing arrests that merely scatter threats across harder-to-monitor platforms.

The evasion of sanctions by Garantex actors via cryptocurrency can be compellingly explained through Transnational Organized Crime Theory. At its core, sanctions evasion is merely an illicit enterprise. It involves moving prohibited value across borders covertly, akin to smuggling funds. TOC theory captures the organized, networked, and cross-border nature of this behavior. Sanctioned oligarchs and their facilitators often operate like a transnational criminal network: they utilize shell companies in offshore havens, enablers in third countries, and now cryptocurrency exchanges, to launder money and bypass financial controls (Allison & Erausquin 2023). By applying TOC theory, it's easy to frame these individuals not just as isolated sanction cheats, but as part of a broader organized illicit network responding to the market opportunity created by sanctions (the opportunity being the premium on moving funds secretly).

One important aspect of TOC theory is the exploitation of jurisdictional asymmetries, and this is clearly present in Russian crypto evasion. For example, while the US and EU enforce strict sanctions, certain third countries (e.g. in the Middle East or post-Soviet states) do not impose those sanctions. Evasion networks take advantage of this by routing transactions through exchanges or banks in those third countries which is precisely the behavior TOC scholars describe where third-party facilitators or "black knights" undermine economic restrictions (Early, 2011). A recent analysis by RUSI (2023) identified five categories of Russian sanctions evasion, including the use of financial facilitators in third countries and complex corporate networks. This mirrors classic organized crime tactics: just as drug cartels use transit countries to move contraband, sanctioned Russians use friendly jurisdictions and crypto platforms there to move money. TOC theory's emphasis on networks of cooperation helps explain how, for instance, a Belarusian OTC broker, a UAE shell company, and a Russian exchange might collude to transfer crypto that ultimately converts to cash for a sanctioned oligarch. These are effectively transnational crime networks, with each node playing a role (technical expert, money mule, complicit business, etc.) and it shares an analysis not readily gleaned from a purely economic or political theory of sanctions.

A purely international relations theory (e.g. Realism or economic statecraft theory) might view sanctions evasion in terms of state behavior or policy failure, but might underplay the criminal entrepreneurship at work. Transnational Organized Crime Theory brings into focus the profit motive and illicit skillsets of actors who facilitate evasion. Many sanction evasion schemes are essentially profit-making ventures for facilitators (for example, crypto exchange operators charging fees to move sanctioned funds). TOC theory accounts for this by treating sanction-busting as a service provided by illicit networks as akin to money laundering services for drug money. Moreover, TOC theory helps situate Russian crypto evasion in the continuum of organized crime activities because it often involves the same actors or methods used in organized crime (corrupt bankers, false documentation, clandestine movement of value). For instance, a sanctioned oligarch hiding assets in Bitcoin may rely on the same offshore lawyers and front companies that an arms trafficker or corrupt official would use. Thus, TOC theory unifies what might seem like contrasting elements (cybercrime, money laundering, sanctions evasion) under one conceptual roof because they are all part of the illicit transnational economic activity that thrives in an age of globalization.

In practice, the study will leverage TOC theory to identify patterns. For example, if it's observed that all major evasion cases involve a small set of other exchanges or intermediaries, that suggests an organized network effect rather than coincidence. TOC theory acts as a guide to look for structures (who is connected to whom?) and processes (how illicit value is moved?) that are characteristic of organized crime. It also highlights the importance of things like safe havens and corrupt officials, which we will keep in mind as potential explanatory factors (for instance, why Garantex could operate is possibly due to tacit state tolerance or protection, a classic TOC feature). In sum, Transnational Organized Crime Theory enriches an understanding by framing Russian crypto-based sanctions evasion as not just individual circumvention, but as the work of adaptive, profit-driven illicit networks operating across borders. Ultimately, a perspective that is essential for a holistic explanation.

2.3 Network Theory

Network Theory is based on the importance of connections. Essentially, the ties linking individual nodes, rather than focusing solely on the attributes of each node in isolation. Barabási, in his work on complex networks, observes that many real-world systems exhibit scale-free properties, where a small number of nodes hold disproportionately large numbers of links, forming "hubs" that mediate flows across the network (Barabási, 2003). In cryptocurrency ecosystems, these nodes might take the form of centralized exchanges, over-the-counter brokers, or mixer services that channel high transaction volumes between disparate parts of the blockchain. Once a node achieves hub status, it becomes integral to how funds circulate among smaller wallet clusters, sometimes exerting a "choke point" effect that enforcement agencies

could exploit. Conversely, the presence of multiple hubs or the emergence of new, undiscovered hubs ensures that illicit actors under sanctions can rapidly re-route flows if one path becomes compromised. This phenomenon highlights the adaptive resilience of networked crypto transactions and explains why single crackdowns, such as sanctioning a particular exchange, often yield only temporary disruptions.

Network Theory is crucial for this thesis because crypto-based sanctions evasion is inherently a networked phenomenon. Each cryptocurrency transaction creates a link between two addresses; cumulatively, these links form a transaction network. Simply looking at individual transactions or actors in isolation would miss the larger picture of how illicit flows are organized. By applying Network Theory, it's easier to identify patterns and key nodes in the web of crypto transactions that facilitate sanctions evasion. For instance, an oligarch might use ten different Bitcoin addresses over time and network mapping can show if those addresses all funnel through one or two intermediary wallets (suggesting a central hub in their evasion scheme). Network analysis can also uncover previously unknown connections. Perhaps two sanctioned individuals, thought to operate separately, in fact share common counterparties or co-use the same exchange, meaning their evasion networks converge. Traditional analysis might not catch that, but by visualizing and measuring the network, such overlaps become evident.

Using concepts like centrality (explained above), it's to quantitatively pinpoint which actors or platforms are most crucial in the evasion network. For example, if a particular stablecoin address (say a Tether treasury address) has very high betweenness centrality in the flow network, it means many evasion paths rely on that address as a bridge. This could indicate a chokepoint where enforcement could focus (e.g., pressuring Tether to freeze that address). On the other hand, if the network is very decentralized with no obvious hubs then enforcement must adapt strategy. Meaning no single takedown will suffice because a broader net is needed. In short, Network Theory provides the analytical umph to assess resilience vs. fragility of the evasion network. Is the crypto network spider's web that breaks if the center is cut, or a starfish network that regenerates if a limb (node) is removed? Empirical analysis will guide these conclusions as well. But this is far more informative than a simple list of bad actors.

Network Theory also serves as a bridge between the other theoretical pillars. Disruptive Innovation gave the technological premise of how crypto introduced a new system; TOC gave the actor premise of organized illicit collaboration; Network Theory knits these together by analyzing the structural premise: how actors utilize technology to form a functional evasion network. It operationalizes concepts from TOC theory (e.g., "flexible networks" and "cells") into measurable elements. For example, TOC theory might say Russian evaders form cells to move funds; Network analysis can test this by detecting clusters of addresses that interact densely internally but have few external links (a structure indicative of cell-like subgroups). Likewise, if Disruptive Innovation suggests crypto evasion evolved organically in niches, Network Theory

could trace the growth of the network from a small cluster to a larger web over time, thereby illustrating the disruptive upmarket climb in network terms (perhaps an initially sparse network becoming more richly connected and capable).

In conclusion, Network Theory is justified in this study because sanctions evasion via crypto is a network problem: multiple actors, multiple transactions, across multiple platforms. It provides clarity on the architecture of evasion and where the pressure points and weak links are. This information is vital for both analytical completeness and for any policy recommendations on disrupting these networks. It transforms a complex tangle of transactions into a discernible map of illicit flows, which is indispensable for achieving this research's objectives.

2.4 Sanctions Busting Theory

Sanctions Busting Theory illuminates how states and organizations subject to external economic constraints systematically seek and discover ways to continue pursuing their strategic goals, an idea reinforced by Early, who notes that "sanctioned actors are not passive recipients of coercion; they are active innovators, endlessly probing for weaknesses in the enforcement net" (Early, 2015). This propensity for adaptation means that each time sanctioners impose tighter rules or refine monitoring techniques, the sanctioned party devises new channels or partners to circumvent the measures. In a broader historical context, Hufbauer et al. highlight that sanctioned states, from Zimbabwe to Iran, have consistently demonstrated this pattern, using methods such as reflagging vessels, barter deals, and shell companies (Hufbauer et al., 2007). The emergence of blockchain-based currencies adds a new layer of sophistication to the cycle of sanctions evasion, because it creates opportunities for obfuscation and cross-border transactions on an unprecedented scale.

Katzman, examining Iran's sanctions evasion, remarks that when formal banking options vanish, actors turn to informal mechanisms and alternative value transfer systems (Katzman 2019). Cryptocurrencies represent perhaps the ultimate alternative, since they allow sanctioned individuals to transact directly with one another without needing correspondent banks or large financial institutions. It appears that Russian elites who find themselves barred from Western capital markets, adopting Bitcoin or other digital assets is not just a tactical move; it fits neatly into a broader tradition of resourceful workaround strategies that have historically kept targeted states afloat under external pressure. Cryptocurrencies, by featuring pseudonymous wallet addresses and rapid settlement times, supercharge the speed at which these workaround strategies can operate, allowing flows to traverse the globe without registering in conventional trade or banking data.

One of the recurring themes in sanctions busting, as Early (2015) points out, is that sanctioned actors generally enjoy first-mover advantages within their own illicit networks. They

understand local constraints and often have direct relationships with complicit or poorly regulated entities willing to process their transactions. In Russia's context, oligarchs or state-connected actors can leverage longstanding ties with foreign businesses or financial brokers to funnel crypto-based funds through discrete channels, continuing to engage in activities like purchasing high-value assets or funding overseas ventures that sanctions were meant to block. The synergy between these relationships and the borderless functionality of digital assets embodies what Hufbauer et al. refer to as "prolonged defiance," in which the targeted party establishes sustainable avenues to do business despite the outward appearance of severe financial isolation (Hufbauer et al., 2007).

Moreover, the cyclical nature of sanctions busting means that when the West cracks down on a particular crypto exchange or wallet associated with Russian entities, new addresses or platforms instantly spring up to fill the void. Connolly, focusing on Russia's broader strategies, notes that adaptation is a constant theme in how the Kremlin deals with external pressure (Connolly, 2018). By integrating cryptocurrencies into this adaptation model, sanctioned actors can pivot from one service to another, layering transactions, splitting large amounts into smaller increments, and combining them again. The overarching idea here is that this iterative dynamic places enforcement agencies in a reactive posture, chasing leads and shutting down known addresses only to discover that new clusters have surfaced elsewhere, often operating under fresh domain names or newly minted wallets. Katzman's observations about Iran's use of myriad front companies parallel this Russian scenario because in both cases, digital anonymity reduces the cost and difficulty of establishing such fronts (Katzman, 2019).

The possible creation of a Crypto Ruble, as first reported by CoinTelegraph, raises another intriguing dimension (Buck, 2017). If Russia were to implement a state-backed digital currency, it could do so under a legal framework that normalizes crypto usage within its borders, potentially insulating the currency from Western interference and weaving it into official trade relationships with select countries. This very act would institutionalize sanctions busting on a sovereign level, integrating blockchain-based systems into formal policy rather than relying on ad hoc usage by oligarchs or criminal intermediaries. While it remains speculative how successful such a project might be, Sanctions Busting Theory implies that any means of evading or neutralizing external pressure will be aggressively explored. A national digital currency, if it can attract counterparties willing to defy Western rules, could carve out an alternative financial ecosystem anchored by a Russian regulatory and payment infrastructure.

Then again, Early (2015) also highlights that sanctions busting often thrives in geopolitical climates where multiple powers are not aligned with the sanctioning coalition. Russia, having formed or deepened alliances with China and other non-Western states, may find external partners ready to transact in digital assets or bilateral trade agreements that bypass Western financial systems. This alignment erodes the clinch that gives Western sanctions teeth

and emboldens Russia to accelerate crypto adoption. Cryptocurrencies, as a globally accessible network, dovetail with the necessity of building cross-border trade without passing through markets dominated by U.S. or EU jurisdictions. On a more technical level, mixers, decentralized exchanges, and cross-chain bridges further reduce the friction that used to slow down alternative routes for financial transactions.

It is important to note that sanctions busting has not always yielded decisive victory for targeted states; Hufbauer et al. stress that in many historical cases, evasion partially mitigates the damage but rarely fully nullifies the combined economic pressure (Hufbauer et al. 2007). However, the presence of digital assets changes the speed and scope at which these partial mitigations can unfold. Whereas setting up a network of shell companies or smuggling routes might require months or years, generating a new set of blockchain addresses takes mere minutes. This expansion of speed and global reach suggests that modern sanctions busting and especially in technologically adept countries like Russia, achieve a level of real-time evasion that few earlier examples can match. The overall implication is that Western actors must consistently update their enforcement playbooks, venturing into technical realms like blockchain analysis to remain effective in blocking these new channels.

In sum, Sanctions Busting Theory reveals an ongoing cat-and-mouse cycle, wherein every clampdown by sanctioning coalitions spurs innovation among sanction targets. Building on the insights of Early (2015) and Hufbauer et al. (2007), Russian actors adoption of cryptocurrency-based methods to sidestep restrictions exemplifies how a state combines historical patterns of evasion with modern decentralized technologies to preserve critical financial functions. Whenever a specific wallet address or exchange is blacklisted, a host of alternative addresses or services emerges and some are even legitimate but unregulated, others blatantly complicit in laundering schemes. The cycle continues indefinitely, driven by the inherent adaptability of blockchain-enabled transactions and the willingness of Russia's political and economic elite to push the boundaries of compliance. This phenomenon highlights the very essence of sanctions busting which is a perpetual search for and exploitation of loopholes by sanctioned actors determined to safeguard their economic lifelines.

2.5 Synthesis of Theoretical Perspectives and Link to Empirical Analysis

A synthesis of the four perspectives begins with Disruptive Innovation Theory, which explains how permissionless blockchains shattered the core design assumptions of twentieth-century financial regulation. Because cryptocurrencies validate transactions through decentralized consensus rather than correspondent banks, they sidestep every institutional choke point that traditional sanctions regimes were built to exploit. The theory's signature insight is the incumbent's dilemma. This is where regulators and legacy institutions, optimized for incremental tweaks to familiar rails, react too slowly to a technology that offers a wholly new value

proposition. In this case that is borderless transfers inside an adversarial network. That lag creates an innovation window in which early adopters, including sanctioned actors, prototype evasion tactics before rule-makers grasp the threat. Into that window pours the logic of Transnational Organized Crime Theory. Where Disruptive Innovation sketches the technological supply, TOC identifies the entrepreneurial demand of brokers, OTC desks, mixers, shell-company agents, and complicit professionals who converge on the new rails because arbitraging regulatory asymmetries is profitable. TOC emphasizes that these facilitators operate as market intermediaries, stitching together buyers of secrecy and sellers of technical expertise. Just as narcotics traffickers long exploited gaps between customs regimes, crypto launderers exploit gaps between financial-crime frameworks. The result is an illicit service industry that industrializes sanctions evasion, packaging wallet-obfuscation, cross-chain swaps, and fiat off-ramps as products.

Network Theory zooms out to reveal how those products interlock. Empirical mapping of block-chain flows shows a small number of hubs which are usually major exchanges, high-volume mixers, large OTC brokers who often carry a disproportionate share of value, while a long tail of small nodes provides redundancy. This topology matters for sanctions because it couples efficiency with resilience. High-betweenness hubs speed transactions, but if enforcement knocks one off-line, value can reroute along alternative bridges almost instantly. Essentially, removing one hub, and its spokes reattach elsewhere or new hubs emerge. Thus network structure institutionalizes the cat-and-mouse dynamic noted by scholars earlier. That dynamic is formalized in Sanctions Busting Theory, which treats evasion as an iterative feedback loop. Each regulatory tightening of an OFAC blacklist, an EU travel-rule mandate, a FATF recommendation effectively alters the cost landscape. Evasion networks respond by shifting tactics and spinning up new wallet clusters, migrating to privacy-enhanced chains, leveraging DAO treasuries, or sheltering under jurisdictions that resist compliance pressure. Sanctioners then adjust, prompting yet another round of innovation. The theory's crucial lesson is once an actor masters a disruptive tool and embeds it inside a durable network, every enforcement nudge yields diminishing returns unless accompanied by system-level reforms. Whether that be cohesive KYC standards or real-time cross-border data sharing. Integrated, the four theories depict a self-reinforcing ecosystem.

Moreover, Russia's non-traditional methods would be reflected in the proactive creation of transient financial hubs which are just digital equivalents of shell corporations that appear and disappear rapidly on blockchain ledgers, thwarting traditional compliance and investigative techniques. The inherent resilience described by Network Theory would enable a dynamic financial architecture that can reconstruct itself almost instantaneously in response to external pressure. Rather than merely reacting to enforcement measures, this architecture would proactively anticipate potential disruptions, distributing financial flows across multiple alternative pathways even before any single route is compromised.

In this synthesized theoretical perspective, sanctions evasion is not an isolated act but a continuously evolving practice, deeply embedded within Russia's statecraft and geopolitical strategy. Sanctioned actors would consistently innovate and iterate their techniques in alignment with Early's understanding of sanctions busting as cyclical and adaptive. As Western regulators target specific crypto exchanges or wallets, Russian entities would respond by diversifying their financial mechanisms, potentially exploring state-endorsed digital currencies like a Crypto Ruble or integrating blockchain-based finance into official institutional frameworks to render sanctions fundamentally less effective. This theoretical synthesis stresses a critical reality for policymakers where traditional financial sanctions mechanisms are ill-equipped to counteract the agility and adaptability enabled by blockchain-based evasion. Therefore, future regulatory responses must emphasize real-time blockchain analytics, proactive rather than reactive enforcement, and significantly enhanced international coordination. It necessitates a comprehensive understanding that sanctions evasion through cryptocurrencies will likely become standard practice rather than an exceptional scenario.

Moving forward, the analysis section of this research will apply this synthesized theoretical model, examining concrete instances of cryptocurrency use linked to Russia's sanctioned entities. By closely tracking digital asset flows, analyzing specific blockchain-based evasion techniques, and evaluating pilot programs or state-sponsored crypto initiatives, the research will empirically validate whether these theoretical dynamics accurately capture the complexity and innovative nature of Russia's sanctions evasion methods. Ultimately, this combination of theoretical synthesis and empirical investigation aims to provide critical insights into how evolving digital strategies can be effectively countered through equally innovative and agile international governance measures.

