

Journal of Digital Science



ISSN 2686-8296

Volume 8 Issue 1

2026

Institute of Cited Scientists (ICS)

Regulatory Challenges of Virtual Assets Financing in Pakistan

Amjad Fraz¹[0009-0002-6395-3805], Zahid Khan¹[0000-0003-3756-1058]

¹ Centre for Aerospace and Security Studies (CASS), Lahore, Pakistan

Received 11.03.2026/Revised 29.06.2026/Accepted 29.06.2026/Published 30.06.2026

<https://doi.org/10.33847/2686-8296.8.1> 1

Abstract. This research paper examines how Pakistan can reduce the risks of terrorist financing (TF) linked to virtual assets (VAs) by enhancing data-intensive workflow for pre-existing authorities. Using a qualitative content analysis approach, the study takes statutes, regulator circulars, and institutional analyses and reports as primary sources, triangulated with reputable secondary reporting. The findings highlight three recurring gaps: the absence of a settled licensing and inspection regime for virtual-asset service providers, missing Travel-Rule messaging, and weak evidentiary continuity between alert and arrest. These stratifications are magnified by high grassroots adoption of the VAs and a significant cash usage dependency. Priority recommendations include the designation of a virtual-asset service provider (VASP) supervisor, the creation of a national "Travel-Rule" utility, the creation of rapid-freeze and evidence-continuity protocols, and publishing sector-specific red flags using standardised suspicious transaction report (STR) crypto fields. Taken together, these measures can provide admissible, timely evidence while protecting lawful innovation and strengthening cross-border investigative cooperation capacity.

Keywords: Pakistan Cryptocurrency Council; virtual assets; terrorist financing; VASP licensing; Travel Rule; Raast/NADRA.

1. Introduction

Crypto assets have dual-use potential. They not only accelerate cross-border transfers and widen access to the masses, but they can also frustrate counter-terrorist financing (CTF). They offer pseudonymous rails that can disguise fraudulent proceeds and cross-border transfers with minimal friction. Owing to this backdrop, global policies now extend anti-money laundering (AML)/CTF duties to virtual assets (VAs) and the firms that handle them. For instance, the Financial Action Task Force (FATF) highlights that unhosted wallets, mixers/bridges and some stablecoins can impede attribution and cross-border information-sharing [1].

In light of similar concerns, states are adopting policies to streamline VA flow in their economies. China, for instance, has tightened its administrative tools to address the harms. Associated with online fraud and money laundering, its Anti-Telecom and Online Fraud Law makes enabling money laundering that uses cryptocurrency an offence [2]. Extending the judicial cover to the VA crimes, China's top court issued a joint judicial interpretation that explicitly recognises laundering "through virtual-asset transactions and financial-asset exchanges," pulling crypto into mainstream money-laundering prosecutions [3].

These concerns are also relevant to Pakistan, given its retail-heavy profile. The Federal Investigation Agency (FIA)'s 2024 report documents a significant increase in cybercrime caseloads, including recurring crypto-linked frauds, whose proceeds are transferred across chains or liquidated through over-the-counter (OTC) cash-outs, which complicates recovery efforts [4]. Concurrently, regulators have reported mass takedowns of more than a hundred predatory financial apps through the coordination

of the State Bank of Pakistan (SBP), the Securities and Exchange Commission of Pakistan (SECP), and the Pakistan Telecommunication Authority (PTA), demonstrating that distribution control is feasible when triggers are clear [5].

Additionally, a 2018 State Bank circular prohibits banks, payment firms, and electronic money institutions (EMIs) from dealing in virtual currencies or tokens, which shifted the VA activity to peer-to-peer (P2P) channels and offshore platforms beyond locally supervised perimeters [6]. Yet adoption has remained high by global measures, driven by retail savers, gig-economy earners paid in stablecoins, and remittance-adjacent flows. As of Q3 FY2025, there are approximately 22.6 million mobile-banking users in Pakistan and around 68.5 million branchless bank accounts, providing a sufficient scope for VA-based risk controls [7]. These figures underscore both the opportunity for compliant controls with broad digital reach and the risk that large user cohorts remain exposed to unsupervised operators.

The problem lies in the fact that Pakistan relies on prohibition rather than supervision for VAs. Resultantly, most crypto activity has shifted to P2P. This creates blind spots for CTF where stablecoin inflows, remittance-style payments and online fraud proceeds mix with hawala [8] and cash networks. Since exiting the FATF grey list in 2022, Pakistan has maintained an intensified focus on expediting intelligence sharing, strengthening investigations, and deepening cross-border cooperation. These are the capabilities that are decisive for the effective prosecution of VA offences [9]. Nonetheless, the responsibilities for VAs are still split across SBP, SECP, FMU and FIA, and there is no common framework for VASP supervision, the Travel Rule or crypto-specific suspicious-transaction reporting.

Against this backdrop, this paper asks: What regulatory and institutional challenges does Pakistan face in preventing the misuse of cryptocurrencies and other virtual assets for terrorist financing, and how can these challenges be addressed without undermining lawful economic use? To answer this question, the paper maps Pakistan's emerging VA risk architecture and examines how existing AML/CTF authorities apply to cryptocurrencies and related intermediaries. Second, it identifies regulatory, supervisory and operational gaps that limit the detection, freezing and prosecution of crypto-enabled TF.

