The Missing Denominator

Assessing digital payment token risk without a reliable comparison to banks, cash, trade and property

23 July 2026

Executive Summary

1. **Digital payment tokens are used for serious crime and national-security threats.** Public evidence shows their use in money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud and theft. Chainalysis says sanctioned entities received US$104 billion of its US$154 billion 2025 total and that the A7A5 stablecoin processed more than US$93.3 billion. [1, 2]

2. The evidence does not show how digital payment token use compares with other channels. No published dataset reviewed for this article shows what share of all money laundering, terrorist financing or proliferation financing is conducted through digital payment tokens rather than through banks, cash, trade or property. Nor have we found an equivalent cross-channel share for those other channels. The Financial Action Task Force's 2026 reports add useful case and market information, but they do not answer that comparison. [3, 4]

3. The Monetary Authority of Singapore's higher-risk assessment should inform a firm's own assessment, not replace it. A firm must rate its own digital payment token exposures—its customers, products, services, transactions and channels. The sector assessment is evidence that helps the firm rate those exposures. It is not a separate exposure and does not complete the firm's enterprise-wide risk assessment. [5, 6, 7]

4. **The missing comparison affects how much weight a firm can place on the word "higher".** It does not show that the sector assessment is wrong or that digital payment token risk is low. It means a financial institution firm cannot verify how misuse of digital payment tokens compares with other channels across the wider market. A firm should weigh the assessment alongside its own exposure, evidence of actual illicit use, concentration, potential harm and the reliability of each source. Its risk score before controls may be lower,

the same or higher than one based mainly on the sector assessment. Strong controls may still be necessary. [5, 6, 7]

5. **The comparison is missing because no one holds the full dataset.** Governments hold case and enforcement data; firms hold customer, transaction and control data; and analytics providers hold blockchain attribution and network data. The datasets use different categories and methods, and legal, confidentiality and technical limits make them hard to link. Common definitions, standard reporting and lawful data sharing would improve understanding of where the risk sits and where controls should focus. The Monetary Authority of Singapore has said that its information-sharing framework may expand over time. [8] Subject to legal and policy design, Singapore could consider participation by relevant digital payment token service providers in that framework, or create a parallel aggregate reporting system.

Introduction

Digital payment tokens ("**DPTs**") can be used for money laundering ("**ML**"), terrorist financing ("**TF**") and proliferation financing ("**PF**"). Singapore's national risk assessments treat DPTs as posing higher inherent ML/TF/PF risks. [5] The issue in this article is not whether the risk is real. It is how DPT misuse compares with misuse of banks, cash, trade, property and other channels.

The public evidence shows serious misuse and identifies some of the products and routes involved. It does not provide a comprehensive account of how often illicit actors use DPTs, where that use is concentrated or how it compares with other channels.

For a financial institution, including a DPT service provider ("**DPTSP**") or another virtual asset service provider ("**VASP**"), the practical task is to rate its own customers, products, services, transactions and channels. That work forms part of its enterprise-wide risk assessment ("**EWRA**"). The risk assessment by the Monetary Authority of Singapore (the "**Authority**") is evidence that helps the firm rate those exposures; it is not a separate exposure or the completed EWRA. [5, 6, 7]

Internal data can show a financial institution's own business and control results, but they cannot supply the missing comparison with the wider market. That gap does not invalidate the EWRA or prevent precautionary controls. Structural vulnerabilities and potential harm may support a high rating even before comprehensive data on actual use exist. The gap instead affects the confidence placed on the part of the assessment that says DPT risk is higher than risk in other channels.

In this article, a "**matched denominator**" means a comparison using the same offence, place, time period and unit of measure as the numerator. Two questions must be kept separate: the share of all DPT activity that is illicit, and the share of all corresponding ML, TF or PF activity that uses DPTs. They answer different questions.

