GLOBAL DIGITAL FINANCE

block

TRM

2026

REPORT ON SELF-CUSTODY WALLETS AND THEIR ROLE IN DIGITAL FINANCE

TABLE OF CONTENTS

03 **1. PREFACE**

04 **2. FOREWORD**

05 **3. CONTRIBUTORS & ACKNOWLEDGEMENTS**

06 **4. EXECUTIVE SUMMARY**

06 - Report Findings
08 - Recommendations to Policymakers

09 **5. INTRODUCTION**

09 - Introduction and Background
11 - Methodology
11 - How This Report is Structured

13 **6. SELF-CUSTODY WALLETS – FUNCTION AND DESIGN**

13 - Design Principles and Operation
14 - Custodial vs Self-Custodial
16 - Key Management and Usability
18 - Security and Operational Resilience
19 - Infrastructure, Intermediaries, and Modern Compliance

20 **7. USE CASES AND BENEFITS – EVIDENCE AND CONTEXT**

21 - Storage
22 - Payments and Remittances
27 - Financial Inclusion
28 - Decentralized Finance and Tokenized Assets

31 **8. ADDRESSING MISCONCEPTIONS - THE FOUR CORE MYTHS**

31 - Myth 1: Self-hosted wallets are predominantly used for illicit purposes
39 - Myth 2: Self-hosted wallets enable anonymous, untraceable transactions
43 - Myth 3: Illicit activity is concentrated in privately controlled accounts rather than regulated platforms
47 - Myth 4: Restricting or banning self-custody wallets is the appropriate regulatory response

49 **9. REGULATORY TREATMENT AND THE EXISTING COMPLIANCE ARCHITECTURE**

50 - On and Off Ramp Controls
51 - Blockchain Analytics and Transaction Monitoring
53 - Travel Rule
54 - Tiered, Risk-Based Treatment

56 **10. CONCLUSIONS & RECOMMENDATIONS**

58 **APPENDICES**

58 - Data methodologies, secondary sources

1. PREFACE



Chrysty Esperanza
Chief Legal Officer
Block

At Block, our purpose is economic empowerment. It's why we think about self-custody and digital assets like Bitcoin every day. It's why we built Bitkey, a Bitcoin wallet designed to make true financial ownership accessible to everyone.

There's nothing radical about self-custody, or the simple idea that people should be able to own and control their digital assets directly, without handing the keys to someone else. Self-custody is only becoming more important in a world where Bitcoin is used as a form of everyday money, and where tokenized assets, stablecoins, and other digital forms of representation are flowing throughout the digital economy.

The digital asset ecosystem is maturing fast, and the policy conversation is keeping pace. Governments, regulators, standard-setters, and industry are all working to define the right frameworks. They are asking important questions about where risk sits, what role intermediaries should play, how consumers are protected, and how innovation can be supported responsibly.

Different jurisdictions are finding different answers with a wide variety of ecosystem participants bringing distinct perspectives to the table. Exchanges, wallet providers, analytics firms, law enforcement, and customers each see the landscape differently. This is healthy as it also reveals the strong commonalities that policy is built on. These are serious efforts in good-faith to ensure we get digital assets policy right, and the conversation is richer for the range of voices and perspectives involved.

What's missing is a shared evidence base. Too often, the conversation about self-custody starts from assumptions rather than data, such as who uses wallets, what they are used for, and what risks they pose. This report is our attempt to fill that gap.

Working with Global Digital Finance and other partners across the industry, we are launching the first self-custody study grounded in real-world, on-chain transaction flows to understand how self-custody is actually used in the real world.

The findings speak for themselves. Across more than 318,000 wallet addresses and $40.6 billion in transaction volume, 92% of transactions were below $1,000, consistent with everyday payment activity, while nearly 38% flowed to or from regulated exchanges, reflecting users moving assets into self-custody for safe storage alongside their use of regulated platforms. Our findings show that just 1% of these transactions involved exposure to illicit counterparties; in the UK, where robust AML/CFT controls are already in place at exchange level, that figure dropped to just 0.1%.

What emerges is a picture of ordinary financial lives being conducted through a new and different kind of tool, while meeting existing regulatory expectations. For a growing number of people globally, self-custody is becoming core infrastructure for how they store and move value.

Block is committed to working openly with governments, regulators, and industry partners in every market where we operate. We built Bitkey because we believe people deserve true ownership of their financial lives. That goal is stronger when it's supported by proportionate, evidence-based regulation. This report is our contribution to getting it right. ■

2. FOREWORD



Lawrence Wintermeyer
Company Board Chair
Global Digital Finance (GDF)

Banks became popular in Western society in the nineteenth century as the industrial revolution transformed the lives of millions through regular employment in growing urban areas. Banks provided a safe place to store your currency and offered a practical way to transfer money without having to physically hold it or carry it around, leaving it prone to loss or theft.

In the latter part of the twentieth century, thanks to payroll automation, online banking transfers, and tap and go cards, we entered the era of electronic money with many of us no longer using physical cash for making payments. Electronic money on Web2 was a killer app as it drove many of our online purchase behaviors, especially with the rapid adoption of smartphones: from the ordering of food or a taxi to shopping for just about anything and booking our holidays.

Digital money is now a killer app on Web3 blockchain and distributed ledger technology with stablecoins offering a safe and reliable digital store of value for your currency and a real-time frictionless transfer of value to the person or company of your choice, across town, across the country, or across the world.

You don't need a bank to store your currency; you store it on your digital wallet, also known as a self-custody wallet, on your mobile phone. You don't need a bank to transfer money; you transfer it from your self-custody wallet on your mobile phone to the self-custody wallet of the person or company of your choice – on your phone, 24/7/365.

As the digital finance economy grows beyond stablecoins to tokenized stocks and shares, and commodities like gold and silver, which are now becoming popular for many consumers, the role of the self-hosted wallet is extending beyond currency to the buying and selling real-world assets and managing your investment portfolio.

Though self-hosted wallet technology has been in the market for over 16 years, since the early days of the blockchain, the improvements in privacy, security, and usability have positioned them for mass adoption. At the heart of this fundamental change is the move to a "wallet-based" structure with self-hosted wallets, from the "account-based" structure we have with banks and financial intermediaries today.

In this halcyon era of digital policy and regulatory clarity, the acceleration to digital finance for consumers could see the self-hosted wallet become a revolutionary technology like the computer, the internet, or the smartphone, delivering new personal agency and independence in finance for consumers.

I would like to thank the Block team and GDF executive branch for their leadership through the development of this report. A big thanks also goes to TRM Labs and Coinbase for powering the report with substantive industry data and further insights from the market and practitioners.

This report is a must read for industry executives, policymakers, and regulators and highlights the growth and importance of self-hosted wallets in digital finance, the big use cases, and debunks the myths about the role of self-hosted wallets in financial crime.

It is through member-led initiatives like this report that GDF delivers its mission of convening industry-led best practices and advocacy for digital finance to the industry. ■

3. CONTRIBUTORS & ACKNOWLEDGEMENTS

BLOCK



Will Paul
Head of Payments, Hardware, &
Small Business Public Policy

GLOBAL DIGITAL FINANCE (GDF)



Elise Soucie Watts
Executive Director



Fabienne Vivien van Kleef
Graduate Analyst

TRM LABS



Isabella Chase
Head of Policy, EMEA



Ben Braik-Scivyer
Blockchain Intelligence Analyst

COINBASE



Aadi Kulkarni
International Policy



Felix Haynes
International Policy

ACKNOWLEDGEMENTS

This report was developed in collaboration with Block and draws on contributions from a wide range of industry experts, researchers, and practitioners committed to advancing evidence-based dialogue on digital finance and self-custody wallets.

We thank the teams at Block, TRM Labs, and Coinbase for their expertise, support, and contributions throughout the development of this report. Their input on research, data analysis, technical review, and industry insights helped ensure the report reflects both practical market experience and rigorous analysis.

We are also grateful to the policymakers, academics, compliance professionals, technology specialists, and industry participants who shared perspectives, provided feedback, and contributed to discussions that informed the report's findings and recommendations.

The views and conclusions presented in this report are intended to support informed policy discussion and contribute to a greater understanding of the role of self-custody wallets within the evolving digital finance ecosystem.

4. EXECUTIVE SUMMARY

Self-custody wallets are software and hardware tools that enable individuals and businesses to hold and transact digital assets without relying on a third-party custodian. They represent a broader shift in how financial control is allocated, giving users direct agency over their assets by removing the requirement for intermediation at the point of holding.

As jurisdictions in the United States, the United Kingdom, the European Union, the Emirates, and APAC regions advance distinct frameworks for digital asset oversight, self-custody has become a focal point of global regulatory debate. The treatment of self-custody represents many important policy choices with critical implications for financial innovation, consumer and commercial protections, and illicit finance risk management.

This report presents an empirical, evidence-based analysis of self-custody wallet activity and provides observations to support practical recommendations to policymakers for emerging policy and regulations across jurisdictions.

The analysis draws on extant published data along with original transaction analysis commissioned for this report conducted by TRM Labs, across 318,930 unhosted wallet addresses on five major blockchains (Bitcoin, Litecoin, Ethereum, Polygon, and Tron), encompassing approximately $40.6 billion in total transaction volume.

In addition, the report incorporates a second, more targeted dataset derived from a smaller subset of wallets, which enabled more granular analysis of transactional behavior and user activity patterns. While this supplementary dataset covered a narrower sample, it provided deeper behavioral insights and forms the basis for several of the more detailed findings presented throughout the report.

The report also incorporates anonymized wallet activity data provided by Coinbase relating to the usage of legacy Coinbase Wallet and the Base App ecosystem. This dataset comprised a population of approximately 1.95 million wallets that had transacted at least once since January 2025 across seven blockchain networks: Base, Ethereum, Arbitrum, Optimism, BNB Smart Chain (BSC), Polygon, and Avalanche.

For the purposes of this analysis, the Coinbase dataset focused specifically on: (i) token send transactions initiated through the Coinbase Wallet and/or Base App user interface; and (ii) token inflows received by wallets that had interacted with the applications at least once during the observation period. The inclusion of this dataset provided additional insight into real-world self-custody wallet usage patterns across a broad multi-chain retail user base, complementing the transaction-level blockchain analysis conducted independently for this report.

REPORT FINDINGS

- **The shift to digital finance is accelerating.** Digital-native tools have begun to fundamentally change how people access and manage money. Mobile banking, real-time payments, and digital wallets have made financial services faster, cheaper, and more widely available. Adoption of self-custody wallets is growing as users seek greater control, privacy, and flexibility.

- **Self-custody wallets are multi-purpose infrastructure.** Self-custody wallets are not only tools for holding assets, but also a key component of a broader shift toward more user-controlled models of financial participation and digital ownership. Innovations, especially in key management, are making

self-custody significantly more accessible, particularly for less technical users.

- **Payments and remittances are a primary 'today' use case.** Cross-border payments can be expensive, slow, and operationally fragmented in many corridors, particularly for smaller-value transfers. The World Bank reports that officially recorded remittance flows to low- and middle-income countries reached approximately USD 656 billion in 2023, underlining the scale and economic significance of these payment flows.

- **Stablecoins are central to this activity.** Stablecoins combine the transferability of blockchain networks with relative price stability, making them practical for routine payments and remittance activity. The stablecoin market capitalization now exceeds USD 230 billion, with rapid growth expected. Stablecoin withdrawals to self-custody wallets are a normal and expected feature of user behavior, representing functional infrastructure for the storage and movement of digital cash.

- **Transaction patterns are consistent with legitimate consumer and business activity:** 80% of stablecoin transfers from self-hosted wallets were below USD 1,000; Approximately 97% were below USD 10,000. This is consistent with consumer payments, remittance flows, and routine peer-to-peer transfers. Transfers between USD 50,000 and USD 500,000 represented less than 1% of transaction count but nearly one-third of total transaction volume, consistent with treasury management, liquidity operations, and business settlement activity.

- **Self-custody is relevant for underserved or financially constrained users.** In some jurisdictions, individuals and small businesses face limited access to banking services, high remittance costs, weak payment infrastructure, capital controls, or persistent currency instability. In such settings, digital wallets offer an additional channel for storing and transferring value. Activity was recorded across more than 150 countries, including markets where users face higher friction in traditional financial channels

- **Self-custody wallets provide the access layer for decentralized finance (DeFi) and the emerging tokenized asset ecosystem.** Many DeFi protocols require users to connect a wallet they control directly, enabling participation in lending, borrowing, swapping, and collateral management without opening an account with a conventional intermediary.

- **Illicit exposure is minimal and illicit fund flows are not concentrated in wallets.** Only 1% of analyzed transaction volume involved direct exposure to counterparties categorized as illicit, substantially lower than commonly assumed and comparable to or below estimates for traditional financial channels. Illicit fund flows transit through the broader ecosystem, with regulated platforms serving as critical nodes for liquidation.

- **Interaction with regulated entities is significant.** 37.7% of total transaction volume involved transfers to or from Virtual Asset Service Providers (VASPs), including exchanges, brokers, and payment providers; indicating that self-custody activity already intersects with existing compliance infrastructure.

- **Activity patterns indicate sustained, purposeful use.** 28.1% of wallet addresses were active for one to five years and 20.9% for 91–360 days; 18% showed single-day activity, inconsistent with profiles typically associated with illicit "burner" wallets.

- **A layered compliance architecture already applies.** On-ramp/off-ramp controls, blockchain analytics, travel rule obligations, and tiered risk-based treatment collectively provide multiple points of oversight.

- **Blanket restrictions are disproportionate, unenforceable, and inconsistent with international consensus.** Major jurisdictions are converging on risk-based approaches that focus on regulated touchpoints rather than on the act of holding assets directly.

RECOMMENDATIONS TO POLICYMAKERS

1. Adopt risk-based, evidence-informed approaches. Regulatory frameworks should calibrate obligations to demonstrate risk rather than applying blanket restrictions to self-custody as a category. For example, the UK HM Treasury's 2022 conclusion that self-custody transactions should not automatically be viewed as higher risk remains well-supported by the data.

2. Preserve the infrastructure-intermediary distinction. Self-custody tools function as infrastructure (analogous to physical wallets or safes) rather than intermediaries which safeguard client assets or process orders. Regulatory obligations designed for intermediaries are poorly suited to non-custodial software and risk displacing activity to less observable channels.

3. Anchor AML/CFT obligations at regulated touchpoints. Compliance requirements should apply to intermediaries — exchanges, brokers, payment providers, and stablecoin issuers — rather than to providers of self-custody wallet software or its users directly. This reflects established regulatory principles and practical enforceability.

4. Reject automatic higher-risk classification of self-custody transactions. Regulatory frameworks and supervisory guidance should not treat transfers to or from unhosted wallets as inherently elevated risk. Risk assessment should be driven by transaction characteristics, counterparty exposure, and behavioral indicators not by custody model alone.

5. Engage with technological evolution. The binary distinction between "custodial" and "non-custodial" is giving way to a spectrum of hybrid arrangements. Regulatory frameworks should be sufficiently flexible to accommodate this evolution without requiring repeated legislative revision focusing on the substance of activity and the location of control.

6. Invest in blockchain analytics as a supervisory tool. The inherent transparency of public blockchains provides investigative and monitoring capabilities that should be integrated into both firm-level compliance programs and regulatory supervisory practice to allow for risk-sensitive approaches rather than blanket restrictions.

7. Coordinate internationally to avoid fragmentation. Divergent approaches across jurisdictions — particularly more restrictive frameworks like the EU's Transfer of Funds regulation, risk regulatory arbitrage and compliance complexity. Continued multilateral engagement and consistent international standards through FATF, IOSCO, and other standard-setting bodies remain essential.

8. Commission further empirical research. The evidence base would benefit from longitudinal studies tracking wallet cohorts over time, comparative analysis across additional jurisdictions, and continued investment in address attribution to reduce the large unclassified category.

As digital asset markets continue to mature, self-custody wallets are likely to become an increasingly important component of the global financial and digital infrastructure landscape. The evidence presented in this report suggests that self-custody is not a niche or inherently high-risk activity, but rather an emerging layer of financial participation supporting payments, savings, remittances, decentralized finance, and broader forms of digital ownership.

Policymakers face an important opportunity to develop regulatory frameworks that mitigate genuine risks while preserving the open, innovative, and globally interoperable characteristics that make these technologies valuable. Forward-looking regulation should seek to balance financial integrity objectives with technological neutrality, consumer choice, and continued innovation, ensuring that emerging frameworks remain adaptable as wallet technology, blockchain infrastructure, and digital asset markets continue to evolve. ■

5. INTRODUCTION

INTRODUCTION AND BACKGROUND

For most of modern history, participating in the financial system has meant relying on trusted intermediaries. Banks hold deposits. Payment providers move money. Custodians safeguard assets. These institutions brought scale, standardization, and regulatory accountability to financial services, but with some key trade-offs, such as friction, cost, and barriers to entry. Access has depended on geography, documentation, credit history, and the willingness of an intermediary to serve a given customer. For billions of people worldwide, these barriers remain real.

Over the past two decades, digital-native tools have begun to fundamentally change how people access and manage money. Mobile banking, real-time payments, and digital wallets have made financial services faster, cheaper, and more widely available, reducing dependence on physical infrastructure and expanding access for underserved communities. The emergence of digital assets and blockchain-based financial infrastructure - including decentralized finance (DeFi) - mark a significant shift in global finance, moving from highly intermediated systems toward more decentralized models of ownership and exchange.

This is a new paradigm in which individuals can directly control and transfer value, hold assets in self-custody wallets, transact peer-to-peer, and interact with decentralized applications. These models strengthen individual autonomy, broaden access to financial services, lower system-wide costs, and support greater transparency. Centralized intermediaries continue to play an important role - providing on-ramps between traditional and digital currencies, safeguarding assets for those who prefer custodial solutions, and supporting the overall usability and trust of the financial ecosystem - but they work *alongside* individual choice and control, not as a substitute for it.

At the core of this shift lies self-custody: the ability for users to hold and manage digital assets directly, through cryptographic wallets[1], without relying on a third party. Much like how a physical wallet enables individuals to have complete control over their physical cash, self-custody enables the same level of control and autonomy for digital assets such as stablecoins and bitcoin. Self-custody wallets are best understood as user-controlled infrastructure rather than financial intermediaries, part of what the International Monetary Fund has described as a broader trend toward disintermediation, in which traditional financial roles are evolving alongside decentralized protocols and user-controlled systems.[2] Section 6 of this report explains how self-custody wallets work in detail.

[1] Bank for International Settlements, *Cryptocurrencies and Decentralised Finance: Functions and Financial Stability Implications*, BIS Papers No. 156, 2025; World Economic Forum, Decentralized Finance (DeFi) Policy-Maker Toolkit, 2021: https://www.bis.org/publ/bppdf/bispap156.pdf & International Monetary Fund, "The Crypto Ecosystem and Financial Stability Challenges," Global Financial Stability Report, 2023.: https://www.elibrary.imf.org/downloadpdf/display/book/9781513595603/ch002.pdf

[2] Bains, Parma, Arif Ismail, Fabiana Melo, and Nobuyasu Sugimoto. "Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets." FinTech Notes 2022, no. 007 (September 26, 2022).:https://www.imf.org/en/publications/fintech-notes/issues/2022/09/26/regulating-the-crypto-ecosystem-the-case-of-unbacked-crypto-assets-523715

Adoption of self-custody wallets is accelerating. Industry data indicates that millions of users globally now interact with digital assets with increasing migration toward self-managed solutions[3], reflecting a growing demand for greater control, privacy, and flexibility in financial interactions. Importantly, self-custody does not mean disconnection from the regulated financial system, as users routinely move funds between custodial and self-custodial environments, creating natural compliance touchpoints for customer due diligence, transaction monitoring, and risk management within existing regulatory frameworks. This is a dynamic we explore more in sections 6 and 9.

This evolution has rightly been of interest to global regulators, as they assess the impact to global regulatory frameworks, particularly in the context of global anti-money laundering and counter-terrorist financing (AML/CFT) standards. Several concurrent developments make this moment pivotal:

- The **Financial Action Task Force (FATF)** has been central in shaping this discussion, with its recent targeted report on stablecoins and self-custody wallets highlighting concerns around the potential misuse for illicit finance, while acknowledging legitimate uses and the technical challenges associated with applying traditional compliance mechanisms to decentralized systems.[4] More broadly, FATF's guidance confirms that transactions involving self-custody wallets fall within the scope of its risk-based framework.

- In the **European Union**, the Transfer of Funds Regulation extends traceability requirements to transactions involving such wallets, while the Markets in Crypto-Assets Regulation (MiCA) establishes a broader supervisory framework for service providers.