3. Methodology

Having established a multi-theoretical framework in the previous chapter, this chapter details the methodology for investigating the Garantex case – a single-case study of a Russian crypto exchange implicated in international sanctions evasion. The study employs a convergent mixed-methods design, integrating blockchain analytics (quantitative) with qualitative content analysis of investigative and regulatory sources. This chapter is organized as follows: 3.1 Research Philosophy outlines the pragmatist epistemological stance underpinning the study. 3.2 Research Design describes the convergent parallel mixed-methods approach and includes a diagram of our design logic. 3.3 Case Selection explains the rationale for focusing on the Garantex exchange, five specific Russian oligarchs, and the Digital Ruble pilot, addressing issues of typicality and external validity. 3.4 Data-Collection Procedures delineates how

qualitative data (e.g., reports from OCCRP, OFAC listings, RUSI analyses) and quantitative data (blockchain transaction records via web3.py and open-source explorers) were gathered, including inclusion/exclusion criteria and data schema. 3.5 Data-Analysis Procedures details how qualitative coding (with Taguette software, using inductive codes from theory and inductive codes from data) and quantitative network analysis (measuring transaction network metrics, temporal trends, anomalies) were carried out, and how the two strands inform each other. 3.6 Validity, Reliability & Trustworthiness discusses measures taken to ensure rigor, such as triangulation of data sources, intercoder reliability checks, maintaining an audit trail and chain-of-custody for digital evidence, and peer review of findings. 3.7 Feasibility reflects on practical considerations and limitations of data gaps, attribution uncertainties, evolving crypto protocols, and language biases with how the study mitigated these challenges.

3.1 Research Philosophy

This research is guided by the philosophical paradigm of pragmatism, which is well-suited for a mixed-methods inquiry into illicit finance. Pragmatism, as articulated by philosophers like John Dewey and later methodologists like Morgan (2007), centers on the idea that truth is that which works in practice and that research should focus on solving concrete problems (Kaushik & Walsh, 2019). Instead of aligning strictly with positivism (which seeks a single objective truth) or constructivism (which emphasizes multiple subjective realities), pragmatism takes a middle path and it recognizes an external reality (e.g., actual transactions on blockchains) but also that our understanding of it is mediated by interpretation and context. The pragmatic worldview is typically associated with mixed-methods research because it legitimizes using both quantitative and qualitative methods to investigate a question, valuing each for the insights it provides.

In the context of illicit finance and sanctions evasion, a pragmatist stance is especially relevant. The phenomenon is complex, involving technical transaction data and human behaviors in socio-political context. A purely positivist approach might treat blockchain data as the only reality, missing the motives and meanings behind those transactions. A purely constructivist approach might gather narratives about evasion but risk neglecting hard evidence of actual money flows. Pragmatism allows this study to mix numeric evidence with narrative evidence. The pragmatic criterion here is usefulness. Meaning whichever method yields insight into this question is adopted. It's important to judge theories and findings by their ability to explain and predict patterns of evasion in a way that could ultimately inform effective responses, an inherently pragmatic outcome orientation.

Moreover, pragmatism emphasizes flexibility and adaptability. Illicit finance is a fast-evolving field (new evasion techniques, new regulations) and strict adherence to one methodology could be limiting. Under a pragmatist paradigm, the research design could evolve

as new leads emerge, an approach sometimes called “abductive” reasoning by moving back and forth between data and theory to find the best explanations. This is key for this study. That’s because initial qualitative scans informed what data to scrape quantitatively, and initial quantitative findings pointed to new documents to qualitatively analyze. Pragmatism encourages this iteration, because the ultimate goal is practical understanding.

Finally, pragmatism aligns with the illicit finance research context by acknowledging the real-world stakes. Sanctions evasion is not just an abstract theory problem; it affects global policy efficacy and security. A pragmatist researcher is comfortable making methodological choices that best capture this reality. For example, if tracking one oligarch’s transfers required unconventional data gathering (like parsing a leaked dataset), a pragmatist approach would accept that as valid. What matters is producing findings that are credible, actionable, and reflect the complex nature of the problem. By grounding the study in pragmatism, this thesis has a philosophical foundation that legitimizes our mixed-methods design and focuses on outcomes – namely, a robust, well-triangulated understanding of Russian crypto evasion.

3.2 Research Design: Single-Case Mixed-Methods Approach

The study employs a single-case study design with a convergent mixed-methods approach. In practice, this means that one case being Garantex serves as the unit of analysis, and within this case both qualitative and quantitative data are collected and analyzed in parallel. The choice of a case study strategy is appropriate because the research question demands an in-depth understanding of a contemporary phenomenon in its real-world context. Case studies are particularly useful in IR for exploring new or complex issues, allowing the researcher to draw on multiple types of evidence to build a rich understanding (Salmons, 2023). Notably, case study methodology is inherently inclined toward using multiple data sources; a single case can (and in this study does) encompass various forms of evidence (documents, legal records, transaction data) to capture different facets of the phenomenon. This aligns with Yin’s principle that case studies rely on triangulation of evidence to strengthen the validity of findings (i.e. converging information from different sources) (Yin, 2018).

Focusing on Garantex as a single case allows for a detailed institutional analysis that can illuminate broader patterns of sanctions evasion. Garantex is a Russia-linked cryptocurrency exchange that emerged as one of the most scrutinized platforms for potentially facilitating illicit transactions on behalf of Russian users. It was designated by the U.S. Treasury’s Office of Foreign Assets Control (OFAC) in April 2022 for involvement in illicit finance (OFAC, 2022), and subsequent investigations have documented how it continued operations despite sanctions, by exploiting permissive jurisdictions and frequently changing domains. In the span of a few years, Garantex reportedly processed enormous volumes of cryptocurrency (at least $96 billion

in transactions since 2019), of which an estimated $1.3 billion was tied to illicit or high-risk activities (Chainalysis, 2025). This makes Garantex a critical (and data-rich) example of the relationship between crypto exchanges and sanctions evasion. By drilling down into this case, the study can examine how an under-regulated exchange operates as a pivot point for evading international norms, and how enforcement actions interact with on-ground (or on-chain) realities.

The research design is convergent parallel, meaning the qualitative and quantitative components are conducted concurrently and with roughly equal importance, and then integrated. From the qualitative side, the study analyzes text-based sources (described in detail below) to understand narratives, motives, and normative questions surrounding Garantex and sanctions evasion. For example, how actors justify or conceal their actions, or how regulators frame the legitimacy and rule-of-law issues at stake. From the quantitative side, the study performs blockchain analysis to trace actual cryptocurrency flows through Garantex-linked wallets, measuring things like transaction volumes, frequency, and network connections. The two strands are designed to complement and inform each other where the qualitative analysis provides context (the "why" and "how") for the patterns observed in data, while the quantitative analysis provides concrete evidence (the "what" and "how much") that grounds and tests the qualitative insights. For instance, a news report might suggest that after a certain sanction was imposed, activity shifted to a new platform and therefore the quantitative data can then be checked to see if there was indeed a spike or shift in transactions corresponding to that event, thereby corroborating or nuancing the report. Conversely, if the blockchain data reveals an anomalous surge in transactions at a time or route not discussed in policy sources, it can prompt a closer review of qualitative materials to explain that anomaly.

A key feature of this design is methodological triangulation where early findings from one method shape the inquiry in the other, iteratively. For example, initial qualitative coding might highlight a theme of "jurisdictional arbitrage" (actors moving operations to avoid legal reach). This could lead the quantitative analysis to focus on whether Garantex transactions spiked when Russia's domestic regulations tightened or when certain countries took action, thus directly testing the qualitative insight. Likewise, if preliminary blockchain analysis identifies a cluster of addresses peaking in usage around a specific date, the researcher would return to the documents to see if any relevant event (e.g. a new OFAC advisory) occurred around that time. This back-and-forth enriches the analysis, consistent with a convergent design that values both strands equally and seeks a merged understanding. By integrating the results, the study can provide a more nuanced answer to the research question than either method alone. As another example, demonstrating not just that Garantex enabled X volume of evasion (quantitative result) but also explaining the mechanisms and normative implications of how it did so (qualitative result). The mixed-methods approach therefore enhances validity and depth, as each dataset helps to validate and elaborate the findings of the other. The design's convergent nature means that during analysis, neither the qualitative nor quantitative component is subservient; both are

developed in parallel and then converged. This approach reflects Creswell's (2009) model of mixed-methods integration, where the two types of data are merged to provide comprehensive insights. By anchoring narrative claims in empirical transaction evidence (and vice versa), the study increases its explanatory power and practical relevance.

Finally, it's worth noting that using a single-case study does pose considerations for generalizability. This case was selected as a typical and revelatory case. Typical in that Garantex exemplifies a broader class of unregulated exchanges used for evasion, and revelatory in that its public exposure provides unusually rich data. The findings from Garantex are not statistically generalizable to all cases of sanctions evasion; however, they are analytically generalizable in the sense of providing insights into mechanisms and challenges that likely apply in similar contexts (Yin, 2018). In IR literature, single-case studies can yield valuable theory-informed explanations, especially when the case is used to illustrate or probe theoretical concepts like legitimacy or sovereignty under stress. Thus, while caution is used in extrapolating results, the Garantex case is treated as an informative example that can speak to larger debates about the efficacy of sanctions and the adaptability of illicit networks.

3.3 Case Selection

To illuminate how Garantex and its actors exploit cryptocurrency for sanctions evasion, the thesis deploys a single case study approach. Garantex was chosen because of its prominence in investigative reports and enforcement actions as a hub for illicit transactions. Founded in 2019, and despite being officially registered outside of Russia, Garantex is believed to conduct substantial operations within Russia's jurisdiction. It attracted users specifically seeking to bypass strict know-your-customer (KYC) and anti–money laundering (AML) regulations, making it an ideal case to study the interaction between regulatory norms and illicit behavior.. For example, an OFAC notice (2022) reported that significant funds flowing through Garantex were linked to wallets under sanctions or associated with cybercrime. In April 2022, OFAC officially sanctioned Garantex, adding it to the Specially Designated Nationals (SDN) list for facilitating illicit finance. Around the same time, the U.S. Financial Crimes Enforcement Network (FinCEN) issued advisories highlighting Garantex's role in evading sanctions and warning financial institutions of its activities. Elliptic (2023), a blockchain analytics firm, further documented how Garantex continued large-scale operations post-sanction by frequently changing domain names and taking advantage of jurisdictions with lax oversight.

Despite these enforcement efforts, Garantex has remained operational (at least intermittently), showing how digital platforms can leverage regulatory gray areas to persist. For instance, an ICIJ investigation from 2024 found that wallets associated with certain sanctioned

individuals moved funds through Garantex, implying that oligarchs could convert assets under the radar (Laine et al., 2024). This connection illustrates why Garantex is a linchpin case because it sits at the intersection of individual sanction evaders (like oligarchs) and the broader ecosystem of illicit crypto flows. By examining Garantex, the study captures both the micro-level behavior of sanctioned actors and the macro-level structure of an enabling institution.

In defining the case boundaries, the thesis focuses on Garantex's operations and related events primarily between 2019 and 2025. This time frame covers Garantex's emergence, its growth amid increasing sanctions on Russia (especially after 2022), and the immediate aftermath of the exchange being severed by authorities. By bounding the case temporally, the research hones in on the period when cryptocurrency use in Russia notably expanded and became entangled with evading Western sanctions. The case's content scope includes any activities, transactions, or incidents involving Garantex that shed light on sanctions evasion. This encompasses Garantex's corporate actions (e.g. changes in jurisdiction or policy), its platform usage by known illicit actors, and the governmental or industry responses to its activities (sanctions, seizures, public reports). However, the case excludes unrelated aspects of the exchange (for instance, legitimate trading volume that has no bearing on sanctions issues) to maintain focus. The analytical attention is on Garantex as a facilitator of illicit finance in the sanctions context, not on Garantex as a whole business entity beyond that context.

By choosing Garantex as the single case, this thesis employs what methodology literature calls a crucial case or instrumental case approach (Crowe et al., 2011), the case is instrumental to understanding a broader phenomenon (crypto-based sanctions evasion) and is crucial in that it vividly exemplifies the challenges of enforcement. Garantex's characteristics of a high-risk exchange operating in a sanctions-targeted environment make it a typical case for the category of non-compliant exchanges, while also offering a critical case test of international regulatory mechanisms. In terms of typicality, many of the patterns observed (such as moving servers, rebranding, using stablecoins) are likely shared by similar exchanges, thus lessons learned may be applicable beyond Garantex. In terms of external validity, the thesis is cautious because it generalizes findings to theory (e.g. what it says about the effectiveness of international norms or the adaptability of illicit networks) rather than claiming statistical generalization. This is consistent with case study methodology standards, which prioritize depth and theoretical insight over breadth of cases. Ultimately, Garantex serves as a window into how a subset of Russian actors circumvent global financial rules, allowing an exploration of key IR concepts (legitimacy, sovereignty, rule of law, etc.) in a concrete setting. The next sections outline how data about this case was collected and analyzed to answer the research questions.

3.4 Data Collection Methods (Qualitative and Quantitative)

Data collection for the Garantex case combined multiple source types and modalities, in line with the convergent mixed-methods design. All data were gathered systematically using defined inclusion criteria to ensure relevance and reliability. Broadly, the thesis collected two categories of data in parallel. Firstly, qualitative textual data (documents and reports providing narrative and contextual information) and quantitative blockchain data (transaction records providing numeric and network information). This multi-source strategy is crucial for a robust case study, as using several independent sources of evidence allows for cross-verification and a richer understanding of the subject. Below, the data collection process is detailed for each component, including the types of sources, how many were used, why they were chosen, and how data inclusion was bounded.

For the qualitative component, a wide range of textual and documentary sources was gathered to capture insights into Russian crypto-based sanctions evasion as manifested in the Garantex case. The guiding principle was to include sources that shed light on the actions of Garantex and its context (e.g. reports of its illicit use, regulatory responses, relevant norms debates) from credible perspectives. The content had to relate directly to at least two of the three key topics like Russia, cryptocurrency, and sanctions with a clear linkage to Garantex or sanctions evasion. In practice, this meant documents explicitly discussing Garantex or more generally discussing how crypto is used by Russian actors under sanctions (given that Garantex often features in such discussions). For example, an investigative article on Russian sanctions evasion that mentions crypto exchanges would qualify, especially if Garantex is named or an analogous exchange is analyzed.

Preference was given to sources from reputable outlets or institutions. This included peer-reviewed academic articles, established news agencies (Reuters, Bloomberg, etc.), official government releases (e.g. U.S. Treasury press releases, OFAC announcements), and reports by respected research institutes or think tanks (such as the Royal United Services Institute RUSI, or blockchain analytics firms like Chainalysis and Elliptic). When less formal sources were used (like a blog post, forum discussion, or an OCCRP investigative piece featuring anonymous interviews), their information was cross-verified with other independent sources to ensure trustworthiness. This triangulation of document sources helps mitigate the risk of misinformation; for instance, a claim first seen on a crypto forum would only be considered if also reported by a credible news report or referenced in an official document.

The documents collected were published mainly between 2019 and 2025, covering the rise of crypto use in Russia and especially the post-2022 period when sanctions intensified due to geopolitical events (notably, Russia’s invasion of Ukraine in 2022 led to an escalation of sanctions). This timeframe captures the most relevant developments in Garantex’s operations and

the surrounding policy discourse. Earlier important documents (pre-2019) were included sparingly for background context if they shed light on foundational evasion techniques or regulatory frameworks prior to Garantex's existence. For example, a policy report from 2015 on general crypto money laundering might be referenced to compare past and present techniques.

Using these criteria, the study assembled a total of 27 qualitative sources. These sources can be categorized by type as follows: Research Reports (10 sources): These are in-depth analytical reports by research institutions or industry groups examining cryptocurrency risks and sanctions. For example, a RUSI report from 2022 analyzing Russian crypto evasion strategies was included, as well as annual Crypto Crime Reports by Chainalysis (2023 edition) that provided data and insight into illicit crypto trends. Such reports papers were chosen for their comprehensive data and expert analysis, which offer grounded context on norms (like AML standards) and big-picture trends. Government and NGO Briefings (4 sources): These include concise documents such as policy briefs by think tanks, advisories by agencies, or expert briefs. Notably, a FinCEN advisory from 2022 that raised red flags for Russian crypto evasion was used, as well as briefings from organizations like the Financial Action Task Force (FATF) on virtual asset regulation. These were selected because they reflect the official and semi-official normative responses which tend to highlight issues of sanctions-busting or the networks at play, thus directly tying to our theoretical framework concepts. Regulatory and Legal Documents (5 sources): Key documents here were the OFAC designation notice for Garantex (2022) and related U.S. Treasury press releases, as well as a U.S. Department of Justice indictment unsealed in 2025 against Garantex administrators. These sources were chosen as primary evidence of the legal labeling of Garantex's activities as illicit, illustrating the rule-of-law aspect and providing specifics like dates of actions, reasons for sanctions, and legal charges which are important factual anchors. Investigative Journalism Articles (6 sources): Investigative pieces from major news outlets (e.g. Reuters, Bloomberg) and investigative conglomerates (e.g. OCCRP) form a large portion of the articles. These articles often contained detailed narratives of how Garantex operates in practice, sometimes uncovering information not in official reports (such as interviews with insiders or leaks). For instance, Reuters (2023) detailed how sanctioned oligarchs purportedly funneled money via Garantex, and traced suspicious flows through the exchange. These articles were included for their on-the-ground insights and as a check against official narratives; they frequently address questions of legitimacy (by exposing illicit behavior) and feeding into the inductive codes. Others (5 sources): This category covers miscellaneous but relevant sources such as forum posts by blockchain experts analyzing Garantex transactions, transcripts of interviews or webinars with compliance experts, or Russian-language news pieces that were translated. These were used sparingly and always cross-validated, but they sometimes provided unique data points (for example, a forum post by a blockchain analyst might list newly identified Garantex wallet addresses). Their inclusion was justified when they added value not found in mainstream sources, with careful verification. In total, 27 documents were analyzed qualitatively, including the above types. This diverse source base was deliberate because it

enables data triangulation, meaning the same event or claim can be found in multiple independent sources, boosting confidence in its accuracy.

For the quantitative component, the thesis gathered blockchain transaction data specifically related to Garantex's operations. This data captures the flow of cryptocurrencies through addresses associated with Garantex and its users, allowing analysis of volumes, patterns, and networks of transactions. Collecting such data required first identifying relevant blockchain addresses and entities, and then retrieving their transaction histories. The research began by compiling a list of cryptocurrency addresses known to be linked to Garantex. These were obtained from credible sources such as government reports and blockchain analytics publications. For example, the OFAC designation of Garantex (2022) and the U.S. Justice Department press release (2023) named a few specific addresses (for Bitcoin and Ethereum) as controlled by Garantex or its operators. Additionally, investigative articles and crypto tracing reports sometimes revealed clusters of addresses believed to belong to Garantex (or its users) that were not explicitly in official documents. The criterion for including an address in our list was that it had to be corroborated by at least two independent sources (e.g. listed in an OFAC document and mentioned by a Chainalysis report). Any address for which evidence was weaker or singular (only one mention without verification) was treated with caution and generally excluded or set aside pending further confirmation. This conservative approach, guided by practices in investigative research (Neuman, 2014), ensured that the quantitative analysis rested on a reliable foundation of known associations, minimizing false positives in the data.