Meanwhile, on 21 July 2026, the Financial Action Task Force ("**FATF**") published its Targeted Report on Regulatory Challenges from Decentralised Finance (the "**DeFi Report**"). [4] Five days earlier, FATF published the Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs (the "**Seventh Targeted Update**". [3] Neither report supplies the matched cross-channel comparison examined here. [3, 4] The Authority also published new supervisory expectations for DPTSPs on 13 July 2026. [9]

What the headline numbers tell us

Chainalysis estimates that illicit cryptocurrency addresses received at least US$154 billion in 2025, a stated increase of 162% from 2024. [1] It also estimates that illicit activity remained below 1% of attributed cryptocurrency transaction volume. [1] These figures answer different questions. The first is an amount received by addresses classified as illicit. The second is a share of attributed on-chain activity. Neither compares DPTs with all ML, TF or PF conducted through other channels.

The below-1% figure also needs context. It is a gross-flow ratio, not a measure of unique criminal proceeds, victim loss or harm. Repeated transfers can increase the denominator, and later attribution can change the numerator. Chainalysis initially estimated US$40.9 billion for 2024 and revised that figure to US$57.2 billion one year later. [1] The data are useful, but their scope and date matter.

Other analytics firms use different definitions and methods. TRM Labs estimates US$158 billion of illicit crypto volume in 2025 and a 1.2% share of attributed on-chain volume. [10] Elliptic reports more than US$21.8 billion for the narrower category of illicit or high-risk cross-chain activity. [11] These figures are not interchangeable. A firm should identify what a dataset includes before relying on its headline percentage.

What is driving the total

Of Chainalysis's US$154 billion total, US$104 billion was received by sanctioned entities. [1, 2] Chainalysis separately says the rouble-backed A7A5 stablecoin processed more than US$93.3 billion in less than a year. [1, 2] On those published figures, A7A5's processed volume is equivalent to about 61% of the headline total and almost 90% of sanctioned-entity receipts. [1, 2] These ratios show concentration, not an exact reconciliation, because the underlying measures and periods differ. Chainalysis also reports that stablecoins accounted for 84% of all illicit transaction volume. [1]

A7A5 is both a stablecoin and a rail linked to sanctioned entities. The 84% stablecoin figure and the US$104 billion sanctions figure therefore overlap; they are not separate pools. Chainalysis also says 2025 would still have been a record year if sanctioned-entity receipts had stayed flat. [1] The point is not that DPT risk is low. It is that a total driven heavily by one category—and substantially by one instrument—cannot support the same conclusion for every token, service, business model or jurisdiction.

The categories also need to be kept apart. ML, TF, PF, sanctions evasion, fraud and theft can overlap, but they are not the same. Lawfully earned funds can be used for terrorism without first being laundered. Some sanctions relate to proliferation and others do not. Receipt by a sanctioned entity does not mean that the full amount is laundered criminal proceeds. A firm cannot judge prevalence if these categories are combined without explaining the overlap.

Why actual use matters for an EWRA

The Authority's anti-money laundering and countering the financing of terrorism ("**AML/CFT**") notices require regulated firms to identify, assess and understand their ML and TF risks, with references to ML including PF. [12] MAS Notice 626, for example, requires banks to assess their business, customers, jurisdictions, products, transactions and delivery channels. [12]

MAS Notice PSN02 imposes the same basic duty on DPT services. [13] Its guidelines require a consolidated EWRA and, as far as possible, both qualitative and quantitative analysis. They also identify measures such as the number and profile of higher-risk customers and the volume and size of transactions and transfers. [7]

Those customers, products, services, transactions and channels are the risk factors the firm must rate. The Authority's sector-level assessment is evidence used to rate them. It is not another risk factor, and it should not by itself determine the firm's score or where the firm spends its compliance resources. [5, 6, 7, 13]

A useful EWRA keeps four questions separate. What is the firm exposed to? How likely is the threat to arise in that exposure? How serious would the harm be? How effective are the controls? Structural features such as speed, pseudonymity and cross-border reach show what could happen. Evidence of actual use shows what has been detected in practice. Both matter, and both have limits.