- In the **United Kingdom**, the Financial Conduct Authority and Bank of England have emphasized the need to balance innovation with consumer protection and financial stability, including in relation to self-custody solutions, with the Bank of England explicitly expressing concerns about self-custody wallets.[5]

- In the **Emirates,** the different regulatory agencies have adopted risk-based approaches to balance consumer protection and to mitigate risks of illicit finance and bad actors where the regions Securities and Commodities Authority (SCA) explicitly recognize and classify non-custodial wallets as arrangements where the client has full, independent control over their digital assets.

- In **Asia**, authorities such as the Monetary Authority of Singapore have adopted a risk-based approach, seeking to mitigate illicit finance risks while supporting innovation and the development of responsible digital asset markets.

- The **United States** illustrates how quickly the regulatory debate can shift. In 2020, FinCEN proposed rules that would have required banks and money service businesses to collect, verify, and retain information on certain transactions involving self-custody wallets, signaling a more restrictive and risk-focused approach to self-custody. That proposal drew substantial industry and civil society opposition on the grounds that it was disproportionate to the actual risks, would impose significant privacy and data-security burdens on consumers, and would push

[3] Financial Conduct Authority, *Cryptoassets Consumer Research 2023 (Wave 4)*, 2023; Bank of England, *Financial Stability Report*, 2023: .https://www.fca.org.uk/publication/research-notes/research-note-cryptoasset-consumer-research-2023-wave4.pdf & U.S. Department of the Treasury, Illicit Finance Risk Assessment of Decentralized Finance, 2023; Financial Crimes Enforcement Network, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," Notice of Proposed Rulemaking: https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf

[4] Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (FATF, 2021): https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html?utm_source=chatgpt.com

[5] Financial Conduct Authority, *Cryptoassets Consumer Research 2023 (Wave 4), 202 ; Bank of England, Financial Stability Report*, 2023.: .https://www.fca.org.uk/publication/research-notes/research-note-cryptoasset-consumer-research-2023-wave4.pdf

activity toward less observable channels rather than enhance law enforcement visibility. The proposal was never finalized and was later withdrawn. Under the current administration, the policy direction has shifted in the opposite direction; recent executive and legislative initiatives increasingly framed self-custody as a legitimate exercise of individual control over digital assets rather than a primary compliance risk. This shift is reflected in legislative proposals such as the GENIUS Act and the CLARITY Act, which carve self-custody out from parts of the regulatory perimeter, and in the SEC's broader move away from enforcement-led warnings toward a greater emphasis on retail education.

These contrasting divergences in regulatory approaches underscore a central tension in digital asset policy: how to balance the principles of decentralization and individual autonomy with proportionate oversight, risk mitigation, and financial integrity. While some policymakers view self-custody wallets primarily through the lens of illicit finance risk, their predominant real-world use cases - including payments, remittances, decentralized finance, and long-term asset storage[6] - are diverse, legitimate, and thriving. With FATF's ongoing review, MiCA's implementation, and active legislative debate in the United States, the window for shaping proportionate, evidence-based policy is open now.

This report examines the role of self-custody wallets in the digital finance ecosystem, drawing on original quantitative analysis, public regulatory documents, academic literature, and industry data. It provides:

1. A clear, technically accurate explanation of how self-custody wallets function and how they are evolving;

2. An empirical assessment of actual transaction patterns and risk profiles, grounded in blockchain analytics;

3. A comparative overview of regulatory approaches across major jurisdictions; and

4. Evidence-based recommendations for proportionate policy design.

It aims to contribute to ongoing global discussions on how to integrate decentralized technologies into the financial system in a way that supports both innovation and trust.

METHODOLOGY

The quantitative analysis underpinning this report was conducted by TRM Labs, a blockchain intelligence firm providing transaction monitoring and compliance tools to financial institutions and government agencies globally. The dataset covers over 300,000 unhosted wallet addresses across Bitcoin, Litecoin, Ethereum, Polygon, and Tron, representing approximately $40.6 billion in total transaction volume.

A probabilistic UK-linked subset of approximately 5,000 addresses ($85.6 million in volume) was identified via a combination of UK VASP exposures and analysis of transaction flow timings. Supplementary evidence is drawn from published reports by FATF, the World Bank, BIS, IMF, HM Treasury, and other public authorities. Full methodology is set out in the Appendix. A.

HOW THIS REPORT IS STRUCTURED

This main body of the report is organized into a series of thematic sections, followed by a section with the report conclusions.

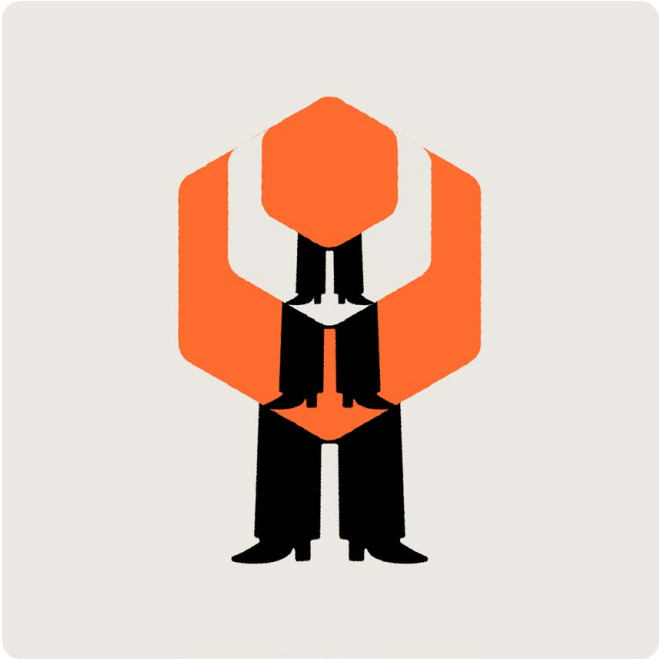
Section 6: What is a Self-Custody Wallet? Explains what self-custody wallets are, how they work, and how they differ from custodial services. It covers key management, the distinction between custodial and non-custodial models, and recent innovations that are making self-custody more accessible.

[6] TRM Labs, 2024 Crypto Adoption and Illicit Exposure Report, 2024: https://www.trmlabs.com/reports-and-whitepapers/2024-crypto-adoption-and-illicit-exposure-report & International Monetary Fund and Financial Stability Board, *IMF-FSB Synthesis Paper: Policies for Crypto-Assets*(September 2023). https://www.fsb.org/2023/09/imf-fsb-synthesis-paper-policies-for-crypto-assets/

Section 7: Everyday Use Cases examines the practical functions self-custody wallets serve, including payments and remittances, stablecoin use, access to decentralized finance, tokenized assets, and operational resilience. It draws on industry data and public sources to show that the predominant use cases are legitimate and economically significant.

Section 8: Addressing Misconceptions responds to four common claims about self-custody wallets — that they are predominantly used for illicit purposes, that they enable anonymous and untraceable transactions, that illicit activity is concentrated in self-custody, and that restricting or banning them is an appropriate policy response. Each is evaluated against available evidence.

Section 9: Regulatory Treatment maps the existing compliance architecture that applies when self-custody wallets interact with regulated entities, including on-ramp and off-ramp controls, blockchain analytics, travel rule obligations, and tiered risk-based treatment. It argues that effective oversight already exists at regulated touchpoints and that proportionate policy should build on those foundations. ■



6. WHAT IS A SELF-CUSTODY WALLET?

KEY TAKEAWAYS

- Self-custody wallets are key management tools — software or hardware — that give users direct, unilateral control of their private keys and therefore their digital assets, without relying on any third-party intermediary; unlike custodial accounts, no institution holds assets on the user's behalf or can restrict access.

- The core operations of a self-custody wallet involve three functions: generating and storing a cryptographic key pair, signing transactions using the private key, and broadcasting signed transactions to the relevant blockchain network — at no point does a third party gain custody or control.

- Innovations including multi-signature schemes, social recovery, hardware wallets, and smart contract ("account abstraction") wallets are significantly lowering the technical and security barriers that historically limited self-custody adoption, making it increasingly accessible to non-technical users.

Self-custody wallets (also referred to as “self-hosted,” “unhosted,” or “non-custodial” wallets) provide users direct and unilateral control of their private keys, or the cryptographic credentials required to authorize transactions and access assets recorded on a blockchain, without requiring reliance on a third-party. The terminology itself carries regulatory connotations. "Unhosted wallet" implicitly frames the technology in relation to hosted services such as “central custody services”, suggesting an absence of oversight. "Self-custody wallet" and "personal wallet" are more descriptively neutral, emphasizing user agency. This report uses "self-custody wallet" as the primary term, noting alternatives where relevant to specific regulatory contexts.

In traditional financial systems, ownership depends on accounts held with institutions. In blockchain systems, control depends on who holds the private keys. A self-custody wallet is not an account held at an institution but a tool (software and/or hardware) that holds these keys and interfaces with public blockchain networks. As such, self-custody represents a fundamental shift in the concept of asset ownership, replacing institutional trust with cryptographic verification.

DESIGN PRINCIPLES AND OPERATION

Digital wallets do not store assets in the conventional sense that a financial account may be considered to hold financial assets. Digital assets exist on blockchains, or distributed ledgers that track which assets are associated with which addresses. A transaction on a blockchain is simply an instruction to update the ledger so that an asset formerly assigned to one address is now assigned to another.

A self-custody wallet holds a blockchain address, which consists of a key pair: a public key and a private key. Both are cryptographically derived strings of characters. The public key generates an address that can be shared with others, equivalent to a phone number that people can be given in order to send value. The private key is what controls access. Whoever holds the private key can authorize transactions from that address. These keys provide the essential link between an owner and the assets associated with their address on the blockchain.

Wallets function as key management systems. Hardware and software wallets are the most common form, but they are not the only way to hold private keys. Users could memorize their key (a "brain wallet"), write it on paper (a "paper wallet"), or engrave it into a physical medium (a "titanium wallet"). Any of these methods constitutes a wallet. Hardware and software wallets are popular because they offer advantages in terms of security and convenience. Self-custody is the self-management of keys; wallets are the function through which people do this.

The operation of a self-custody wallet involves three core functions:

1. **Key generation and management.** The wallet generates a cryptographic key pair: a private key (which must remain secret and is used to authorize transactions) and a corresponding public key (from which a blockchain address is derived). The private key is typically generated from a random seed, often represented as a mnemonic 'seed' phrase (a sequence of 12 or 24 words that enables recovery).

2. **Transaction signing.** When a user wishes to transfer assets, the wallet constructs a transaction message and signs it using the private key. This cryptographic signature proves that the transaction was authorized by the key holder without revealing the private key itself.

3. **Broadcasting.** The signed transaction is broadcast to the relevant blockchain network, where it is validated by network participants (miners or validators) and recorded on the distributed ledger.

At no point in this process does a third party take custody of the user's assets or gain access to the private key. The wallet software facilitates interaction with the network but does not intermediate the transaction in the manner of a bank, broker, or payment processor.

Once broadcast and confirmed, the transaction is recorded permanently on a public ledger. This means that while self-custody gives users control over when and whether to transact, the transactions themselves are typically recorded on transparent, auditable infrastructure. Self-custody enables direct, peer-to-peer transfer of value without centralized clearing or settlement, but not without a record.

The majority of digital assets held in self-custody wallets — including Bitcoin, Ethereum, and major stablecoins — exist on public blockchains where transaction data is permanently recorded and publicly accessible. A smaller subset of assets operates on privacy-enhanced networks with different transparency characteristics, but these currently represent a minority of overall transaction volume and market capitalization.

CUSTODIAL VS SELF-CUSTODIAL

The distinction between custodial and self-custodial wallets is best understood as a trade-off between convenience and control. In a custodial model, a third-party provider, typically a centralized exchange or financial platform, holds users' private keys and executes transactions on their behalf. This offers simplified onboarding, account recovery, and customer support, but introduces counterparty risk: users must rely on the custodian's security and operational integrity.[7]

Self-custody removes that dependency, and users have full control over their assets, enabling greater autonomy and independence from centralized platforms. In practice, both models coexist; custodial solutions are often preferred by newer users, while self-custody is more commonly adopted by those seeking greater flexibility and direct ownership.[8] Many market participants use a combination of both, depending on function and risk tolerance.

[7] Kraken, Custodial vs Non-Custodial Wallets; Gemini, Crypto Wallets: Custodial vs Non-Custodial.: https://www.kraken.com/learn/custodial-non-custodial-crypto-wallet
[8] Kraken, Custodial vs Non-Custodial Wallets; Coinbase, Custodial and Non-Custodial Wallets.: https://www.kraken.com/learn/custodial-non-custodial-crypto-wallet

Beyond their role in enabling asset transfers, self-custody wallets also serve as a gateway to decentralized applications and services. They allow users to interact with blockchain-based systems, manage tokenized assets, and participate in emerging digital financial infrastructure. In practice, they are also often used alongside exchanges and other financial institutions, which continue to providing access, liquidity, and regulated services within the ecosystem.

As such, self-custody wallets are not only tools for holding assets, but also a key component of a broader shift toward more user-controlled models of financial participation and digital ownership.[9]

Dimension	Custodial (Hosted)	Self-Custodial
Key control	Third party holds private keys	User holds private keys
Account relatioship	User has account with provider	No institutional relationship required
Regulatory status	Provider is typically a VASP subject to AML/CFT obligations	Wallet software is infrastructure; no intermediary to regulate
Recovery mechanism	Password reset, identity verification	Seed phrase, social recovery, or multisig (varies by design)
Counterparty risk	Provider insolvency, hack, or freeze may affect access	No counterparty risk (but user bears operational risk)
Transaction visibility	Provider maintains internal records; reports to authorities	Transactions recorded on public blockchain; no centralized record-keeper
Access control	Provider may freeze, restrict, or close accounts	User retains access unless private key is lost or compromised
Applicable analogy	Bank account or brokerage account	Physical wallet, safe, or bearer instrument

[9] Binance Academy, Custodial vs Non-Custodial Wallets; Trust Wallet, Web3 and Self-Custody Wallets.: https://www.binance.com/en/academy/articles/what-are-web3-wallets

KEY MANAGEMENT AND USABILITY

This control comes with heightened user responsibility. If private keys are lost, stolen, or mismanaged, access to assets can be permanently lost, as there are not always built-in recovery mechanisms comparable to those in traditional financial systems. Self-custody of digital assets requires careful key management, including secure storage and protection against cyber threats such as phishing or malware attacks, explaining the popularity of self-custody wallets that help to make this simpler for users.[10]

Innovations are making self-custody significantly more accessible, particularly for less technical users. The usability gap is narrowing as technological developments help to mitigate these risks.

- **Multi-signature (multisig) wallets** require multiple private keys to authorize a transaction (e.g., 2-of-3 or 3-of-5 configurations). This distributes risk: no single compromised key can result in asset loss, and recovery is possible if one key is lost.

- **Social recovery wallets** designate trusted contacts or institutions as "guardians" who can collectively authorize key recovery without (they themselves) having the ability to initiate transactions. This preserves self-custody while providing a safety net.

- **Hardware wallets** store private keys on dedicated offline, air-gapped devices that never expose keys to internet-connected systems, protecting against remote compromise.

- **Smart contract wallets** (also termed "account abstraction" wallets) encode access logic into on-chain smart contracts, enabling features such as spending limits, time-locked recovery, session keys for specific applications, and programmable inheritance — all without surrendering custody to a third party.



[10] CoinTracker, *Custodial vs Non-Custodial Wallets; Cobo, Custodial vs Non-Custodial Wallet Explained.*: https://www.cointracker.io/blog/custodial-vs-non-custodial-wallets

Bitkey, built by Block (the parent company of Square and Cash App), illustrates how self-custody wallet design is evolving to address the usability and security challenges that have historically limited adoption.

Bitkey combines a mobile app with a dedicated hardware device, using a 2-of-3 multisignature architecture. Three keys protect the wallet: one held on the user's mobile device, one on the Bitkey hardware device, and a third encrypted on a server. Any two of the three keys are required to authorize a transaction. Critically, the user holds two of the three keys. Bitkey holds only one — and that single key cannot authorize any transaction or move any funds on its own. This means Bitkey, as the wallet provider, never has the ability to access, control, or move a user's Bitcoin. The user can always act without Bitkey; Bitkey can never act without the user.

This architecture reflects the core distinction between self-custody wallet providers and traditional custodians. Bitkey does not hold assets on behalf of users, does not execute transactions on their behalf, and does not maintain custody relationships. It provides the tools through which individuals manage their own assets directly.

The design also addresses several of the key management challenges described above. If a user loses their phone, they can recover access using the hardware device and the server key. If they lose the hardware, the app key and server key can restore access to a new device. If both are lost, recovery is possible through designated trusted contacts. Bitkey does not use seed phrases — the 12- or 24-word backups that most self-custody wallets rely on and that represent a significant usability barrier and security risk for less technical users.

The hardware device uses biometric authentication (fingerprint) to authorize transactions, and stores private keys offline to protect against remote attacks. Bitkey also provides an Emergency Exit Kit — an encrypted backup that allows users to move funds independently if the Bitkey service is ever unavailable, reinforcing the principle that no third party — including Bitkey itself — can prevent a user from accessing their own assets.

Bitkey does not require identity verification to set up a wallet, consistent with the self-custody model described in this report. Compliance obligations arise at the regulated touchpoints where users interact with exchanges and other financial services to acquire or convert digital assets — not at the wallet level itself.

Bitkey also incorporates an inheritance feature, allowing users to designate another Bitkey owner to receive their Bitcoin in the event of a claim, with built-in safeguards against accidental or unauthorized transfers. This reflects a broader trend in self-custody design: building for real-life scenarios — loss, recovery, succession — rather than treating self-custody as a purely technical exercise.



SECURITY AND OPERATIONAL RESILIENCE

Self-custody also provides security and operational resilience benefits beyond key management. Users adopt self-custody to reduce counterparty exposure, diversify custody arrangements, and maintain access to assets independently of centralized platforms, including in the event of service outages, platform failures, or custodial disruptions. Users also use self-custody to maintain access outside the operational constraints of centralized platforms, segregate treasury holdings, or satisfy internal risk-management requirements. This can be particularly relevant for businesses users operating across jurisdictions, or individuals seeking redundancy in custody arrangements. As a result, many market participants adopt hybrid custody strategies, combining custodial and non-custodial arrangements depending on risk tolerance and operational needs.

As self-custody is based on cryptographic keys, users are not locked into any single wallet provider. A user can access the same assets through any compatible wallet software, switch providers entirely, or use multiple wallets simultaneously, without requiring permission or cooperation from the original provider. This portability reinforces the distinction between self-custody wallets and account-based financial services, strengthening operational resilience by preventing 'locked' funds.

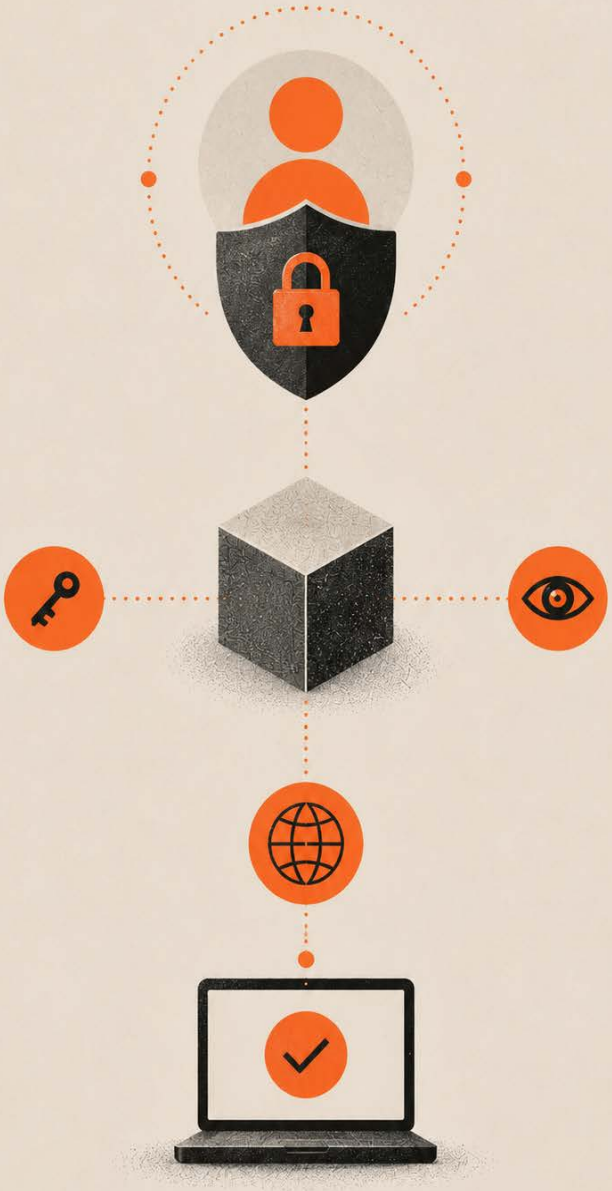
Most self-custody wallet software is also open-source, meaning its code is publicly available for independent audit and verification. This transparency allows users and security researchers to verify that a wallet operates as described. It also means that self-custody tools are not dependent on any single provider or jurisdiction.