In this enquiry, the Pakistan Crypto Council (PCC) is treated not as a substitute regulator but as a coordination hub. Its practicality could be assessed by how it can align the SBP, SECP, Financial Monitoring Unit (FMU), and FIA on a single supervision model. The model includes supervision of virtual-asset service providers (VASPs), a standardised Travel-Rule, [10] and a consolidated suspicious transaction report (STR) for crypto data. Grounded in an institutionalist understanding of regulation, the research tests how a PCC-led coordination across the above-mentioned chokepoints can measurably reduce TF abuse while preserving innovation.

2. Literature Review

2.1 Global policy frameworks on virtual assets

Global policy outlook on VAs and VASPs has coalesced around the FATF Recommendation 15 and its Interpretive Note, which extend AML/CFT obligations that include customer due diligence, record-keeping, suspicious transaction reporting, targeted financial sanctions, and the Travel Rule to VA activity [11]. The FATF's 2025 targeted update documents highlight lagging implementation and persistent blind spots with a call for stronger cross-border cooperation [12]. Complementing this, the IMF strategy reviews frame crypto oversight as a public-policy challenge that links financial integrity with macro-financial stability and spillovers from weak regimes [13]. Similarly, the Bank of International Settlements (2025) argues that compliance should leverage public provenance on blockchains (including stablecoins) and be

embedded in market infrastructure, rather than relying solely on ex-post policing [14].

2.2 Regulatory models in mature jurisdictions

Another recurring observation was that regulatory effectiveness is most observable where jurisdictions operationalise the Travel Rule, authorise VASPs on a risk-tiered basis, and impose clear conduct/marketing and client-asset safeguarding duties. The European Union's Transfer of Funds Regulation (TFR) (2023/1113) extends wire-transfer transparency norms to "certain crypto-assets," while Markets in Crypto-Assets (MiCA) Regulation supplies an authorisation and conduct regime, particularly for asset-referenced tokens and e-money tokens [15]. The United Kingdom (UK) implemented the Travel Rule in 2023 and is moving toward a comprehensive regime for exchange and custody activities under the Financial Conduct Authority (FCA), with a focus on information sharing and supervision [16].

Singapore's Payment Services Act framework and ongoing Monetary Authority of Singapore (MAS) notice (PSN02) emphasise licensing breadth, risk-based capital/liquidity, and Travel Rule compliance [17]. Similarly, Dubai's Virtual Assets Regulatory Authority (VARA) has promulgated activity-specific rulebooks that combine prudential conduct and marketing controls [18]. These varied, mature-regime approaches converge on three instruments associated with better outcomes: (i) enforceable Travel Rule utilities; (ii) authorisation with proportionate inspections and sanctions; and (iii) explicit consumer-protection and disclosures that restrict retail exposure to high-risk products.

2.3 Pakistan's regulatory stance and infrastructures

Pakistan-specific scholarship and public documentation reveal a different starting point. The SBP in 2018 prohibited regulated entities from dealing in virtual currencies and Initial Coin Offering (ICO) tokens, a position that effectively pushed crypto activity to P2P and offshore channels [19]. Pakistan's Financial Monitoring Unit (FMU) has since published a strategic analysis highlighting VA-related ML/TF vulnerabilities and signalling the need for systematic suspicious-reporting pathways that capture crypto on/off-ramp [20] behaviour [21].

Meanwhile, Pakistan's payments and identity infrastructures, Raast (instant payments) and National Database and Registration Authority (NADRA)'s biometric Electronic Know Your Customer (e-KYC) services have matured, creating strong theoretical chokepoints for AML/CFT controls at cash-in/cash-out, even in the absence of a modified VASP regime [22]. Recent reporting on the PCC and proposals to channel surplus electricity into mining and data-centre infrastructure suggest a policy pivot from blanket prohibitions toward managed integration of digital-asset activity, with implications for authorisation, supervision, and cross-border cooperation [23].

Research Gap: All in all, the global canon identifies what works (Travel Rule implementation, VASP authorisation, conduct rules) and why (alignment of chokepoints and data flows), while Pakistan-focused literature under-specifies how domestic payment identity rails and inter-agency practice could be harnessed to reduce TF misuse without stifling innovation. This gap is what the present study addresses.

3. Data and Methodology

For this research paper, a qualitative content analysis-based design [24]. This was best-fit because (a) the research question relies on institutional coordination; (b) authoritative meaning, what regulators require, permit or prohibit, is embedded in legal/institutional texts, not readily reducible to numeric representations; and (c) core

outcomes, e.g., time-to-freeze; evidentiary continuity, are influenced by procedural linkages traceable through documents, not easily captured by statistics.

Primary data sources comprise: (a) binding instruments i.e., the *Virtual Assets Ordinance, 2025* (setting the statutory frame and the Pakistan Virtual Assets Regulatory Authority, PVARA); (b) regulatory circulars and public notices from the (SBP) defining the treatment of virtual currencies in the banking and payments perimeter; (c) financial-intelligence outputs from the Financial Monitoring Unit (FMU), including its strategic analysis of VA-related ML/TF vulnerabilities; and (d) official disclosures/press communiqués evidencing institutional milestones. Secondary sources include reputable newswires and industry outlets, but they are carefully used only to corroborate timing and policy emphasis. Documents were retrieved from official portals.

Conceptually, this paper is based on new institutional economics, which sees institutions as “the rules of the game in a society” which structure the incentives and transaction costs for economic actors [25]. In this view, formal rules such as laws, regulations and supervisory mandates and informal norms e.g. cash preference, trust in hawala and tolerance of grey-zone platforms, jointly determine how, and through which channels, value moves. Drawing on Coase, transaction costs like the effort required to verify counterparties, move funds across borders or comply with due-diligence requirements are at the heart of understanding why some actors prefer to use pseudonymous crypto rails instead of supervised banking channels [26]. Williamson’s work on structures of governance emphasises the way they provide very different bundles of monitoring and enforcement of transactions as well as residual risk by changing the governance structure of a system, i.e. working with bank-centred systems, licensed virtual-asset service providers or lightly policed P2P markets [27].

