**Addressing Gaps in VASP Policy Frameworks and Fintech Collaboration:**

**By,**

**Sonu thomas: 26 September 2025.**

**The Problem !! : Patchy VASP Rules Around the World:**

The rules for **Virtual Asset Service Providers (VASPs)**—things like crypto exchanges, mobile wallets, and DeFi platforms—are still inconsistent across the globe. The **Financial Action Task Force (FATF)** has been pushing its members on implementation process since 2019 to apply standards like *Recommendation 15*. That basically means licensing VASPs, enforcing proper KYC, and following the **Travel Rule** (sharing sender/receiver details for crypto transfers above $1,000).

But here’s the reality: as of **June 2025**, only about **55% of 138 countries** have fully adopted these measures but gap persist in 45% per the FATF’S 2025 update. That’s an improvement from 25% in 2024, but still far from where it needs to be (FATF, June 2025 VASP report).

This “patchwork” approach is risky. In some regions—especially parts of **Africa and Southeast Asia**—regulators don’t have the tools to monitor blockchain activity, and in some cases, they don’t even realize the urgency yet. Several countries have ended up becoming **unofficial hubs for global exchanges** without much oversight.

Take Africa as an example: crypto adoption jumped **52% in 2025**, the third fastest growth worldwide, largely driven by **mobile wallet use**. That’s great for Technological advancement to introduce Fintech state by inclusion ,empowering unbanked users in places like Kenya in E-commerce and digital wallet , but it also makes the region on spot light for illicit actors , without proper policy on the top to monitor the platforms it might turn into a playground for Gen Z laundering place . On top of that, moves like declaring **Bitcoin legal tender** in certain places clash with existing international treaties, adding another layer of uncertainty.

Meanwhile, bad actors know how to exploit these gaps. They simply move money through “light regulation” zones using unregistered wallets or exchanges. And if even a giant like [**Binance got slapped with a $4.3 billion AML fine in 2023**](https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.justice.gov/archives/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution%23:~:text%3DBinance%2520Holdings%2520Limited%2520(Binance)%252C,to%2520register%2520as%2520a%2520money&ved=2ahUKEwiW2PfS-vOPAxUSSGcHHU-pBGwQFnoECCAQAw&usg=AOvVaw3YGWIP0B2utXf0dsWHB_YW), you can imagine how much goes undetected in smaller markets with fewer resources.

**Why Industry Should Step Up**

If we wait for every government to sort this out, it’ll take forever. A faster option is for **startups and fintech’s to share tools and knowledge**. That way, compliance doesn’t have to raise massive budgets.

1. **Onboarding clients (KYC):**  
   Startups can use the same Artificial intelligence screening tools mainly like **AMLBot** or **Comply Advantage** to validate customers against sanctions lists and flag dodgy wallets. Groups like **Global Digital Finance (GDF)** already do this by letting firms share anonymized data, which helps spot patterns without breaking privacy rules.
2. **Transaction monitoring:**  
   Instead of every small company trying to build its own system from scratch, they can rely on platforms like **Chainalysis** or **Elliptic**. This makes it easier to comply with the **Travel Rule** (the one that requires sender/receiver info for $1,000+ transfers).
3. **Real-world examples:**  
   In **Nigeria**, where the VASP rules are on paper but weak in practice, startups have started holding **community webinars** to swap monitoring tricks. And on the global side, companies like **Novastro** are just building AML checks right into their systems from the start, which sets a good example for others.

**Why One-Size-Fits-All Doesn’t Work for Blockchains**

Attempting to standardise all blockchains is ineffective, as each blockchain has its own unique characteristics.

Ethereum is a powerhouse for smart contracts, while Bitcoin is transparent and pseudonymous in its core nature. Ripple, on the other hand, focuses on smoother cross-border payments. Solana’s built-in lightning speed for trading is Efficient. However, applying a single set of rules to all these platforms—while ignoring their niche technologies and uses—can create chaos rather than harmony. This is why a cookie-cutter approach fails. In the following sections, I’ll explain how we can tailor regulations to each platform’s strengths—preserving innovation while ensuring stability.