Self-custody wallets can also provide benefits for privacy. Whilst self-custody wallets do not provide complete anonymity, particularly on transparent public blockchains where transaction activity can be analyzed using blockchain analytics tools, they can reduce dependence on account-based intermediaries and give users greater control over how and when they share transactional information with third parties. FATF's work recognizes the role of such analytics providers in examining on-chain activity and tracing flows associated with wallet addresses.[11]

This forms part of the broader appeal of the digital asset ecosystem for users: not anonymity in an absolute sense, but increased control over transactional exposure. These characteristics coexist with risk-based monitoring, analytics, and supervisory frameworks, and are part of the evolving balance between user autonomy and financial transparency.



[11] FATF, Targeted Report on Stablecoins and Unhosted Wallets (2026).: https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stable-coins-and-unhosted-wallets.pdf.coredownload.inline.pdf



INFRASTRUCTURE, INTERMEDIARIES, AND MODERN COMPLIANCE

Self-custody fundamentally changes how control is allocated within the financial system. In traditional models, intermediaries hold assets and execute transactions on behalf of users. With self-custody, individuals maintain direct control of their keys and authorize their own transactions. Wallet providers and software developers typically do not control user funds, execute transactions on behalf of users, or maintain custody relationships. They provide the tools and infrastructure through which individuals and businesses manage their own assets.

This is not merely a technical distinction, but a determinant of where regulatory obligations can and should be materially covered. Compliance obligations sit with the regulated intermediary, not with the wallet software or its developer. Applying a control-based standard is an evolution, not a revolution, in financial regulation, ensuring that it is still the actual intermediary, counterparty, or service provider that is subject to obligations. Indeed, a control-based standard is essential as the full, evolving spectrum of wallets that sit between custodial and self-custodial situations becomes clear. It is only through focusing on control can a proper regulatory perimeter be applied:

- Pure self-custody: Single private key held solely by the user.
- Enhanced self-custody: Multisig or smart contract wallets where the user retains ultimate control while third-party key holders support account recovery, without participating in transaction authorization.
- Hybrid models: Arrangements where a service provider holds one key in a multisig scheme, providing co-signing or recovery services without unilateral control.
- Delegated custody with user override: Smart contract wallets that delegate routine operations to a service provider but retain user-controlled emergency withdrawal mechanisms.
- Full custody: Traditional model where a VASP holds all keys and the user holds a contractual claim.

We discuss the implications of this in more detail in section 6. ■

7. EVERYDAY USE CASES: EVIDENCE AND CONTEXT

KEY TAKEAWAYS

- Payments and remittances represent the dominant real-world use case: with the World Bank recording USD 656 billion in remittance flows to low- and middle-income countries in 2023 and global average transfer costs still around 6.2%, self-custody wallets and stablecoins offer a faster, cheaper alternative — evidenced by 80% of stablecoin transfers being below USD 1,000, consistent with consumer and retail payment behaviour.

- Self-custody wallets serve a meaningful financial inclusion function, with activity recorded across more than 150 countries including markets characterised by limited banking access, currency instability, or high remittance costs; they also function as the essential access layer for decentralised finance (DeFi), with 12.5% of analysed transaction volume flowing to DeFi protocols for lending, borrowing, liquidity provision, and tokenised asset management.

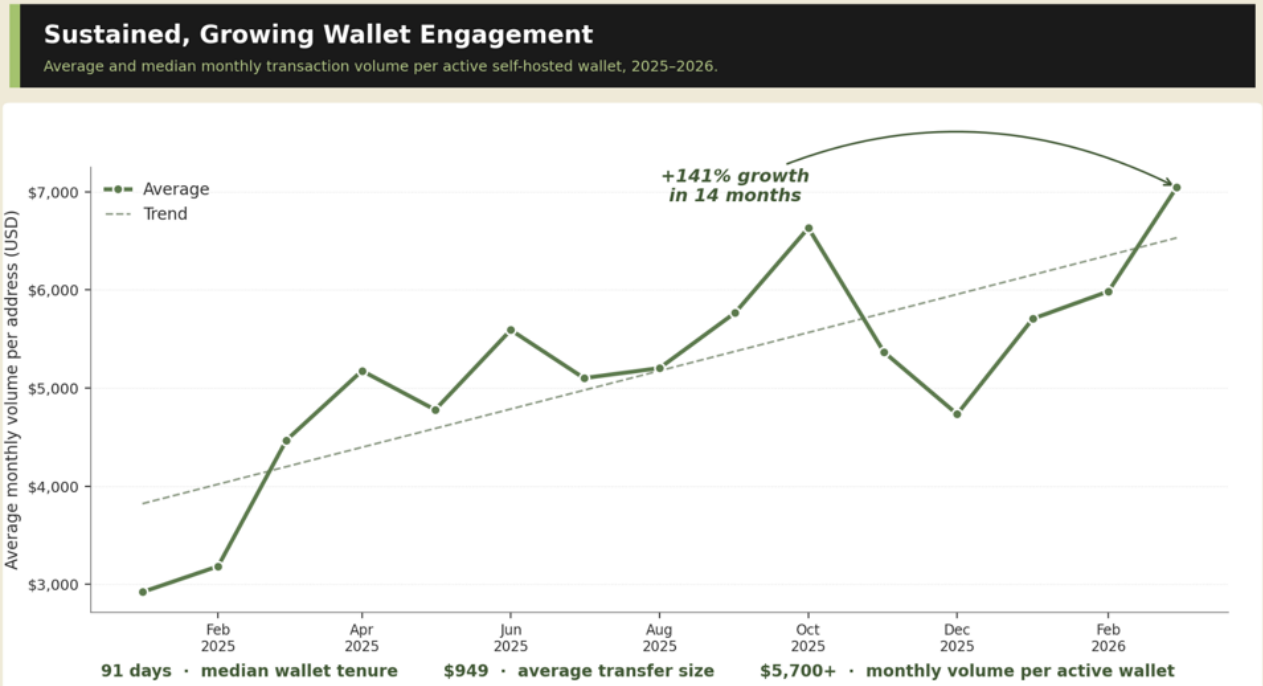
- The transaction evidence collectively shows that self-custody wallets are multi-purpose financial infrastructure — not passive storage tools or inherently illicit instruments — supporting payments, remittances, stablecoin use, DeFi participation, and tokenised asset management, with usage patterns consistent with sustained, ordinary financial behaviour rather than speculative or criminal activity.

Self-custody wallets serve practical economic and financial functions across the digital asset ecosystem. While these wallets are often discussed in a regulatory context primarily through a risk lens, they, in reality, predominantly serve practical economic and consumer functions.

Self-custody wallets can facilitate peer-to-peer payments, cross-border remittances, access to decentralized finance ("DeFi"), the holding and transfer of tokenized assets, and the storage of stablecoins. For some users, especially those operating in markets with limited financial access, currency instability, or high payment frictions, self-custody wallets also offer greater autonomy over how value is stored and transferred.[12]

The recent growth of the average monthly transaction volume per active self-hosted wallet from USD 2,900 in early 2025 to over US 7,000 in early 2026, an increase of over 140% in 14 months, demonstrates the growing adoption of this tool for popular use cases.

[12] FATF, *Virtual Assets and Virtual Asset Service Providers: Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs* (2021): https://www.fatf-gafi.org/en/publications/Fatf-recommendations/Guidance-rba-virtual-assets-2021.html



To evidence these use cases, this section draws on three categories of data: publicly available on-chain analytics and market data, which provide insight into transaction patterns and asset flows; findings from international bodies including FATF, the World Bank, and the Bank for International Settlements; and primary data from industry participants, including transaction-level insights from virtual asset service providers and wallet providers. This section examines the principal use cases, supported by available data, to provide a grounded understanding of why individuals and entities choose self-custody.

STORAGE

As discussed, self-custody wallets permit user autonomy and operational resilience by allowing users to retain direct control over access credentials rather than relying entirely on a centralized intermediary. They also offer a degree of privacy through pseudonymity, reducing dependence on account-based intermediaries and giving users greater control over how and when they share transactional information with third parties. Transfers to self-custody are often part of ordinary asset management behavior, rather than an indicator of misconduct.[13] Observed transaction flow patterns support this interpretation: significant volumes of activity involve transfers from regulated exchanges and payment platforms into wallets that subsequently exhibit limited onward movement or periodic rebalancing behavior, consistent with users storing assets, managing savings, or maintaining operational treasury balances rather than engaging in rapid transactional layering or concealment activity typically associated with illicit finance.

[13] FATF, Updated Guidance for a Risk-Based Approach to VA and VASPs (2021).: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

PAYMENTS AND REMITTANCES

One of the clearest use cases is payments and remittances. Cross-border payments can be expensive, slow, and operationally fragmented in many corridors, particularly for smaller-value transfers. The World Bank reports that officially recorded remittance flows to low- and middle-income countries reached approximately USD 656 billion in 2023, underlining the scale and economic significance of these payment flows.[14]

The global average cost of sending $200 was still around 6.2% — well above the UN Sustainable Development Goal target of 3%. For certain corridors (particularly those serving Sub-Saharan Africa), costs remain substantially higher. In that context, blockchain-based payment rails and self-custody wallets can provide an alternative mechanism for transferring value directly between users, including across borders, without relying on multiple correspondent intermediaries.

Broader transaction flow patterns are also consistent with these payment and remittance use cases. In particular, the significant share of transaction volume involving regulated VASPs suggests that users commonly move funds between exchanges and self-custody wallets as part of ordinary cross-border payment, transfer, and settlement activity.

USE CASE

Cross Border Payments and Remittances

Self custody wallets are increasingly used alongside traditional remittance channels to transfer value across borders. Users commonly move funds from a regulated exchange to a personal wallet for family support, payroll, merchant settlement, or treasury management. TRM Labs data provided for this report shows that the dominant flow pattern for self custody wallets is movement between regulated VASPs and personal wallets, consistent with everyday payment and transfer behaviour rather than speculative or illicit activity.

SUPPORTING EVIDENCE

37.7% — **of total volume flows to or from regulated VASPs**
The single largest counterparty category for self custody wallets is regulated exchanges and brokers, the on ramps through which users acquire digital assets.

64% — **of addresses have fewer than 50 lifetime transfers**
Most wallet activity is low frequency, consistent with periodic transfers for payments, remittances, or personal asset management, not high volume trading.

$40.6B — **total volume analysed across 300,000+ addresses**
The scale of activity at self custody wallets across five major blockchains reflects meaningful economic activity, not marginal or niche usage.

Key takeaway.
The VASP to wallet to VASP flow pattern dominates self custody wallet activity, reflecting the same deposit, hold, transfer cycle seen in traditional payments, with compliance obligations applied at each regulated touchpoint.

Source. TRM Labs data provided to GDF (2026). Over 300,000 unhosted wallet addresses across Bitcoin, Litecoin, Ethereum, Polygon, and Tron. World Bank, remittance flows to LMICs reached USD 656 billion in 2023.

[14] World Bank, Remittances (updated 18 September 2024).: https://www.worldbank.org/en/topic/migration/brief/remittances-knomad

Stablecoins are particularly important within this payment architecture because they combine the transferability of blockchain networks with relative price stability, making them more practical for routine payments and remittance activity than more volatile digital assets. They are serving both as a transactional bridge within digital asset markets and as a broader consumer tool for storing and moving digital cash. The total stablecoin market capitalization now exceeds USD 230 billion, with rapid growth expected in coming years.

FATF's recent work highlights both the rapid growth of stablecoins and their frequent interaction with self-custody wallets, particularly in peer-to-peer activity.[15] Users hold stablecoins in self-custody wallets for several reasons: to transfer value quickly across platforms, to reduce exposure to local currency volatility, to maintain operational liquidity outside business hours, or to interact with on-chain services that require direct wallet connectivity. Stablecoin withdrawals to self-custody wallets are a normal and expected feature of user behavior as a result and are forming functional infrastructure for the storage and movement of digital cash.[16]

The observable transaction patterns are consistent with these practical use cases, particularly the use of stablecoins for payments, liquidity management, cross-platform transfers, and interaction with decentralized financial infrastructure. A significant share of stablecoin-related activity is linked to smart contract interactions and decentralized finance infrastructure, rather than direct transfers between identifiable counterparties.

As illustrated, 43.8% of observed volume was categorized as unclassified activity, largely consisting of smart contracts and bridge transactions, reflecting the role of stablecoins in swaps, liquidity management, and cross-chain transfers. A further 12.5% of flows were connected to DeFi protocols, demonstrating the extent to which self-custody wallets are used to access lending, borrowing, and other on-chain financial services.

At the same time, illicit exposure across all analyzed addresses remained limited at approximately 1% of total volume, indicating that the overwhelming majority of stablecoin activity through self-custody wallets is associated with legitimate financial behavior rather than misconduct.



[15] FATF, Targeted Report on Stablecoins and Unhosted Wallets (2026).: https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stable-coins-and-unhosted-wallets.pdf.coredownload.inline.pdf

[16] FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs (2024/2025 updates).: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf

USE CASE

Stablecoin Storage and Transfer

Stablecoins are among the most actively used assets in self custody wallets, serving as a digitally transferable, relatively price stable form of value. Users hold stablecoins in self custody for a range of legitimate reasons: transferring value across platforms, reducing local currency exposure, maintaining liquidity outside business hours, or interacting with on chain services. TRM Labs data for a stablecoin-active subset of self-hosted wallets confirms that smart contract activity and DeFi interaction account for a significant share of stablecoin flows.

SUPPORTING EVIDENCE

55%

of stablecoin volume flows to unclassified counterparties

This category includes smart contracts, other self-hosted wallets, bridges and untagged addresses. The pattern is consistent with stablecoin usage, where tokens move through smart contract protocols for transfers, swaps, and liquidity management.

15%

of stablecoin volume flows to DeFi protocols

A meaningful share of stablecoin activity involves decentralised finance, where these tokens are commonly used for lending, borrowing, liquidity provision, and yield generation.

<1%

total illicit exposure across the stablecoin subset

Despite policy concerns about stablecoin misuse, only 0.4% of total stablecoin volume at these wallets involved illicit-categorised counterparties, confirming that the vast majority of activity, including stablecoin flows, is legitimate.

Key takeaway.

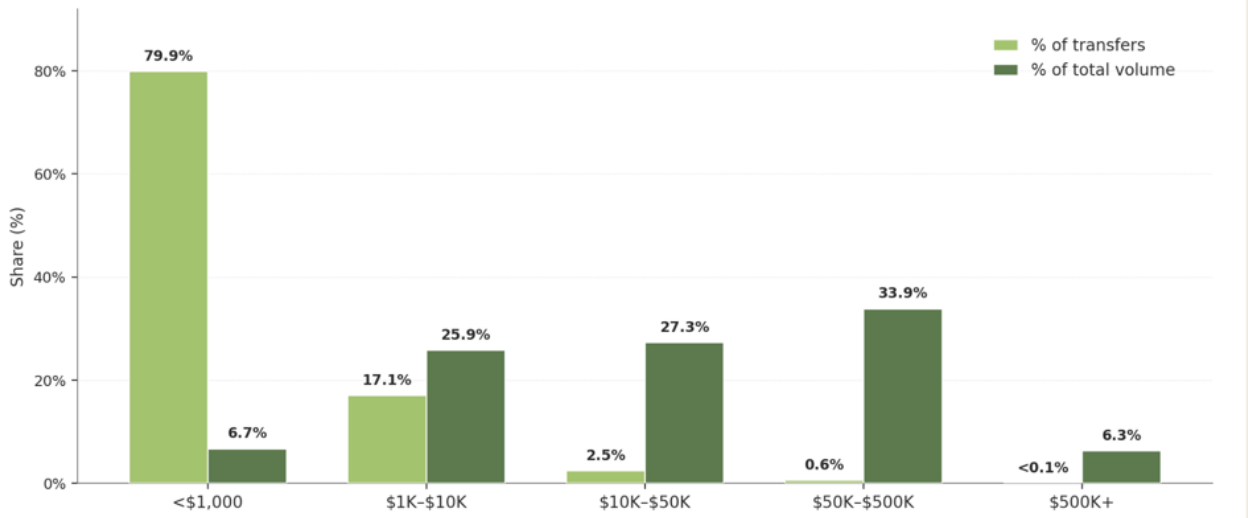
Stablecoin withdrawals to self custody wallets are a normal and expected feature of user behaviour. The data shows these flows are dominated by smart contract interactions and DeFi usage, functional infrastructure for the storage and movement of digital cash, not indicators of misconduct.

Source. TRM Labs data provided to GDF (2026). Analysis based on a stablecoin-active subset of the 300,000+ unhosted-wallet universe. FATF Targeted Report on Stablecoins and Unhosted Wallets (2026) confirms rapid stablecoin growth and frequent interaction with self custody wallets.

Additionally, 80% of stablecoin transfers from the stablecoin-active subset of self-hosted wallets were below USD 1,000, while approximately 97% were below USD 10,000. These smaller-value transfers account for most of the transaction activity and are more consistent with consumer payments, remittance flows, and routine peer-to-peer transfers than with high-value illicit movement. By contrast, transfers between USD 50,000 and USD 500,000 represented less than 1% of transaction count, despite accounting for roughly one-third of total transaction volume, a pattern more consistent with treasury management, liquidity operations, or business settlement activity.

Stablecoin Transfer Size Distribution

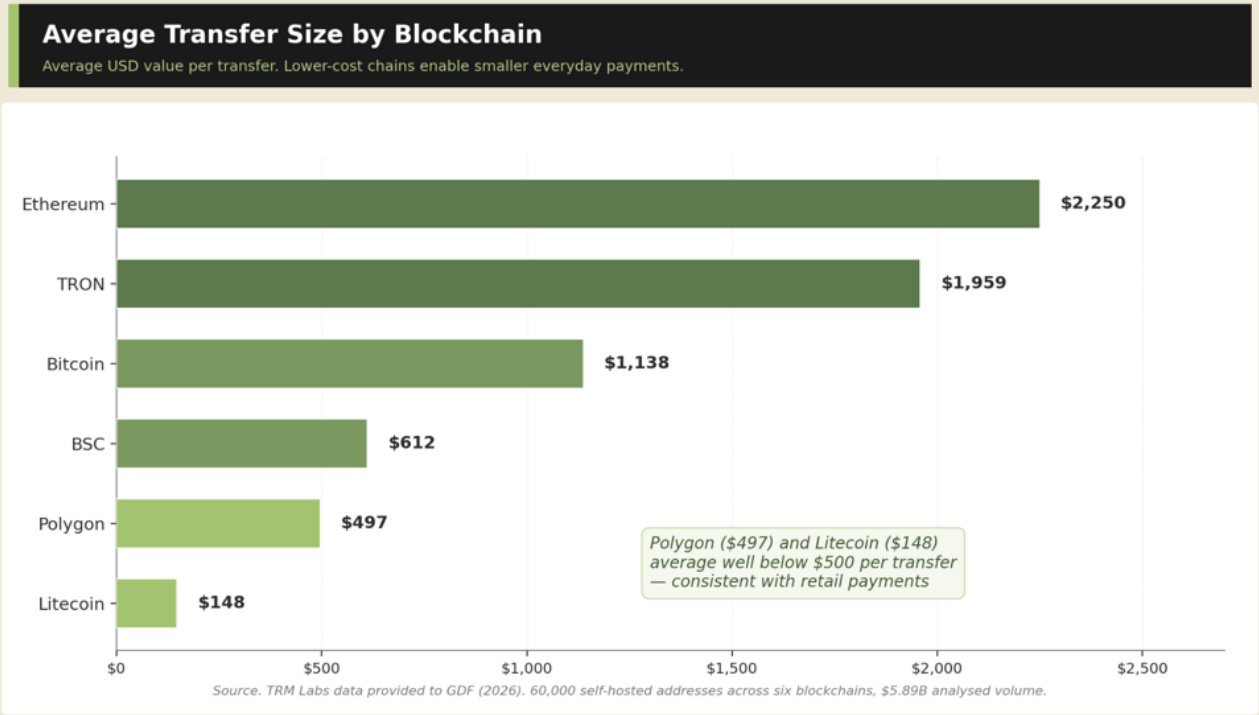
Stablecoin-active subset of the 300,000+ unhosted-wallet universe. Share of transactions vs share of volume.



Source. TRM Labs data provided to GDF (2026). Stablecoin-active subset: over 30,000 addresses, $2.64B volume across 2.08M USDT/USDC transfers.