Applied to the landscape of the virtual assets in Pakistan, such a framework implies that the financing of terrorist activity by means of crypto is not simply a product of technology, but of mismatched rules and organisations. Prohibitions, an absent domestic VASP licensing regime, and missing or weak evidence generation routines lower the expected costs of misuse and increase the costs of coordinated enforcement. Conversely, proposed reforms, PVARA, coordination by Pakistan Crypto Council, a national Travel-Rule utility and fast-freeze protocols, are known to be an attempt to reset the institutional rules of the game, so that data travels with value and terrorist financiers face more friction and legal risk.

Moreover, this study exhibits two limitations. Firstly, policies are changing fast: Because 2025 is the first year of PVARA, new rules and licensing guides are still surfacing. What this research reports now might need an update as the PCC’s functional typology and jurisdictional contours are further elaborated in future. Secondly, the findings may not be generalisable well: FATF rules are global, but Pakistan’s systems, such as Raast for instant payments and NADRA for e-KYC, are very local. What works here may not work the same way in other countries.

4. Results and Discussion

Financial technology, or FinTech, refers to the use of digital platforms and infrastructures to deliver financial services more efficiently than traditional banking. In Pakistan, this encompasses the *Raast* instant payment system, biometric e-KYC provided by the NADRA, and licensed electronic money institutions (EMIs). Together, these tools widen financial inclusion and reduce costs in remittances and payments, while also creating new chokepoints for anti-money laundering and counter-terrorist financing (AML/CFT) supervision.

Cryptocurrency is a category of virtual assets recorded on blockchain or distributed ledger systems. However, in essence, Crypto assets operate outside state-issued money but can be transferred P2P, held in digital wallets, or exchanged via intermediaries. While their transparency on-chain is valuable for forensic analysis,

anonymity at the conversion points, combined with mixers or cross-chain bridges, allows illicit actors to disguise ownership and movement [28].

Despite challenges, several states have incorporated cryptocurrency or related infrastructure into their policies. El Salvador adopted Bitcoin as legal tender in 2021 to lower remittance costs and promote financial inclusion [29]. Nigeria launched the eNaira in 2021 as Africa’s first central bank digital currency (CBDC) to strengthen cashless payments [30]. China has piloted its digital yuan to modernise domestic payments and reduce reliance on US dollar clearing networks [31]. Pakistan has announced a shift from prohibition to managed integration itself.

The same qualities that make cryptocurrency appealing for innovation, speed, borderless transfer, and programmability, also create vulnerabilities. Terrorist groups have used social media to solicit micro-donations, convert them into stablecoins, and then route them through mixers and bridges. Global cases show how governance gaps are exploited, and how they are closed when data travels with value.

In 2020, a coordinated US action dismantled three terror-finance campaigns linked to al-Qaeda and Islamic State. The authorities seized massive cryptocurrency assets by correlating donation addresses advertised on social media with exchange-side KYC and transaction trails, then obtaining forfeiture orders [32]. In October 2023 and again in 2024, the Office of Foreign Assets Control (OFAC) targeted Hamas facilitators and a Gaza-based virtual currency exchange, describing flows that transited mixers and multiple networks. These seizures relied on linking wallet clusters to named operators and obliging exchanges to act [33].

In March 2025, the US Department of Justice announced court-authorised seizure of around USD 200,000 intended for a terrorist organisation, again illustrating the sequence as illustrated in fig 1: advertisement → stablecoin or Tron-based receipt → mixer or bridge hops → cash-out via compliant or complicit exchangers.

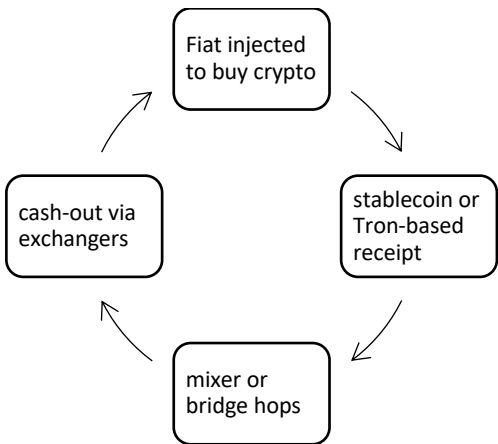


Fig. 1. Terror Finance Value-Transfer Cycle. Source: authors' elaboration.

This cycle was interdicted when analytics and Travel-Rule-type data stitched the path together [34]. Europol’s Terrorism Situation and Trend report (TE-SAT) underscores the same point: crypto is a “component” of a hybrid toolkit, and effectiveness turns on speed, data sharing, and cross-border cooperation [35].

4.1 Pakistan’s Emerging Virtual-Asset and Crypto Risk Architecture

4.1.1 Fiat Payment Rails, Digital Identity and Chokepoints

Pakistan is transitioning from hard cash to instant digital transfers; however, a significant portion of value still resides in notes, which keeps activity off-grid for

AML/CFT controls. The currency in circulation stood at nearly PKR 10.8 trillion in August 2025, accounting for about 27% of broad money, indicating a deep-seated cash habit [36]. At the same time, in Q3 FY25 alone, Raast handled approximately 371 million instant payments worth approximately PKR 8.5 trillion, with retail digital payments reaching PKR 164 trillion for the quarter [37].