**Why It Fails**

* **Decentralized Mess**: DeFi platforms are wildcards. There’s no CEO to call up or headquarters to audit. Who do you regulate—the coders who wrote the protocol? The users swapping tokens on a DEX? Good luck pinning that down. I’ve seen regulators in emerging markets like Nigeria struggle just to define “who’s responsible” when a protocol rug-pulls users for millions.

**Tech Isn’t Uniform**: A Solana-based NFT marketplace moves transactions at breakneck speed, needing real-time monitoring to catch wash trading. Match that to Ripple, where cross-border transfers demand strict Anti-Money laundering checks tied to bank integrations. One-size-fits-all rules miss these nuances, leaving startups either over-regulated or under-protected.

* **Innovation on the Brink**: Heavy-handed laws push talent to jurisdictions with looser rules, like Seychelles or Malta. I talked to a fintech founder in Lagos last year who moved his DeFi startup to Canada because Nigeria’s VASP guidelines were too vague to navigate. Result? Local economies lose business and risks just shift elsewhere.

**How to Make It Happen**

* FinTech’s can’t wait for governments to get their act together—it’s too slow, especially in places like Southeast Asia or Africa, where regulators are stretched thin. The answer? Band together. VASP trade groups, like Global Digital Finance (GDF), are already showing how: they share anonymized KYC data and best practices, helping firms spot high-risk wallets without reinventing the wheel. As a future AML consultant, I’d push for more of these alliances—think regional hubs where startups swap compliance tricks, train staff, and even lobby for clearer rules. Picture a network of African fintech’s pooling resources to license Elliptic for transaction monitoring, cutting costs by 60% compared to building their own systems.

In Nigeria, some crypto startups use Zoom webinars to share open-source monitoring scripts, which can assist others in avoiding scams in a market dominated by P2P trading. Internationally, companies such as Novastro integrate compliance into their platforms from the outset, tokenizing assets with built-in KYC checks. This approach is characterised by proactive collaboration and technology-driven solutions.

**Policy Integration: VASP Collaboration Framework**

To make this real, I’d suggest this approach into an AML policy under “Governance & Roles” as a standalone section. It’s practical, aligns with FATF’s 2025 guidance, and shows regulators you’re serious about compliance without stifling growth. Here’s how it could look:

.

* **Fintech Collaboration for Anti money laundering / CFT**: Join alliances like the GDF to share KYC best practices and anonymized risk data, ensuring compliance without privacy breaches.
* **Risk Assessment**: Deploy AI-driven scoring (eg like , AMLBot’s wallet analytics) to flag high-risk crypto transactions in real time and also track dark-web daels .
* **KYC Onboarding**: Use shared tools like AMLBot or ComplyAdvantage to screen clients against sanctions lists and cluster illicit wallet patterns.
* **Transaction Monitoring**: Leverage Chainalysis or Elliptic for Travel Rule compliance, automating sender/receiver data for transfers over $1,000.

1. Collaboration Framework

Objective: Enforce cost-effective AML/CFT compliance for VASPs through industry partnerships, aligning with FATF’s tech-neutral principles, share best practices and centralized data sharing with FIU when a ground for suspicion is arised

Actions:

- Join hands with VASP alliances (e.g., Global Digital Finance, CryptoUK) to access shared KYC data and compliance training and emphasis on screening tools for onboarding

- Example: Leverage GDF’s anonymized risk data to flag high-risk wallets (e.g., linked to DeFi scams), reducing detection time by 40%.

- Host annual webinars and training to share open-source monitoring tools, modeled on Nigeria’s crypto community initiatives.

- Endorsing for tech-neutral regulations via regional bodies (e.g., ASEAN Blockchain Consortium, African Union fintech working groups).

- Deploy AI tools (AMLBot, Chainalysis) for real-time risk scoring and Travel Rule compliance.

Metrics:

- Compliance cost reduction: Target 50% savings via shared tools.

- Risk detection: Achieve 95% accuracy in flagging illicit transactions.

- Training reach: Engage 100+ fintech staff annually via alliance programs.

2. Implementation Timeline

Q4 2025: Join GDF and pilot AI-driven KYC with AMLBot.

Q1 2026: Launch first webinar series; integrate Chainalysis for monitoring.

Q2 2026: Report cost savings and risk metrics to regulators.

Disclaimer: This report reflects my opinion, informed by relevant research and collected insights.