Key finding.
Nearly 80% of stablecoin transfers from self-hosted wallets are under $1,000, and 97% are under $10,000. This is the transaction profile of consumer payments and remittances, not high-value illicit movement. Larger transfers ($50K–$500K) account for under 1% of activity but 34% of volume, consistent with periodic treasury management or business settlement.

Transfer-size patterns across different blockchain networks further reinforce the role of self-hosted wallets in payments and transactional activity. Lower-cost networks such as Tron and Polygon are associated with retail payments, remittances, and higher-frequency consumer transactions. By contrast, larger average transfer sizes on other networks are more consistent with treasury management, investment activity, or more capital-intensive on-chain financial services.



These transaction-size patterns are important because they align more closely with ordinary consumer and operational activity than with the concentrated movement of large illicit transfers. High-frequency, lower-value transfers are consistent with the practical ways in which self-custody wallets are used within the digital asset ecosystem, including cross-border remittances, merchant payments, payroll distribution, treasury movement, and peer-to-peer transfers. The data supports the view that self-custody wallets are frequently used as part of everyday financial activity rather than primarily for large-scale illicit movement. In our data, the 37.7% of self-custody transaction volume involving VASP interaction is consistent with a pattern where users acquire digital assets through regulated exchanges, transfer them peer-to-peer via self-custody wallets, and recipients convert to local currency through local VASPs or peer-to-peer markets. Self-custody's use case for payments and remittances is especially clear where customers move funds between exchange-hosted environments and personal wallets for family support, payroll transfers, merchant settlement, or treasury management. Self-custody does not replace the formal remittance sector, but it increasingly sits alongside it as part of a broader and evolving cross-border payments landscape.[17]

[17] World Bank, *Remittances Slowed in 2023, Expected to Grow Faster in 2024* (26 June 2024).: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099714008132436612

FINANCIAL INCLUSION

Furthermore, self-custody is also particularly relevant for underserved or financially constrained users. In some jurisdictions, individuals and small businesses face limited access to banking services, high remittance costs, weak payment infrastructure, capital controls, or persistent currency instability. In such settings, digital wallets offer an additional channel for storing and transferring value.

According to TRM Labs, continued growth in digital asset usage reflects expanding participation across global markets, including regions where users rely on digital assets as alternative financial infrastructure.[18] Self-custody wallets are not a complete substitute for financial inclusion, and they do not eliminate risks associated with volatility, fraud, or user error. However, they expand the set of available options for users who face frictions in conventional financial channels.

USE CASE

Financial Inclusion and Underserved Markets

In jurisdictions with limited banking access, high remittance costs, or persistent currency instability, self custody wallets can offer an additional channel for storing and transferring value. TRM Labs data shows that self custody wallet activity spans six major blockchains, including Ethereum and Tron, which together host the majority of stablecoin transfers globally and are widely used in emerging markets. The data confirms broad based participation rather than activity concentrated among a narrow set of sophisticated users.

SUPPORTING EVIDENCE

6

blockchains analysed, including Ethereum and Tron
Ethereum hosts the majority of DeFi and smart-contract activity, while Tron is widely used in emerging markets for low cost, high speed stablecoin transfers, particularly where traditional banking infrastructure is limited or expensive.

~8%

of volume involves smart contracts and on-chain infrastructure
Direct flows to smart contracts and bridges indicate engagement with on-chain services, including stablecoin protocols, DeFi, and payment infrastructure accessible without a bank account. Note: this category may also include unidentified DeFi or VASP infrastructure, and programmable wallets.

47%

of addresses are active for more than 90 days
Sustained wallet activity over months and years indicates that users are integrating self custody into ongoing financial behaviour, consistent with genuine utility rather than one time speculative use.

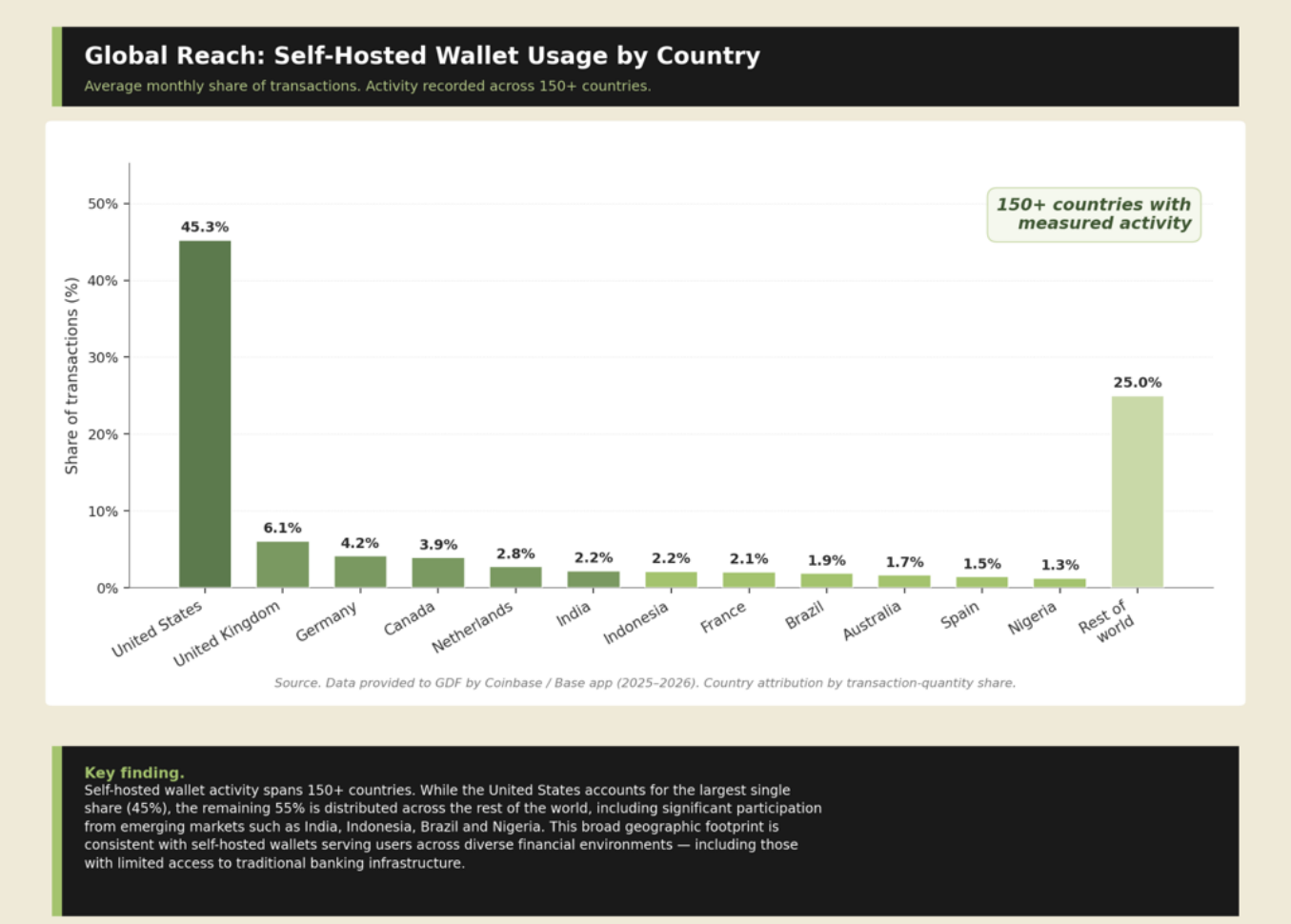
Key takeaway.
Self custody wallets are not a substitute for full financial inclusion, but the data shows sustained, broad based usage across chains commonly associated with low cost transfers in underserved markets, expanding the set of available options for users facing frictions in conventional channels.

Source. TRM Labs data provided to GDF (2026). Analysis based on a 60,000-address sample drawn from the 300,000+ unhosted-wallet universe. World Bank estimates 1.4 billion adults globally remain unbanked (Global Findex 2021).

[18] TRM Labs, ***2026 Crypto Crime Report*** (2026): :https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report

The geographic distribution of self-custody wallet activity further supports the view that these tools are being adopted across a broad range of economic and financial contexts, rather than by a narrow or highly concentrated user base. Activity recorded across more than 150 countries indicates that self-custody wallets are being used in both advanced and emerging markets, including jurisdictions where users face higher remittance costs, currency instability, or more limited access to traditional banking infrastructure. The data also suggests that self-custody usage is not confined to speculative trading activity, but increasingly forms part of wider payment, savings, and digital financial behavior across diverse regions.

This visualization reinforces the global and broadly distributed nature of self-custody adoption. While the United States accounts for the largest single share of observed activity, a substantial proportion is distributed across Europe, Asia, Latin America, and Africa, including countries commonly associated with emerging-market payment and remittance demand. This broad geographic footprint is consistent with self-custody wallets serving practical financial functions across diverse regulatory, economic, and banking environments.



DECENTRALIZED FINANCE AND TOKENIZED ASSETS

Self-custody wallets provide the access layer for decentralized finance (DeFi) and the emerging tokenized asset ecosystem. Unlike custodial accounts, many DeFi protocols require the user to connect a wallet that they control directly. This allows users to participate in activities such as lending, borrowing, swapping, liquidity provision, or collateral management in a DeFi environment without opening an account with a conventional intermediary. The wallet is the technical interface through which a user accesses these services but does not provide intermediary or control-based services.

The TRM Labs analysis found that 12.5% of transaction volumes from the analyzed self-custody addresses involved DeFi protocols. This activity was driven primarily by decentralized exchange (DEX) trading, alongside smaller volumes associated with lending and borrowing, liquidity provision, and other DeFi-related services.

As tokenization expands, users increasingly hold tokenized claims, securities-like instruments, fund interests, and other digitally represented assets in wallets they control directly. The Bank for International Settlements has described tokenization as a transformative innovation with the potential to improve existing financial arrangements and enable new ones, including in cross-border payments and securities markets. .[19] [20] Self-custody wallets function as user-controlled infrastructure for holding and transferring tokenized forms of financial value, a role likely to grow as trading venues, custody models, and secondary market infrastructures continue to evolve.

USE CASE

Tokenised Assets and On Chain Financial Services

As tokenisation expands, self custody wallets are becoming the user controlled infrastructure through which individuals and institutions hold and transfer tokenised claims, securities like instruments, and other digitally represented assets. TRM Labs data shows that self custody wallets are already deeply integrated with on chain infrastructure, with significant volume flowing to smart contracts, DeFi protocols, and cross chain bridges, the building blocks of a tokenised financial ecosystem.

SUPPORTING EVIDENCE

12.5% **of volume flows to DeFi protocols**
Self custody wallets serve as the technical interface through which users access lending, borrowing, swapping, liquidity provision, and asset management services, many of which will underpin tokenised asset markets.

5.8% **of volume flows through cross chain bridges**
Bridge usage reflects movement of assets across different blockchains, a pattern that will intensify as tokenised assets are issued and traded across multiple networks and jurisdictions.

28.1% **of addresses are active for 1 to 5 years**
Long duration wallet activity suggests users are treating self custody as persistent infrastructure for managing digital assets over time, the behavioural foundation for holding tokenised investments, not just transacting.

Key takeaway.
Self custody wallets are not just payment tools. The data shows deep integration with smart contracts, DeFi, and cross chain infrastructure. As tokenisation expands, these wallets will function as user controlled infrastructure for holding and transferring tokenised financial value.

Source. TRM Labs data provided to GDF (2026). BIS Annual Economic Report 2025 describes tokenisation as a transformative innovation in cross border payments and securities markets.

[19] BIS, Annual Economic Report 2025, Chapter III: “The next-generation monetary and financial system.” : https://www.bis.org/publ/arpdf/ar2025e3.pdf
[20] BIS, Annual Economic Report 2025.: https://www.bis.org/publ/arpdf/ar2025e.htm

Regulatory and risk profiles vary across DeFi protocols, but the structural point remains the same: self-custody wallets are often a prerequisite for participation in these markets. Transfers to self-custody reflect movement into other lawful parts of the digital asset ecosystem, rather than an inherent precursor to illicit activity.

Together, these use cases show that self-custody wallets are best understood as multi-purpose infrastructure through which users maintain full and unmediated control over the use of their assets in a variety of ways. They are not merely storage tools, nor are they inherently synonymous with illicit activity. Rather, they sit at the intersection of payments, remittances, stablecoin use, on-chain financial services, tokenization, and user-controlled asset management. Their role in the digital asset ecosystem is broader and more functional than is often assumed, reflecting a wide range of legitimate and everyday financial activity.

Despite this policy discussions often focus narrowly on illicit uses and disproportionately on potential risks. The following section addresses several common misconceptions and evaluates them against available evidence. ■



8. ADDRESSING MISCONCEPTIONS - THE FOUR CORE MYTHS

Policy discussions concerning self-custody wallets frequently concentrate on potential risks while devoting less attention to available empirical evidence. This section evaluates four commonly advanced claims against the data presented in this report and other publicly available sources, acknowledging genuine residual risks while correcting factual inaccuracies.

MYTH 1: SELF-HOSTED WALLETS ARE PREDOMINANTLY USED FOR ILLICIT PURPOSES

A commonly cited concern is that self-custody wallets, by operating outside the perimeter of regulated intermediaries, serve primarily as vehicles for money laundering, sanctions evasion, terrorist financing, and other financial crimes. The absence of mandatory identity verification at the point of wallet creation is said to render self-custody inherently suspect.

However, available evidence suggests that this view does not fully reflect how self-hosted wallets are used in practice. It assigns risk on a blanket basis to a custody model rather than to the behaviors, counterparties, and transactional patterns that have been observed across wider financial markets in determining financial crime exposure.

KEY TAKEAWAYS

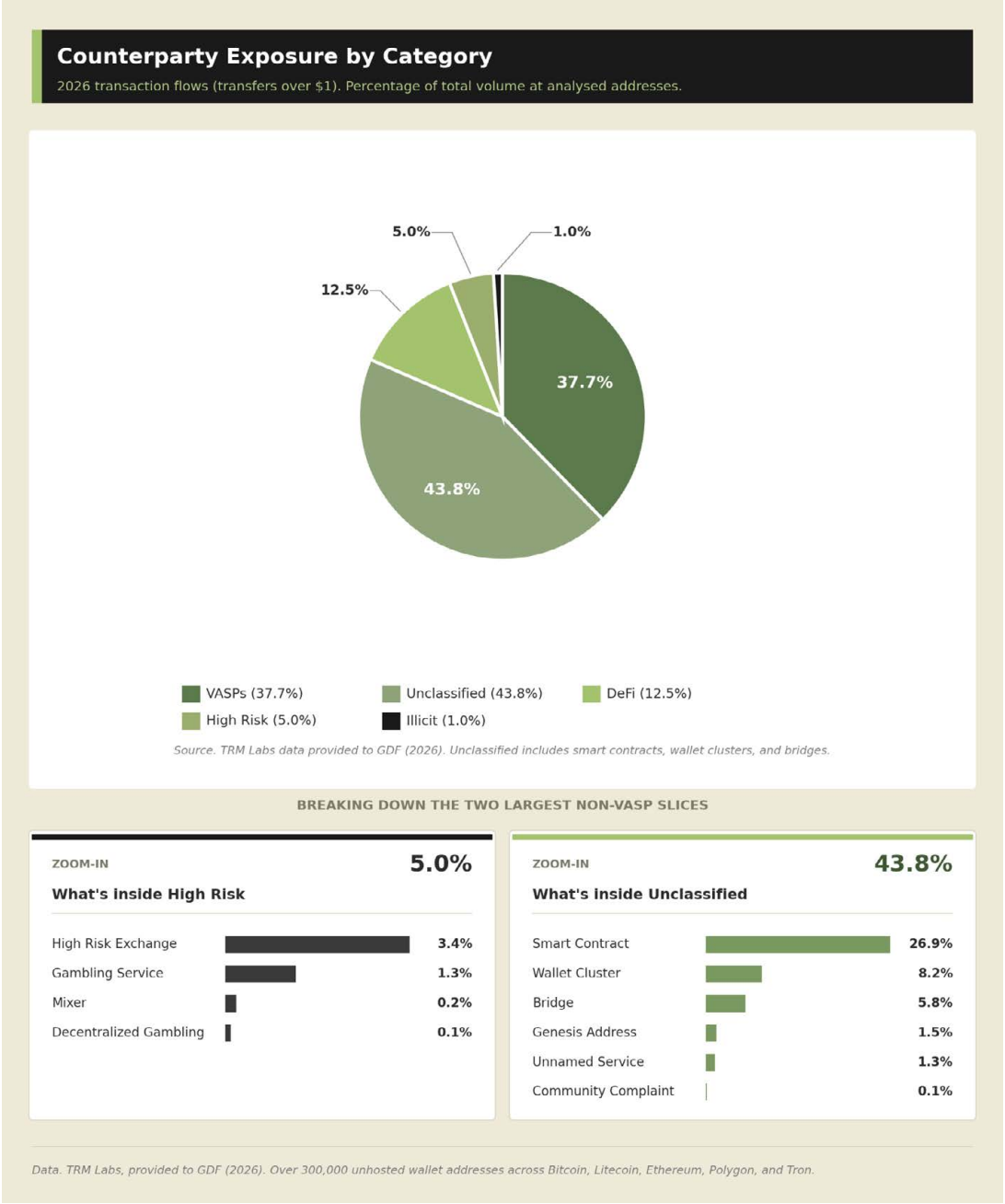
- **Myth 1 (predominantly illicit):** Only 1% of analysed transaction volume involved direct exposure to illicit counterparties, dominated by investment fraud and blocklisted entities rather than the terrorist financing or ransomware most commonly cited in policy debates; activity duration, low transfer frequency, and high VASP interaction all point toward legitimate, sustained financial use rather than criminal typologies.

- **Myth 2 (anonymous and untraceable):** Public blockchains provide pseudonymity, not anonymity — every transaction is permanently recorded on an immutable public ledger, and blockchain analytics tools can trace flows across multiple hops, cluster addresses by behavioural signals, and link activity to real-world identities wherever funds intersect with regulated exchanges or other identifiable services, providing traceability that in key respects exceeds that of cash.

- **Myths 3 & 4 (illicit activity concentrated in self-custody / restrictions are appropriate):** Illicit funds use self-custody wallets as transit points rather than endpoints, ultimately flowing to centralised exchanges and other off-ramp services where KYC and AML controls apply; blanket restrictions are therefore disproportionate, practically unenforceable against software-based tools, and inconsistent with the evidence-based conclusions of HM Treasury (2022), FATF guidance, and the current direction of US legislative proposals.