NADRA's biometric e-KYC and the State Bank's consolidated digital onboarding rules now allow bank-grade verification for remote customers [38]. Several EMIs are licensed, widening access to e-money and wallets [39]. These rails create visibility at chokepoints, but cash preference and off-platform habits still mask many flows. There are technological enablers like device and network artefacts, recycled fingerprints, emulator use, virtual private networks (VPNs), or logins from high-risk autonomous system numbers (ASNs) that often mark mule clusters that conventional KYC misses.

4.1.2 Crypto Adoption, TF Exposure and Structural Frictions

Scale and policy shift in Pakistan's crypto use

Pakistan ranks third among the top global adopters in its overall index for 2025, reflecting significant use in retail and remittance-related sectors [40]. Industry and media estimates commonly place the number of crypto owners in the 15-20 million range, although exact counts vary by method [41]. The policy disposition is also changing. In 2025, authorities announced an allocation of 2,000 Megawatts for bitcoin mining and AI data centres, and the PCC emerged as a coordination forum, even as formal VASP licensing remains pending [42].

Core components of the crypto risk landscape

Beyond traditional VAs, the highest financial-integrity risk in Pakistan's crypto landscape sits where fiat meets crypto [43]. The cryptocurrency risk landscape has three key components as illustrated in fig 2. First, households and freelancers are increasingly parking savings or settling cross-border earnings in stablecoins, sometimes declaring them as generic "digital returns," which complicates tax and AML checks at cash-in/cash-out points. Second, the FIA's 2024 data records thousands of cybercrime cases, including recurring complaints linked to cryptocurrency and challenges in recovering funds that pass through mixers or cross chains [44]. Third, TF risks are small in volume but non-trivial in pattern. The FATF's 2025 update flags small-ticket crowdfunding, mixers/bridges, unhosted wallets, and stablecoin rails as persistent blind spots where supervision is absent in Pakistan [45].

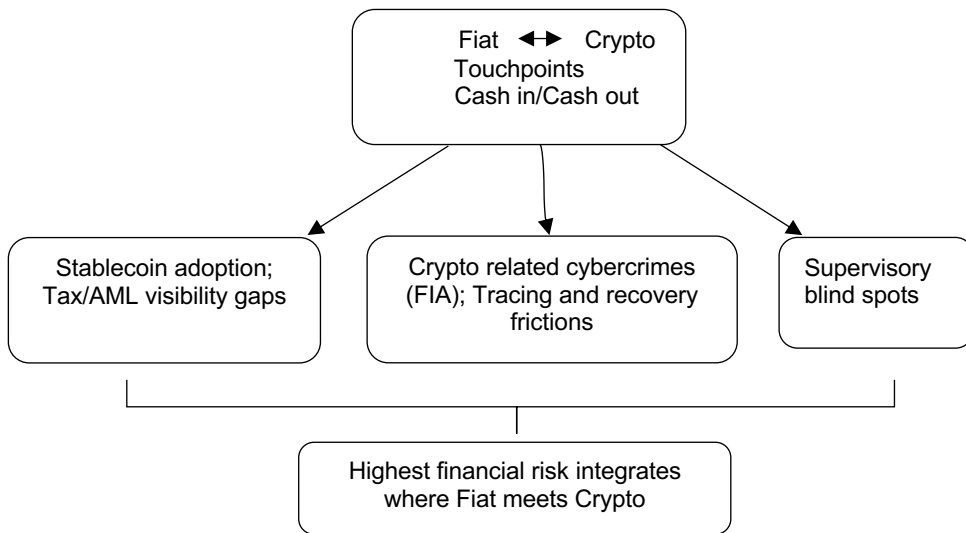


Fig. 2. Pakistan's crypto risk landscape

Fiat–Crypto TF Risk Chain

Pakistan's exposure is structural rather than speculative. Where institutions are already trying to stifle the TF networks, but when crypto does appear, the pattern mirrors global cases. The chain identified as specific to Pakistan has three nodes: small-ticket crowdfunding, rapid chain-hops and offshore cash-outs. At onboarding, weak device-risk controls or recycled biometrics can pass as ordinary payments; in-flight, absent Travel-Rule utilities mean originator and beneficiary data fall away; at exit, P2P OTC encashment and merchant-refund loops break audit trails. The result is weak evidence that impedes timely and ensured prosecutions. The pattern is illustrated in Fig. 3 for better understanding.