How a firm should use the Authority's "higher risk" assessment

Singapore's 2024 ML National Risk Assessment says DPTs pose "inherently higher ML/TF risks". The 2024 Virtual Assets Risk Assessment (the "**VA RA**") uses similar language for ML, TF and PF. [5, 6] "Inherent" means risk before controls. "Higher" implies a comparison. Technical features may support a high inherent-risk assessment even when comparative use is not measured, but they do not tell a firm exactly how DPT risk compares with other channels.

The VA RA draws on reports, investigations, cross-border cases, industry data and typologies. [5] It does not publish a quantitative weighting or a matched dataset from which an outside reader could recreate the comparative conclusion. That does not mean the conclusion is wrong or unusable. The Authority may also rely on confidential supervisory or law-enforcement information that cannot be published. Similar public-data limits apply to other sector ratings in Singapore's national assessments. [6, 14] FATF's 2026 survey shows a similar international problem: many jurisdictions rated peer-to-peer activity high risk even though far fewer reported collecting relevant market data. [3]

Timing also matters. DPTs were assessed largely on structural features and early case evidence before a mature record of observed use could exist. [5, 6] That was a reasonable precaution at an early stage. As the sector develops, a firm should consider later evidence and record whether it confirms, qualifies or leaves unresolved the comparative part of the assessment.

For the firm, the missing denominator limits the weight and confidence that can be placed on the claim that DPTs are higher risk than other channels. It does not remove separate evidence of vulnerability or potential harm. A financial institution should show which parts of its score are supported by the Authority's assessment and how that evidence combines with its own exposure, actual illicit use, concentration and potential consequence. Depending on the full record, its final score may be lower, the same or higher than a score based mainly on the sector assessment. [5, 6, 7]

The same approach should apply to every important source, not only the Authority's assessment. Data on actual use may miss activity because detection and attribution are incomplete. Exposure data may have classification or coverage gaps. Estimates of concentration and harm may rely on assumptions. Control results may be affected by how outcomes are measured. The firm should record the source, date, coverage, limitations and confidence for each important input.

Evidence of repeated illicit use is strong evidence that a theoretical vulnerability has become a real channel. But detected activity can understate actual use. Structural features show what is possible; observed use shows what has been found in practice. To interpret observed-use data, the firm should compare it with the right total. A useful analysis distinguishes:

(1) illicit DPT activity as a share of total DPT activity;
(2) illicit DPT activity as a share of all corresponding ML, TF or PF activity across channels;
(3) the number of distinct illicit actors and cases; and
(4) concentration by token, service, corridor, jurisdiction and typology.

These measures answer different questions. Concentrated use of A7A5 supports a high rating for exposure to that rail; it does not support the same rating for unrelated activity. The VA RA also reports that suspicious or illicit DPT transactions were less than 1% of total virtual-asset transaction value in 2022 and that TF and PF misuse had not then materialised in Singapore. [5] Those findings do not conflict with the sector assessment, but they may affect the weight placed on its comparative part in a firm's score.

Actual use improves both scoring and controls

For scoring, evidence of actual use helps a firm estimate how likely it is to encounter a threat, identify where the threat is concentrated and map external cases to its own business. The firm should use the best available evidence—published cases, regulatory intelligence, blockchain attribution and its own investigations—and state what each source covers and where it may be incomplete. It should record evidence that supports or qualifies the sector assessment, rather than selecting only evidence pointing in one direction. [5, 7]

For controls, actual use shows which actors, rails, intermediaries and corridors need attention. It helps the firm decide which monitoring scenarios to refine, which flows to restrict, where information should be shared, which assets should be traced or frozen and whether activity has moved elsewhere. Controls aimed at populations rarely used by illicit actors may add cost and false positives without disrupting the threat. Controls aimed at a concentrated rail may have a much greater effect.