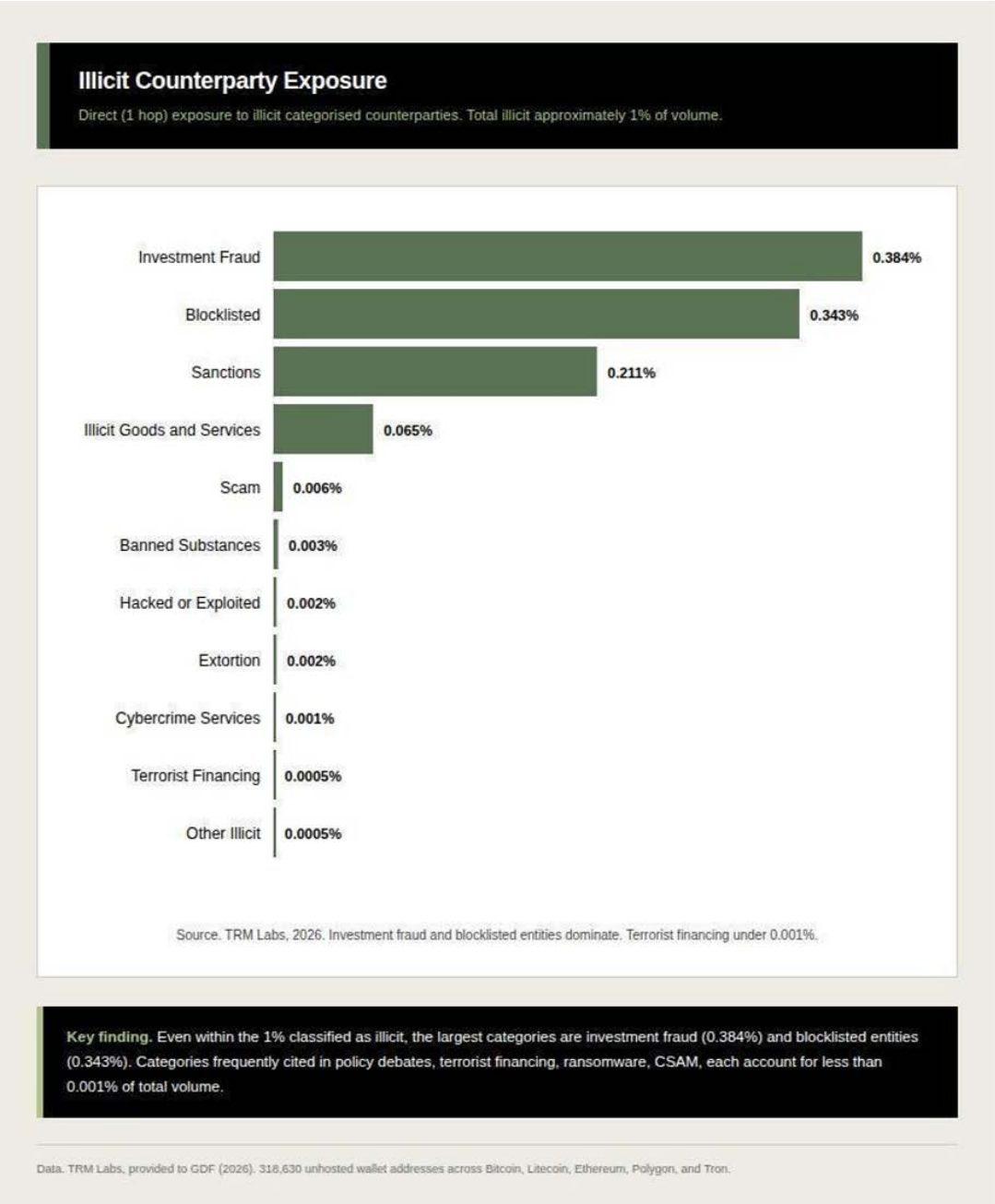
Firstly, interaction with regulated infrastructure is the dominant pattern witnessed. Data provided by TRM Labs for this report, covering over 300,000 unhosted wallet addresses across Bitcoin, Litecoin, Ethereum, Polygon, and Tron, representing $40.6 billion in total volume, confirms that the dominant counterparty for self-custody wallets is regulated infrastructure. 37.7% of total transaction volume at analyzed addresses involved transfers to or from VASPs such as exchanges, brokers, and payment providers, reflecting common user behavior in which individuals transfer assets from regulated platforms to privately controlled wallets for holding or portfolio management purposes.

At the aggregate level, illicit transaction volumes remain marginal. TRM Labs data shows that only 1% of total transaction volume at analyzed addresses involved direct exposure to illicit-categorized counterparties. The remaining activity involved 37.7% with virtual asset service providers (VASPs), 12.5% with DeFi protocols, 5% with high-risk entities, and 43.8% with unclassified entities, predominantly smart contracts and wallet clusters. Importantly, where self-custody wallets interacted with regulated financial infrastructure subject to robust AML/CFT controls, observed risk levels were even lower. UK-linked addresses showed higher interaction with regulated VASPs (42% versus 37.7% globally), while illicit exposure fell to 0.1% compared with 1% across the wider sample.

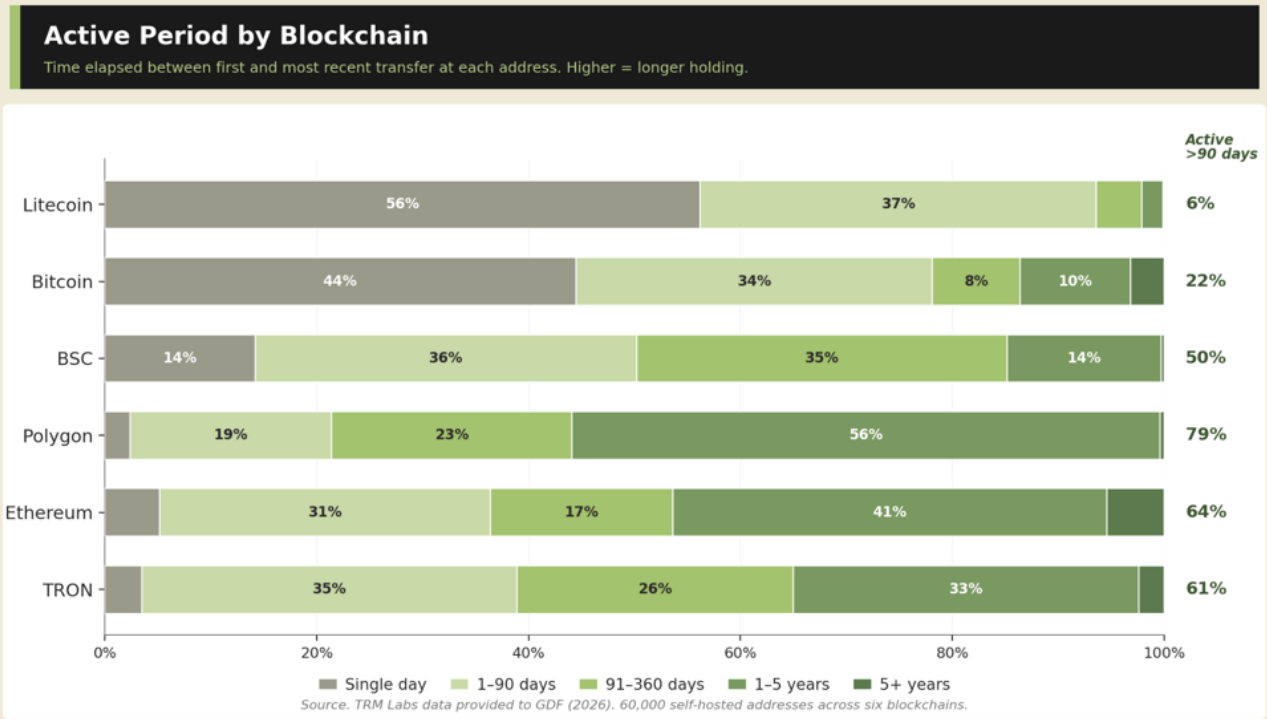


Exposure to higher-risk counterparties was also substantially lower (1.7% versus 5.0%). These patterns are consistent with the conclusion that effective AML/CFT controls at regulated exchanges and intermediary touchpoints can materially reduce risk without requiring blanket restrictions on self-custody wallets themselves. This is also consistent with the Financial Action Task Force's assessment that legitimate activity accounts for the vast majority of transaction volume.[21]

The composition of illicit exposure is narrower than often assumed. Even within the approximately 1% of transaction volume linked to illicit-categorized counterparties, the largest categories consisted primarily of investment fraud and interactions with blocklisted entities, while categories frequently emphasized in policy debates — such as terrorist financing, ransomware-related activity, and cybercrime services — represented only a very small fraction of total analyzed volume. This suggests that the nature of observed illicit exposure is more limited and differentiated than broad characterizations of self-custody wallets as predominantly illicit infrastructure would imply.



[21] TRM Labs, data provided to GDF for this report (2026). Analysis of 318,630 unhosted wallet addresses across five blockchains. See Appendix [X] for full methodology

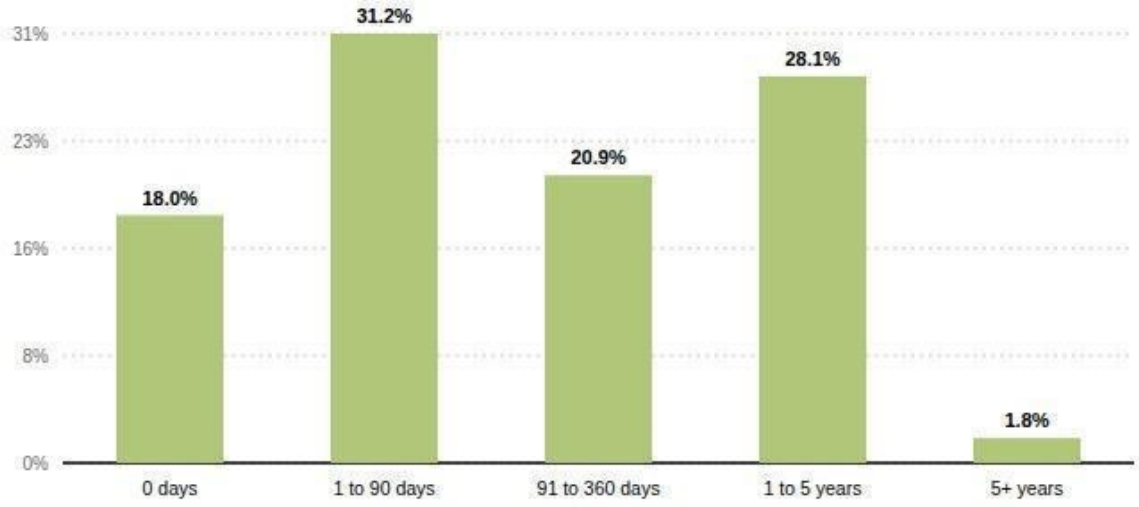


Furthermore, activity patterns are consistent with legitimate use. TRM Labs data shows that 28.1% of addresses were active for 1-5 years, 20.9% for 91-360 days, and only 18% showed activity confined to a single day. This distribution suggests that a substantial proportion of self-hosted wallets function as persistent financial infrastructure used repeatedly over time, such as for investment or storage, rather than as short-lived or disposable accounts designed solely for rapid movement of illicit funds.

These patterns are observable across multiple blockchain networks rather than being confined to a single ecosystem or asset type. TRM Labs data indicates that longer-duration activity patterns appear across Bitcoin, Ethereum, Tron, Polygon, and Litecoin, suggesting that sustained self-custody usage reflects a broader behavioral characteristic of digital asset users rather than isolated activity on any particular chain.

Active Period Distribution

Delta between first and most recent transfer, showing indicative wallet lifespan.



Source. TRM Labs, 2026. Approximately 50% of addresses active 90+ days, consistent with long term holding.

Key finding. 82% of addresses show activity spanning more than a single day, 50.8% are active for more than 90 days, and nearly 30% (1 to 5 years plus 5+ years) remain active for more than a year. This is consistent with investment, savings, and portfolio management behaviour. By contrast, illicit activity typically involves funds resting in a wallet for only minutes or seconds before being moved on to obscure their origin, a pattern that is not visible in this sample.

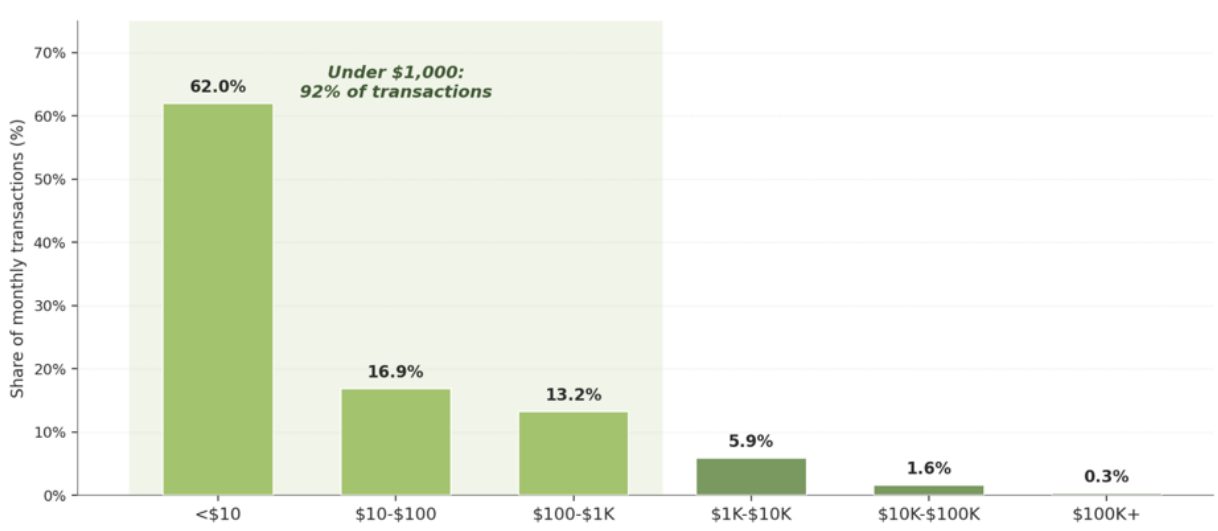
Data. TRM Labs, provided to GDF (2026). 318,630 unhosted wallet addresses across Bitcoin, Litecoin, Ethereum, Polygon, and Tron.

Transaction frequency is low, consistent with known use cases. TRM Labs data shows that 64.2% of analyzed addresses conducted fewer than 50 lifetime transfers, while only 0.9% exceeded 1,000 transfers. This relatively low-frequency transaction profile is more consistent with users managing personal holdings, savings, or periodic transfers over time than with high-volume transactional activity or automated movement patterns typically associated with large-scale illicit operations.

Transaction sizes are consistent with consumer and business activity, differing from high-value, low-frequency patterns commonly associated with illicit activity. Coinbase Wallet / The Base AppCoinbase/ Base App data shows that 92% of self-hosted wallet transactions were below USD 1,000, while transactions exceeding USD 100,000 accounted for only 0.3% of total activity. This distribution is more consistent with routine consumer payments, small remittances, and ordinary on-chain financial activity than with concentrated movement of large illicit sums.

Transaction Size Distribution

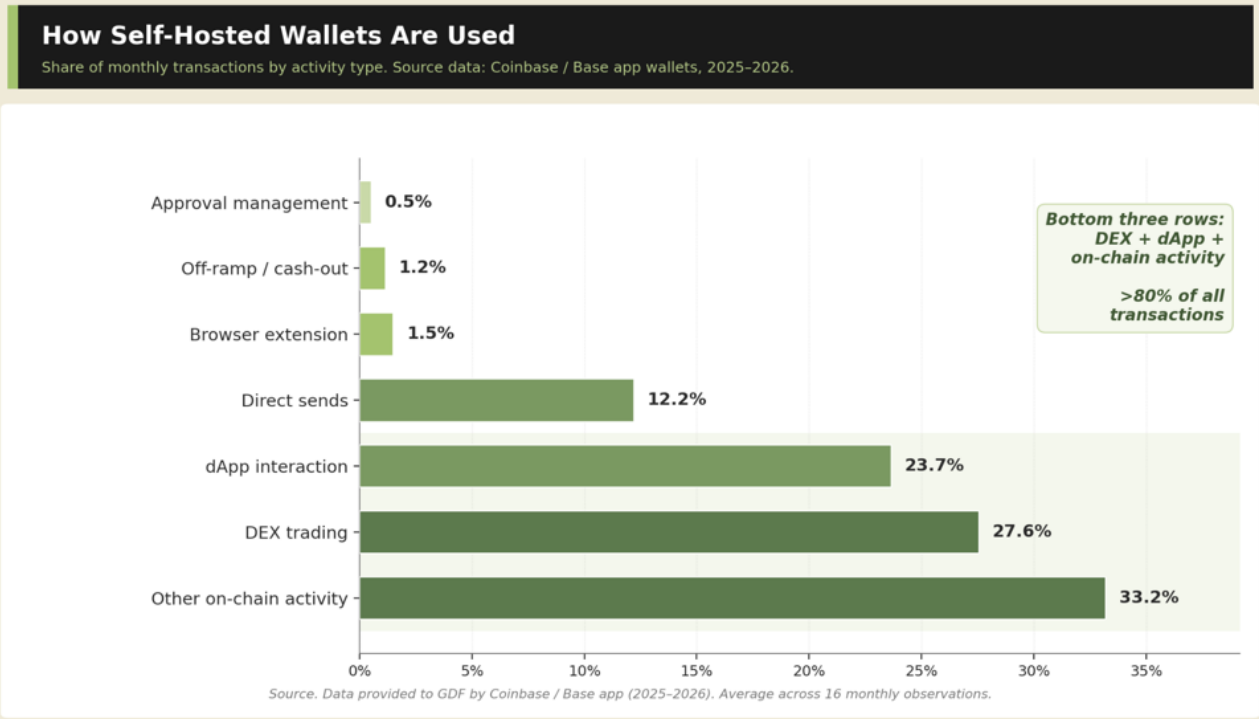
Average monthly share of self-hosted wallet transactions by transfer size, 2025–2026.



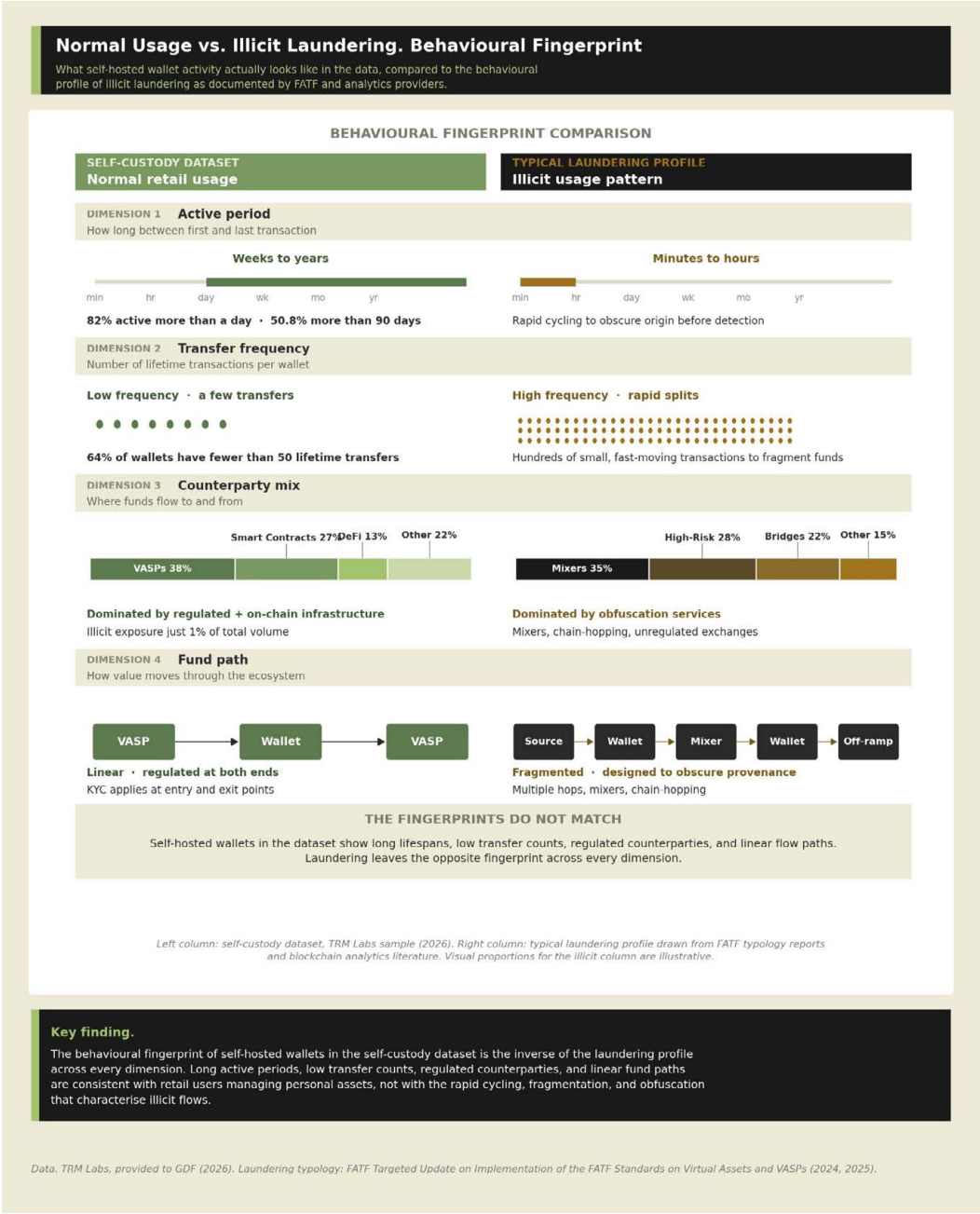
Source. Data provided to GDF by Coinbase / Base app (2025–2026). Average across 16 monthly observations.

Key finding.
92% of self-hosted wallet transactions are below $1,000, and 79% are under $100. Transactions over $100,000 represent just 0.3% of all activity. This distribution is consistent with retail payments, small remittances, and routine on-chain interactions — the everyday economic behaviour of consumers, not the high-value, low-frequency profile typically associated with money laundering or sanctions evasion.

The data reveals that self-hosted wallets function primarily as user-controlled interfaces for broader on-chain economic activity rather than simply as passive storage tools. A substantial share of observed wallet usage involves interaction with decentralized exchanges, on-chain applications, and other blockchain-based financial services, reflecting the role of self-hosted wallets in payments, trading, liquidity provision, tokenized assets, and wider participation in the digital asset ecosystem.