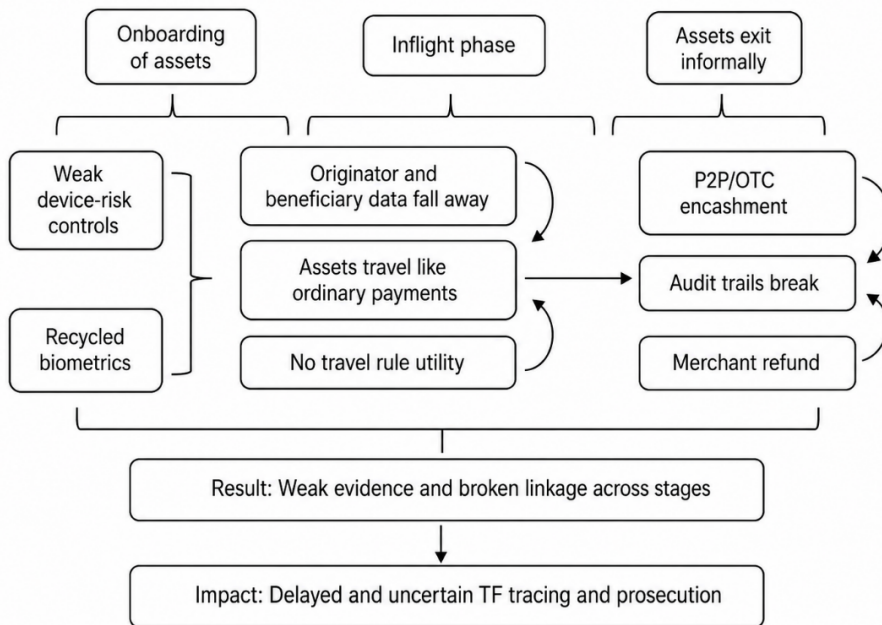


Fig. 3. Pakistan’s high-risk transaction chain

Structural frictions between detection and prosecution

Seen against this flow, three frictions repeatedly break the chain from detection to interdiction. First, licensing and supervision remain undefined for VASPs serving Pakistani users. Following SBP’s 2018 prohibition, a lack of a domestic licensing rulebook for exchanges, custodians, or brokers, record-keeping, audits, and inspections remains largely out of reach. Second, Travel-Rule plumbing is missing. There is no national utility or mandated data schema to ensure originator and beneficiary information accompanies cross-border transfers, blurring money trails whenever a Pakistani user interacts with a foreign platform. Third, evidentiary continuity is uneven. Case files can lack wallet-control proof or reproducible path traces, precisely the materials that prosecutors abroad now expect.

Pakistan’s enforcement actors are active. The SECP has helped block over 130-140 illegal financial apps; however, distribution control alone cannot substitute for VASP-side supervision and data interoperability [46]. Pakistan’s institutions and controls can now be assessed for licensing and inspections, Travel-Rule plumbing, evidentiary continuity and freezing powers.

4.2. Institutional Architecture of Pakistan’s Virtual-Assets Regime

4.2.1 Institutional Perimeter: SBP-SECP-FMU/FIA-PTA

Pakistan’s cryptocurrency perimeter is defined less by a single “crypto law” than by how the nature of existing financial crimes and market conduct are applied to the virtual assets market and its intermediaries.

The SBP remains the decisive gatekeeper because it regulates banks, payment

service providers and EMIs, the very channels that convert rupees into and out of crypto. The SBP prohibits regulated entities from dealing in virtual currencies or tokens, and in practice, this has pushed activity to P2P rails, offshore exchanges, and informal OTC cash-outs.

Secondly, the Securities and Exchange Commission of Pakistan (SECP) influences crypto where services resemble investment or market-intermediation, e.g., custody and exchange-like functions, and its recent campaigns against illegal crypto trade and parking apps also show a willingness to police the apps even if servers sit offshore [47]. Recently, coordinated actions with SBP and SECP have removed dozens of illicit financial apps, signalling that distribution control is feasible if triggers are clear.

The Financial Monitoring Unit (FMU) is the country's FIU; it receives STRs/CTRs, conducts financial-intelligence analysis, and disseminates cases to law enforcement. Its fundamental task is flagging ML/TF vulnerabilities and calling for systematic capture of on/off-ramp behaviours in suspicious reporting [48].

Moreover, the FIA handles cyber-enabled fraud, asset seizure/freezing, and digital forensics. Lately, the FIA has been receiving numerous crypto-linked complaints. The FIA warns that the recovery challenges against the frauds persist because the funds move across chains or through OTC encashment networks [49]. Similarly, the Pakistan Telecommunication Authority (PTA) provides the takedown lever for high-risk apps, wallets, and phishing infrastructure that target local users.

Finally, the Pakistan Crypto Council (PCC) has been signalled as a policy co-ordination forum; public reporting in 2025 links the PCC's emergence to broader digital-asset ambitions, including the government's announcement to allocate 2,000 MW for bitcoin mining and AI data centres. These initiatives, like this, however, raise traceability questions at scale if they proceed without a supervised VASP perimeter.

4.2.2 The Two-Pillar Model and the PCC's Role

The background established above lays the impetus for Pakistan's pivot to a two-pillar framework: a statutory regulator to license and supervise the market, and a policy hub to knit disparate institutions into a workable whole.

The first is the Pakistan Virtual Assets Regulatory Authority (PVARA), established by the Virtual Assets Ordinance, 2025 (Ordinance No. VII of 2025); the second is the PCC, an executive coordination body under the Ministry of Finance [50]. The Ordinance, promulgated on 8 July 2025 and published in the Gazette the following day, authorises PVARA to license, regulate and supervise virtual-asset service providers (VASPs) and to issue rules in line with international standards [51].

PVARA's early institutional signals have been concrete. It convened an inaugural board meeting in Islamabad in late August 2025, and soon after, invited global exchanges and other VASPs to submit expressions of interest for Pakistan's entry under the new regime [52]. This sequencing matters: it anchors market development in licensing, prudential safeguards, and surveillance, rather than allowing for permissive ambiguity.

Within that policy architecture, the PCC functions as the system's connective tissue. It is not a licensing authority; rather, it convenes the Ministry of Finance, SBP, SECP, FMU, and relevant law enforcement bodies to ensure that the rules PVARA writes can be executed across the payments, securities, taxation, and criminal justice domains. In practice, this means helping VASPs adhere to a common template while banks and payment firms understand their obligations at the on- and off-ramps [53].

This alignment is especially important for CFT. Pakistan's FMU has, for some years, flagged virtual assets as higher-risk for money laundering and terror finance because of pseudonymous P2P flows. In concrete terms, PVARA can mandate Travel-Rule compliance, sanctions and politically exposed person (PEP) screening, wallet-risk scoring, use of blockchain analytics, and timely suspicious-transaction reporting to FMU. The PCC's role is to make those mandates operable across agencies and industry

so that data flows can be synchronised and supervised.