The Authority's 2020 EWRA paper calls for both qualitative and quantitative analysis, including payment-flow and network analysis, and says control-testing results should feed back into the assessment. [15] The practical loop is simple: detection results, investigations, stopped transactions, restrained assets and evidence of displacement should update the EWRA; the revised EWRA should then retarget controls. Because observed use is affected by detection and reporting bias, the firm should compare several sources and state the uncertainty. [5, 7, 9]

What Singapore's national risk assessments show

Singapore's 2024 ML National Risk Assessment considers threats, consequences, vulnerabilities and controls. [6] Its methodology includes the prevalence of predicate offences, the amount of ML that has materialised and the likelihood that threats will arise within a sector. [6] It rates banks as Singapore's highest ML-risk sector and DPTSPs as medium-high. [6] It also says DPT activity is not material compared with traditional financial activity, that DPTs are not actively used domestically as a means of payment, and that most DPT-related cases involved fraud or cyber offences. [6] These findings can sit together: a sector can present serious vulnerabilities without being the largest channel by value or frequency.

The 2024 TF National Risk Assessment raised DPTSPs from medium-low to medium-high risk, while rating national TF risk medium-low, money remittances high and banks medium-high. [14] It also found no strong evidence of widespread DPT use for TF in Southeast Asia, no known domestic TF cases involving DPTs and continued dominance of fiat. [14] The higher DPTSP rating supports vigilance, especially because low-value TF can have severe consequences. It does not show that DPTs are the principal TF channel.

The national risk assessments provide useful threat and vulnerability analysis, but they do not publish a matched percentage of Singapore ML proceeds, ML cases, TF value or PF activity conducted through DPTs rather than other channels. Nor do they link the reported cases and values to the relevant DPT transaction populations. That is the comparison that would help firms calibrate their EWRAs and target controls more precisely. [5, 6, 14]

Why there is no reliable global percentage

For ML, FATF refers to a 2009 estimate equal to 2.7% of global gross domestic product ("**GDP**") and a 1998 range of 2%–5% of global GDP. [16] It also cautions that precise statistics are unavailable and that no definitive global figure can be produced. [16] Those broad estimates cannot be matched reliably with a 2025 address-based crypto total that covers several different illicit categories. The Seventh Targeted Update adds case information but no matched global or national denominator. [3]

TF poses a different measurement problem. The funds may come from lawful or unlawful sources, the amounts may be small, and the risk depends heavily on intended use and potential harm. The reviewed FATF and Singapore materials describe serious DPT typologies but do not provide a comprehensive global TF total. [3, 14, 17] PF is narrower than sanctions activity generally. Treating all receipts by sanctioned entities as PF would compare different things.

The same cross-channel gap exists elsewhere. We have not found a reliable global dataset showing the share of all ML conducted through banks, cash, trade or property. Traditional sectors have longer supervisory histories, more reporting and stronger internal baselines, which help firms assess their own exposure. They do not solve the global comparison. The point is not to single out DPTs: every sector should use measured exposure where relevant data can reasonably be obtained, and no sector label should replace the firm's own analysis.

What the 2026 FATF reports add

The Seventh Targeted Update adds useful case evidence. FATF reports that a Cambodia-based financial services conglomerate laundered at least US$4 billion between August 2021 and January 2025, including at least US$37 million linked to cyber heists by the Democratic People's Republic of Korea ("**DPRK**"). [3] It also reports an alleged €460 million investment-fraud laundering network in Spain, an artificial-intelligence-enabled recruitment scam involving more than US$1 million in virtual assets, and a freeze of more than US$29 million held in a wallet linked to the Cambodian conglomerate. [3]

These figures cannot be added into one global DPT total. The Spanish case involved cash, bank transfers and virtual-asset transfers; the US$29 million is an amount frozen; and the US$37 million is part of the US$4 billion. The report also does not say what share of all ML, TF or PF these cases represent, or what share of the relevant proceeds moved through virtual assets rather than other channels. Its approximately 97% figure

concerns the market coverage of a Recommendation 15 implementation table, not the coverage of illicit activity. [3]