To streamline the identification and verification of Garantex-related addresses, the study leveraged the Arkham Intelligence platform. Arkham is a blockchain analytics platform that uses algorithms to match addresses to real-world entities (Arkham Intelligence). By using Arkham's database for the entity "Garantex," a set of labeled addresses associated with Garantex was obtained. Arkham's labels and data served as a cross-check against the manually compiled seed list, and indeed expanded it. For instance, Arkham identified dozens of additional deposit and withdrawal addresses used by Garantex on Ethereum and Tron networks that were consistent with patterns reported by other analysts. Because Arkham allows direct SQL-like queries through its API, it programmatically retrieves comprehensive transaction logs for these addresses. For example, using Arkham's API, one could execute a query to pull all transactions involving the Garantex entity within a given date range. The figure below is used as an example and will be further analyzed during the analysis but the data includes sending and receiving addresses, timestamped amounts, and relevant token types.

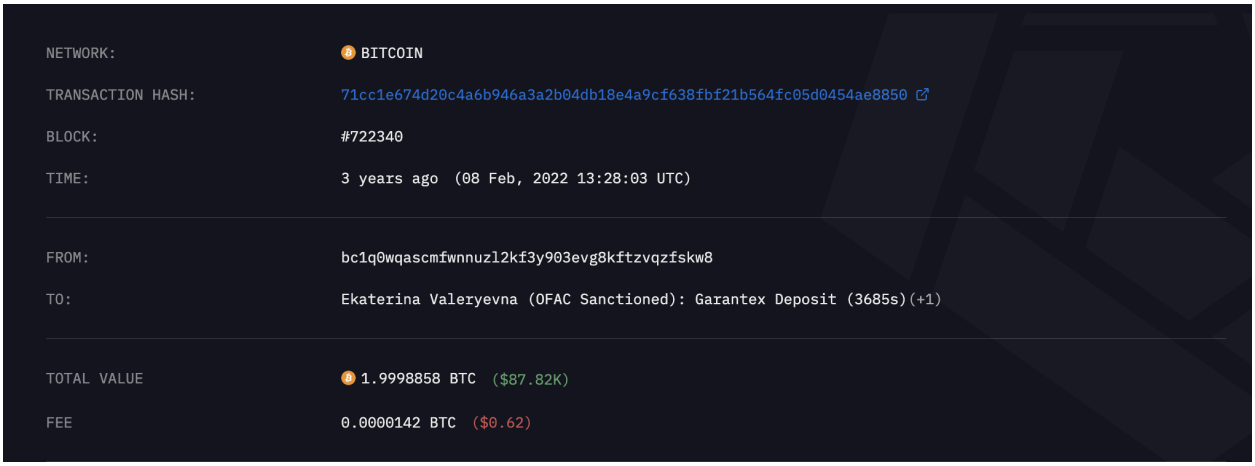


Figure 1: A Bitcoin blockchain record showing that on 8 Feb 2022 about 2 BTC were sent from address bc1q0… to a Garantex deposit wallet attributed to OFAC-sanctioned Ekaterina Zhadanova.

3.5 Data-Analysis

Data analysis was carried out separately for qualitative and quantitative datasets initially, followed by an integration phase where results were compared and combined. The procedures were designed to iterate between methods, consistent with a convergent mixed approach where one can inform the other to refine analysis. Here there's detail how qualitative content analysis and quantitative blockchain analysis were conducted, including specific techniques (like coding schemes and network metrics) and how rigor was ensured (e.g., intercoder reliability for qualitative, anomaly detection for quantitative). Also, descripting points of iteration where findings from one method led to revisiting the other, thereby enriching the overall analysis.

3.5.1 Qualitative Data Analysis

The qualitative component of this study employed a content analysis strategy to systematically identify and interpret patterns across a curated set of textual sources. Content analysis involves coding data using a pre-established framework derived from the study's central research concerns. In this case, the coding was not based on abstract international relations concepts like norms or sovereignty but was instead constructed around concrete, operational categories directly related to sanctions evasion via cryptocurrency. The coding was performed using Taguette, an open-source tool that facilitated structured tagging of excerpts within documents including OFAC press releases, investigative journalism, financial intelligence reports, and blockchain analytics publications.

The coding was developed inductively to align with seven empirically grounded categories: Garantex's Self-Perception, Sanctions-Evasion Techniques, Related Actors, Enforcement Response, Adaptation and Resilience, On-Chain Indicators, Regulatory Arbitrage. These categories were selected because they reflect recurring structural features and behavioral patterns observable in the Garantex case and surrounding ecosystem. Each code served as a conceptual lens for organizing and interpreting data. For example, any discussion of Garantex, Bitzlato, or similar platforms operating in defiance of regulatory norms was tagged under Regulatory Arbitrage. This code captures descriptions of exchanges that facilitate high-risk transactions, evade KYC protocols, or continue operating despite international sanctions.

Category	Codes	Open Codes
Sanction-Evasion Techniques	Shift to A7A5 Stablecoin	Ruble-pegged token issued via Kyrgyzstan to replace frozen USDT

Table 1: Sample set of code that is used as an example to visualize clearly the coding for this thesis.

The darknet and cybercrime networks code applied to excerpts referencing criminal infrastructures such as ransomware syndicates, darknet markets (e.g., Hydra), or malware campaigns that used cryptocurrency for operational financing. This included mentions of ransomware proceeds moving through Garantex, or darknet vendors relying on Russian exchanges to launder funds. The code for money laundering facilitators was used for descriptions of actors who serve as intermediaries in financial obscuring of funds and this could include OTC brokers, Telegram-based exchangers, shell companies, and mixers. These entities often played a role in "off-ramping" crypto into fiat or fragmenting transactions to disguise their origins, particularly in relation to ruble-to-USDT conversions.

The code for sanctioned elites and oligarchs was assigned to any text identifying specific high-net-worth individuals or politically exposed persons engaged in crypto transactions post-sanctions. This included narratives about oligarchs like Zhdanova moving funds through Garantex, especially when linked to efforts at asset concealment or sanctions circumvention. Instances of actors transferring funds rapidly after sanctions designations, often described as "panic conversions," were included in this category. The crypto evasion techniques code captured operational practices such as peel chains, chain-hopping, domain obfuscation, or the switch from USDT to alternative stablecoins like A7A5. This code was critical for tracing how technical strategies were deployed to avoid detection or legal seizure, often in coordination with other categories like laundering or exchange use.

The regulatory and enforcement gaps code applied to content discussing institutional shortcomings which would be included as lax AML regimes, non-cooperative jurisdictions, and legal blind spots that actors like Garantex exploited. Reports noting, for example, that Russia failed to prosecute crypto KYC violations or that Estonian authorities initially failed to act on red flags fell under this category. Finally, the enforcement actions/responses code captured official designations, takedowns, legal indictments, and international cooperation efforts aimed at disrupting Garantex and its ecosystem. These included OFAC's 2022 designation, the March 2025 seizure of Garantex's infrastructure by a U.S., German, and Finnish task force, and advisories issued by FinCEN and FATF. This code also included the narrative framing of such actions in public documents, such as referring to Garantex as a "critical hub" in Russian illicit finance.

Coding was performed line-by-line, and the categories were applied across all sources with overlapping codes allowed where excerpts addressed multiple themes simultaneously. For example, a paragraph describing an oligarch using peel chains to route funds through Garantex would receive three codes. Each code's application was logged in Taguette. The resulting dataset allowed for both descriptive mapping and deeper interpretive synthesis. This coding strategy enabled the research to construct a grounded narrative of how crypto-based sanctions evasion is practiced, supported, and targeted, with Garantex serving as the empirical focal point.

These seven inductive code categories reflect the operational and institutional dimensions that underpin this research. By coding the data using these categories: Garantex's Self-Perception, Sanctions-Evasion Techniques, Related Actors, Enforcement Response, Adaptation and Resilience, On-Chain Indicators, Regulatory Arbitrage. The analysis remains tightly aligned with the empirical objectives of this thesis. Rather than focusing on abstract theoretical principles, this coding framework directs attention to the mechanisms and actors that sustain and exploit sanctions-evading ecosystems. In practice, the analysis asked of each document: where are the exchanges operating beyond the law? Who facilitates laundering or converts assets for sanctioned actors? What enforcement responses were made, and how effective were they? Importantly, these codes were not mutually exclusive; individual excerpts were often tagged with multiple labels when they captured overlapping behaviors or relationships. For instance, a paragraph describing an oligarch using a Telegram-based OTC broker to launder USDT through Garantex would receive three codes simultaneously as sanctioned elites and oligarchs, money laundering facilitators, and illicit crypto exchanges. The coding process was conducted line-by-line across all documents. Inductive codes were applied wherever thematically relevant content appeared. As coding progressed, the definitions and applications of each category were periodically reviewed. If a code appeared to be applied too loosely like "money laundering facilitators" being used for any wallet-to-wallet transfer. Then

the definition was tightened, and previously coded excerpts were re-evaluated to ensure consistency.

All coded excerpts were aggregated and read comparatively to identify overarching patterns, divergences, and illustrative examples. For instance, under the “regulatory arbitrage” code, the analysis revealed repeated emphasis across fifteen sources on how Garantex exploited weak KYC protocols and regulatory arbitrage to maintain liquidity for high-risk actors. Under “darknet and cybercrime networks,” twelve sources highlighted links between Garantex and ransomware groups or darknet vendors, often emphasizing wallet clustering patterns. The “crypto evasion techniques” code yielded particularly rich content on the shift from USDT to rouble-pegged stablecoins and on the use of Telegram bots to enable pseudonymous trades after formal exchange sanctions. Similarly, “regulatory and enforcement gaps” was among the most frequently coded themes, with documents citing Russia’s lack of enforcement and delayed regulatory responses as enablers of illicit crypto flows.

An attempt to find co-occurrence was also conducted by reviewing excerpts tagged with multiple codes to trace the interdependence of actors and behaviors. For example, several documents discussing enforcement actions also detailed the circumvention strategies actors adopted in response. Then these would link enforcement actions, crypto evasion techniques, and illicit exchange behavior within a single transactional episode. These thematic overlaps deepened the explanatory value of the analysis, showing how evasion is not a linear process but an interlocking system of actors and tools. Overall, this content analysis yields a structured, empirically grounded map of the Garantex ecosystem and the broader landscape of Russian crypto-based sanctions evasion. It revealed patterns of adaptation in the face of enforcement, recurring infrastructure dependencies such as OTC brokers and darknet partners, and widespread structural vulnerabilities in the international regulatory environment. These qualitative findings set the stage for triangulation with the blockchain data analysis, which follows in the next chapter.

3.5.2 Quantitative Data Analysis

This thesis drew its on-chain dataset to corroborate the findings of the content analysis. In addition, a tightly drawn “announcement window” meaning the seven days before and the fourteen days after a new OFAC, EU, or U.K. sanctions designation. That’s because that is when evasive behaviour is most detectable. In fact a study done by the New York Fed showed that crypto flows react almost immediately to sanctions shocks: transaction volume through the sanctioned Tornado Cash smart-contract pools, for example, fell by roughly 72 % in the week following its August 2022 designation, while rouble-for-Bitcoin and rouble-for-Tether trading spiked the moment Western measures against Russia were announced (Brownworth et al,. 2024). Focusing on these high-signal intervals maximises causal leverage, allowing changes in routing

tactics, address reuse, or mixer reliance to be linked more convincingly to the sanctions event rather than to background market noise. By constricting the dataset inside the windows an observer can clearly see the odds that any jump or crash in Garantex traffic is driven by the sanctions themselves rather than by normal crypto volatility.Transactions outside these windows are incorporated only when the thesis calls for analysis of actors associated with Garantex to provide a clearer picture or to provide context as to what are normal transaction patterns. For example, the figure below provides a visual in spiked transactions on April 6, 2022. Most notably, this is the following day that OFAC had first sanctioned Garantex.

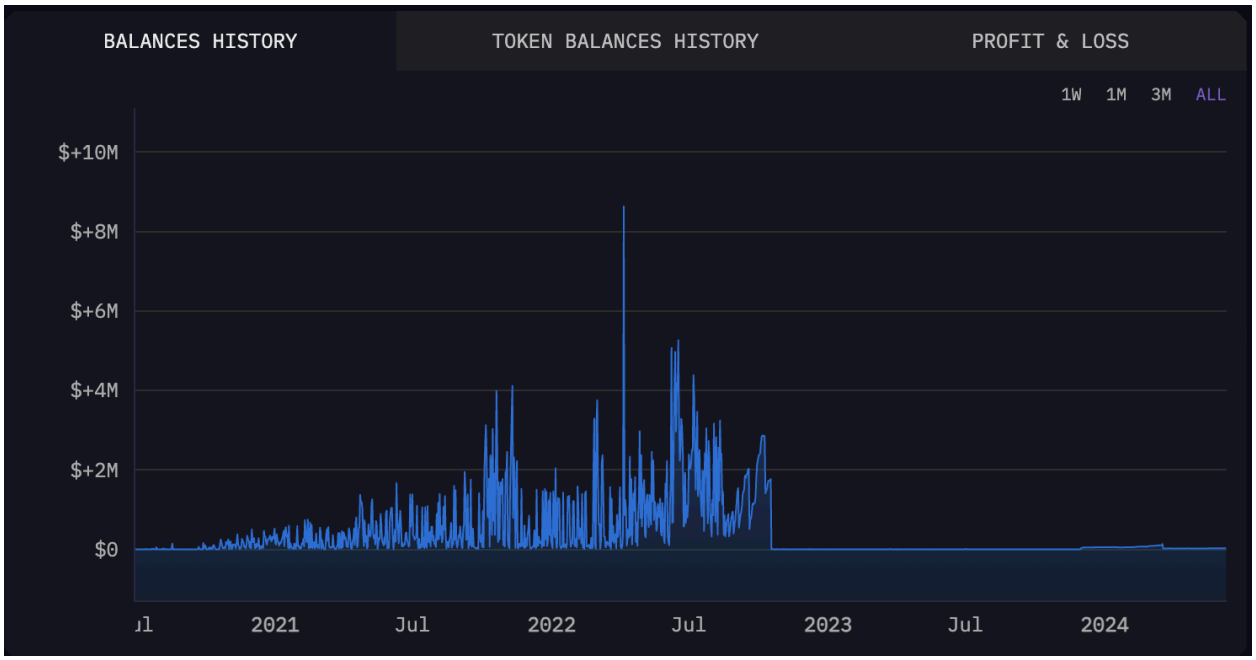


Figure 2: From Arkham this figure shows exchanges token balance grew modestly through 2021, spiked to almost $9 million in early 2022, fluctuated at lower highs for the rest of that year, and then fell essentially to zero from mid-2023 onward.

3.6 Validity, Reliability, and Trustworthiness

Ensuring the quality and credibility of research findings is critical, especially in a mixed-methods case study that draws from diverse data sources. This section discusses the steps taken to maximize validity, reliability, and overall trustworthiness of the study, in line with

established IR methodological standards. Multiple strategies were employed like triangulating sources, maintaining a clear chain of evidence, being transparent about limitations, and following conventions for rigorous qualitative and quantitative analysis.

Triangulation refers to using multiple sources or methods to cross-check information. This was a cornerstone of the design. Triangulated within the qualitative data (by comparing what different documents said about the same event) and between qualitative and quantitative data. For instance, if an OFAC press release claimed a certain wallet was Garantex's, that information was corroborated with blockchain data. If the blockchain analysis saw a surge on a date, multiple sources were checked to see if an event explains it. By not relying on any single source, the thesis reduces the chance that the findings are remnants of one particular perspective or dataset. The consistent convergence of evidence from different angles (as highlighted above) strengthens the validity of the conclusions. In cases where sources conflicted – say one source said "X happened" and another said "X did not happen" this was flagged and sought either additional evidence or reported the discrepancy in our analysis, rather than choosing one arbitrarily. This practice follows recommendations by Bryman (2016) on handling conflicting accounts being to explicitly acknowledge and investigate further. By doing so, the thesis aims to present a balanced account and not overstate certainty where it's not warranted.

The methodology is grounded in well-established techniques. The inductive coding scheme was derived from theory and followed a directed content analysis approach as per scholarly guidance (e.g., Hsieh & Shannon, 2005 on content analysis). On the quantitative side, common metrics and tools in blockchain analysis were used, as seen in industry reports (Chainalysis, Elliptic). Essentially benchmarking the approach against what experts use. Adhering to these standards enhances reliability because another researcher following the same approach should in principle be able to replicate the steps and observe similar patterns (given the same data). All technical terms and measures were defined as they were introduced, to avoid ambiguity. For example, when "peel chains" or "chain-hopping" was used in documents, those were explained (peel chain: a series of transactions each slightly smaller, used to launder funds) so that coding such terms is transparent and could be repeated by others.

3.7 Feasibility of the Study and Proper Approach

No study of this scope can be without limitations. It's important to acknowledge these candidly to contextualize the findings and avoid overgeneralization in the research. Despite best efforts at data collection, there are inherent gaps. Blockchain data, while rich, is pseudonymous and someone cannot always ascertain who is behind a given address. There was reliance on secondary sources (e.g., OFAC or analytics firms) for linking addresses to actors, and these attributions may not cover all relevant addresses. It is likely that some crypto transactions related to sanction evasion went undetected in the dataset because they were not linked to known

entities. Likewise, qualitative data on illicit activities is by nature incomplete; actors do not publicize their evasion. Therefore, the analysis could under-represent evasion that is happening in harder-to-observe channels (for instance, peer-to-peer trades happening entirely off-exchange). This limitation means the quantifications (like volume estimates) should be taken as indicative minimum, not exact totals.

When researchers link an on-chain event to a sanctions evasion motive, there is a degree of inference. Correlation in time (e.g., a surge of transactions after a sanction) does not guarantee causation. Triangulation is used to strengthen causal claims, but some ambiguity remains. For example, if oligarch A's assets moved via crypto after sanctions, someone could assume evading sanctions was the motive, but theoretically it could also be for other reasons (market speculation or fear of ruble devaluation). The analysis will do its best to rule those out via context, but caution that human motives can rarely be known with certainty, especially with deliberate secrecy. Similarly, while sources might attribute certain addresses to an oligarch's network, it's hard to be absolutely certain unless confirmed by authorities.The crypto landscape and sanctions environment are continually evolving. New evasion techniques (using privacy coins, decentralized mixers, NFT-based transfers, etc.) may have emerged even as this thesis was being written. The study might not capture the latest shifts, especially given a cut-off in data collection. For instance, if Russia develops state-sanctioned mining or new bilateral crypto agreements, those developments would be outside of the scope.

A delimitation is that concentration was pinpointed on a Russian case specifically, meaning the theories and findings are contextualized to Russia's geopolitical situation, its actors, and the Western sanctions regime against it. This was intentional, but it means one should be careful in generalizing results to other sanctioned states like Iran or North Korea. Also, Russia has unique attributes, with a relatively tech-savvy population, a large economy, and a certain degree of integration with global markets (at least pre-2022) – all of which influence how crypto is used for evasion. Other regimes might not replicate these patterns. However, many insights (like the adaptability of networks) have broader relevance.