The PCC's second CFT benefit is speed. Pakistan's recent energy-and-compute policy, allocating 2,000 MW to bitcoin mining and AI data centres, puts large, electricity-intensive operations under licensing [54]. Conditions that tie such operations to verified beneficial ownership and rapid-freeze protocols that can accelerate operational disruption capacity when risks surface. That same logic applies to exchanges and custodians seeking market access: PVARA's licensing can require data-sharing memoranda with FMU with enhanced incident-response standards, while PCC coordinates the government side choke points (banks, telcos, cloud providers), who react consistently.

The wider macro-financial frame is also shifting. SBP has signalled plans for a central bank digital currency (CBDC) pilot, positioning Pakistan in a regional cohort experimenting with a sovereign digital pipeline. While a CBDC is distinct from crypto assets, building capacity around digital ledgers, messaging, and identity rails tends to improve supervisory tooling as well, especially if FMU, PVARA, and SBP design interoperable reporting interfaces [55]. Meanwhile, the experts noted that the Ordinance brings Pakistan closer to its peers in adopting risk-based regulation for virtual assets, which could improve access to investment and talent if licensing proceeds credibly and predictably [56].

None of this eliminates TF risks immediately; it relocates them into a structure where they can be measured and countered effectively. The task for PCC is essentially strategic plumbing: keeping ministries and regulators synchronised; sequencing reforms (licensing first, scale second); and ensuring that public communication drives users out of informal P2P channels into supervised venues that generate usable data trails. If those basics hold, the digital asset environment would follow a structure in which PVRA writes clear rules, FMU receives high-quality reports, SBP and SECP align the fiat and capital market edges, and law enforcement can obtain timely freezes. In turn, Pakistan's digital-asset regime can expand innovation while enhancing CFT outcomes.

The insights from this institutional set-up led the research to trace workable policy recommendations to help Pakistan in its fight against TF.

4.3 Policy Recommendations

4.3.1 Designate a VASP supervisor and publish a full authorisation and inspection rulebook

The Parliament and the executive can confirm the competent authority for VASPs (licensing, ongoing supervision, and enforcement), which should then issue a VA and cryptocurrency policy covering proper criteria, client-asset safeguarding and segregation, custody standards, outsourcing controls, cyber and incident reporting, audit trails, and marketing rules. This mirrors the EU's MiCA authorisation and conduct regime which channel activity onshore, leveraging examination quality.

4.3.2 Establish a national Travel-Rule utility backed by hard-wired inter-agency SOPs

Pakistan can implement FATF Recommendation 15 by mandating access to messaging utility that carries originator/beneficiary information with VA transfers. The definitive data set must include names, account/wallet identifiers, transaction hash, service identifier, and risk flags for expedited message exception handling. The inter-agency SOPs should mandate participation by banks/EMIs and licensed VASPs and provide simulation environments to get hands-on experience. The SOPs can be concluded among SBP-regulated entities, licensed VASPs, FMU, FIA, and PTA, so identity and risk information can be interrogated in near real time. This replicates the

EU Transfer of Funds Regulation (2023/1113) model while aligning with MAS PSN02 in Singapore on scope and controls.

4.3.3 Create rapid-freeze and evidence-continuity protocols tied to court-grade crypto artefacts

Publish standard operating procedures (SOPs) for 24/7 restraint requests that include: (i) a national crypto-seizure toolkit (ii) a template for outgoing requests to foreign platforms; (iii) a national contact point to collaborate in urgent scenarios; and (iv) judicial guidance on the admissibility of blockchain evidence, consisting of (a) timestamps and (b) clustering analytics. Global experience shows this works: US multi-agency disruptions in 2020 and subsequent terrorism-linked seizures in 2023–2025 succeeded because exchange Know-Your-Customer (KYC), Travel-Rule-equivalent identity checks, and reproducible on-chain artefacts travelled with the funds. To duplicate this choreography, Pakistan can bind FMU triggers to FIA actions and PTA front-end disruption, shortening the time lag between Suspicious Transaction Report (STR) and asset freeze.

The policy directives specifically address Pakistan’s breakpoints without employing esoteric technology or blanket legislative changes. All recommendations are technically viable, aligned with global best practice, and testable against local realities.

5. Conclusion

This study shows that Pakistan’s capacity to curb terror financing via digital assets is less about creating novel laws and more about integrating existing authorities into a coherent, data-rich workflow. The findings isolate three breakpoints that repeatedly undermine outcomes: the absence of a settled licensing and inspection regime for virtual-asset service providers (VASPs); missing “Travel Rule” plumbing to move originator-beneficiary data at the same speed as value; and uneven evidentiary continuity from alert to arrest. Set against high grassroots adoption, large cash usage, and fast-scaling retail payments infrastructure, these seams convert technical traceability into procedural delay. The policy path is clear and practical. First, designate the VASP supervisor and publish a phased authorisation and inspection. Second, stand up a national Travel-Rule utility and common data schema, binding banks, EMIs, and licensed VASPs to interoperable identity messaging with service-level targets. Third, issue rapid-freeze and evidence-continuity protocols, 24/7 contact points and judicial guidance, so actionable artefacts travel with funds. Each measure is administratively feasible and benchmarked to mature regimes. Taken together, these steps convert today’s fragmented signals into admissible, timely evidence without stifling lawful use, aligning Pakistan’s practice with global expectations and its own financial-stability goals. From an institutionalist perspective, they amount to a reset of the rules and routines that govern virtual assets in Pakistan, shifting the balance of incentives away from opaque, off-grid channels and towards supervised venues that generate usable data trails.