The data gap is especially clear for peer-to-peer ("**P2P**") activity. Among 66 respondents to one question, 58 (88%) rated P2P transactions as high risk. [3] Separately, 31 of 133 respondents (23%) said they collected and assessed relevant market metrics. [3] The figures measure risk ratings and data-collection practices, not the value or number of illicit P2P transactions. FATF says company data differed significantly, and the survey was self-reported and used different question paths for different respondents. [3]

The DeFi Report contains useful denominators, but they answer other questions. It estimates that DeFi represents around 4%–6% of the virtual-asset market, reports US$86.644 billion of total value locked as at 10 May 2026 and describes geographic and protocol concentration. [4] It also reports how many jurisdictions have assessed, regulated or licensed DeFi arrangements. [4] FATF cautions that total value locked is not a complete measure of a protocol's footprint or risk. [4]

The DeFi Report also describes two April 2026 attacks attributed to the DPRK, of about US$285 million and US$292 million. Together they accounted for about 76% of reported virtual-asset hacking losses at that point, and about US$75 million from the latter attack was frozen. [4] The 76% statistic has a denominator, but it is a denominator of hacking losses, not ML, TF or PF. The DeFi Report does not provide a single DeFi ML/TF/PF total or a matched comparison with total DeFi activity or other channels. That is not a criticism of the report; its main purpose is to explain the regulatory perimeter and appropriate controls.

FATF's recommendations point towards a practical response. Risk assessments should consider materiality—how important the exposure is in the relevant market—and specific exposure to offshore VASPs ("**oVASPs**"), stablecoins, DeFi, P2P transactions and unhosted wallets. [3] The DeFi Report likewise calls for resources proportionate to national exposure. [4] FATF also recommends that institutions assess offshore and unhosted-wallet exposure and look for nested oVASP activity. [3, 17, 18] In other words, firms should combine structural vulnerability with evidence of actual use and their own direct or indirect exposure, then focus controls on the concentrations they find.

Questions for a financial institution's EWRA

Table 1 sets out practical questions for mapping external evidence to a financial institution's own business.

Table 1. Questions for an EWRA grounded in actual illicit use

Dimension	Questions for the EWRA
Evidence	What reliable evidence shows which DPT products, services, counterparties, corridors and transaction patterns illicit actors use? What total activity is that use compared with?
Source quality	How current and reliable is each source? What does it cover, what may it miss, and how should that uncertainty affect the score?
Counterparties	How much exposure comes from licensed, offshore, unlicensed, sanctioned or nested counterparties, including oVASPs that may present themselves as retail users?
Activity	What value, number of cases and share of activity relate separately to ML, TF, PF, sanctions, fraud, theft or other conduct?

Dimension	Questions for the EWRA
Products	Which tokens, issuers or features are actually used by illicit actors? How concentrated is that use, and what blocking, freezing, seizure or burn capabilities exist?
Channels and places	What is the exposure through DPT and fiat flows, regulated intermediaries, unhosted wallets, cross-chain tools and domestic or cross-border corridors?
Outcomes	Which controls detected, stopped, restrained or displaced illicit activity, and how should those results change the EWRA?

A financial institution should make the source and weight of the sector assessment visible in its scoring method, then test that evidence against its own exposure. Repeated illicit use should raise the likelihood rating for the product, corridor or counterparty in which it occurs, not for unrelated activity. An offshore typology may be immaterial to a firm with no relevant exposure; a small overall category may be very important to a firm concentrated in that niche.

A firm should also measure outcomes. Files reviewed, alerts generated and customers escalated show that work occurred; they do not show that risk was reduced. Useful outcomes include detection quality, transactions stopped, assets restrained or recovered, victim losses prevented, investigation time, false-positive burden and movement to less transparent channels. Those results should feed back into the EWRA.