4. Analysis

Russia's full-scale invasion of Ukraine in 2022 triggered unprecedented international sanctions designed to isolate its economy. In response, Russian non-state actors which are anywhere from illicit crypto exchanges to oligarchs and criminal networks have increasingly turned to cryptocurrencies to move and conceal wealth outside the traditional financial system. This analysis examines how these actors, centered on the case of the Garantex exchange, exploit crypto to evade sanctions, and what this means for the effectiveness of current sanctions regimes. The evidence is drawn from investigative reporting, government reports, blockchain analytics firm research, and expert studies (27 sources in total). Key themes include the role of rogue

crypto exchanges, darknet and cybercrime links, money laundering facilitators, sanctioned elites' tactics, evasion techniques, regulatory blind spots, and enforcement countermeasures.

4.1 Garantex's Self-Perception

Garantex consistently portrays itself as a legitimate business caught in the crossfire of geopolitical disputes rather than an intentionally illicit actor. In public communications, the exchange has claimed to follow compliance norms and has dismissed Western accusations as politically motivated. For example, Garantex obtained a license in Estonia in 2019, presumably to project an image of legitimacy, but failed to implement basic Know-Your-Customer rules. An Estonian inspection found that "over 90% of the customers have been subject to the breach of the duty to verify identity" and that much of the volume flowing through Garantex Europe OÜ was tied to criminal wallets (FIU, 2022). The Estonian Financial Intelligence Unit concluded that although Garantex "applied for an authorisation in Estonia" it "did not take steps to…comply with [the rules] in substance. Service providers like this do not have a place in Estonia" (FIU, 2022). This stark contrast between Garantex's licensed status and its actual non-compliance supports the notion of a compliance facade because of the public claim of following the rules that masked lax or willfully poor controls. Such a facade reflects the exchange's self-perception (or at least public presentation) as a lawful enterprise, even as evidence mounted of its deficiencies.

Garantex's leaders also frame external sanctions and crackdowns as unjust foreign interference rather than as responses to wrongdoing. After U.S. authorities unsealed charges against its operators in 2025, Garantex issued a defiant statement to Russian media, rejecting the allegations as politically driven. According to RBC, the exchange argued it had become merely a pawn in a larger US–Russia standoff, "We consider these accusations political and plan to defend our good name in court… Today we have become a chess piece on the board in the Russia–USA match" (RBC, 2025). In the same statement Garantex "emphasized that the exchange had always actively cooperated" with authorities (RBC, 2025). Garantex was trying to protect its self-image as compliant and claimed to be unfairly vilified. This "non-interference" narrative was portraying Western sanctions as illegitimate meddling in Russia's domestic crypto market and often recurred throughout Garantex communications. For instance, when the stablecoin issuer Tether froze Garantex-related wallets in March 2025, Garantex told users that "Tether has entered the war against the Russian crypto market", characterizing the asset freeze as an assault on Russia rather than a lawful enforcement action (Crawley, 2025). By framing a corporate compliance issue as part of a "war against the Russian crypto market," Garantex aligned itself with a nationalist narrative of resistance. The company assured users, "We will fight, and we will not give up" (Fabrichnaya & Marrow, 2025), casting itself as a resilient victim of Western aggression. Such messaging suggests that internally Garantex views or at least wants its audience to view the sanctions as an extension of East–West hostilities rather than as a consequence of its own facilitation of illicit finance.

This confidence reflects the Kremlin's line that Russian initiatives (like a digital ruble or sanctions against Western actors) can "neutralize OFAC" and other external pressures, a belief that Garantex publicists appeared to share. While no direct quote of Garantex explicitly mentioning Russia's counter-sanctions was found in the dataset, the sentiment is apparent in its communications. The notion that Garantex is just a scapegoat of a "crypto Cold War" emerged in Russian press narratives and the exchange's messaging alike. As one Russian-language outlet summarized, the exchange presented itself as a "chess piece 'in the match Russia–USA'", highlighting that it viewed the U.S. charges as political, not criminal (RBC, 2025).

Overall, Garantex's self-perception centers on legitimacy and victimhood. The theme of Garantex insisting on its full compliance, despite evidence to the contrary and branding foreign sanctions as political, was seen often. This pattern demonstrates a clear strategy by Garantex actors to utilize nationalist and anti-Western framing to maintain customer trust and social license. By emphasizing its role as a patriotic actor under unjust attack, Garantex seeks to assure users and partners that it is not a criminal enterprise but rather a persecuted business. This reinforces the exchange's ability to continue operations by rallying sympathy and skepticism toward the sanctions. Crucially, this stance also implies a challenge for sanctions effectiveness. For example, if targets refuse to acknowledge wrongdoing and are bolstered by a host government's narratives, sanctions alone may have limited impact on their behavior. Garantex's internal narrative of compliance and persecution thus sets the stage for how it adapts to and evades the very international measures aimed at stopping it.

4.2 Sanctions-Evasion Techniques

A core focus of the data is how Garantex and its users deploy cryptocurrencies to evade international sanctions. This category was among the most frequently coded. Notably, it shifted much of its volume to the Tron blockchain version of USDT. This shift was strategic because of Tron's low fees and perceived lax oversight made it attractive for high-risk transactions. According to Senator Warren at a senate hearing, vast sums of crypto flowed through Garantex in USDT despite the sanctions. Authorities in the U.S. and U.K. eventually uncovered that over $20 billion in cryptocurrency transactions "passed through [Garantex] after sanctions went into effect" and largely via USDT (Warren, 2024). This staggering figure represents one of the largest breaches of Russian sanctions to date. Chainalysis analysts confirmed that Garantex continued to operate unabated post-designation, noting that it was a prime example of a sanctioned exchange "still operating in a jurisdiction where they don't care about sanctions" (Grauer, 2024). By 2024, over 80% of Garantex's transaction volume was reportedly occurring in USDT, predominantly on Tron's network (Elliptic, 2023). The use of Tron-based USDT provided Garantex users with a dollar-pegged asset that could be transacted outside the traditional banking system, thereby

bypassing banks that might block sanctioned accounts. Elliptic also noted that “the highest volume of transactions [post-sanction] occurred in the USDT stablecoin, on the TRON blockchain” (Elliptic, 2023). In short, Garantex leaned on stablecoins to replace the banking services that sanctions cut off. The reliance on USDT was so pronounced that it was likely even too reliant on USDT as a freeze from Tether could come at any time, and eventually did. Even after Tether, the company, took action in 2025 to freeze Garantex-linked funds, Garantex had already moved much of its liquidity into other channels (discussed below). The centrality of USDT usage as it was appearing in dozens of coded instances shows how critical crypto-stablecoins have been for sanctions evasion, effectively providing a USD-equivalent lifeline to sanctioned actors.

Shifting to alternative tokens and networks is another technique Garantex employed to stay a step ahead of enforcement. Anticipating further crackdowns on USDT, Old Vector developed a ruble-pegged stablecoin called A7A5. According to TRM Labs, “The A7A5 token, which claims to be pegged 1:1 to the Russian ruble, was announced on Telegram two weeks before the Garantex takedown. It is now available on Ethereum and TRON, and listed on the obscure exchange BiFinance, reportedly based in the British Virgin Islands and founded by an individual known only as “Bob” (TRM Labs, 2025). In addition, “Garantex addresses began moving funds into A7A5 as early as January 2025, suggesting premeditated efforts to create a sanctions-resistant asset. The token promises daily profit-sharing to holders and has been advertised as a way for Garantex users to recover frozen assets. During an interview with Satoshkin, Garantex executives explicitly stated that A7A5 was developed to facilitate such transfers (TRM Labs, 2025).

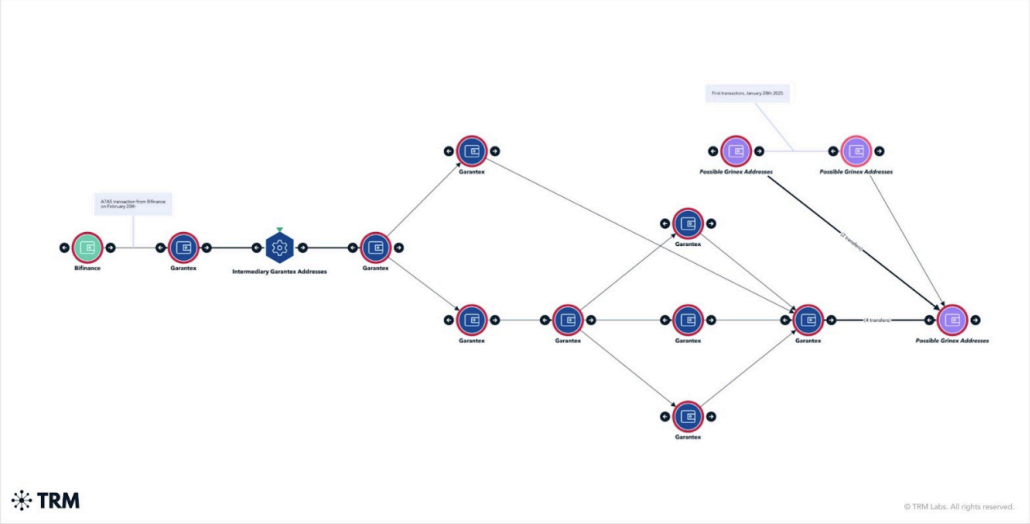


Figure 3: A TRM Labs flow graph tracing cryptocurrency from Bitfinance through several Garantex wallets and intermediaries to clusters of addresses flagged as possible Grinex endpoints.

These maneuvers illustrate regulatory arbitrage through token substitution because when a mainstream stablecoin became risky to use another was simply engineered. Users were incentivized to convert their stranded USDT into the new ruble stablecoin (reports indicate promises of high yields, up to 20% APY, to encourage uptake of A7A5). By shifting into A7A5, Garantex attempted to create a parallel value transfer system outside the reach of Western companies like Tether. Although A7A5's longevity is uncertain, the tactic demonstrates the adaptability of evaders by creating new crypto instruments on the fly to maintain liquidity. This technique was coded frequently in the sources, emphasizing how sanctioned actors turn to innovation (like new stablecoins) to blunt the effect of sanctions.

In addition to stablecoins, Garantex facilitated classic money laundering tactics in crypto form, such as mixing and wallet-hopping. U.S. prosecutors found that after the OFAC designation, Garantex operators "redesigned Garantex's operations to evade and violate U.S. sanctions," including "moving its operational cryptocurrency wallets to different…addresses on a daily basis" to thwart tracking (DOJ, 2025). By rotating deposit and withdrawal addresses, Garantex made it difficult for compliance systems at other exchanges to flag its transactions, a practice akin to traditional money launderers frequently changing bank accounts. This daily address rotation was essentially an in-house "mixer" technique to break the traceability of funds. In some cases, users also sent funds through third-party mixers (like the Ethereum-based Tornado Cash or Bitcoin mixers such as Sinbad and others) before or after moving through Garantex, further obscuring the trail (DOJ, 2025). One report noted Garantex's links to known mixer services, indicating that people would "hop" coins through several intermediate wallets and mixer pools en route to or from Garantex (TRM Labs, 2023). The inclusion of terms like "TornadoCash" and "Sinbad" in the coding highlights that multiple sources identified the use of those mixers in conjunction with Garantex. Mixing and address-hopping techniques were referenced in at least a dozen instances, providing insight into their importance in the evasion toolkit. By blurring the on-chain link between origin and destination of funds, these methods exploit cryptocurrency's pseudonymity to defeat sanctions screening. The net effect is that even if authorities identified certain Garantex addresses, the exchange could quickly shift to new ones and users could obscure their tracks, rendering blacklist-based sanctions less effective.

Garantex actors also engaged in domain-hopping and platform rebranding to evade web takedowns and legal bans. In the 18 months following the initial U.S. sanctions, Garantex changed its official domain multiple times to stay accessible. The exchange's website moved from garantex.com to alternative domains (e.g. grn-service.com, then grinex.io) as it cat-and-moused with regulators (Global Ledger, 2025). Each time a domain was seized or blocked, the operators would simply stand up a new site with a different name, often alerting users via Telegram or forums. This agility in shifting online presence is a classic in cybercrime services facing law enforcement pressure. By the time of the 2025 takedown, Garantex had

already launched “Grinex”, a full-fledged rebrand marketed as “a new platform with familiar functionality” (TRM Labs, 2025). Grinex was essentially Garantex in new clothing. But from a technical standpoint, the key is that continuous domain and name changes hampered enforcement. Users could quickly migrate to the new domain, and casual observers might not realize Grinex was the sanctioned Garantex reborn. This platform arbitrage allowed Garantex’s business to persist through sanctions, illustrating how simply banning one website or name is not sufficient if the underlying operators remain at large.

A further evasion method was peer-to-peer (P2P) trading and off-book transactions facilitated by the exchange. As compliance pressure increased, Garantex added a P2P marketplace feature that allowed users to trade crypto-for-fiat directly with each other, outside of the central order book. This shift meant that some trades occurred wallet-to-wallet between users (with Garantex taking a commission but not necessarily matching orders on an open exchange order book). The intent was to move activity “off radar” and since P2P trades could be presented as direct user transfers, making them harder for outsiders to distinguish from personal transactions. This adaptation aligns with broader tactics observed among Russian OTC (over-the-counter) crypto brokers who often operate via Telegram chats and informal networks to skirt institutional scrutiny (Center for Strategic and International Studies, 2022). In effect, Garantex blended formal exchange functions with informal brokered deals, which served to partially decentralize the laundering process. By providing tools for users to trade directly (and even advertise offers via Telegram channels associated with Garantex), the exchange enabled its community to self-organize trades that would be more difficult for regulators to monitor. This indicates that sanctions evasion was not only a high-tech affair but also relied on old-fashioned cash movement and underground exchangers. The convergence of street-level cash conversion with crypto rails made Garantex a hub bridging the conventional and digital underground economies.

4.3 Related Actors

The Garantex case involves a web of related actors, ranging from individual facilitators and cybercriminal groups to larger networks in the dark economy. Understanding who these actors are is crucial to grasping how Garantex functions as an illicit hub. The evidence shows that Garantex did not operate in a vacuum and it served the needs of sanctioned Russian oligarchs, laundered proceeds for ransomware gangs, absorbed users from darknet markets like Hydra, transacted with other shady exchanges, and tapped into global hotspots like Dubai’s financial havens. One prominent set of actors are Russian elites and oligarchs seeking to move wealth abroad. Garantex became a channel for sanctioned wealthy individuals to bypass restrictions on their funds. The U.S. Treasury’s designation of Ekaterina Zhdanova in November 2023 shines light on this connection. Zhdanova, a Russian national, was sanctioned as a “key

facilitator" who used both fiat and crypto to help sanctioned elites launder money (OFAC, 2023). Critically, Zhdanova "uses…cryptocurrency exchanges that lack AML/CFT controls including the designated Russian exchange Garantex" (TRM Labs, 2023) Reuters reported that in one case, Zhdanova helped a Russian oligarch attempt to transfer over $100 million through such methods (Reuters, 2023). To do so, she relied on Garantex among other virtual currency entities, since Garantex was known as a permissive platform. In fact, "to facilitate large cross-border transactions, Zhdanova used…Garantex, a prominent Russia-based darknet market site and cryptocurrency exchange"(OFAC, 2023). This example illustrates how Garantex directly enabled sanctioned oligarchs to expatriate funds. Zhdanova not only moved millions through fraudulent bank accounts, but "also used virtual currency exchanges to help oligarchs" who had relocated, with Garantex specifically named as a go-to venue.

TIME	FROM	TO	VALUE	TOKEN	USD
3 years ago	Ekaterina Valeryevna (OFAC	Garantex: Hot Wallet (b…	0.00728	BTC	$337.7
3 years ago	bc1q9enrwrce0hmfpmyccge7r…	Ekaterina Valeryevna (OFAC	0.00728	BTC	$337.27
3 years ago	Ekaterina Valeryevna (OFAC	Any Cash (3AVhh)	0.5	BTC	$19.3K
3 years ago	Ekaterina Valeryevna (OFAC	Any Cash (383PZ)	0.001	BTC	$37.06
3 years ago	Blockchain.com: Blockch…	Ekaterina Valeryevna (OFAC	0.5	BTC	$18.53K
3 years ago	Block: Blockchain.c… (+1)	Ekaterina Valeryevna (OFAC	0.001	BTC	$37.06
3 years ago	Ekaterina Valeryevna (OFAC	3CSZ8iaxpxgv4DmR45NNj… (+2)	0.219	BTC	$8.42K
3 years ago	3KK4xeoV9JxmW6PywS2GEtyHr…	Ekaterina Valeryevna (OFAC	0.219	BTC	$8.42K
3 years ago	Ekaterina Valeryevna (OFAC	Garantex: Hot Wallet (b…	1.807	BTC	$79.36K
3 years ago	bc1q0wqascmfwnnuzl2kf3y90…	Ekaterina Valeryevna (OFAC	1.807	BTC	$79.36K
3 years ago	Ekaterina Valeryevna (OFAC	Garantex: Hot Wallet (b…	0.0145	BTC	$635.83
3 years ago	bc1qst2wphn2qmsmsu8z9… (+2)	Ekaterina Valeryevna (OFAC	0.0145	BTC	$635.83
3 years ago	Ekaterina Valeryevna (OFAC	bc1qd9vyztw4s4c72exeetazw…	0.53	BTC	$21.99K
3 years ago	Ekaterina Valeryevna (OFAC	Binance Deposit (1Ayn… (+2)	1.11	BTC	$42.79K
3 years ago	Ekaterina Valeryevna (OFAC	Garantex: Hot Wallet (b…	29.1	BTC	$1.12M
3 years ago	Ekaterina Valeryevna (OFAC	Ekaterina Valeryevna (OFAC	29.1	BTC	$1.12M

Figure 4: This is a transaction table from Arkham showcasing Zhadanova's movement on chain. Also note, this is one of 30 pages of transactions from Zhdanova.

What is interesting with the figure is that at first glance the table looks like just another slice of blockchain. But with information as to context with Ekaterina the figure showcases activity used by a crypto laudress facilitating sanctions evasion. That context recasts an ordinary transfer log into a map of potential sanctions-evasion because you can see layering (small fractional deposits and withdrawals), cycling through intermediary self-custody addresses, and

occasional larger lumps, all funneling liquidity toward a black-listed exchange that stayed online in Russia after its 2022 designation. In other words, what looks like routine bookkeeping is, once the identities are known, direct evidence of a sanctioned user actively using Garantex and OTC ramps to move and redeem bitcoin outside the regulated banking perimeter.

To better provide a visualization of the network of Zhdanova the figure below is Chainalysis flow diagram visualizes a layering scheme in which cryptocurrency originating from a single "service-provider" address is divided among four intermediary wallets; each intermediary subsequently consolidates its transfers into a personal wallet attributed to Zhdanova. From that point the funds are routed to two Garantex deposit addresses. The multi-step structure illustrates a classic money-laundering pattern because the funds are fragmented, re-consolidated, and finally introduced to exchanges where they can be converted or withdrawn while the presence of sanctioned endpoints underscores the transaction chain's role in sanctions evasion rather than routine settlement.