Considered collectively, the transaction patterns observed across the dataset do not resemble the behavioral profile typically associated with illicit laundering activity. Rather than showing rapid cycling, fragmented transfers, and repeated movement through obfuscation services, the analyzed self-hosted wallets display comparatively long activity periods, low transfer frequency, substantial interaction with regulated VASPs, and relatively straightforward transaction flows. The data points toward sustained and ordinary financial usage patterns that are materially different from the typologies commonly identified by FATF and blockchain analytics providers in connection with money laundering and sanctions evasion.



These findings are consistent with assessments by both FATF and UK HM Treasury. FATF has noted that legitimate activity accounts for the vast majority of transaction volume on public blockchains. The UK Government meanwhile noted in 2022 response to the consultation on amendments to the Money Laundering Regulations that it "*does not agree that self-custody wallet transactions should automatically be viewed as higher risk*," and that many people use self-custody wallets for legitimate purposes, including for their customizability and potential security advantages such as cold-wallet storage, which involves storing private keys on devices not connected to the internet). HM Treasury further concluded that there was "*not good evidence that self-custody wallets present a disproportionate risk of being used in illicit finance.*"[22]

In the same section, the government modified its proposal so that firms would collect originator and beneficiary information only for transactions identified as posing an elevated risk of illicit finance, rather than for all self-custody wallet transfers. That is a significant policy judgment: it rejects the idea that self-custody activity should, by default, be treated as higher risk, and instead endorses a more targeted, risk-based approach.

As a result, the available evidence does not support the characterization of self-custody wallets as

[22] HM Treasury, Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017: Response to the Consultation (June 2022).: https://assets.publishing.service.gov.uk/media/62aaf6148fa8f503af595b33/MLRs_SI_2022_-_Consultation_Response_final.pdf

predominantly illicit instruments. Self-custody wallets, like other forms of financial infrastructure, can be used for lawful or unlawful purposes. However, the available evidence confirms that the vast majority of use is legitimate and legal, and indicates that automatic consideration of self-custody as 'high-risk' is not based on clear evidence. The data further suggests that where self-custody wallets interact with regulated entities operating robust AML/CFT frameworks, illicit exposure declines even further, reinforcing the importance of risk-based controls at regulated touchpoints rather than blanket restrictions on self-custody itself. The relevant question for policymakers, regulators, and firms is not whether a wallet is self-hosted, but whether the surrounding facts indicate elevated risk. That is where effective controls should be directed.

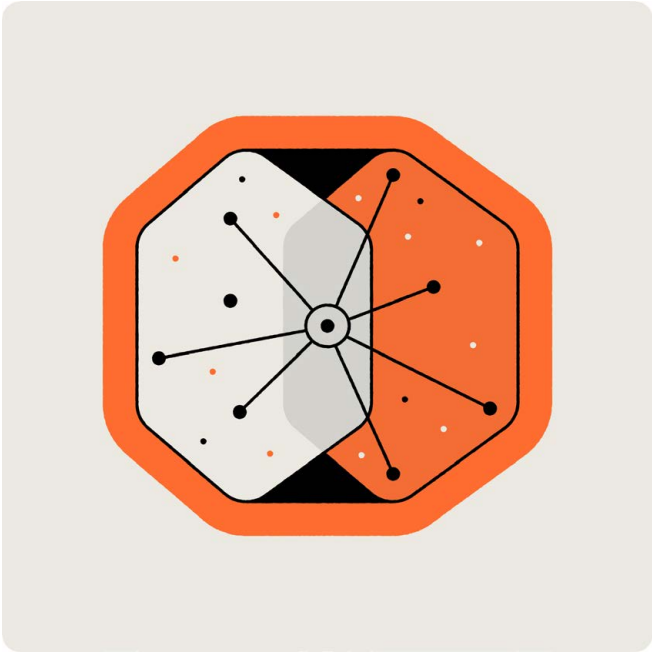
MYTH 2: SELF-HOSTED WALLETS ENABLE ANONYMOUS, UNTRACEABLE TRANSACTIONS

Another commonly raised concern is that self-hosted wallets enable anonymous and untraceable transactions, placing activity beyond the reach of law enforcement or regulatory oversight.This view conflates pseudonymity with anonymity and overstates the level of privacy provided by most blockchain networks. This distinction is fundamental to understanding how public blockchains operate.

Anonymity means activity can never be linked to a specific person. Pseudonymity means a persistent identity (such as a blockchain address) exists which can be used to link and trace activity attributable to a single actor, across multiple transactions and over time.
As a basic design principle, public blockchains are therefore transparent. The majority of assets held through self-hosted wallets exist on public blockchains. Those blockchains record transactions on a permanent, immutable, and publicly auditable ledger. Core transactional data, including wallet addresses, counterparties, amounts, and timestamps, is recorded and remains available for retrospective analysis. A self-hosted wallet maybe created without the same onboarding requirements as an account with a regulated intermediary, but its on-chain activity does not occur in a hidden system. It takes place within a ledger environment that is designed to preserve an enduring record of transfers.

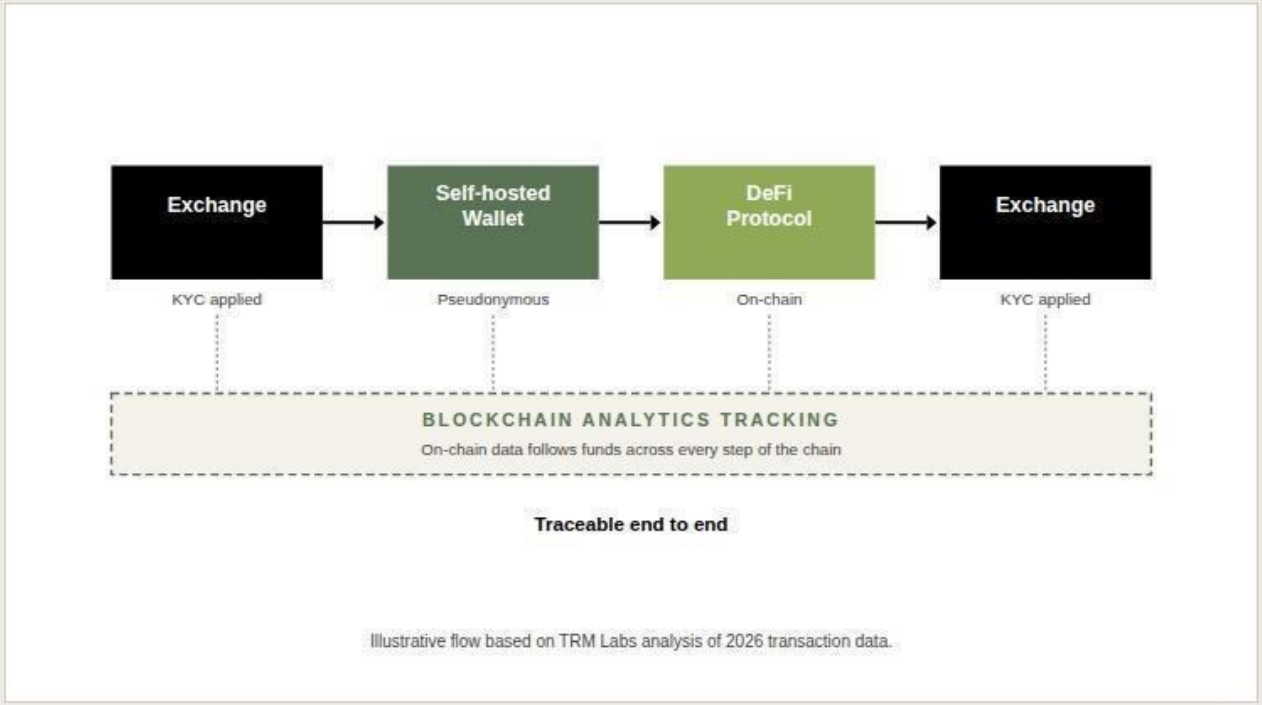
As a result, traceability is maintained through on-chain and off-chain attribution, even as pseudonymity exists within the system. Where funds originate from a regulated exchange, or are later sent to one, blockchain activity can be linked to identifiable persons or entities through customer due diligence, transaction records, and related evidential sources. The use of a self-hosted wallet does not sever the traceability of funds. It simply means that tracing depends on a combination of on-chain analysis and off-chain attribution, rather than on account records alone.TRM Labs data confirms this: 37.7% of transaction volume involved regulated VASPs, creating identifiable points at which blockchain activity intersects with compliance controls.

This traceability persists even without direct exchange interaction.. A substantial share of activity involves transfers between regulated VASPs, self-hosted wallets, and on-chain services such as DeFi protocols, creating identifiable points at which blockchain activity intersects with customer due diligence and other



End to End Traceability Across the Transaction Chain

Self-hosted wallets do not sever the traceability of funds. Each step, whether regulated or on-chain, leaves an auditable record.



Key finding. A typical user journey moves funds from a regulated exchange, to a self-hosted wallet, through a DeFi protocol, and back to an exchange. TRM Labs data shows 37.7% of total volume flows to or from regulated VASPs, giving analytics firms clear attribution points at both ends of the chain. Every on-chain step in between is recorded on a public ledger and remains visible to blockchain analytics tools.

Data. TRM Labs, provided to GDF (2026). 318,630 unhosted wallet addresses across Bitcoin, Litecoin, Ethereum, Polygon, and Tron.

compliance controls. Rather than existing outside observable financial infrastructure, self-hosted wallets frequently operate within transaction chains that remain visible to blockchain analytics tools, such as TRM Labs, and capable of retrospective attribution. Even in scenarios where transactions do not directly involve a regulated exchange, traceability remains a core feature of public blockchain systems. For example, funds move between multiple self-hosted wallets or through decentralized applications, but each transfer is still recorded on the public ledger. This creates a continuous and transparent transaction history that can be analyzed step by step. Blockchain analytics tools are well equipped to follow these flows across multiple transactions, identify consistent behavioural patterns, and group together addresses that are likely controlled by the same user.

While an immediate link to a verified identity does not always exist, attribution can develop over time through interactions with identifiable services such as merchants, payment processors, or token issuers, as well as through established investigative techniques that combine on-chain and off-chain data. In practice, this means that the absence of a regulated exchange in a transaction path does not necessarily reduce the inherent transparency of the system. Rather, it highlights the strength of blockchain-based traceability, where transaction histories remain accessible,

analyzable, and capable of supporting effective oversight through a combination of technological tools and investigative methods.

In many important aspects, public blockchains provide stronger traceability than cash. A cash transaction leaves no inherent transactional record once value changes hands. By contrast, a blockchain transfer generates a permanent record that cannot be altered or deleted after confirmation. That feature does not make all transactions immediately attributable to a named individual, as indicated in the examples above, but it does mean that flows can be followed across time and across addresses in a way that is not possible with physical cash. The use of self-hosted wallets does not change that structural feature of the underlying ledger.

While certain privacy-enhancing technologies can introduce additional complexity, it is important to distinguish them from self-hosted wallets, which are neutral tools for holding and transferring assets. Technologies such as mixers, privacy-focused assets, or cross-chain “chain-hopping” raise distinct considerations where they are designed to enhance privacy or obscure provenance – such as by protecting users from broadcasting their wealth on transparent ledgers or enabling anonymous charitable donations. These mechanisms raise distinct policy and supervisory considerations that are separate from the use of self-custody wallets themselves. A self-hosted wallet is a neutral tool for holding and transferring assets, whereas privacy-enhancing services or assets can potentially introduce additional risk factors depending on their design and use.

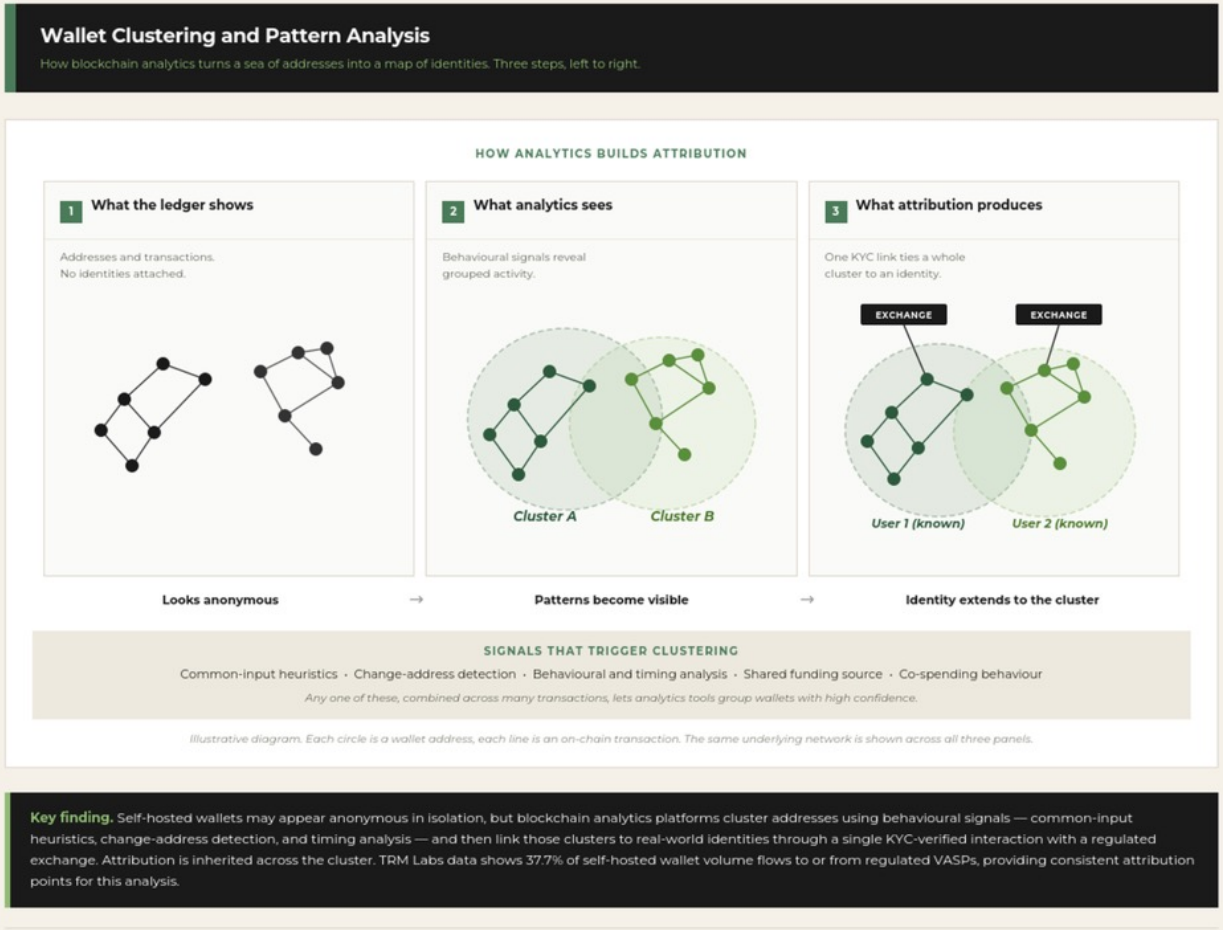
Blockchain analytics is now a standard part of compliance and enforcement precisely because public ledger data can be examined systematically. Analytics tools can trace the movement of funds from one address to another across multiple transaction hops, cluster addresses that are likely controlled by the same person or entity, and identify interactions with known services such as regulated exchanges, darknet markets, sanctions-designated addresses, ransomware wallets, gambling sites, mixers, or fraud-linked infrastructure.This also includes scenarios where threat actors use self-hosted wallets.

They can also flag transactional patterns that indicate layering or other higher-risk behavior, such as rapid movement through multiple newly created wallets, splitting funds into repeated smaller transfers, chain-hopping between different assets or networks, or repeated use of intermediary services designed to obscure provenance. Where one point in that transaction chain can be linked to a real-world identity, for example through exchange KYC records, account registration data, merchant records, device seizures, or other investigative material, the surrounding wallet activity can often be analyzed in context and connected to a broader pattern of conduct.

Blockchain analytics therefore supports not only the tracing of value flows, but also the identification of counterparties, service usage, and risk exposure across a transaction network. The relevant point is not that every transaction is immediately self-identifying, but that public blockchain activity is highly amenable to tracing, clustering, and retrospective investigation.

The effectiveness of blockchain analytics derives not from any single transaction revealing a user’s identity in isolation, but from the ability to analyze transaction behavior across an entire network over time. Repeated transaction patterns, shared funding sources, common withdrawal timings, reused addresses, and interactions with identifiable services can allow analytics providers





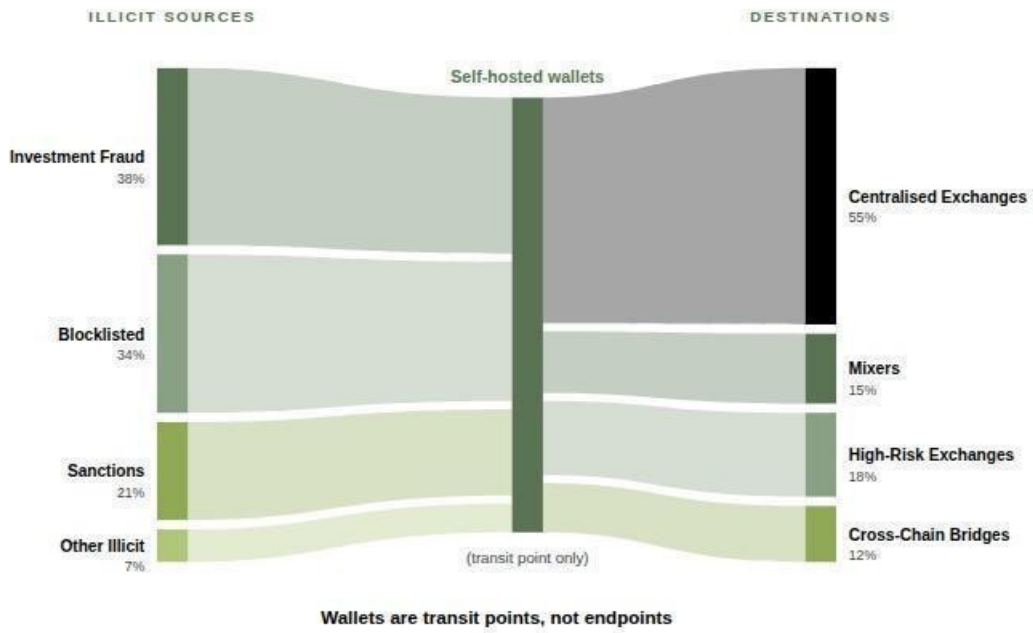
and investigators to group wallet addresses into behavioral clusters and attribute those clusters to particular users or entities with increasing confidence. Where one point in that transaction chain becomes linked to a verified identity — for example through exchange KYC records or other investigative material — that attribution can often extend across a broader network of related wallet activity.

A more accurate framing is therefore that public blockchains generally provide pseudonymity rather than anonymity. That privacy is contextual and depends on whether a wallet address can be linked to a real-world identity, whether through a regulated exchange, a payment interaction, consistent transaction behavior, or other evidential connections. Once such a link is established, the historical activity associated with that address becomes visible in a way that is often more comprehensive and granular than many traditional payment mechanisms.

The claim that self-hosted wallets enable anonymous, untraceable transactions therefore overstates the privacy they provide and understates the transparency of the blockchain systems on which they operate. A more accurate conclusion is that self-hosted wallets provide users with a degree of pseudonymous control over assets, but they do not remove the ability to trace transactions, analyze patterns, or build evidential links between on-chain activity and real-world actors.

Flow of Illicit Funds. Wallets as Transit, Not Endpoint

Illicit funds rarely remain in self-hosted wallets. They are eventually moved to services that provide liquidity, conversion, or fiat access, where compliance controls apply.



Illustrative Sankey flow. Thickness represents relative volume. Source and destination proportions based on TRM Labs illicit exposure data and FATF reporting on centralised off-ramp concentration.

Key finding. The majority of illicit funds flowing through self-hosted wallets eventually reach centralised exchanges, where KYC and AML controls apply. TRM Labs data shows illicit exposure accounts for just 1% of total self-hosted wallet volume, and the remaining transit activity terminates at regulated touchpoints where enforcement is operationally effective.

Data. TRM Labs, provided to GDF (2026). 318,630 unhosted wallet addresses across Bitcoin, Litecoin, Ethereum, Polygon, and Tron.

MYTH 3: ILLICIT ACTIVITY IS CONCENTRATED IN PRIVATELY CONTROLLED ACCOUNTS RATHER THAN REGULATED PLATFORMS

Another frequently expressed concern is that self-hosted wallets represent the primary locus of illicit financial activity in the digital asset ecosystem. In reality, illicit activity is concentrated not at the level of self-custody but at the points where value is converted and intermediated, which is where it can most effectively be detected and disrupted.