What the missing denominator means for the score and controls

The missing denominator affects one part of the score: how confidently the firm can say that DPT risk is higher than risk in other channels. It does not remove evidence of structural vulnerability or potential harm. The firm's method should show how all of those inputs combine and how confidence in each source affects the result. [5, 6, 7]

That does not automatically mean weaker controls or delayed action. Control design should respond to the resulting inherent risk, the seriousness of the threat, the firm's actual exposure and applicable requirements. Control effectiveness should then inform residual risk. A small share can still represent substantial value, and state-linked sanctions evasion, TF, PF, industrialised fraud or major theft may justify intensive preventive controls. Better comparative data should improve the scope and targeting of controls, not postpone them. [7]

A7A5 also shows why a firm must look beyond the tokens it lists directly. A Singapore-licensed DPTSP may encounter the rail through customers, wallets, counterparties, bridges or fiat and DPT on- and off-ramps. FATF recommends monitoring links to unlicensed or weakly supervised offshore platforms. [3, 18] The response combines baseline due diligence, screening and monitoring with targeted measures for linked exposures, designations, disruption, information sharing and legally required freezing or rejection. Concentration helps target controls; it does not replace baseline controls.

Why the denominator is missing—and how it can be built

Public blockchains create a useful measurement opportunity because much of the transaction layer is visible. But visibility is not the same as identification. Attribution, off-chain activity, privacy tools and cross-chain

movement remain important limits. [1, 10, 11] DPTs are still a practical place to begin because more of the transaction layer can be observed than in several traditional channels.

The gap exists because the relevant data were created for different purposes, use different definitions and sit in different systems. Case records identify particular events or actors but may not show the full transaction population from which they arose. A firm's data describe its own business but not the wider market. Blockchain analytics add attribution and network information, but providers use different taxonomies and may reach different conclusions. Legal, confidentiality, privacy, proprietary and investigative limits can also prevent data from being pooled or published.

No one sees the whole picture. Governments hold investigation and enforcement data. Firms hold customer, transaction and control data across fiat and DPT rails. Analytics providers hold address attribution and network data. Building the denominator therefore requires agreed definitions, consistent periods and units, lawful data sharing and clear governance—not simply more one-off surveys.

Practical steps include separating ML, TF, PF, sanctions, fraud and theft; collecting channel-level metrics on a consistent basis; and publishing matched numerators and denominators in national risk assessments. Firms could contribute standardised, privacy-protected data through structured public-private arrangements and feed intervention results back into their EWRAs. FATF's P2P findings show why comparable market data matter. [3]

Singapore already has a framework for structured collaboration. The Collaborative Sharing of ML/TF Information & Cases platform ("**COSMIC**"), launched by the Authority and six major banks on 1 April 2024 under Part 4A of the Financial Services and Markets Act 2022 ("**FSMA**"), allows prescribed firms to share customer-risk information within legal safeguards. [8] PF is one of its initial priority areas. [8] COSMIC is a case-sharing framework, not a statistical dataset, and its current prescribed participants are specified banks. The Authority has said that COSMIC's coverage may expand over time. [8] Subject to legal and policy design, participation by relevant DPTSPs—or a parallel aggregate reporting system—could support both case sharing and privacy-protected measurement across fiat and DPT channels.

Evidence may exist outside the public record

We have not identified a reliable matched denominator, but that does not prove that none exists. Relevant information may sit in non-public supervisory or law-enforcement systems, proprietary analytics, academic research or institutional datasets. Readers who know of such evidence are invited to share its definitions, coverage and method where lawful. Wider access would help firms improve their EWRAs and direct interventions to the channels actually used.

Conclusion

The Authority's assessment that DPTs pose inherently higher ML/TF/PF risks is important evidence for a firm's EWRA. [5, 6, 7] It is not itself one of the firm's exposures, and it does not complete the firm's assessment. The firm must still decide where DPT risk arises in its own business, how reliable the available evidence is and whether its controls address the threats it actually encounters. The missing denominator limits the precision of the comparison; it does not justify inaction.