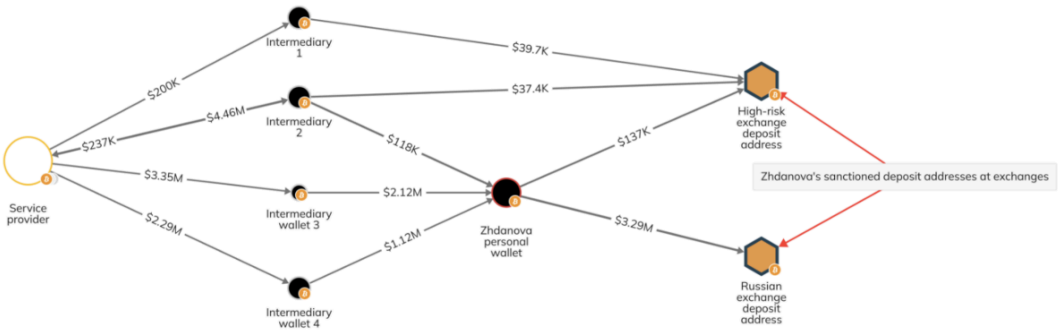


Figure 5: A Chainalysis flow diagram depicting Zhdanova's network.

Another critical category of related actors comprises ransomware gangs and cybercriminal organizations. Multiple sources connect Garantex to ransomware operations, identifying it as a preferred laundering exchange for groups like Conti, LockBit, and Black Basta. In early 2022, OFAC explicitly alleged that over $100 million transacted on Garantex was associated with illicit actors "including the notorious Russian ransomware gang Conti" (OFAC, 2022). Elliptic's research in 2023 further confirmed that "cryptocurrency assets from ransomware gangs like Conti, LockBit, and Black Basta have been found to be sent to Garantex after sanctions were imposed" (Elliptic, 2023). This indicates that even after Garantex's OFAC designation, ransomware actors continued (or even increased) their use of the exchange to cash out proceeds. Chainalysis found that Garantex served as a "major laundering hub for ransomware groups…including some of the largest attacks in the last three years" (Chainalysis, 2025). By providing liquidity and cash-out services, Garantex essentially functioned as the ransomware

world's bank. The exchange converted crypto ransoms into other cryptocurrencies or into fiat via intermediaries, allowing groups like Conti to enjoy their illicit gains. Elliptic's co-founder emphasized "Garantex has been used in sanctions evasion by Russian elites, as well as to launder proceeds of crime including ransomware, darknet market trade, and thefts attributed to North Korea's Lazarus Group" (Lakshmanan, 2025). This quote encapsulates the breadth of Garantex's clientele.

It is also critical to recognize the involvement of other crypto exchanges and services that intersected with Garantex. Garantex did not operate in a vacuum; it had counterparts and feeders. Notably, Suex and Chatex who are two exchanges sanctioned by the U.S. in 2021 and preceded Garantex in the high-risk Russian crypto market, and in fact all three had a direct connection because they "operated out of the same building in Moscow, Russia" (Elliptic, 2022). That building, Federation Tower in Moscow City, became a hub for shadowy crypto operations. After Suex and Chatex were blacklisted for laundering ransomware funds, much of their customer flow appears to have migrated to Garantex. Chainalysis observed that "when OFAC blacklisted Suex in September 2021, ransomware payments detoured through Garantex in less than 48 hours" (Chainalysis, 2025). This immediate migration suggests a close relationship among operators of these exchanges and a ready-made pipeline to absorb displaced illicit volume. Furthermore, other exchanges emerged to serve similar clientele as by 2024, the U.S. sanctioned Bitpapa and Cryptex, Russia-based crypto trading platforms that facilitated millions for Hydra and also had links to Garantex's user base (OFAC, 2024). The no-KYC exchanges that proliferated (with names like "PM2BTC" or "UAPS" as identified in U.S. and European investigations) often had backend connections to Garantex or at least overlapping customers (Chainalysis, 2025). For example, FinCEN in 2023 named one such exchange as a "primary money laundering concern", highlighting how these services formed an interconnected web. Garantex was a large hub in illicit exchanges. Yes, some were shut down (Suex, Chatex), others newly sanctioned (Bitpapa, Cryptex), and yet others still at large. But many of them shared liquidity and clientele. This broader network of related actors ensured that if one platform fell, others could pick up the slack.

Finally, Garantex's ties extended even into domains like Russian state-linked companies and malign actors. In an unusual but telling connection, Garantex was linked to transactions involving firms that supply the Russian military. The United Kingdom's National Crime Agency found evidence of crypto payments, via Garantex, reaching companies responsible for components of Russian weapons used in Ukraine (TRM Labs, 2025). Additionally, Chainalysis (2025) found that one of Garantex's on-chain counterparties was SouthFront, a pro-Russian disinformation outlet under sanctions for malign influence operations. Even more strikingly, Chainalysis also identified Lazarus Group as having on-chain links to Garantex. Lazarus was behind the massive $1.5 billion Bybit exchange hack and has long laundered stolen crypto through complex routes and the mention of Lazarus suggests that some of those stolen funds may have passed through Garantex or affiliated Russian brokers (Chainalysis, 2025). This is an

important piece of the puzzle because it implies that Garantex's network was perhaps part of a global illicit finance supply chain, connecting Russian money launderers with not just domestic criminals but also sanctioned actors in other countries (North Korea, Iran, etc., which have collaborative illicit finance relationships with Russian networks). The inclusion of such actors in Garantex's web proves the exchange's role as a "hub" for transnational illicit finance.

4.4 Enforcement Response

The story of enforcement involves escalating actions: an initial wave of sanctions and license revocations in 2022, followed by continued monitoring, and culminating in a coordinated takedown operation in 2025. Despite this multi-pronged response from OFAC sanctions to EU asset freezes to Secret Service seizures Garantex managed to operate for years. Ultimately, raising questions about enforcement gaps. The first major enforcement action was the U.S. Treasury's sanctioning of Garantex in April 2022. OFAC designated Garantex under Executive Order 14024 for "operating or having operated in the financial services sector of the Russian Federation economy"(OFAC, 2022). This action, announced alongside the takedown of Hydra, was groundbreaking because it was the first time the U.S. had sanctioned a cryptocurrency exchange for facilitating criminal activity at such a scale. The Treasury's press release alleged that more than "$100 million in transactions done on the exchange are associated with illicit actors and darknet markets, including the notorious Russian ransomware gang Conti, and the darknet market Hydra" (U.S. Treasury, 2022). By explicitly naming Garantex's links to Conti and Hydra, the U.S. framed the exchange as a clear conduit for prohibited transactions. The OFAC designation meant that Garantex was added to the SDN list, freezing any of its assets under U.S. jurisdiction and prohibiting U.S. persons from dealing with it. The impact of this move was partly symbolic (demonstrating that crypto exchanges aiding criminals will be treated akin to narco banks) and partly practical (cutting off Garantex from any direct use of U.S.-linked services, and deterring regulated exchanges from transacting with it). Following OFAC's lead, the Estonian Financial Intelligence Unit quickly moved to revoke Garantex Europe's license. As noted earlier, the Estonian FIU had found extensive AML failures and concluded that Garantex Europe was essentially a shell that "did not…comply" with Estonia's rules and was moving criminal funds (FIU, 2022). In doing so, Estonia eliminated Garantex's legal cover in the EU. Together, these early enforcement steps in 2022 aimed to cripple Garantex's operations and send a warning to the crypto industry.

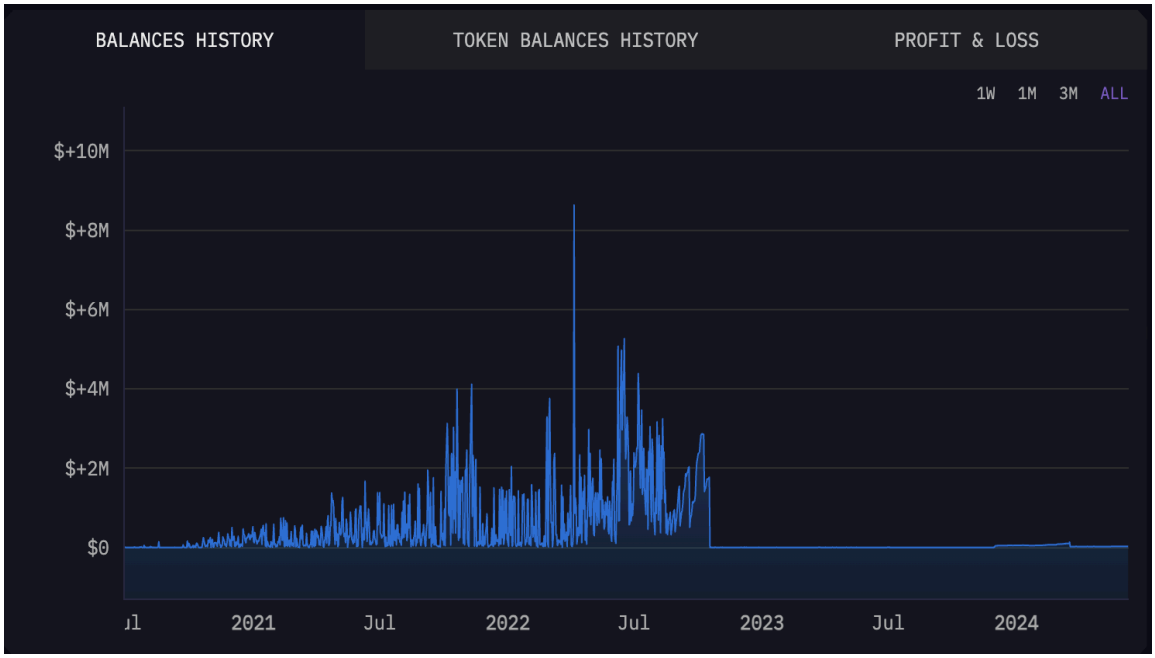


Figure 6: From Arkham this graph shows the massive spike on April 6, 2022 in transactions when a multitude of sanctions were announced.

The vertical spike on 6 April 2022 sits squarely inside a three-day barrage of Russia-related sanctions. In this context the brief surge likely reflects money racing through Garantex before off-ramps shut and either the exchange hurriedly pooling customer balances for redeployment, or clients rushing to withdraw while they still could. The graph therefore visualizes the instant liquidity shock that sweeping sanctions can impose on a once-functioning crypto hub. What follows is just as telling because balances collapse to a flatline once compliance desks worldwide blacklist Garantex, showing that the spike was not organic volume but sanctions-evasion maneuvering. In short, the single spike and the long drought that follows illustrate more of the dynamic of sanctions enforcement. A frantic burst of on-chain activity to launder or relocate assets, followed by a near-total choke-off once monitoring tools and counterparties catch up.

The European Union joined the fray as well, especially in response to Russia's war in Ukraine. In February 2023 and again in 2025, the EU added Garantex to its own sanctions list. The EU's 16th package of sanctions (adopted in late February 2025) was notable for including Garantex and it was the first time the EU sanctioned a crypto exchange. The EU stated it was targeting Garantex for its role in Russian sanctions evasion and noted the exchange "is closely associated with EU-sanctioned Russian banks" (Council of Europe, 2025). This likely refers to Garantex's connections with institutions like Sberbank or Tinkoff that had been cut off from SWIFT; Garantex was apparently facilitating those banks' clients or dealing with their digital

assets. By freezing any of Garantex's assets within Europe and forbidding Europeans from interacting with it, the EU sought to complement U.S. efforts and squeeze Garantex's operational freedom. Estonia's prior revocation of the license was a national step, but the EU-wide sanction harmonized the approach across all member states. These coordinated sanctions on both sides of the Atlantic significantly raised the stakes for Garantex and anyone doing business with it.

Critically, U.S. law enforcement also "froze over $26 million in funds" tied to Garantex's activities (DOJ, 2025). These funds likely included cryptocurrency held on Garantex's behalf in wallets that U.S. agencies managed to identify and secure, as well as perhaps fiat accounts abroad. At the same time, DOJ charged two key operators: Aleksej Besciokov and Aleksandr "Mira" Serda. They were accused of money laundering conspiracy, operating an unlicensed money transmitter, and (for Besciokov) conspiracy to violate the International Emergency Economic Powers Act (the law underlying U.S. sanctions) (DOJ, 2025). According to the indictment, these admins knowingly continued Garantex's illicit operations "despite the widespread publicity of the sanctions" and took steps to evade them (DOJ, 2025). The charges effectively assert that Garantex's leadership willfully curtailed U.S. law after being put on notice in 2022, thereby crossing from administrative violation into criminal territory. DOJ highlighted egregious conduct such as providing false information to Russian regulators and moving wallets daily to avoid detection (DOJ, 2025). By unsealing the indictment, DOJ signaled that if these individuals are ever in a jurisdiction with U.S. extradition treaties (as Besciokov was in India), they would be arrested. Indeed, as mentioned, "Aleksej Besciokov, one of the administrators of Garantex, was arrested in India at the request of the United States" (DOJ, 2025)The arrest of a Garantex co-founder is a significant enforcement milestone – it demonstrates the personal risk facing those behind such platforms. The DOJ operation in 2025, with its global coordination, was portrayed as a major victory: "The takedown marks a significant victory as international efforts escalate to disrupt illicit crypto activity" (DOJ, 2025)

Overall, from April 2022 to early 2024, Garantex still moved tremendous volume. This points to gaps in enforcement that sanctions alone did not shutter the exchange. Notably, Russia did not take any domestic action to shut down Garantex; indeed, Russian authorities seemingly tolerated it. A DOJ official remarked that Besciokov and Serda violated sanctions "with personal knowledge of them" and even misled Russian law enforcement when asked for info, indicating that Russian authorities at some point inquired about Garantex accounts but took no further steps (DOJ, 2025). The lack of Russian cooperation created a regulatory haven for Garantex. This meant Western enforcement had to rely on extraterritorial moves which are inherently slower and legally complex.

4.5 Adaptation and Resilience

Despite the intense enforcement pressure described above, Garantex and its operators demonstrated a high degree of adaptation and resilience. A recurring theme in the Garantex case is the remarkable adaptability and resilience displayed by the illicit network in the face of enforcement efforts. Each time authorities attempted to disrupt their activities, whether through sanctions, shutdowns, or seizures. The actors involved found ways to reconfigure and continue operations. This highlights the evolutionary nature of crypto-based sanctions evasion. Garantex and its associated actors responded to crackdowns by innovating new methods, shifting bases, and even reconstituting under new identities, exemplifying what Manzi & Calderoni described as a complex adaptive system in the illicit finance space. One clear illustration of rapid adaptation was observed in September 2021. When the U.S. sanctioned Suex, one of the first Russian crypto exchanges to be targeted. There was a concern that illicit flows would be disrupted. Instead, as noted earlier, criminals wasted no time in finding an alternative and within 48 hours, ransomware payments that would have gone to Suex were re-routed to Garantex (Chainalysis, 2025). A Chainalysis heat map captured how Bitcoin address clusters associated with ransomware "hopped" from Suex to Garantex almost immediately after the sanction, like commuters changing trains (Chainalysis, 2025). This agile redirection demonstrates the resilience of the illicit network; it had multiple nodes and was able to survive the loss of one node (Suex) by simply funneling activity to another (Garantex). The network thus behaved in a redundant fashion because if one branch was cut off, another branch took over the traffic. This is characteristic of transnational organized crime networks, which are often compared to hydras or starfish organisms that regenerate when cut. The Garantex ecosystem effectively "grew a new limb" to keep the flow of dirty money going.

Garantex itself exhibited resilience after being directly hit with sanctions in April 2022. One might expect that being placed on OFAC's SDN list would cripple an exchange's business, isolating it from law-abiding customers and partners. Indeed, Garantex did lose access to some infrastructure (for example, U.S.-based cloud services or any assets under U.S. jurisdiction). However, the exchange's activity not only persisted but grew post-sanction. As stated earlier, between April 2022 and early 2025 being the period during which Garantex was officially blacklisted it processed over $100 billion in cryptocurrency transfers (TRM Labs, 2025). In that timeframe, over 70% of the volume to and from sanctioned entities worldwide flowed through Garantex (TRM Labs, 2025). Rather than diminishing, Garantex became more central to the illicit finance ecosystem after its designation. This counterintuitive outcome exemplifies how partial measures can sometimes even solidify an illicit actor's niche. That's because once legitimate exchanges started blocking Russian illicit transactions (due to sanctions compliance), almost all that volume moved around the one major player that remained openly defiant. Thus, Garantex's sanction backfired in the short term, making it a monopolistic provider for sanctioned users. The exchange adapted by leveraging its sanctioned status as a badge of convenience to criminals: it no longer even had to pretend to follow international rules, since it was cut off from the lawful world anyway, and it doubled down on serving the black market. This phenomenon

reflects the adaptive feedback loop described by Sanctions Busting Theory, where every clampdown by authorities spurs innovation and counter-strategies by targets (Passas, 2003). Garantex's continued operation and growth under sanction demonstrate the limits of sanctions when not paired with immediate enforcement. The exchange simply hunkered down in Russia's jurisdiction and catered even more to illicit actors, knowing U.S. sanctions alone could not physically disable it.

A major test of Garantex's resilience came with the Hydra Market takedown in April 2022. Hydra's shutdown by German law enforcement (with $25 million in Bitcoin seized) was a significant blow to a huge chunk of the Russian darknet economy. It's to be expected that the closure of Hydra would dry up a major source of illicit volume for Garantex. Initially, there was a dip, but soon adaptation set in. Multiple smaller darknet markets sprang up to fill Hydra's void, and they quickly latched onto Garantex as a ready-made cash-out channel. In fact, the overall darknet activity rebounded and even exceeded prior levels within months (TRM Labs, 2025). This reflects modular substitution in the illicit ecosystem because removing one big module (Hydra), and a dozen smaller modules take its place, reusing the existing connections (like Garantex) to reestablish the flow. The broader point is that the illicit network dynamically adjusts in response to enforcement. Hydra gone? Use Garantex with other markets. Suex gone? Move to Garantex. These shifts happened rapidly, often in a matter of days or weeks, showcasing a high degree of agility.

4.6 On-Chain Indicators

One key indicator is the volume of illicit cryptocurrency handled by Garantex. According to Chainalysis data, from 2019 up to its dismantling in 2025, Garantex processed at least $96 billion in total cryptocurrency transactions (Chainalysis, 2025). Of this, an estimated 1.35% (over $1.3 billion) was directly linked to illicit activity (Chainalysis, 2025). While 1.35% may sound small, it is nearly 10 times the illicit share seen at compliant exchanges which average around 0.14% illicit volume. Based on those numbers Garantex was an extreme outlier in serving criminal transactions. In absolute terms, over a billion dollars in dirty crypto flowing through a single platform is staggering. TRM Labs provided an even sharper statistic being since OFAC's sanction in April 2022, Garantex was responsible for 82% of all crypto volume associated with sanctioned entities worldwide (TRM Labs, 2025). This means that if someone tallied all identified crypto transactions involving sanctioned actors (whether they be darknet markets, terrorist groups, sanctioned individuals, etc.), four-fifths of that value touched Garantex. That is a dramatic concentration of illicit finance in one platform. It indicates that once compliant exchanges ejected sanctioned actors, those actors had few places to turn, and Garantex eagerly absorbed them. Additionally, TRM noted that in 2024 specifically, Garantex (along with an Iranian exchange, Nobitex) accounted for 85% of crypto inflows to sanctioned entities and

jurisdictions (TRM Labs, 2025). These figures highlight the systemic importance Garantex had in the underground economy and it was not a small node but the central hub for sanction evaders in the crypto space. To help provide more of a visual for the sheer amount of transactions below is a graph depicting flows.