This reflects what wallets actually do. Self-hosted wallets are tools for storing assets and moving value; they are not, in themselves, the points where funds are converted between cryptoassets and fiat currency, where illicit activity is organised, or where AML/CFT controls can be applied. Effective financial crime controls are generally exercised at points of conversion and intermediation, where customer relationships exist, transactions can be monitored, and regulatory obligations can be enforced. For this reason, the most significant opportunities for detecting and disrupting illicit finance typically arise at regulated on-ramps, off-ramps, and other identifiable service providers, rather than at the level of self-custody itself.

Self-hosted wallets are only one component of a broader transaction chain. They are used to store assets, transfer value, or access on-chain services, but

their presence in a flow does not, on its own, indicate where criminal activity is being organized, where value is being converted, or where controls can most effectively be applied.

That distinction is critical because illicit funds typically do not remain indefinitely in self-hosted wallets. In many cases, they are eventually moved to a service that provides liquidity, asset conversion, trading, or access to fiat currency. The most significant illicit-finance risk arises where these funds are routed to non-compliant exchanges and other intermediaries that operate with weak or non-existent AML controls and are unresponsive to law enforcement requests. By contrast, compliant, regulated exchanges serve as critical chokepoints where existing KYC, AML, and sanctions controls are highly effective at detecting and disrupting illicit flows. Effective regulatory and enforcement focus should be directed at non-compliant intermediaries that serve as the principal off-ramps for illicit funds Innovative existing public-private disruption networks within the cryptocurrency industry are accelerating outcomes in this area.

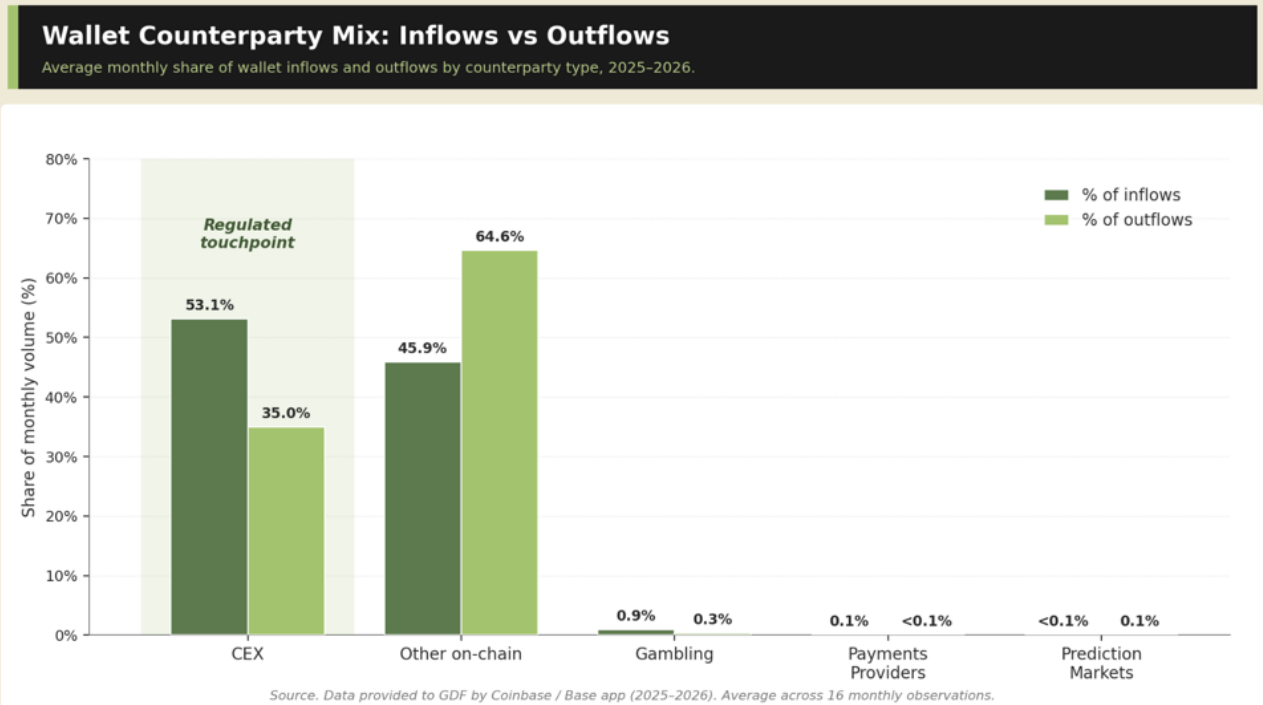
Beacon Network is a real-time intelligence-sharing system that helps law enforcement, crypto exchanges, DeFi services, and stablecoin issuers stop illicit funds before they are withdrawn. Built by TRM Labs in collaboration with leading industry players, this crypto crime response network enables verified investigators to flag addresses linked to financial crime, immediately alerting exchanges and triggering risk-based responses.

Since its inception in August 2025, millions of dollars in illicit funds have been blocked from off-ramping, including a law enforcement agency that traced funds linked to a global scam. Through Beacon Network, they alerted exchanges in time to help freeze $1.5 million in real time before it could be withdrawn. In another case, a global exchange flagged scammer wallets after an impersonation attack. When funds reached a prepaid crypto card service, the withdrawals were blocked and linked devices were blocklisted.

T3 Financial Crime Unit is a first-of-its-kind public-private initiative launched by TRON, Tether, and TRM Labs in September 2024 to combat illicit activities on the blockchain. This groundbreaking public-private partnership works directly with law enforcement agencies worldwide to identify and disrupt criminal networks. Since its inception, T3 FCU has frozen over $250 million in criminal assets held in self-hosted wallets across five continents, established rapid response capabilities to address threats, and demonstrated how industry collaboration can effectively combat financial crime while supporting blockchain innovation.

When conducting an analysis of illicit activity, it is more accurate to focus on transaction flows than on wallet type alone. The key question is not whether a self-hosted wallet appears somewhere in the chain. The key question is where funds are being sent, how they are being moved, and which services are being used along the way. For example, illicit risk becomes more meaningful where funds move to a mixer, a sanctioned service, a darknet-linked address, a high-risk exchange, or a cross-chain bridge used to obscure provenance. Those touchpoints will likely be more informative and also can lead to more effective prevention and risk mitigation measures, than a binary focus on self-custody wallets vs custodial wallets.



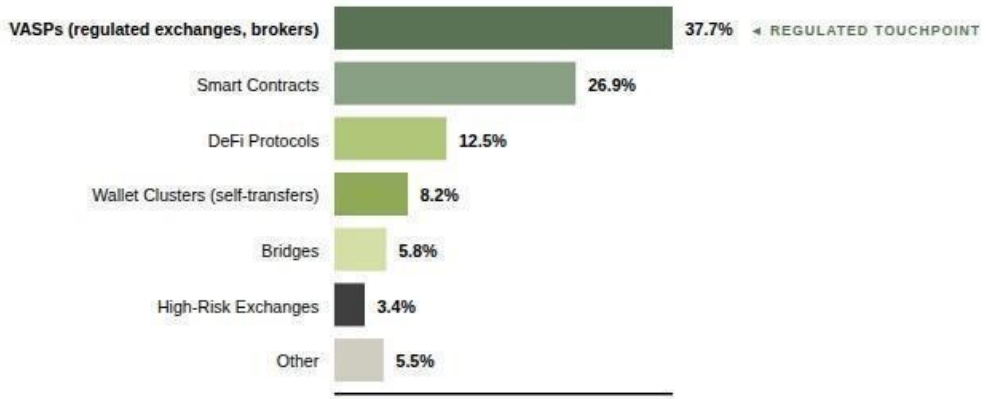


Key finding.
Centralised exchanges are the single largest counterparty category for self-hosted wallet activity: 53% of inflow volume and 35% of outflow volume passes through regulated CEXs where KYC, AML and sanctions screening apply. Higher-risk categories (gambling, prediction markets) account for under 1.5% combined. Compliance controls already engage at the points where wallets meet the regulated system.

this point directly. Coinbase/Base App data shows that 53.1% of wallet inflow volume and 35% of outflow volume passed through regulated centralized exchanges (CEXs), demonstrating that a substantial proportion of self-hosted wallet activity already intersects with KYC, AML, and sanctions-screening controls. By contrast, categories frequently associated with elevated risk represented only a very small share of observed activity: gambling-related counterparties accounted for 0.9% of inflows and 0.3% of outflows, while payment providers and prediction markets each represented approximately 0.1% or less. The data suggests that regulated exchanges remain the dominant touchpoints within self-hosted wallet transaction flows and that higher-risk counterparties constitute only a marginal proportion of overall activity.

Destination of Self-Hosted Wallet Outflows

The largest single destination for self-hosted wallet volume is regulated VASPs. Funds re-enter the regulated system, where compliance applies.



Source. TRM Labs, 2026. Percentages reflect total transaction volume at analysed addresses. Categories may overlap.

Key finding. The largest single destination category for self-hosted wallet outflows is regulated VASPs at 37.7%, where KYC, AML, and sanctions screening apply. Combined with smart contracts (26.9%) and DeFi protocols (12.5%), most wallet activity resolves at on-chain infrastructure or regulated exchanges, not at untraceable endpoints.

Data. TRM Labs, provided to GDF (2026). 318,630 unhosted wallet addresses across Bitcoin, Litecoin, Ethereum, Polygon, and Tron.

The broader destination profile of wallet outflows further reinforces this conclusion. TRM Labs data shows that the single largest destination category for self-hosted wallet outflows was regulated VASPs at 37.7% of total volume. Significant additional activity involved smart contracts (26.9%) and DeFi protocols (12.5%), reflecting the role of self-hosted wallets within broader on-chain financial infrastructure rather than as isolated endpoints for illicit activity. By contrast, flows to high-risk exchanges represented only 3.4% of observed volume. These patterns suggest that most self-hosted wallet activity ultimately resolves either through regulated exchanges or through transparent on-chain infrastructure rather than through inherently opaque or illicit destinations.

The destination data supports a more targeted understanding of risk. The critical compliance question is not whether self-hosted wallets are used within a transaction chain, but where funds ultimately move, where liquidity is accessed, and where conversion into fiat or other assets occurs. Those points remain concentrated around regulated exchanges, identifiable services, and observable on-chain infrastructure.

Recent patterns in illicit finance also support this more targeted view. A significant share of illicit activity in 2024 and 2025 involved stablecoin flows and sanctioned actors leveraging centralized infrastructure, including exchanges and other virtual asset service providers, according to the Financial Action Task Force.[23] More

[23] Financial Action Task Force (FATF), *Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs* (2024).: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html

broadly, centralized exchanges continue to be a major destination for funds sent from illicit addresses. This indicates that the main compliance and enforcement points are already well established at regulated on- and off-ramps, rather than at the level of self-custody itself.

The more accurate conclusion is that illicit activity is not concentrated in self-hosted wallets as such. Self-hosted wallets form part of a transaction chain, but the more meaningful points for risk assessment are the services, destinations, and behavioral patterns associated with the movement and monetization of illicit funds. Regulation and risk mitigation should instead focus on how funds flow through the ecosystem, rather than assuming that self-custody wallets are the primary locus of crime.

MYTH 4: RESTRICTING OR BANNING SELF-CUSTODY WALLETS IS THE APPROPRIATE REGULATORY RESPONSE

Building on the previous myths, it is frequently claimed that given the risks associated with unhosted wallets, regulators should restrict or prohibit self-custody to ensure that all digital asset activity occurs within the supervised perimeter. That proposition conflates the private holding of digital assets with higher-risk transactional behavior, treating the private holding of digital assets as inherently suspect, rather than as a neutral form of possession that is functionally analogous to long-established practices in traditional finance.

Self-custody is not a new activity in substance. Individuals have always been able to hold value directly, whether in the form of cash, physical assets, or funds stored outside of an intermediary. A self-hosted wallet performs the same function in a digital context. It is a mechanism for control and storage, not in itself, a means of evasion. The existence of that capability, on its own, does not necessarily create elevated risk, any more than holding cash or storing valuables privately does. As noted above, the continued traceability of self-custodied assets creates greater transparency than these analogue alternatives. Risk is more appropriately assessed and contained at the touch points with the wider financial system, including through risk-sensitive controls applied by centralized intermediaries that provide liquidity, conversion, or settlement services.

This distinction is reflected in how financial regulation has historically been structured, focused on intermediaries not the act of holding. Compliance obligations attach to entities like banks, payment providers, and exchanges because those are the points at which transactions can be monitored, identities can be verified, and controls can be applied at scale. The act of holding value privately has not in itself been subject to prior authorization or blanket reporting requirements.

Extending such requirements to self-hosted wallets would represent a significant departure from this approach, effectively treating the digital equivalent of holding cash as a risk by default. Most importantly - with only 1% of total transaction volume at analyzed addresses involved direct exposure to illicit-categorized counterparties, it would unfairly and imprecisely penalize the 99% of transactions which are legitimate.

Policymakers have already recognized that an evidence-led approach is unlikely to justify blanket ascriptions of risk to entire custody models or technologies As discussed throughout this report, UK HM Treasury concluded in 2022 that self-custody wallet transactions should not automatically be treated as higher risk and that there was not good evidence that self-custody wallets present a disproportionate risk of being used in illicit finance.[24] A similar direction for regulatory oversight can be observed in the United States, where recent policy discussions and legislative proposals have increasingly recognized self-custody as a legitimate exercise of individual control over digital assets, rather than treating it as inherently high risk. This includes a move away from earlier proposals that would have imposed broad data collection requirements on self-custody transactions, toward a more measured and risk-based framing of user-controlled wallets within the financial system. That assessment is directly relevant because it addresses

[24] HM Treasury, *Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017: Response to the Consultation* (June 2022), p 29. https://www.gov.uk/government/consultations/amendments-to-the-money-laundering-terrorist-financing-and-transfer-of-funds-information-on-the-payer-regulations-2017-statutory-instrument-2022



the central premise behind proposals for blanket restrictions. Where a technology does not, by its nature, generate disproportionate risk, a general prohibition or broad-based constraint is difficult to justify on a risk-based basis.

International standard-setting has also, so far, taken a targeted approach. FATF's work focuses on AML/CFT obligations for VASPs and other relevant intermediaries, alongside supervisory tools such as transaction monitoring, information sharing, and asset freezing.[25] These measures are directed at points in the system where controls are operationally effective, rather than restricting the underlying ability of users to hold assets in self-custody.

There are also practical limitations to a prohibitive approach to neutral infrastructure. Self-hosted wallets are software-based tools that can be created and used without reliance on a central provider. As a result, restrictions that extend beyond regulated entities are inherently difficult to enforce in a consistent manner. Measures that are overly broad have limited effectiveness, while creating incentives for activity to move towards less visible or less regulated channels. That outcome would not strengthen oversight and in some cases, reduce it.

Self-custody also serves legitimate privacy and autonomy interests beyond financial management. For users in jurisdictions with weak rule of law, political instability, or authoritarian governance, self-custody provides a means of protecting assets from arbitrary seizure or politically motivated account closures. International human rights organizations have documented cases in which financial access has been weaponized against dissidents, journalists, and civil society groups. In such contexts, the ability to hold assets independently of any institution is a fundamental safeguard. A proportionate policy framework should account for these legitimate uses.

The more appropriate framing is not whether self-custody should be permitted, but how risk should be managed where self-hosted wallets interact with the regulated financial system. It is at those interaction points, exchanges, brokers, payment providers, and other service intermediaries, that customer onboarding and due diligence, transaction monitoring, sanctions screening, and reporting obligations can be applied in a proportionate and effective way.

Restricting or banning self-hosted wallets does not represent a proportionate response to financial crime risk. A risk-based approach is better served by focusing on transactional behavior and on the regulated touchpoints through which funds enter, exit, and move within the financial system, rather than on the mere fact that a user holds assets directly. ■

[25] FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*(2025): https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf

9. REGULATORY TREATMENT AND THE EXISTING COMPLIANCE ARCHITECTURE

Self-custody does not create a regulatory vacuum. Digital assets held in unhosted wallets interact with the regulated financial system at multiple points, each subject to existing compliance obligations. This section maps the layered architecture of controls that currently applies and sets out how it controls for risks appropriately.

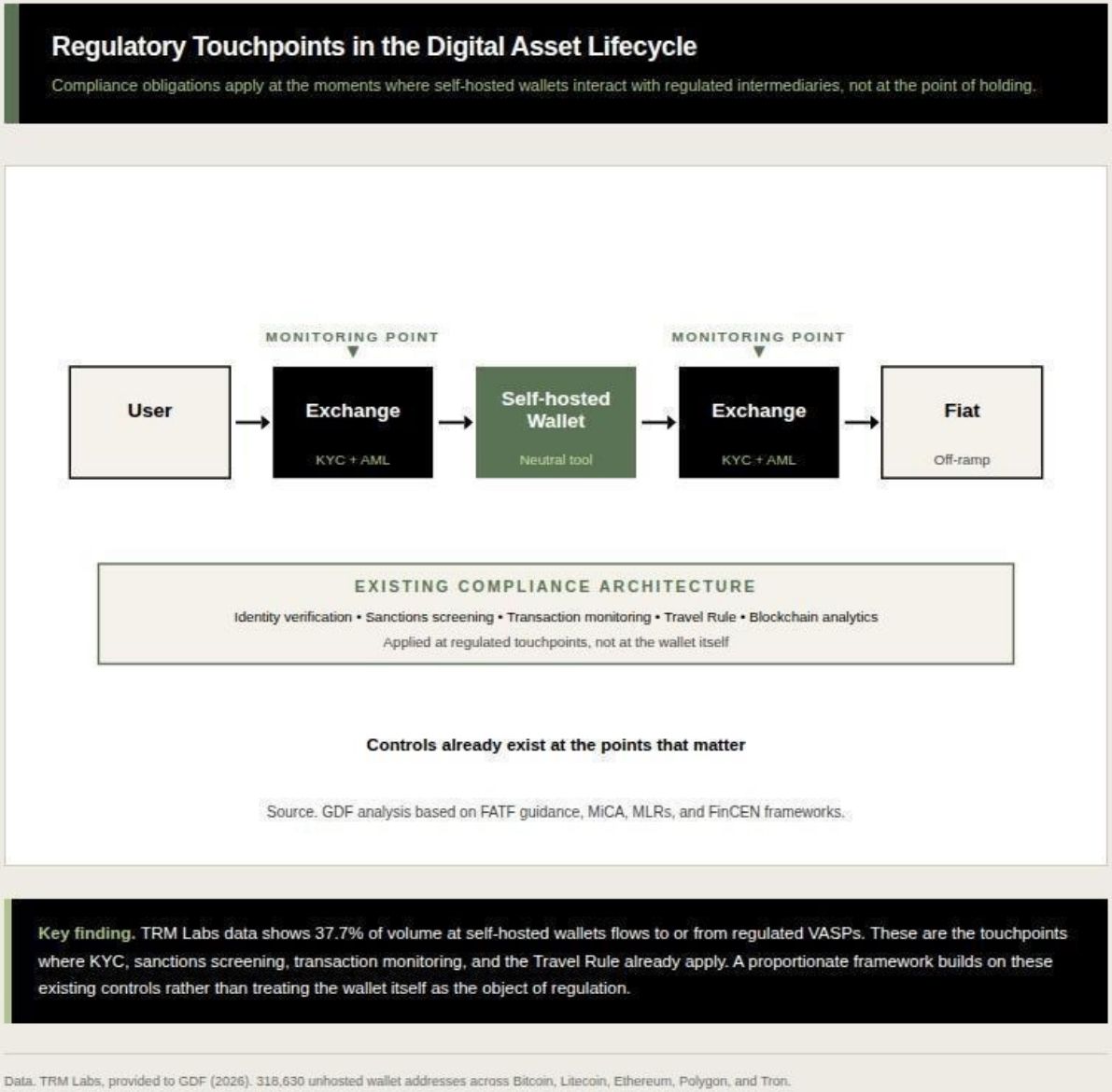


KEY TAKEAWAYS

- A layered compliance architecture already applies to self-custody wallet activity at every point it intersects with the regulated financial system: on- and off-ramp controls enforce customer due diligence, sanctions screening, and transaction monitoring at exchanges and payment providers, while the inherent transparency of public blockchains enables blockchain analytics firms to monitor flows, cluster addresses, and identify risk exposure independently of wallet holder cooperation.

- The UK data provides direct empirical validation of this architecture: UK-linked wallet addresses — operating under FATF-aligned FCA and MLR requirements — showed 42% VASP interaction versus 37.7% globally, illicit exposure of 0.1% versus 1% globally, and high-risk exposure of 1.7% versus 5.0% globally, demonstrating that effective AML/CFT controls at regulated touchpoints materially reduce risk without requiring restrictions on self-custody itself.