Acknowledgments

Amjad Fraz conceptualised the study, conducted the literature review, analysed Pakistan’s regulatory and institutional framework, and drafted the manuscript. Dr. Zahid Khan supervised the research design, refined the theoretical and policy framing, reviewed the analysis, and contributed to the final revision of the manuscript.

References

1. Financial Action Task Force. (2025). Comprehensive update on terrorist financing risks. <https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Comprehensive-Update-on-Terrorist-Financing-Risks-2025.pdf.coredownload.inline.pdf>
2. Wei, C., & Hu, T. (2022). Legislation summary: China's new law to fight telecom and internet fraud. NPC Observer. <https://npcobserver.com/2022/09/07/legislation-summary-chinas-new-law-to-fight-telecom-and-internet-fraud>
3. JunHe LLP. (2025). A look at the evolution of China's virtual currency regulation through a Shanghai court case. Lexology. <https://www.lexology.com/library/detail.aspx?g=9b0c0ab7-2d07-47d7-8624-10ff1e5f8531>
4. Federal Investigation Agency, Pakistan. (2025). Performance 2024. <https://www.fia.gov.pk/files/tickers/1788909745.pdf>
5. Securities and Exchange Commission of Pakistan. (2025). List of illegal personal loan apps & platforms. <https://www.secp.gov.pk/document/list-of-illegal-digital-apps/>
6. State Bank of Pakistan. (2018). BPRD Circular No. 03 of 2018: Prohibition of dealing in virtual currencies/tokens. <https://www.sbp.org.pk/bprd/2018/C3.htm>
7. State Bank of Pakistan. (2025). Third quarterly payment systems review—FY25 [Press release]. <https://www.sbp.org.pk/press/2025/Pr-25-Jun-2025.pdf>
8. Boy. (2025). The difference between on-ramps and off-ramps in crypto transactions. INDODAX Academy. <https://indodax.com/academy/en/difference-between-on-ramps-and-off-ramps-in-crypto/>
9. Financial Action Task Force Asia/Pacific Group. (2022). Pakistan: Follow-up reports. <https://www.fatf-gafi.org/publications/mutualevaluations/documents/fur-pakistan-2020.html>
10. Federal Financial Institutions Examination Council. (n.d.). Assessing compliance with BSA regulatory requirements. In BSA/AML Manual. <https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/09>
11. Financial Action Task Force. (2024). Virtual assets: Targeted update on implementation of the FATF standards on VAs and VASPs. <https://www.fatf-gafi.org/en/topics/virtual-assets.html>
12. FATF. (2025). Targeted update on implementation of the FATF standards on VAs and VASPs. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html>
13. International Monetary Fund & Financial Stability Board. (2023). IMF-FSB synthesis paper: Policies for crypto-assets. <https://www.fsb.org/uploads/R070923-1.pdf>
14. Aldasoro, I., Doerr, S., Frost, J., & Yousefi, S. R. (2025). An approach to AML compliance for cryptoassets (BIS Bulletin No. 111). Bank for International Settlements. <https://www.bis.org/publ/bisbull111.htm>
15. European Union. (2023). Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets. Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng>
16. European Securities and Markets Authority. (2024). Markets in crypto-assets regulation (MiCA). <https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica>
17. UK Financial Conduct Authority. (2023). FCA sets out expectations for UK cryptoasset businesses complying with the Travel Rule. <https://www.fca.org.uk/news/statements/fca-sets-out-expectations-uk-cryptoasset-businesses-complying-travel-rule>
18. Monetary Authority of Singapore. (n.d.). Notice PSN02: Prevention of money laundering and countering the financing of terrorism – Digital payment token service. <https://www.mas.gov.sg/regulation/notices/psn02-aml-cft-notice---digital-payment-token-service>
19. State Bank of Pakistan (2018). BPRD Circular No. 03 of 2018: Prohibition of Dealing in Virtual Currencies/Tokens, <https://www.sbp.org.pk/bprd/2018/C3.htm>; FE Circular No. 03 of 2018, 18 April 2018, <https://www.sbp.org.pk/epd/2018/FEC3.htm>
20. Boy. (2025). The difference between on-ramps and off-ramps in crypto transactions. INDODAX Academy. <https://indodax.com/academy/en/difference-between-on-ramps-and-off-ramps-in-crypto/>
21. Financial Monitoring Unit (2022). Strategic Analysis Report: Virtual Assets, <https://www.fmu.gov.pk/docs/2022/Strategic-Analysis-Report-Virtual-Assets.pdf>
22. State Bank of Pakistan, (2022). Raast: Pakistan's Instant Payment System, <https://www.sbp.org.pk/dfs/Raast.html>; World Bank, Pakistan—RAAST Case Study, SBP (2019), Regulations for Digital On-Boarding of Merchants—NADRA verification clause, <https://www.sbp.org.pk/bprd/2019/C5-Annex.pdf>