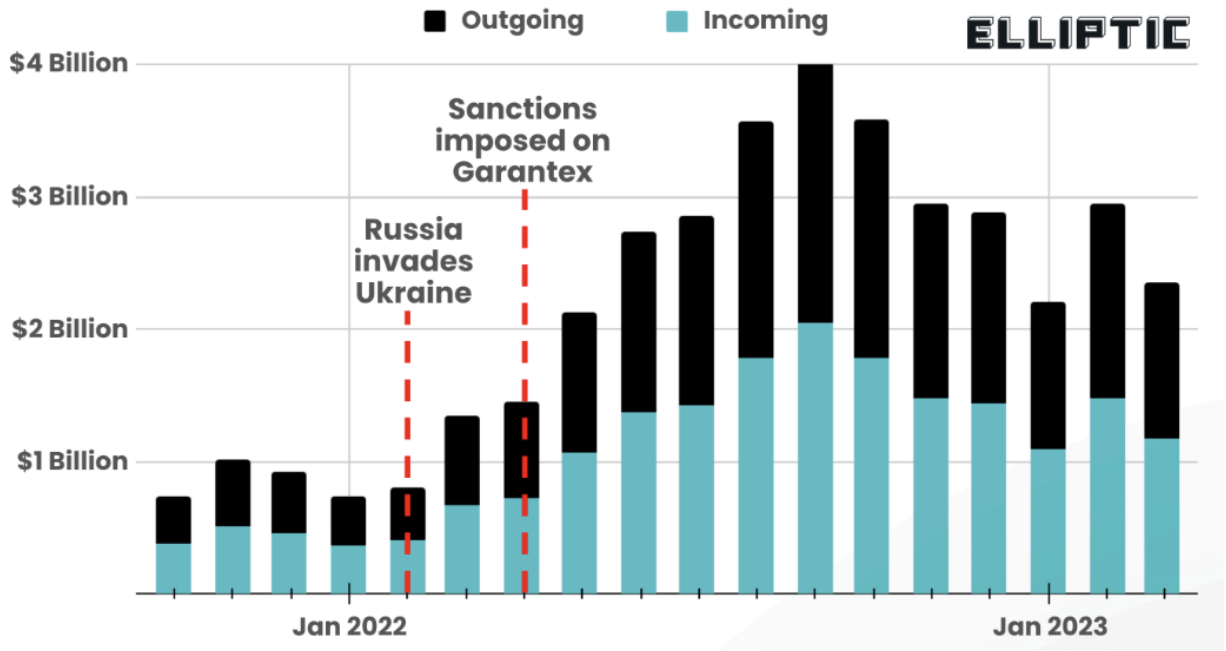


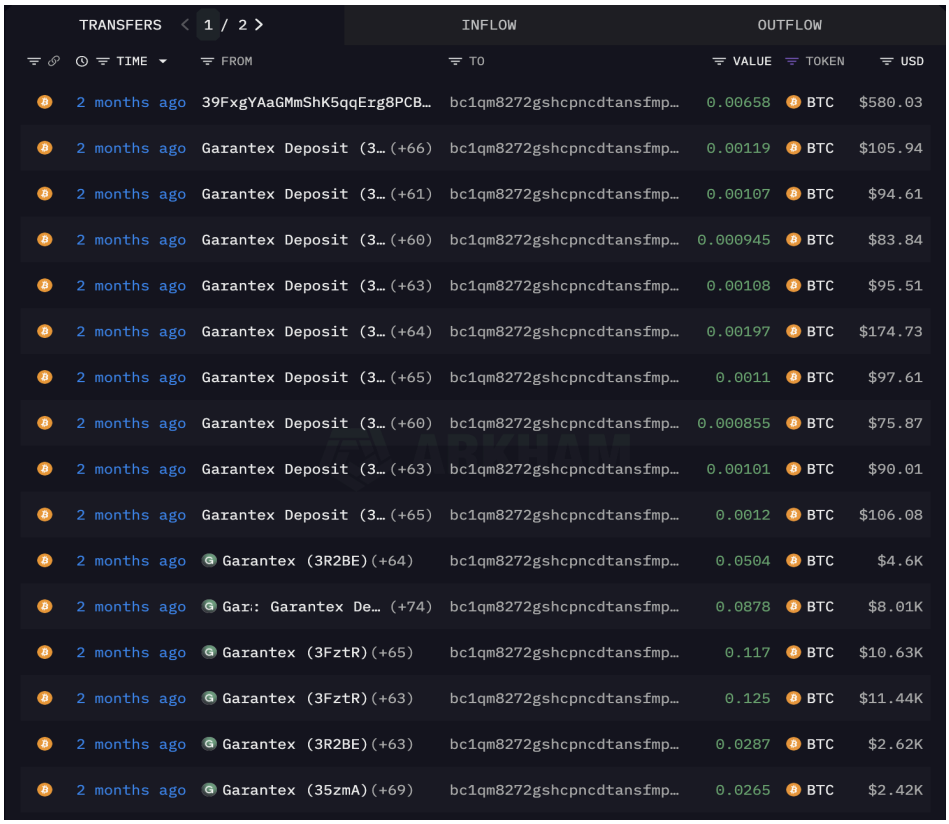
Figure 7: This figure from Elliptic shows crypto transactions per month as there's a significant surge after sanctions in April, 2022.

On-chain analysis has also shed light on the types of illicit activity funneled through Garantex. Chainalysis broke down the illicit sources of Garantex's crypto inflows and found that the majority came from scams, darknet markets, and other illicit organizations (Chainalysis, 2025). Another notable connection uncovered on-chain was with Lazarus Group. As part of the analysis of Garantex's crypto flows, Chainalysis identified that Garantex had direct on-chain links with addresses associated with Lazarus (Chainalysis, 2025). This suggests that some of the proceeds from Lazarus's hacks (like the Bybit hack) may have been laundered through services that ultimately interacted with Garantex. The presence of North Korea is a strong indicator of how globally connected these crypto laundering networks are, bridging state-sponsored hackers in one country with criminal exchanges in another. Furthermore, Chainalysis noted ties to multiple darknet markets (specifically naming OMG!OMG! Market, Mega Darknet Market, and Solaris) as part of Garantex's relationship graph (Chainalysis, 2025).

Another interesting on-chain indicator is the temporal pattern of transactions, especially around enforcement events. Blockchain data shows spikes or shifts corresponding to major events like sanctions or raids. For example, as mentioned, a swift diversion of flows from Suex addresses to Garantex addresses around late September 2021. Similarly, on March 6, 2025, right after Tether froze Garantex's USDT, traceable large movements of funds as Garantex scrambled to convert or secure assets (TRM Labs, 2025). The publication by TRM of 89 crypto addresses that Garantex said were frozen provides investigators with a starting point to trace how those addresses were funded and where their balances went. By watching those addresses on-chain, analysts observed that funds were shifted into A7A5 and then moved to new addresses presumably under Grinex's control (Ratex42, 2025). Thus on-chain monitoring caught the liquidity migration in real time. In general, the blockchain's transparency meant that even as Garantex attempted evasion through address hopping, those addresses could often eventually be clustered (via common spending patterns or attribution from leaks or blockchain analytics heuristics) and then visualized. Graph visualizations published by TRM and Chainalysis depict complex webs of addresses connecting Garantex to many illicit entities (Chainalysis, 2025; TRM Labs, 2025). Seeing these webs helps illustrate just how entangled the exchange was with a host of bad actors. For instance, an on-chain graph might show a cluster of addresses (Garantex's wallets) in the center, with lines going out to clusters representing Conti, Hydra, etc., demonstrating money flows.

Another on-chain metric concerns the use of stablecoins and particular blockchains. The Chainalysis Crypto Crime Report 2025 pointed out "stablecoin shifts" in the illicit realm (Chainalysis, 2025). Specifically, it noted that illicit actors increased their usage of Tether on Tron and even explored alternative stablecoins as enforcement against Ethereum-based stablecoins tightened. For example, by late 2022 and 2023, a higher proportion of illicit stablecoin transactions were occurring on the Tron network rather than Ethereum, reflecting a move to where there were fewer compliance checks (Chainalysis, 2025). This on-chain trend correlates with Garantex's practices because Garantex heavily utilized Tron USDT for transactions. When Tron too saw Tether addresses frozen (as happened in March 2025 for Garantex), the shift to an entirely new stablecoin (A7A5) was another adjustment visible on-chain as a new token contract suddenly became active with large volume. On-chain token transfer data would show an abrupt spike in transactions of A7A5 in early 2025 originating from wallets tied to Garantex, effectively announcing the birth of this new evasion coin (Merkle Science, 2025). A notable case cited by Chainalysis was that Garantex laundered at least $22 million stolen from a hacked U.S.-based blockchain platform (Chainalysis, 2025). On-chain tracking of those stolen funds presumably led to seeing the funds end up at Garantex deposit addresses. That signals the trust hackers placed in Garantex to cash out such a large theft. Finally, on-chain indicators can measure the effect of enforcement. For example, after the March 2025 takedown, it's visible whether illicit flows through Garantex addresses cease or decrease. As

seen in the figure below some of the last transactions indicate a consolidation. Often consolidation is just opposite of peeling. Essentially chain peeling is a money-laundering technique in which an actor places a large lump of cryptocurrency into one address, then repeatedly moves the funds through a series of new wallets, shaving off a small slice at each hop; the small peeled-off portion is sent to yet another clean address while the remaining balance is forwarded to the next intermediary wallet, where the process is repeated. After dozens or even hundreds of these incremental transfers, the original sum has been fragmented into many modest-sized wallets that appear unrelated to the tainted source, and when the launderer finally mixes, swaps, or cashes out those fragments.



TRANSFERS 1 / 2 | INFLOW | OUTFLOW

TIME	FROM	TO	VALUE	TOKEN	USD
2 months ago	39FxgYAaGMmShK5qqErg8PCB…	bc1qm8272gshcpncdtansfmp…	0.00658	BTC	$580.03
2 months ago	Garantex Deposit (3… (+66)	bc1qm8272gshcpncdtansfmp…	0.00119	BTC	$105.94
2 months ago	Garantex Deposit (3… (+61)	bc1qm8272gshcpncdtansfmp…	0.00107	BTC	$94.61
2 months ago	Garantex Deposit (3… (+60)	bc1qm8272gshcpncdtansfmp…	0.000945	BTC	$83.84
2 months ago	Garantex Deposit (3… (+63)	bc1qm8272gshcpncdtansfmp…	0.00108	BTC	$95.51
2 months ago	Garantex Deposit (3… (+64)	bc1qm8272gshcpncdtansfmp…	0.00197	BTC	$174.73
2 months ago	Garantex Deposit (3… (+65)	bc1qm8272gshcpncdtansfmp…	0.0011	BTC	$97.61
2 months ago	Garantex Deposit (3… (+60)	bc1qm8272gshcpncdtansfmp…	0.000855	BTC	$75.87
2 months ago	Garantex Deposit (3… (+63)	bc1qm8272gshcpncdtansfmp…	0.00101	BTC	$90.01
2 months ago	Garantex Deposit (3… (+65)	bc1qm8272gshcpncdtansfmp…	0.0012	BTC	$106.08
2 months ago	Garantex (3R2BE) (+64)	bc1qm8272gshcpncdtansfmp…	0.0504	BTC	$4.6K
2 months ago	Gar…: Garantex De… (+74)	bc1qm8272gshcpncdtansfmp…	0.0878	BTC	$8.01K
2 months ago	Garantex (3FztR) (+65)	bc1qm8272gshcpncdtansfmp…	0.117	BTC	$10.63K
2 months ago	Garantex (3FztR) (+63)	bc1qm8272gshcpncdtansfmp…	0.125	BTC	$11.44K
2 months ago	Garantex (3R2BE) (+63)	bc1qm8272gshcpncdtansfmp…	0.0287	BTC	$2.62K
2 months ago	Garantex (35zmA) (+69)	bc1qm8272gshcpncdtansfmp…	0.0265	BTC	$2.42K

Figure 8: This ledger from Arkham shows small inputs from different “Garantex Deposit” addresses are converging into a single bc1qm… wallet

On-chain data will continue to be crucial in that analysis, as it provides objective metrics of crime money movement that can be compared across periods. The blockchain does not lie and it corroborates the narrative of Garantex’s central role with hard numbers and connections. On-chain indicators help the argument that Garantex was a pivotal sanctions-evasion hub. The hope is that such data will show a decline in the overall illicit volumes (or at least a fragmentation that reduces efficiency for criminals). Continuous monitoring of on-chain

indicators will be the way to measure whether the sanctions and takedown of Garantex truly curbed the abuse, or whether the Hydra effect occurs again in the financial sense.

4.7 Regulatory Arbitrage

A significant factor enabling Garantex's rise was the exploitation of regulatory and jurisdictional gaps. The exchange's history exemplifies regulatory arbitrage, wherein actors strategically shift their activities to jurisdictions with lax enforcement or exploit inconsistencies in global regulations to avoid scrutiny. Garantex's trajectory from a licensed entity in one country to an unregulated rogue actor in another highlights how differences in national approaches to crypto oversight create vulnerabilities that illicit actors can capitalize on. Garantex initially took root in the relatively permissive regulatory environment of Estonia. In the late 2010s, Estonia became known for its liberal issuance of licenses to virtual asset service providers (VASPs). Garantex Europe OÜ obtained an Estonian license to provide cryptocurrency services on 27 November 2020 (Estonian Financial Intelligence Unit, 2022). At the time, Estonia was issuing hundreds of such licenses and by the end of 2021, there were 381 licensed crypto service providers in Estonia, the most per country in the world (Estonian Financial Intelligence Unit, 2022). This oversupply, coupled with limited supervisory capacity, meant that many licensed firms in Estonia were operating with minimal oversight. Garantex clearly "stood out" among these for its high risk and it handled over €5 billion in annual transactions, with the majority of its business and customers linked to Russia and other high-risk countries (Estonian Financial Intelligence Unit, 2022). Essentially, Garantex used Estonia as a legitimate front to enjoy the credibility of a European license while actually conducting most of its high-risk operations in Russia. This is a textbook case of regulatory arbitrage because incorporating in a jurisdiction with light-touch regulation (or one that at the time was not rigorously vetting business plans) to mask the true nature of the operations.

When Estonian authorities caught up to Garantex's malfeasance, the exchange swiftly re-localized to Russia. In late 2021, Estonia's FIU conducted an on-site inspection of Garantex Europe OÜ. The findings were problemsome because of the "systemic and systematic deficiencies" in anti-money laundering controls, 90% of customers not properly verified, use of fake identities (shell customers presented as natural persons), huge turnovers by those shells (tens of millions of euros), failure to report suspicious transactions, and clear evidence that funds passing through were linked to criminal wallets (FIU, 2022). The FIU concluded that Garantex was essentially a facade using Estonia's jurisdiction "for illegal purposes" and moved to revoke its license. Sensing the imminent shutdown, Garantex Europe then surrendered its Estonian license on 24 February 2022 (the very day Russia invaded Ukraine) rather than wait for revocation (Estonian Financial Intelligence Unit, 2022). This allowed the operators to avoid some legal wrangling and quietly move out. Within weeks, Garantex had fully shifted its operations to Moscow. According to the U.S. Treasury, by April 2022 Garantex was "operating

out of Federation Tower in Moscow, Russia," alongside other sanctioned exchanges like Suex and Chatex (U.S. Department of the Treasury, 2022). Federation Tower essentially became a haven where Russian authorities allowed these crypto businesses to run unfettered. The move from Estonia to Moscow was a deliberate arbitrage play because once Estonia tightened its regime (indeed, Estonia passed a new law on 23 February 2022 to crack down on crypto licensing abuses), Garantex fled to a jurisdiction where enforcement was minimal or where it could count on protection. As Nikos Passas's concept of "regulatory asymmetry" predicts, illicit operations will "shift dynamically toward jurisdictions where compliance costs dip below projected profits" (Passas, 2003). Garantex's relocation was exactly this shift. Moscow offered a setting where compliance costs were essentially zero because local regulators had no will to enforce Western sanctions or AML standards on a Russian-run exchange serving Russian clients. By sheltering behind Russia's borders and corporate opacity, Garantex insulated itself from the kind of oversight it faced in Estonia. This allowed it to preserve its customer base and liquidity, essentially trading strict-rule Estonia for laissez-faire Russia.

The international regulatory landscape for cryptocurrency has been uneven, and Garantex thrived in those seams. A major gap has been the patchy implementation of the FATF Travel Rule and other global standards. In a 2023 targeted update, the Financial Action Task Force reported that only 10 out of 20 G-20 member jurisdictions had fully implemented the Travel Rule for virtual assets, leaving plenty of "hop-scotch corridors" where crypto businesses can operate without sharing sender/recipient information (FATF, 2023). Russia is one of the jurisdictions with weak implementation of such standards. The lack of Travel Rule enforcement means exchanges like Garantex could send and receive funds from foreign exchanges without any required transmission of customer identity data attached to transactions. This makes it easy for Garantex to interact with semi-compliant exchanges abroad by essentially exploiting the weakest link. If even one exchange in the chain isn't following the rule, the information trail breaks. FATF's report showed that such harmonization glitches amplify systemic risk, as criminals will route funds through jurisdictions or services that are not yet compliant (FATF, 2023). Garantex leveraged exactly this arbitrage because it operated in a jurisdiction (Russia) that had not implemented robust AML for crypto, and it connected with other non-compliant services worldwide.