Better matched data would improve the substance of risk assessment, not just its transparency. They would give firms and authorities a firmer basis for judging relative likelihood, concentration and exposure, allocating resources and testing whether controls work. Until those data exist, firms should state the uncertainty attached to each important source, separate the offence categories, combine structural vulnerability with actual use and their own exposure, and update the EWRA as control results emerge. Governments, firms and analytics providers should build that evidence base together—or, where the data already exist, test and share them within lawful limits. [3, 4]

How HM Strategy can help

At HM Strategy we help financial institutions prepare practical, evidence-led enterprise-wide risk assessments. We identify what the firm can measure, where the wider evidence is incomplete, how much confidence to place in each source, and how the findings should drive monitoring, escalation and outcome testing.

The board and senior management of financial institutions are responsible for the enterprise-wide risk assessment itself — for understanding and overseeing its basis, not merely approving a final rating. Where we have not prepared the assessment, we advise independently on the reasonableness of the methodology, evidence, assumptions and scoring used, and on whether the control framework is appropriately calibrated to the risks identified. The result gives the board a contemporaneous record that it considered the available evidence, challenged material assumptions and reached a reasoned view on the firm's risks and controls.

For further information, contact:

Chris Holland, Partner | chris.holland@hmstrategy.com

Acknowledgement

We thank our summer associate, Reva Segireddy, for her assistance with this article.

Sources and Notes

[1] **Chainalysis, *"Crypto Crime Reaches Record High in 2025 as Nation-State Sanctions Evasion Moves On-Chain at Scale"* (8 January 2026). The article reports at least US$154 billion received by identified illicit addresses in 2025, a stated 162% year-on-year increase, an illicit share below 1% of attributed transaction volume, stablecoins at 84% of illicit volume, A7A5 processing more than US$93.3 billion, and a revised 2024 estimate of US$57.2 billion. Chainalysis describes the figures as lower-bound estimates and explains its attributed-volume denominator. Accessed 23 July 2026.**

[2] **Chainalysis, *"Crypto Crime in 2025 Was Primarily Driven by 694% Surge in State-Driven Sanctions Evasion Volume"* (5 March 2026). The article reports US$104 billion received by sanctioned entities and US$93.3 billion processed by A7A5. The indicative 61% and 90% ratios in this article compare processed volume with value received over different periods and therefore show concentration rather than an exact component reconciliation. Accessed 23 July 2026.**

[3] **FATF, *Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs* (16 July 2026), Introduction para. 3; Executive Summary recommendations 1 and 5–6; paras. 29–31, 34–35, 37–38, 41 and 45–48; and Annex A. PDF. The survey was self-reported, not independently verified and subject to conditional branching. The case amounts cited in this article measure different things and should not be aggregated. The report does not provide a matched estimate of the share of all ML, TF or PF conducted through virtual assets; its approximately 97% figure concerns the market coverage of the Recommendation 15 implementation table. Accessed 23 July 2026.**

[4] **FATF, *Targeted Report on Regulatory Challenges from Decentralised Finance* (21 July 2026), Executive Summary; para. 1 and footnotes 1–3; para. 20; Box 2; paras. 23–29; and recommendations. PDF. The report provides market, concentration, implementation and incident-specific denominators, including the April 2026 attack figures discussed in the article, but no harmonised DeFi ML/TF/PF numerator or matched cross-channel denominator. Accessed 23 July 2026.**

[5] Singapore, *Virtual Assets Risk Assessment Report* (2024), paras. 1.2, 1.4–1.6, 2.2.3–2.2.4 and 3.1.1–3.1.6, including footnote 22. The report states the "higher" and "higher inherent" risk propositions, describes its methodology and data sources, records that suspicious or illicit DPT transactions comprised less than 1% of total virtual-asset transaction value in 2022, and states that TF and PF misuse had not then materialised in Singapore. Accessed 23 July 2026.

[6] Singapore, *Money Laundering National Risk Assessment* (2024), especially paras. 3.2, 3.12–3.14, 5.1–5.3 and 7.4.1–7.4.17. The report describes the national methodology, rates banks as the highest ML-risk sector and DPTSPs as medium-high, and states that DPT activity is not material compared with traditional financial activity in Singapore. Accessed 23 July 2026.