23. Reuters (2025). Pakistan Turns to Bitcoin Miners, AI Data Centres to Use Surplus Power. <https://www.reuters.com/world/asia-pacific/pakistan-turns-bitcoin-miners-ai-data-centers-use-surplus-power-2025-04-09/>
24. Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation* (4th ed.). Jossey-Bass.
25. North, D. C. (1990). *Institutions, institutional change and economic performance* (pp.3-7), Cambridge University Press.
26. Coase, R. H. (1988). The marginal cost controversy. In *The firm, the market and the law* (pp. 75–94). University of Chicago Press.
27. Williamson, O. E. (2006). The economic institutions of capitalism: Firms, markets, relational contracting. In G. Disterer (Ed.), *Das Summa Summarum des Management: Die 25 wichtigsten Werke für Strategie, Führung und Veränderung* (pp. 61–75). Gabler. (Original work published 1985).
28. Financial Action Task Force. (2021). Virtual assets and virtual asset service providers: Guidance for a risk-based approach. <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-VA-VASP.pdf>
29. Central Reserve Bank of El Salvador. (2021). Ley Bitcoin. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/8EE85A5B-A420-4826-ABD0-463380E2603B.pdf>
30. Central Bank of Nigeria. (2021). Design paper for the eNaira. <https://enaira.gov.ng/design-paper/>.
31. People's Bank of China. (2021). Progress of research & development of e-CNY in China. <https://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021072014364791207.pdf>
32. US Department of Justice. (2020). Global disruption of three terror finance cyber-enabled campaigns. <https://www.justice.gov/archives/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>
33. US Department of the Treasury (2023). Following Terrorist Attack on Israel, Treasury Sanctions Hamas Operatives and Financial Facilitators, <https://home.treasury.gov/news/press-releases/jy1816>
34. US Department of Justice. (2025). Justice Department disrupts Hamas terrorist financing scheme through seizure of cryptocurrency. <https://www.justice.gov/opa/pr/justice-department-disrupts-hamas-terrorist-financing-scheme-through-seizure-cryptocurrency>
35. Europol. (2024). European Union terrorism situation and trend report 2024. <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2024-eu-te-sat>
36. Profit by Pakistan Today. (2025). Pakistan's currency in circulation reaches Rs10.8 trillion. <https://profit.pakistantoday.com.pk/2025/08/28/pakistans-currency-in-circulation-reaches-rs10-8-trillion-up-27-4-of-total-money-supply/>
37. State Bank of Pakistan. (2025). Third quarterly payment systems review—FY25. <https://www.sbp.org.pk/press/2025/Pr-25-Jun-2025.pdf>
38. National Database and Registration Authority, Pakistan. (n.d.). Biometric / e-KYC services. <https://www.nadra.gov.pk>
39. State Bank of Pakistan. (2025). List of authorised electronic money institutions (EMIs). <https://www.sbp.org.pk/ps/PDF/List-of-EMIs.pdf>
40. Chainalysis Team. (2025). The 2025 global adoption index: India and the United States lead cryptocurrency adoption. <https://www.chainalysis.com/blog/2025-global-crypto-adoption-index/>
41. Fakunle, A. (2025). The rise in popularity of crypto in Pakistan. *Disruption Banking*. <https://www.disruptionbanking.com/2025/08/05/the-rise-in-popularity-of-crypto-in-pakistan>
42. Reuters. (2025). Pakistan allocates 2,000 MW to Bitcoin mining, AI data centres. <https://www.reuters.com/sustainability/boards-policy-regulation/pakistan-allocates-2000-megawatts-electricity-bitcoin-mining-ai-data-centres-2025-05-25/>
43. TRM Labs. (n.d.). Fiat currency. In *TRM Glossary*. <https://www.trmlabs.com/glossary/fiat-currency>
44. Federal Investigation Agency, Pakistan. (2025). Performance 2024. <https://www.fia.gov.pk/files/tickers/1788909745.pdf>
45. FATF. (2025). Targeted update on implementation of the FATF standards on VAs and VASPs. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html>
46. Ashraf, A. (2023). Pakistan's crime agency to ask telecom authority to block crypto websites: Report. *CoinDesk*. <https://www.coindesk.com/business/2022/01/17/pakistans-crime-agency-to-ask-telecom-authority-to-block-crypto-websites-report>

47. Securities and Exchange Commission of Pakistan. (2025). List of illegal personal loan apps & platforms. <https://www.secp.gov.pk/document/list-of-illegal-digital-apps/>
48. Financial Monitoring Unit, Pakistan. (2022). Strategic analysis report: Virtual assets. <https://www.fmu.gov.pk/docs/2022/Strategic-Analysis-Report-Virtual-Assets.pdf>
49. Federal Investigation Agency, Pakistan. (2025). Performance 2024. <https://www.fia.gov.pk/files/tickers/1788909745.pdf>
50. Virtual Assets Ordinance. (2025). Ordinance No. VII of 2025: National Assembly of Pakistan. https://www.na.gov.pk/uploads/documents/68babbb0b32b8_903.pdf
51. Hukhari, H., & Haq, I. (2025). Virtual Assets Ordinance 2025: Explanation and comments—I. Business Recorder. <https://www.brecorder.com/news/40372482>
52. Press Information Department, Pakistan. (2025). Pakistan Virtual Assets Regulatory Authority (PVARA) holds first board meeting (PR No. 248). https://pid.gov.pk/site/press_detail/30135
53. Ministry of Finance, Government of Pakistan. (n.d.). Press releases. https://www.finance.gov.pk/press_releases.html
54. Shahzad, A. (2025). Pakistan allocates 2,000 megawatts to Bitcoin mining, AI data centres. Reuters. <https://www.reuters.com/sustainability/boards-policy-regulation/pakistan-allocates-2000-megawatts-electricity-bitcoin-mining-ai-data-centres-2025-05-25/>
55. Reuters. (2025). Pakistan central bank to launch pilot for digital currency, says governor. <https://www.reuters.com/world/asia-pacific/pakistan-central-bank-launch-pilot-digital-currency-says-governor-2025-07-09/>
56. HKTDC Research. (2025). Law to regulate crypto and digital assets approved. <https://research.hktdc.com/en/article/MjA5OTc0NzY5NW> .