Moreover, Russia's own regulatory posture towards cryptocurrency during 2022-2023 can be described as ambivalent by creating openings that actors like Garantex could exploit. While the Russian central bank was initially opposed to cryptocurrency, the sanctions following the Ukraine invasion prompted a pivot. By 2023, Russia passed legislation to allow cryptocurrency payments in international trade (Reuters, 2023) and explored accommodating crypto mining. Essentially, Russia signaled that it would not only tolerate but potentially endorse the use of crypto to circumvent financial isolation. For example, in August 2022, the head of the Financial Monitoring Service (Rosfinmonitoring) acknowledged that crypto was being used by

Russians to bypass restrictions and said the agency was working to regulate it, which in practice meant not clamping down too hard (Winston, 2022). This stance can be seen as a form of regulatory arbitrage at the state level because the Russian government realized that by not enforcing strict controls on crypto, it could provide its economy and sanctioned actors an outlet that Western regulators could not easily touch. Garantex benefited from this environment and it's unlikely a coincidence that despite international sanctions, Russian authorities never shut down Garantex. In fact, when Russian law enforcement did engage with Garantex, it appears to have been half-hearted. The DOJ indictment reveals that when Russian law enforcement requested information on one of Garantex's accounts (linked to its executive), Garantex provided false information and nothing apparently came of it (DOJ, 2025). This implies a degree of impunity granted by local authorities. As long as Garantex was not scamming Russian citizens or threatening Russian state interests, its role in aiding sanctions evasion was accepted, if not encouraged. The Russian regulators' decision to let Garantex run (and indeed later their acceptance of Grinex in Kyrgyzstan) shows how jurisdictional arbitrage is sometimes aligned with geopolitical interests. That's because Russia had an interest in undermining Western sanctions, and a rogue exchange facilitating that was left alone.

In contrast to Russia, Western jurisdictions and allied countries steadily tightened crypto regulations after 2019, which had the effect of pushing illicit activity into unregulated spaces. For instance, the European Union's 8th sanctions package in October 2022 banned all crypto services to Russian persons above a small threshold. Stating, "The ban concerns the following services to Russia or Russian persons: crypto-asset wallets, accounts or custody … accounting, auditing, bookkeeping and tax consulting … IT consultancy and legal advice"(Council of the European Union, 2022). Once that ban was in place, compliant European exchanges cut off Russian users entirely, likely driving even more Russian volume into home-grown exchanges like Garantex. Similarly, the United States enhanced its enforcement guidance as seen in FinCEN's March 2022 alert to financial institutions flagging typologies like the use of non-U.S. exchanges and mixers, essentially warning that Russian evaders would turn to platforms outside U.S. reach (Financial Crimes Enforcement Network, 2022). Those warnings were predictive and Garantex was exactly the type of platform described. But while Western regulators were alerting banks and crypto firms to watch out, the fact remained that Garantex operated from a sanctuary jurisdiction, beyond direct reach. The exchange could thus arbitrage between two worlds: the compliant world (which it avoided or used only indirectly via nested accounts) and the non-compliant world (in which it firmly planted itself).

Another dimension of regulatory arbitrage in this case is the use of companies and foreign fronts to bypass restrictions. That's evident with the Kyrgyz firm that issued the A7A5 stablecoin. Kyrgyzstan was likely chosen because it had even less oversight on crypto than Russia and perhaps to give a cover of non-Russian origin for the stablecoin (making Western companies less immediately wary of it). In the laundering networks exposed by authorities, there

were numerous instances of companies in third countries being used to hide Russian ownership or to move funds. The TGR money laundering network, "who facilitated illicit transactions through corporate structures in the UK, UAE, Thailand" (Chainalysis, 2025). Those companies would then interact with crypto exchanges or banks to blur the Russian connection. Garantex itself was originally an Estonian legal entity with ostensibly EU-based management; behind that legal front, the real control was Russian. Even after relocation, maintaining an Estonian entity until license surrender may have allowed some continued interaction with Western services for a period under the guise of a legit company. This is arbitrage of legal identity because using foreign corporate registrations to arbitrage between legal regimes.

The lack of a unified international response to illicit crypto exchanges until 2025 also speaks to a regulatory gap that Garantex exploited. Before the March 2025 joint operation, actions against Garantex were piecemeal (U.S. sanctions, later UK sanctions, finally EU sanctions). Garantex managed to operate for nearly three years between its founding and its takedown, precisely because it could play off the differences. It was only until 2022 it flew under the radar with an Estonian license; after 2022, it relied on Russia's protective umbrella while most of Europe and the U.S. could only watch from outside. The eventual international operation (involving the U.S., EU member states, and others) was a long time coming. In the interim, Garantex grew immensely. This delay is attributable in part to the jurisdictional complexities because evidence had to be gathered across borders, servers had to be located in friendly jurisdictions. Ultimately, Garantex's critical servers were found in Germany and Finland, which is why those could be seized in 2025 (U.S. Department of Justice, 2025), and legal processes aligned. But until this alignment, Garantex enjoyed a form of regulatory arbitrage by default because it was safe where it was, and those who wanted to stop it had limited reach.

In summary, Garantex's story is a prime example of how actors "route around" regulation, much like how data routes around network blocks on the internet. Whenever and wherever regulations tightened, the exchange and its users shifted to venues with looser rules. Estonia started enforcing? Move to Russia. Tether enforces blacklisting? Use a Kyrgyz-issued stablecoin. Western exchanges implement KYC? Use Russian exchanges that don't. Such arbitrage is possible only because of uneven global implementation of crypto oversight. As the Estonian FIU Director lamented, service providers like Garantex "do not have a place in Estonia" but if they find a place in Moscow, they can continue until every jurisdiction that hosts key infrastructure (servers, domain registries, etc.) cooperates to shut them down (Estonian Financial Intelligence Unit, 2022). The implication is that any regulatory gaps will be found and exploited by savvy illicit actors. Garantex's operation out of Federation Tower with other blacklisted exchanges symbolized a physical concentration of regulatory arbitrage and literally under one roof, they clustered to enjoy Russia's hands-off stance while servicing crime worldwide. Closing these gaps requires an equally coordinated international regulatory stance,

which, as will be discussed in the enforcement section, has begun to take shape but still has room to grow.

4.8 Discussion

The case of Garantex demonstrates how cryptocurrency-based financial infrastructure can be strategically leveraged by non-state actors to systematically evade international sanctions. Through the detailed analysis a picture emerges of an exchange that not only enabled but actively optimized for sanctions circumvention. What is most revealing is not merely the volume of illicit funds processed by Garantex, but the seeming intentional and adaptability with which the exchange operated. Rather than a passive platform exploited by criminals, Garantex was purpose-built to serve sanctioned actors, ransomware syndicates, and darknet markets all while projecting a public image of compliance and victimhood. This dissonance between external perception and operational reality captures a core challenge in assessing the effectiveness of sanctions regimes in the digital age.

Garantex's self-presentation was both strategic and culturally embedded. The exchange routinely cast itself as a victim of Western aggression, framing enforcement actions as politically motivated rather than legal responses to criminal facilitation. This narrative was amplified in Russian media, where Garantex was depicted as a chess piece in a broader East–West standoff. In Telegram announcements and public statements, Garantex insisted on its compliance with local laws and characterized sanctions as attacks on the Russian crypto sector more broadly. This allowed the exchange to retain user trust and resist reputational collapse. Most like an outcome that would occur for a similarly sanctioned institution in the West. By aligning itself with nationalist sentiment and presenting Western sanctions as illegitimate, Garantex reinforced a moral framework in which evasion was not only defensible but patriotic. This type of rhetorical strategy, echoed in other Russian sanctioned entities, undermines the normative power of sanctions and makes enforcement politically untenable in the host state.

From a technical standpoint, the methods employed by Garantex actors to bypass restrictions were both diverse and deeply embedded into the platform's operations. Stablecoin usage, particularly USDT on the Tron network, played a pivotal role in facilitating liquidity while avoiding the formal banking system. The exchange routed billions in post-sanction volume through these rails, effectively creating a USD-denominated ecosystem decoupled from regulated dollar access. When asset freezes targeted these flows, Garantex shifted to a ruble-pegged stablecoin, A7A5, which was developed via companies in jurisdictions with minimal oversight. The rollout of A7A5 demonstrates how evasion tactics are no longer just reactive but preemptive because of anticipating enforcement and engineering around it in advance. The daily rotation of wallets, use of third-party mixers, adoption of Telegram bots, and the introduction of peer-to-peer systems further emphasize the sophistication of Garantex's operational design. Each

of these adaptations not only complicated tracing and interdiction but also signaled to users that the exchange was resilient by design.

This resilience was further reflected in the network of actors associated with Garantex. From designated money launderers like Ekaterina Zhdanova to ransomware syndicates like Conti and LockBit, Garantex served as a clearinghouse for funds originating in both traditional sanctions-evading circles and emergent cybercrime economies. The integration with Hydra Market vendors following Hydra's takedown, and the continued flow of assets from new darknet markets, reveal that Garantex was not simply tolerating risk but actively cultivating it. The exchange's ties to actors in the UAE, the laundering of North Korean hacking proceeds, and the involvement of OTC brokers point to a decentralized and transnational laundering ecosystem centered around the exchange. These actors suggest that Garantex was more than an endpoint; it was a hub in global illicit finance. Its ability to connect sanctioned oligarchs, cybercriminals, and dark market operators through a single crypto rail highlights the extent to which cryptocurrency is dissolving the segmentation between categories of illicit finance.

Despite expanding enforcement tools Garantex continued operations for nearly three years post-sanction. This length of time challenges assumptions about the sufficiency of traditional enforcement mechanisms. The sequencing of enforcement from Estonia's license revocation to the eventual arrest of one co-founder in India. Everything illustrates how long it takes for multilateral efforts to converge in a meaningful way. During that window, Garantex moved billions in crypto and developed successor platforms all while continually maintaining their user base. While the final 2025 takedown was effective in disrupting core infrastructure, it did not prevent the rebranding of Garantex as Grinex or the rollout of A7A5. These successor entities signal that enforcement without follow-up, and without systemic targeting of the entire evasion network, yields only temporary disruption. Garantex's rapid rebound under a new name and token affirms the limits of one-time interventions in a dynamic and distributed ecosystem.

Perhaps most consequential are the patterns of regulatory arbitrage that allowed Garantex to thrive. Initially operating under a license from Estonia, the exchange quickly relocated operations when that jurisdiction tightened compliance standards. It found regulatory shelter in Russia, where enforcement of international sanctions is politically unlikely, and set up financial and legal proxies in places like Kyrgyzstan. This jurisdictional agility reveals the critical importance of harmonized regulation. The patchwork nature of crypto oversight creates an exploitable landscape in which determined actors can always find a permissive node. Garantex's ability to issue new tokens and register new domains demonstrates that so long as these arbitrage opportunities exist, actors will reroute rather than cease. Effective sanctions enforcement requires sealing these gaps, which in turn demands cooperation across regulatory systems that often have divergent priorities.

On-chain indicators further confirmed the depth of Garantex's integration into illicit finance. Blockchain analytics showed that Garantex processed disproportionate volumes of illicit funds compared to legitimate exchanges and maintained transactional links to addresses associated with sanctions violations, ransomware, and darknet markets. That 82% of all global crypto volume tied to sanctioned entities flowed through Garantex is perhaps the most interesting quantitative evidence of its centrality. On-chain data not only mapped its connections but tracked the flow of funds through multiple evasion tactics illustrating how Garantex functioned as both a financial router and a cloaking mechanism. These flows also provided forensic evidence supporting enforcement actions and allowed seizure of at least some assets. However, the blockchain's transparency also revealed enforcement lag by showing that billions continued to move even after sanctions and that only a small fraction of tainted funds were ever frozen. This points to a strategic need to move from retrospective tracing to real-time interdiction in the crypto domain.

In all, the findings across all categories, the pattern is clear as Garantex thrived in the gaps of legal, jurisdictional, regulatory, and temporal. It exploited the speed and opacity of cryptocurrency, the fragmentation of global enforcement, and the political protection of its home jurisdiction to operate at scale. It adapted to every enforcement action, retained a resilient support network, and even began to reconstitute under a new identity. This case reveals that sanctions regimes rooted in the traditional financial system are vulnerable to circumvention by actors who understand and exploit the architecture of decentralized finance. Unless enforcement becomes equally agile, sanctions targeting non-state actors will remain reactive and incomplete. The future of sanctions policy must therefore be as dynamic as the adversaries it seeks to constrain.

5.0 Conclusion

Reflecting on the foregoing analysis, this thesis suggests that cryptocurrencies are doing far more than simply adding a novel layer to existing financial infrastructure; they are quietly reshaping the rules of engagement in ways that regulators and policymakers have only begun to understand. Examining the case of Garantex makes visible a new front where DeFi is neither a peripheral irritant nor an outright replacement for the banking system, but an adaptive space that can both cooperate with and circumvent the traditional order depending on incentives and design choices. Rather than framing DeFi as an existential "threat," it may be more accurate to see it as an emergent domain in which the familiar logic of sanctions enforcement and financial crime now play out under altered technological conditions.

The thesis was motivated by a noticeable gap in sanctions literature as the absence of consensus about how well sanctions work once they intersect with borderless digital ledgers and algorithmic markets. By tracing the operations of Garantex, the thesis exposes not a single rogue

exchange outsmarting Western authorities, but an ecosystem in which opacity and agility are marketed as features. Yet declaring the entire sanctions architecture "obsolete" would be premature. Many of its core principles still matter: naming, shaming, and constraining high-value targets can impose real costs. What the evidence shows, however, is that these tools now encounter parallel rails whose design assumptions prioritise censorship-resistance and jurisdictional neutrality. That design tension, rather than any one bad actor, is the deeper structural challenge.

The most striking empirical insight and one that has not been meaningfully addressed in the broader literature is that sanctions regimes, by pushing bad actors out of the formal financial system, may have unintentionally driven them into far more opaque terrain. The example of SWIFT is instructive. When sanctioned entities were in SWIFT, they were trackable. Once banned, their transactions migrated to pseudonymous systems like USDT. The West may have gained moral clarity, but lost operational visibility. This inversion where the moral high ground yields informational disadvantage is both paradoxical and profound. It suggests that sanctioning financial access without a compensatory mechanism for surveillance may do more to obscure than to constrain illicit activity. Even more so it poses the question as to whether visibility is a better weapon than exclusion? In designing architecture, sanctions regimes may have inadvertently created the ecosystem themselves.

Another key finding from this thesis is its demonstration that sanctions evasion is no longer a game of isolated actors finding clever workarounds. It is a mature industry with its own services, brokers, marketing strategies, and technological R&D. The A7A5 ruble-pegged stablecoin is a case in point. It shows that when legitimate assets are frozen, these networks don't just switch currencies but they manufacture new ones. This is the reality of sanctions evasion now, where individuals and networks build workarounds on demand. A7A5 also represents a quiet but significant leap. It has gone from co-opting decentralized finance to actively shaping it. This shift highlights an interesting realization that cryptocurrency innovation is now being hijacked not just for evasion but for sovereignty substitution. It suggests the arrival of a post-sanctions world, not where sanctions are ignored, but where they are priced into the cost of doing business.

The theoretical frameworks used here reveal this not just as a story of one rogue exchange but as a signal of systemic transition. Disruptive Innovation Theory shows how cryptocurrency displaces traditional financial choke points, creating new infrastructures where central banks and regulators once had authority. TOC Theory reveals how evasion networks function as illicit service providers, coordinating expertise, capital, and logistics across borders. Network Theory demonstrates how resilience is baked into their design and if one node falls, another absorbs the traffic. And Sanctions Busting Theory captures the adaptive evolution of these networks over time, identifying the logic of circumvention as iterative rather than

exceptional. Together, these theories do more than explain. The work of evasion is now modular, global, and technologically scalable. Its speed of adaptation will likely continue to outpace the tempo of governance unless structural paradigms are overhauled. And because adaptation is not limited by legal frameworks or diplomatic consensus, but by technological bandwidth, the enforcement community risks permanently trailing behind. The enforcement community still treats sanctions evasion as a matter of bad actors and weak compliance. But this thesis argues the opposite where the problem is not failure to enforce, but failure to understand the new terrain. Enforcement actions, even well-executed ones, operate at human speed. The actors operate at a speed where they're able to act first. The weaponization of decentralization has created a new kind of financial arms race, one where latency being both technical and bureaucratic is a vulnerability. Institutions built for hierarchical command structures are now contending with decentralized adversaries whose strength lies precisely in their lack of hierarchy.

This thesis depicts that cryptocurrencies being used as sanction evasion is an anomaly but a new financial operating system. One that treats regulations as obstacles to be routed around, not rules to be obeyed. One that builds privacy into its infrastructure, not as a bug but as a feature. And most crucially, one that has learned to monetize sanctions resistance. Sanctions are now a market opportunity, not a deterrent. And just as importantly, they are a political rallying cry. In a multipolar world, the very act of being sanctioned now garners strategic sympathy and accelerates investment into alternative rails. Being blacklisted by the U.S. Treasury, in some circles, has become a mark of defiance or a digital badge of opposition. The symbolic economy of sanctions now competes with their material effects. By examining Garantex, this thesis brings into focus the institutionalization of digital illicit finance. Sanction regimes will be forced to rethink how they measure effectiveness. If the goal is to disrupt flows, the evidence shows sanction regimes are one step behind. If the goal is deterrence, the data suggest innovation is being incentivized. This thesis has taken the case of one exchange and drawn a much broader conclusion. That the sanctions regimes as currently conceived are mismatched to the shape of the world they think they are confronting. That's because the failure of enforcement keeps getting redefined as to what is enforceable..

The conclusion, then, is not that cryptocurrencies are inherently malign, nor that sanctions have run their course. Instead, the evidence points to a financial environment that is decentralized, programmable, and increasingly contested. Jurisdictional borders blur and speed differentials between regulators and technologists can decide outcomes. By situating Garantex within this wider context, the thesis does not proclaim a definitive end to traditional financial authority; it highlights an ongoing enactment over how authority is constructed, delegated, and challenged in a digitized world. Whether the next chapter favors opacity or accountability will depend less on adversarial cat-and-mouse tactics and more on how quickly enforcement paradigms internalize the logic of decentralization. In short, the future of sanctions effectiveness

is unlikely to hinge on banning the right coin; it will turn on understanding the socio-technical systems in which value now moves.