[7] Monetary Authority of Singapore, *Guidelines to MAS Notice PSN02* (last revised 1 July 2025), especially paras. 1-4-1 to 1-4-9A and 4-3 to 4-18. The Guidelines require a consolidated EWRA, identify quantitative exposure factors and link the assessment to resource allocation and risk mitigation. Accessed 23 July 2026.

[8] Monetary Authority of Singapore, *"MAS Launches COSMIC Platform to Strengthen the Financial System's Defence Against Money Laundering and Terrorism Financing"* (1 April 2024); Financial Services and Markets Act 2022, Part 4A; Financial Services and Markets (Information Sharing Scheme for Prescribed Financial Institutions) Regulations 2024; and MAS, *"MAS and Financial Industry to Use New Digital Platform to Fight Money Laundering"* (1 October 2021). The 2024 Regulations currently prescribe specified banks. Any extension to DPTSPs would require legal and policy design. Accessed 23 July 2026.

[9] Monetary Authority of Singapore, *AML/CFT Supervisory Expectations for Digital Payment Token Service Providers* (13 July 2026), Introduction and sections 1 and 4. Footnote 2 to section 1 states that references to ML include PF. Accessed 23 July 2026.

[10] TRM Labs, *2026 Crypto Crime Report* (28 January 2026), reporting US$158 billion of illicit crypto volume and a 1.2% share of attributed on-chain volume in 2025. Accessed 23 July 2026.

[11] Elliptic, *"New Elliptic Report: Cross-chain money laundering reaches $22 billion"* (17 July 2025), covering illicit and high-risk cross-chain activity. Accessed 23 July 2026.

[12] Monetary Authority of Singapore, *MAS Notice 626 on Prevention of Money Laundering and Countering the Financing of Terrorism—Banks* (last revised 30 June 2025), paras. 4.1–4.2. Footnote 1 states that references to ML include PF; equivalent risk-assessment obligations apply under notices issued to other classes of FIs. Accessed 23 July 2026.

[13] Monetary Authority of Singapore, *MAS Notice PSN02 on Prevention of Money Laundering and Countering the Financing of Terrorism—Digital Payment Token Service* (last revised 30 June 2025), especially paras. 4.1–4.3 and 5.1–5.3. Accessed 23 July 2026.

[14] Singapore, *Terrorism Financing National Risk Assessment* (2024), especially paras. 16, 20, 27, Table 1 and paras. 47–55. The report rates DPTSPs medium-high, national TF risk medium-low, money remittances high and banks medium-high; it records no known domestic TF cases involving DPTs and states that fiat remains dominant. Accessed 23 July 2026.

[15] Monetary Authority of Singapore, *Enhancing Robustness of Enterprise-Wide Risk Assessment on Money Laundering and Terrorism Financing* (August 2020), especially pp. 3, 10, 13–14 and 19. The information paper is based on thematic inspections of banks but states that its desired outcomes and good practices are relevant to other FIs on a risk-based and proportionate basis. Accessed 23 July 2026.

[16] FATF, *Frequently Asked Questions*, section "How much money is laundered per year?". FATF states that precise statistics are unavailable, refers to the historical 2%–5% range and 2.7% estimate, and says a definitive global figure cannot be produced. Accessed 23 July 2026.

[17] FATF, *Targeted Report on Stablecoins and Unhosted Wallets—Peer-to-Peer Transactions* (3 March 2026). The report addresses stablecoin and unhosted-wallet typologies, issuer controls, P2P vulnerabilities and proportionate mitigation. Accessed 23 July 2026.

[18] FATF, *Understanding and Mitigating the Risks of Offshore Virtual Asset Service Providers* (11 March 2026), especially paras. 3–11, 21–33, 47–71 and 79–88. PDF. The report addresses activity-based regulation, nested relationships, offshore exposure and institutional controls. Accessed 23 July 2026.