Appendix

Categories	Codes	Remarks
Garantex’s Self-Perception	Compliance Facade	Publicly touts 'full AML-KYC compliance' despite lax onboarding
	Non-interference narrative	Frames Western measures as foreign meddling in domestic trade
	Counter-sanctions	Echoes Kremlin line that counter-sanctions will neutralize OFAC
Sanctions-Evasion Techniques	Stablecoin USDT	More than 20 B USDT via Tron after April 2022 designation
	Shift to A7A5 stablecoin	Ruble-pegged token issued via Kyrgyz shell to replace frozen USDT
	Mixer / wallet-hop	Daily deposit address rotation; links to TornadoCash, Sinbad
	Domain-hopping	garantex.org to grn-service.com to grinex.io within 18 months
	NFT Laundering	Small but notable use of illiquid NFTs for value transfer
	Privacy coin	Monero
	Tron	Prefers low-fee, high-anonymity TRON network for stablecoins
	OTC Ruble	Cash deposits at Moscow kiosks & QIWI vouchers feeding exchange
Related Actors	Ekaterina Zhadanova	Designated laundress

		funneling oligarch funds through Garantex
	Ransomware gangs	LockBit, Conti proceeds traced to Garantex hot wallet
	Hydra	Post-shutdown vendors shifted coin flows here
	PM2BTC	Mixing service with Garantex ties
	Dubai desks	Offshore liquidity suppliers for USDT-ruble trades
Enforcement Response	OFAC	Initial designation under E.O. 14024
	FinCEN	Identifies Garantex as primary money-laundering concern
	EU 16th sanctions package	Adds Garantex to EU asset freeze list

	Arrests	Admin arrested in India
	Wallet blacklists	Tether freezes ≈ $27 M across 350 addresses
	Domain seizure	"Secret Service & German BKA seize servers, websites"
Adaptation and Resilience	Grinex	"New UX, same backend; offers 'asset recovery' for blocked users"
	Jurisdictional arbitrage	Registers entities in Kyrgyzstan and maybe even Seychelles
	A7A5 incentives	Up to 20% APY reward for users

	P2P	Adds P2P module to shift trades off main order book
	Darkpool	Internal mixer?
	Telegram bot	Automates trades & withdrawals via bot commands
	Offshore	Transferring cold wallets
On-Chain Indicators	Ransomware wallet inflows	More than 100m from Conti
	Outbound to OTC desks	Large batched withdrawals to specific OTC clusters
	Tron-USDT	More than 80% of all exchange volume by 2024
	Cluster	Elliptic clusters 12 K addresses to single entity
	Volume resilience	"On‑chain volume dipped 30 % post‑seizure, rebounded within 6 weeks"
	Flash trades	Artificial volume padding
Regulatory Arbitrage	Domestic stablecoin	Push for RUB‑backed state‑approved stablecoin
	Payment processor	Local banks handle fiat settlement for A7A5 issuer
	Label	SaaS?
Media and Public Image	Western frame	Ransomware laundromat

	Telegram statements	Updates via public Telegram channel
	PR	Deny wrongdoing
	Russian Press	Garantex is scapegoat of crypto Cold War

Bibliography:

Andreas, P. (2000). Border games: Policing the U.S.–Mexico divide. Cornell University Press. https://www.researchgate.net/publication/257234304_Border_Games_Policing_the_US-Mexico_Divide

Arkham Intelligence. (n.d.). Garantex entity labels [Dataset]. Arkham Intelligence.

Atlantic Council. (2023). Central-bank digital-currency tracker. https://www.atlanticcouncil.org/cbdctracker/

Bloomberg. (2024, January 30) Russia Races to Legalize Crypto as Sanctions Weigh on Firms. https://www.bloomberg.com/news/articles/2024-07-30/russia-races-to-legalize-crypto-as-sanctions-weigh-on-companies

Barabási, A.-L. (2003). Linked: The new science of networks. https://www.researchgate.net/publication/220327363_The_New_Science_of_Networks

Berwick, A., & Foldy, B. (2024, April 1). Inside the Russian Shadow Trade for Weapons Parts, Fueled by Crypto. The Wall Street Journal. https://www.wsj.com/finance/currencies/crypto-fuelsrussian-shadow-trade-for-weapons-parts-1bfdc1a1

Bitcoinist. (2024, July 30). Total crypto ban in Russia imminent—lawmakers confirm. https://bitcoinist.com/total-crypto-ban-russia-imminent-lawmakers-confirm/

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), 213-238. https://www.aeaweb.org/articles?id=10.1257/jep.29.2.213

Brownworth, A., Durfee, J., Lee, M. J., & Martin, A. (2024). Regulating decentralized systems: Evidence from sanctions on Tornado Cash (Staff Report No. 1112). Federal Reserve Bank of New York. https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr1112.pdf

Bryman, A. (2016). Social research methods (5th ed.). Oxford University Press. https://ktpu.kpi.ua/wp-content/uploads/2014/02/social-research-methods-alan-bryman.pdf

Buck, J. (2017, October 15). BREAKING: Russia issuing “CryptoRuble”. Cointelegraph. https://cointelegraph.com/news/breaking-russia-issuing-cryptoruble

Casey, M. J., & Vigna, P. (2018). The truth machine: The blockchain and the future of everything. St. Martin's Press.

Castells, M. (2000). End of millennium (2nd ed.). Wiley-Blackwell. https://www.mediastudies.asia/wp-content/uploads/2016/09/Manuel_Castells_End_of_Millennium_The_Information_Age.pdf

Cavicchioli, M. (2020, February 24). Cryptocurrency wallets: adoption is on the rise. The Cryptonomist. https://en.cryptonomist.ch/2020/02/24/cryptocurrency-wallets-adoption-on-the-rise/

Chainalysis. (2023). 2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking. https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/

Chainalysis. (2024). Global crypto adoption index 2024. https://www.chainalysis.com/blog/2024-global-crypto-adoption-index/

Chainalysis. (2025). Crypto crime report 2025. https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf

Chainalysis. (2025, March 10). International action dismantles notorious Russian crypto exchange Garantex. https://www.chainalysis.com/blog/russian-exchange-garantex-dismantled/

Christensen, C. M. (1997). The innovator's dilemma. Harvard Business School Press. http://lib.ysu.am/open_books/413214.pdf

Congressional Research Service. (2022). Russia sanctions and cryptocurrencies: Policy issues (CRS Insight No. IN11939). https://www.congress.gov/crs-product/IN11920

Connolly, R. (2018). Russia's response to sanctions. Cambridge University Press. https://www.cambridge.org/core/books/russias-response-to-sanctions/EBC2355170FF2F318FE75AE1859D3B19

Council of the European Union. (2025, February 24). Sixteenth package of EU sanctions on Russia's war of aggression against Ukraine. Council of the European Union.

https://www.consilium.europa.eu/en/press/press-releases/2025/02/24/16th-package-of-sanctions-on-russia-s-war-of-aggression-against-ukraine-eu-lists-additional-48-individuals-and-35-entities/pdf/

Council of the European Union. (2014, July 30). Council Implementing Regulation (EU) No 826/2014. Official Journal of the European Union, L 226, 16-19. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2014:226:TOC

Council of the European Union. (2022, October 6). Eighth sanctions package: Full ban on crypto-asset services for Russian nationals. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2022:259I:TOC

Crawley, J. (2025, March 6). Tether freezes $28M of USDT on Russian crypto exchange Garantex. CoinDesk. https://www.coindesk.com/policy/2025/03/06/tether-freezes-usd28m-usdt-on-russian-crypto-exchange-garantex

Creswell, J. W., (2009). Designing and conducting mixed methods research (3rd ed.). SAGE. https://www.ucg.ac.me/skladiste/blog_609332/objava_105202/fajlovi/Creswell.pdf

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. BMC Medical Research Methodology, 11, Article 100. https://bmcmedresmethodol.biomedcentral.com/articles/10.1186/1471-2288-11-100

Early, B. R. (2015). Busted sanctions: Explaining why economic sanctions fail. Stanford University Press.

Edwards, A., & Gill, P. (2003). The politics of transnational organized crime. British Journal of Criminology, 43(2), 319-340. https://www.researchgate.net/publication/27650247_The_Politics_of_'Transnational_Organized_Crime'_Discourse_Reflexivity_and_the_Narration_of_'Threat'

Elliptic. (2023). Sanctions Compliance in Cryptocurrencies 2023. https://www.elliptic.co/resources/elliptic-guide-to-sanctions-compliance-in-crypto-2023

Elliptic. (2025). Elliptic in Action: Uncloaking Garantex for law enforcement and sanctions compliance. https://www.elliptic.co/blog/elliptic-in-action-garantex

Estonian Financial Intelligence Unit. (2021). Estonian Financial Intelligence

Unit Yearbook 2021.
https://fiu.ee/sites/default/files/documents/2022-07/RAB_aastaraamat_ENG_veebi.pdf

Estonian Financial Intelligence Unit. (2022, March 10). Garantex Europe OÜ lost right to provide virtual-currency services.
https://fiu.ee/en/news/garantex-europe-ou-lost-right-provide-virtual-currency-services

Fabrichnaya, E., & Marrow, A. (2025, March 6). Sanctioned Russian crypto exchange suspends services as Tether blocks wallets. Reuters.
https://www.reuters.com/technology/sanctioned-russian-crypto-exchange-suspends-services-tether-blocks-wallets-2025-03-06/

Financial Action Task Force. (2023). Targeted update on the implementation of the FATF standards on virtual assets and VASPs.
https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/June2023-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf

FinCEN. (2022). Advisory on Russian sanctions evasion using virtual currencies. U.S.-Treasury.
https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Sanctions%20Evasion%20FINAL%20508.pdf

Fintegrity. (2024). Russian Use of Crypto for Sanctions Evasion on the Rise.
https://finintegrity.org/russian-use-of-crypto-sanctions-evasion-on-rise/

Galeotti, M. (2018). The Vory: Russia's super mafia. Yale University Press.
https://archive.org/details/the-vory-russias-super-mafia-2018-mark-galeotti

Global Ledger. (2025). Same Garantex, Different Sauce. "New" Russian Exchange Grinex Launched.
https://www.globalledger.io/same-garantex-different-sauce-new-russian-exchange-grinex-launched/

Grauer, K. (2024, September 5). Russia's cryptocurrency pivot: Legislated sanctions evasion. Chainalysis Blog.
https://www.chainalysis.com/blog/russias-cryptocurrency-legislated-sanctions-evasion/

Gudzowska, J., Lockhart, E., & Keatinge, T. (2024, May 7). Disabling the enablers of sanctions circumvention. Royal United Services Institute.
https://rusi.org/explore-our-research/publications/policy-briefs/disabling-enablers-sanctions-circumvention

Hsieh, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. Qualitative Health Research, 15(9), 1277-1288. https://www.researchgate.net/publication/7561647_Three_Approaches_to_Qualitative_Content_Analysis

Hufbauer, G. C., Schott, J. J., Elliott, K. A., & Oegg, B. (2007). Economic sanctions reconsidered (3rd ed.). Peterson Institute for International Economics. https://dl1.cuni.cz/pluginfile.php/863435/mod_resource/content/0/Gary%20Clyde%20Hufbauer%2C%20Jeffrey%20J.%20Schott%2C%20Kimberly%20Ann%20Elliott%2C%20Barbara%20Oegg-Economic%20Sanctions%20Reconsidered%20%282008%29.pdf

Hume, E., & Rutter, K. (2025, March 11). Sanctions by the numbers: 2024 year in review. Center for a New American Security. https://www.cnas.org/publications/reports/sanctions-by-the-numbers-2024-year-in-review

Katzman, K. (2019, November 15). Iran sanctions (CRS Report No. RS20871). Congressional Research Service. https://www.everycrsreport.com/files/20191115_RS20871_84b40bd275f6ce5988354065f35bb900c1b17c9c.pdf

Kaushik, V., & Walsh, C. A. (2019). Pragmatism as a research paradigm. Social Sciences, 8(9), 255. https://www.mdpi.com/2076-0760/8/9/255

Krippendorff, K. (2019). Content analysis (4th ed.). SAGE. https://books.google.ee/books?hl=en&lr=&id=nE1aDwAAQBAJ&oi=fnd&pg=PP1&dq=Krippendorff,+K.+(2019).+Content+analysis+(4th+ed.)&ots=y_blZveK6A&sig=GHKeLwaBPV_HwK1o9pAnnpcEyXk&redir_esc=y#v=onepage&q&f=false

Kupatadze, A. (2012). Organized crime, political transitions, and state formation in post-Soviet Eurasia. Palgrave Macmillan.

Laine, M., Rosca, M., & Kozyreva, T. (2024, March 13). Firm linked to sanctioned exchange Garantex partners with gang leader. ICIJ. https://www.icij.org/investigations/russia-archive/firm-related-to-sanctioned-crypto-exchange-garantex-is-a-partner-of-moscow-gang-leader-and-has-links-to-kremlin-controlled-rosneft/

Lakshmanan, R. (2025, March 7). U.S. Secret Service seizes Russian Garantex crypto exchange website. The Hacker News. https://thehackernews.com/2025/03/us-secret-service-seizes-russian.html

Levi, M. (2002). Money laundering and its regulation. The Annals of the American Academy of Political and Social Science. https://www.jstor.org/stable/1049742

Manzi, D., & Calderoni, F. (2024). An agent-based model for assessing the resilience of drug trafficking organizations to law enforcement interventions. Journal of Artificial Societies and Social Simulation. https://www.jasss.org/27/3/3.html

Merkle Science. (2025). Same Chain, New Name? Unpacking Grinex's Connection to Garantex. https://www.merklescience.com/blog/same-chain-new-name-unpacking-grinexs-connection-to-garantex

Morgan, D. L. (2007). Paradigms lost and pragmatism regained. Journal of Mixed Methods Research, 1(1), 48-76. https://www.researchgate.net/publication/240730449_Paradigms_Lost_and_Pragmatism_Regained_Methodological_Implications_of_Combining_Qualitative_and_Quantitative_Methods

Morselli, C. (2009). Inside criminal networks. Springer. https://content.e-bookshelf.de/media/reading/L-122-a21a28ff1c.pdf

Neuman, W. L. (2014). Social research methods (7th ed.). Pearson. https://letrunghieutvu.yolasite.com/resources/w-lawrence-neuman-social-research-methods_-qualitative-and-quantitative-approaches-pearson-education-limited-2013.pdf

Office of Foreign Assets Control. (2022). Sanctions advisories and designations: Hydra & Garantex. U.S. Department of the Treasury. https://home.treasury.gov/news/press-releases/jy0701

Office of Foreign Assets Control. (2024, March 25). Russia-related designations; cyber-related designations. https://ofac.treasury.gov/recent-actions/20240325

Pape, R. A. (1997). Why economic sanctions do not work. International Security, 22(2), 90-136. https://web.stanford.edu/class/ips216/Readings/pape_97%20(jstor).pdf

Passas, N. (2003). Cross-border crime and the interface between legal and illegal actors. https://www.researchgate.net/publication/31975954_Cross-border_Crime_and_the_Interface_between_Legal_and_Illegal_Actors

Patton, M. Q. (2014). Qualitative research & evaluation methods (4th ed.). SAGE.

https://archive.org/details/michael-quinn-patton-qualitative-research-evaluation-methods-integrating-theory-/page/n5/mode/2up

RBC. (2025, March 7). Криптобиржа назвала себя “шахматной фигурой” после блокировки активов в США.
https://www.rbc.ru/finances/07/03/2025/67cb4b8a9a79473651152e3a

Ratex42. (2025). Garantex Rebrands as Grinex to Evade Sanctions:A RatEx42 Briefing.
https://ratex42.com/garantex-rebrands-as-grinex-to-evade-sanctions-a-ratex42-briefing/

Reinsch, W. A., & Palazzi, A. L. (2022, December 20). Cryptocurrencies and U.S. sanctions evasion: Implications for Russia. Center for Strategic and International Studies.
https://www.csis.org/analysis/cryptocurrencies-and-us-sanctions-evasion-implications-russia

Reuters. (2023, November 3). US sanctions Russian national for helping elites launder money.
https://www.reuters.com/world/us-sanctions-russian-national-helping-elites-launder-money-2023-11-03/

Reuter, P. (1983). Disorganized crime: The economics of the visible hand. MIT Press.
https://archive.org/details/disorganizedcrim00reut/page/n3/mode/2up

Rogers, E. M. (1962). Diffusion of innovations. The Free Press.
https://teddykw2.wordpress.com/wp-content/uploads/2012/07/everett-m-rogers-diffusion-of-innovations.pdf

Royal United Services Institute. (2023). Track and Disrupt: How to Counter Sanctions-Evasion Networks.
https://www.rusi.org/explore-our-research/publications/commentary/track-and-disrupt-how-counter-sanctions-evasion-networks

Salmons, J. (2023, January 11). Designing research with case study methods. Sage Research Methods Community.
https://researchmethodscommunity.sagepub.com/blog/designing-research-with-case-study-methods

Soska, K., & Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. USENIX Association.
https://www.researchgate.net/publication/308057059_Measuring_the_longitudinal_evolution_of_the_online_anonymous_marketplace_ecosystem

TRM Labs. (2023). The Illicit Crypto Economy. https://uploads-ssl.webflow.com/6082dc5b67056233213587a4/66a93f4124c834f3f4ab175c_TRM_The%20Illicit%20Crypto%20Economy%20Key%20Trends%20from%202023_Report.pdf

TRM Labs. (2025, March 6). The takedown of Garantex: A notorious crypto exchange's role in illicit finance. https://www.trmlabs.com/resources/blog/the-takedown-of-garantex-a-notorious-crypto-exchanges-role-in-illicit-finance

TRM Labs. (2025, April 28). Grinex Emerges as Likely Garantex Rebrand. https://www.trmlabs.com/resources/blog/grinex-emerges-as-likely-garantex-rebrand

U.S. Customs and Border Protection. (2025, January 13). Automated Commercial Environment electronic export manifest for rail cargo [Proposed rule]. Federal Register, 90(7), 2874–2919. https://www.federalregister.gov/documents/2025/01/13/2024-31331/automated-commercial-environment-ace-electronic-export-manifest-for-rail-cargo

U.S. Department of Justice. (2022, April 5). Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace. https://www.justice.gov/archives/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace

U.S. Department of Justice. (2025, March 7). Garantex Cryptocurrency Exchange Disrupted in International Operation. https://www.justice.gov/opa/pr/garantex-cryptocurrency-exchange-disrupted-international-operation

U.S. Department of the Treasury, Office of Foreign Assets Control. (2022, April 5). Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex. https://home.treasury.gov/news/press-releases/jy0701

U.S. Department of the Treasury, Office of Foreign Assets Control. (2023, November 3). Treasury designates virtual currency money launderer for Russian elites and cybercriminals. https://home.treasury.gov/news/press-releases/jy1874

U.S. Department of the Treasury, Office of Foreign Assets Control. (2024, March 25). Treasury designates Russian companies supporting sanctions evasion through virtual asset services and technology procurement. https://home.treasury.gov/news/press-releases/jy2204

U.S. Department of the Treasury, Office of Foreign Assets Control. (2024, September 26). Treasury takes coordinated actions against illicit Russian virtual currency exchanges and cybercrime facilitator. https://home.treasury.gov/news/press-releases/jy2616

Warren, E. (2024, April 9). An update from the Treasury Department: Countering illicit finance, terrorism, and sanctions evasion [Senate hearing transcript]. U.S. Senate Committee on Banking, Housing, and Urban Affairs. https://www.banking.senate.gov/hearings/an-update-from-the-treasury-department-countering-illicit-finance-terrorism-and-sanctions-evasion

Weiss, A. S., & Blanc, J. (2019, April 3). U.S. sanctions on Russia: Congress should go back to fundamentals. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2019/04/us-sanctions-on-russia-congress-should-go-back-to-fundamentals?lang=en

Winston, S. (2022). Russia–Ukraine Conflict Increases Regulatory Risks for Sanctions Evasion Through Crypto-Based Transactions. https://www.winston.com/en/blogs-and-podcasts/global-trade-and-foreign-policy-insights/russiaukraine-conflict-increases-regulatory-risks-for-sanctions-evasion-through-crypto-based-transactions

Yin, R. K. (2018). Case study research and applications (6th ed.). SAGE. https://www.slideshare.net/slideshow/yin-r-k-2018-case-study-research-and-applications-design-andocx/255153005