- Travel Rule obligations and tiered risk-based treatment further demonstrate that self-custody is neither beyond regulatory oversight nor inherently higher risk: obligations attach to the regulated intermediary and its customer relationship rather than to the wallet or its holder, and graduated controls — de minimis thresholds, enhanced due diligence triggers, and elevated-risk indicators — allow proportionate, evidence-led responses rather than blanket assumptions based on custody model alone.



ON AND OFF RAMP CONTROLS

The most significant compliance touchpoints occur when value moves between self-custody and the regulated financial system.

Where users convert fiat into digital assets, redeem digital assets into fiat, or access trading and brokerage services through regulated firms, they are already subject to customer due diligence, sanctions screening, and ongoing AML/CFT monitoring. In practical terms, activity involving self-hosted wallets does not fall outside the compliance framework when it intersects with an exchange, broker, custodian, payment provider, or issuer that is already within the regulatory perimeter. AML/CFT obligations are most appropriately applied at those intermediated points of contact and to identifiable service providers, rather than to self-custodial activity in itself.

These chokepoints are structurally unavoidable for any user seeking to convert between digital assets and fiat currency. A user can hold assets in self-custody indefinitely, but acquiring those assets with fiat currency or liquidating them back to fiat requires interaction with a regulated intermediary.

In this, self-custody is an evolution of cash for a digital age, and regulation so far has drawn such a parallel. An individual can hold cash without being subject to customer due diligence merely by possessing it.

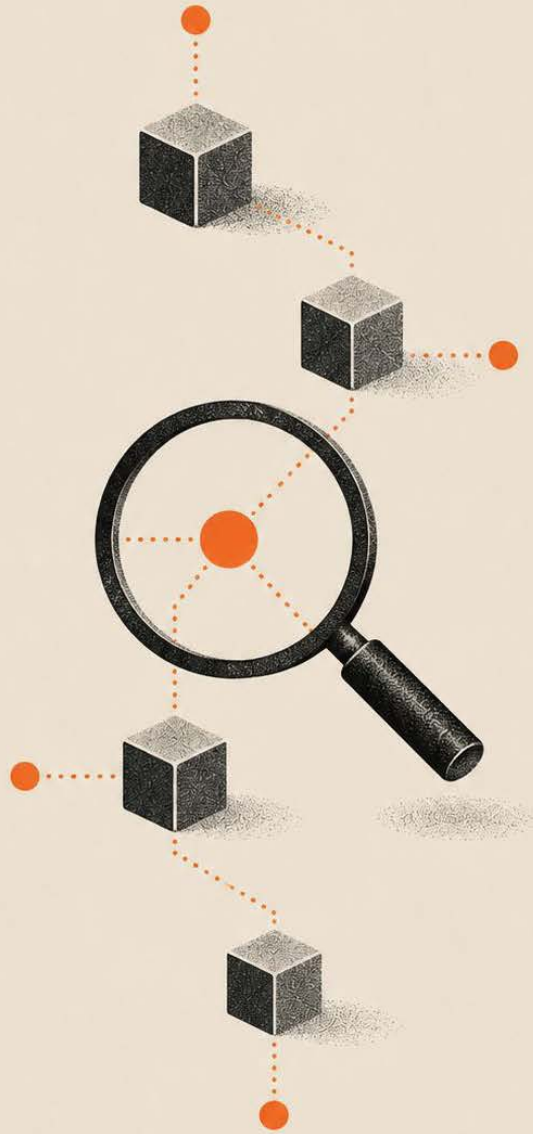
Cash is not regulated at the point of holding but at the point of use. When that cash is deposited into a bank account, used to purchase a high-value good, or transferred through a money service business, compliance obligations arise: identity verification, record-keeping, transaction monitoring, and reporting where required. The regulatory framework does not treat the act of holding cash as inherently suspicious. It focuses on the moments where cash enters or moves through the regulated financial system.

The same principle applies to self-custody wallets. A user can create a wallet and hold digital assets without triggering compliance obligations at the point of possession, because the wallet is a tool for holding and transferring digital assets, not an account-based financial service. Compliance obligations arise when that wallet is used to interact with the broader financial system; when that user acquires digital assets through a regulated exchange, converts them into fiat currency, redeems stablecoins through a regulated issuer, or transacts through a regulated platform, the intermediary applies onboarding checks, identity verification, sanctions screening, and transaction monitoring in accordance with its legal obligations.

BLOCKCHAIN ANALYTICS AND TRANSACTION MONITORING

As discussed, public blockchain infrastructure provides a second layer of control through its inherent transparency. The TRM Labs data provides direct evidence that this compliance architecture is effective. In the UK, where FATF aligned AML/CFT requirements have been fully implemented at exchange level, self-custody wallet activity shows measurably lower risk than the global sample.

The UK subset of the dataset illustrates this relationship particularly clearly. Compared with the global sample, UK-linked self-hosted wallet activity showed higher interaction with regulated VASPs and substantially lower exposure to illicit and higher-risk counterparties. This is significant because the UK has implemented FATF-aligned controls at the exchange and intermediary level, including customer due diligence, transaction monitoring, sanctions screening, and Travel Rule obligations. The observed reduction in illicit exposure is consistent with the view that compliance controls are most effective when applied at regulated on- and off-ramps where blockchain activity intersects with identifiable customer relationships.



Regulatory Implementation and Observed Risk. The UK Evidence

Where FATF aligned regulation has been implemented at exchange level, self-custody wallet activity shows measurably lower risk. The compliance architecture is already working.

UK REGULATORY FRAMEWORK

FATF aligned controls at exchange level

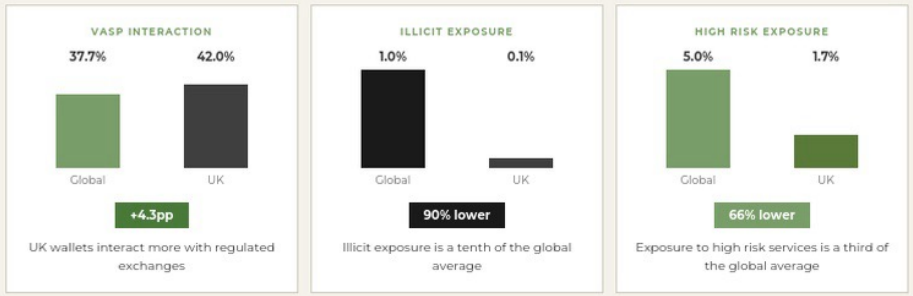
FCA registration for crypto asset businesses
Money Laundering Regulations (MLRs) applied to VASPs
Customer due diligence at onboarding
Transaction monitoring and sanctions screening
Travel Rule obligations on qualifying transfers

THE POLICY QUESTION

If the existing compliance architecture at regulated touchpoints is effective, then self-custody wallets operating in jurisdictions with strong VASP regulation should show **higher interaction with regulated platforms** and **lower illicit exposure** than the global average.

The TRM Labs data allows us to test this directly by comparing UK linked addresses against the whole sample.

WHAT THE DATA SHOWS



THE LOGIC

FATF aligned regulation
KYC, AML, sanctions screening applied at UK exchanges

→

Stronger VASP interaction
UK wallets use regulated on and off ramps more frequently

→

Lower observed risk
Illicit exposure 90% lower than global average

The compliance architecture is already reducing risk at the points that matter.

Restricting the wallet itself is unnecessary when the regulated touchpoints are demonstrably effective.

Source. TRM Labs, 2026. UK linked subset. Around 5,000 addresses, $83.6m volume. Whole sample. Over 300,000 addresses, $40.6B volume.

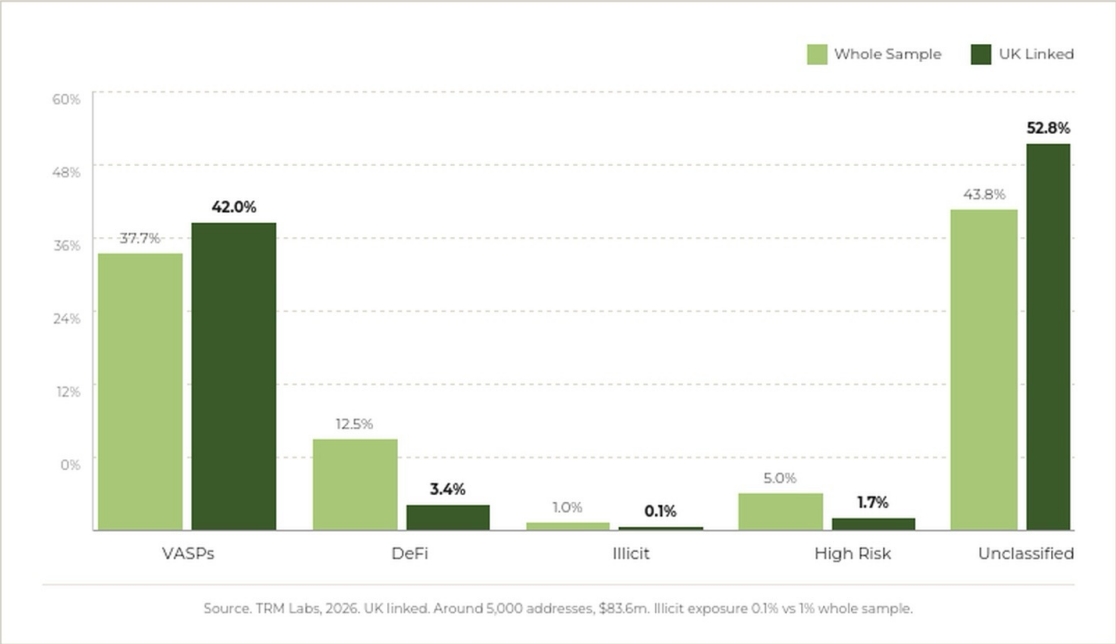
Key finding. In the UK, where FATF aligned AML/CFT requirements have been implemented at exchange level, self-custody wallet activity shows 42% VASP interaction (vs 37.7% globally), 0.1% illicit exposure (vs 1.0%), and 1.7% high risk exposure (vs 5.0%). This pattern is consistent with the conclusion that existing regulatory controls at on and off ramps are already effective at reducing risk. A proportionate framework should build on these demonstrated touchpoints rather than imposing additional restrictions on the wallet itself.

Data. TRM Labs, provided to GDF (2026). UK linked addresses identified via counterparty interaction with UK registered VASPs. Regulatory framework. FCA, MLRs, FATF Recommendations as implemented in the UK.

The comparative data reinforces the broader regulatory logic underlying FATF-aligned implementation. UK linked addresses showed higher interaction with regulated VASPs (42% versus 37.7% globally), while illicit exposure fell to 0.1% compared with 1% across the wider sample. Exposure to higher-risk counterparties was also substantially lower (1.7% versus 5.0%). These patterns are consistent with the conclusion that effective AML/CFT controls at regulated exchanges and intermediary touchpoints can materially reduce risk without requiring blanket restrictions on self-custody wallets themselves.

UK Linked Subset. Comparative Analysis

Around 5,000 UK linked addresses ($83.6m volume) vs. whole sample (over 300,000 addresses, $40.6B).



Source. TRM Labs, 2026. UK linked. Around 5,000 addresses, $83.6m. Illicit exposure 0.1% vs 1% whole sample.

Key finding. UK linked addresses show higher VASP interaction (42% vs. 37.7%), reflecting closer integration with regulated platforms, and significantly lower illicit exposure (0.1% vs. 1%).

COUNTERPARTY TYPE	WHOLE SAMPLE	UK LINKED	DIFFERENCE
VASPs	37.7%	**42.0%**	**+4.3pp**
DeFi	12.5%	**3.4%**	**-9.1pp**
Illicit	1.0%	**0.1%**	**-0.9pp**
High Risk	5.0%	**1.7%**	**-3.3pp**
Unclassified	43.8%	**52.8%**	**+9.0pp**

Data. TRM Labs, provided to GDF (2026). Over 300,000 unhosted wallet addresses across Bitcoin, Litecoin, Ethereum, Polygon, and Tron.

Where a regulated firm receives funds from, or sends funds to, a self-hosted wallet, it can assess the relevant address and transaction pattern using blockchain analytics tools. This enables firms to identify exposure to sanctioned wallets, darknet-linked services, mixers, fraud typologies, and other higher-risk counterparties, and to calibrate their response accordingly. Effective monitoring does not depend on the direct cooperation of the self-hosted wallet holder. Rather, it depends on the ability of regulated firms to assess risk at the point of interaction and to apply enhanced controls where the transaction profile warrants it.

For that reason, regulatory discussions increasingly focus on the risk characteristics of specific services, transaction patterns, and counterparties, rather than on self-custody wallets as a category. Where privacy-enhancing technologies are used, regulated firms can assess associated risk through blockchain analytics, transaction monitoring, and enhanced due diligence at points of interaction. This approach allows regulators and firms to address higher-risk behaviors directly, while preserving the neutral role of self-custody wallets within the broader ecosystem.

TRAVEL RULE

Travel Rule obligations demonstrate that self-hosted wallet interactions are not beyond regulatory oversight in the present system. FATF Recommendation 16 requires regulated virtual asset service providers to



collect, retain, and, where relevant, transmit originator and beneficiary information in relation to their own customers when processing qualifying transfers. In the context of transfers involving self-hosted wallets, the regulatory obligation remains anchored to the regulated firm and its customer relationship and on transaction-level risk indicators, rather than the affirmative collection of non-customer counterparty information (which raises significant privacy and data security concerns). FATF-aligned implementation should, however, remain proportionate and technically workable in the context of self-custody wallet interactions.

TIERED, RISK-BASED TREATMENT

The existing framework allows tiered and risk-sensitive treatment. Not all transfers involving self-hosted wallets present the same level of risk, and the direction of travel across jurisdictions has been toward proportionate controls rather than blanket assumptions. Mature regulatory frameworks apply graduated requirements based on transaction characteristics:

- **De minimis thresholds** below which simplified due diligence applies
- **Enhanced due diligence** for transactions above specified values or presenting risk indicators; and
- **Elevated-risk triggers** such as interaction with flagged addresses or patterns consistent with structuring.

Standards should reflect actual risk profiles and should not impose disproportionate burdens on low-value or low-risk retail transactions.

This logic applies with particular force in stablecoin markets. Stablecoin frameworks increasingly embed direct AML/CFT, sanctions, recordkeeping, and monitoring obligations at the issuer and intermediary level, including controls designed to detect prohibited activity and, where technically possible and legally appropriate, reject or freeze certain transactions. Robust baseline AML/CFT obligations should apply to issuers and other relevant intermediaries, but those obligations should be calibrated proportionately to the functions they actually perform and the entities they directly onboard or interact with.

Table 1: How Key Jurisdictions Treat Self-Custody Wallet Interactions

Jurisdiction	Approach to Self-Custody	Travel Rule Implementation	Key Regulatory Body
FATF Standards	No prohibition; AML/CFT obligations focused on VASPs; risk-based measures for unhosted wallet transfers	Recommendation 16: VASPs collect/retain/transmit originator and beneficiary information; obligation anchored to regulated firm	FATF (standard-setter)
European Union	Permitted; TFR extends traceability to crypto transfers including unhosted wallets	Verification of unhosted wallet ownership required above €1,000; full travel rule for VASP-to-VASP	EBA; national authorities; MiCA framework
United Kingdom	Permitted; HMT rejects automatic higher-risk classification	Risk-based: originator/beneficiary info collected for elevated-risk transactions only	FCA (registration and AML/CFT); OFSI (sanctions enforcement)
United States	Permitted; legislative trend (GENIUS Act, CLARITY Act) frames self-custody as legitimate; FinCEN 2020 rule withdrawn	BSA obligations on exchanges; no direct obligation on wallet holders	FinCEN; SEC; CFTC; state regulators
Singapore	Permitted; risk-based approach	VASPs apply risk-based measures for unhosted wallet transfers	Monetary Authority of Singapore

Together, these layers of control demonstrate that self-hosted wallets are neither beyond regulatory oversight nor inherently higher risk. While residual risks may arise in specific circumstances, the existing compliance architecture already provides multiple moments of supervision and control when self-hosted wallets interact with regulated parts of the financial system. Meaningful risk mitigation occurs at the points of onboarding, conversion, redemption, settlement, screening, monitoring, and reporting. ■

10. CONCLUSIONS & RECOMMENDATIONS

The evidence presented in this report supports a regulatory approach to self-custody that is proportionate, risk-based, and grounded in empirical data rather than assumption. Self-custody wallets are a foundational component of digital asset infrastructure. Frameworks that preserve their legitimate use while applying effective controls at regulated touchpoints offer the most promising path toward both financial innovation and financial integrity. This report has found that:

The evidence presented in this report supports a clear directional conclusion: self-custody wallets are neutral infrastructure whose risk profile is determined by how they are used, not by the fact of their existence. Effective oversight already operates at the points where self-custody intersects with the regulated financial system, such as on-ramps, off-ramps, and service intermediaries that exercise genuine control over customer relationships and transaction execution. Proportionate regulatory frameworks should build on these established compliance touchpoints, grounded in true intermediation and control, rather than treating self-hosted wallets themselves as the object of regulation.

Key Recommendations

1. **Adopt risk-based, evidence-informed approaches.** Regulatory frameworks should calibrate obligations to demonstrated risk rather than applying blanket restrictions to self-custody as a category. HM Treasury's 2022 conclusion that self-custody transactions should not automatically be viewed as higher risk remains well-supported by the data.

2. **Preserve the infrastructure-intermediary distinction.** Self-custody tools function as infrastructure (analogous to physical wallets or safes) rather than intermediaries. Regulatory obligations designed for intermediaries are poorly suited to non-custodial software and risk displacing activity to less observable channels.

3. **Anchor AML/CFT obligations at regulated touchpoints.** Compliance requirements should apply to intermediaries — exchanges, brokers, payment providers, and stablecoin issuers — rather than to self-custody wallet software or its users directly. This reflects established regulatory principles and practical enforceability.

4. **Reject automatic higher-risk classification of self-custody transactions.** Regulatory frameworks and supervisory guidance should not treat transfers to or from unhosted wallets as inherently elevated-risk. Risk assessment should be driven by transaction characteristics, counterparty exposure, and behavioral indicators not by custody model alone.

5. **Engage with technological evolution.** The binary distinction between "custodial" and "non-custodial" is giving way to a spectrum of hybrid arrangements. Regulatory frameworks should be sufficiently flexible to accommodate this evolution without requiring repeated legislative revision, focusing on the substance of activity and the location of control.

6. **Invest in blockchain analytics as a supervisory tool.** The inherent transparency of public blockchains provides investigative and monitoring capabilities that should be integrated into both firm-level compliance programs and regulatory supervisory practice.

7. **Coordinate internationally to avoid fragmentation.** Divergent approaches across jurisdictions — from the EU's Transfer of Funds Regulation to US legislative carve-outs — risk regulatory arbitrage and compliance complexity. Continued multilateral engagement through FATF and other standard-setting bodies remains essential.

8. **Commission further empirical research.** The evidence base would benefit from longitudinal studies tracking wallet cohorts over time, comparative analysis across additional jurisdictions, and continued investment in address attribution to reduce the large unclassified category. ■



APPENDICES

Primary Sources:

Appendix A: TRM Labs Data Methodology

Population: over 300,000 addresses identified as unhosted wallets through TRM Labs' proprietary methodology for detecting addresses exhibiting behaviours consistent with unhosted wallet activity, across Bitcoin, Litecoin, Ethereum, Polygon, and Tron.

Filters applied: Lifetime volume $50–$10,000,000 (incoming + outgoing USD); lifetime transactions 5–5,000; at least one transfer of greater than $10 in 2026. The volume and transaction thresholds reduce the likelihood of including single-use addresses and spam transactions (lower bound) and unidentified custodial services such as VASPs (upper bound). The 2026 activity requirement ensures currency of the data.

UK-Linked Subset: about 5,000 addresses identified from the total sample based on direct 2026 transaction exposure to Coinbase, Kraken, or Revolut (the three largest assessed VASPs by UK user base per TRM's analysis), combined with zero transactions between 00:00–05:59 UTC over the preceding three-year period. This methodology provides an increased likelihood, but not certainty, of UK-based operation, as no comprehensive deterministic method exists for geo-locating unhosted wallets.

Appendix B: Coinbase Data Methodology

Population: 1.95M wallets that have transacted at least once in legacy Coinbase Wallet and/or Base App since January 2025 across Base, Ethereum, Arbitrum, Optimism, BSC, Polygon and Avalanche.

Filters: We analysed token send transactions that were initiated using the Coinbase Wallet and/or Base App user interface and token inflows received by wallets that had transacted in the app at least once.

Secondary Sources

Appendix C:

1. Bank for International Settlements, *Cryptocurrencies and Decentralised Finance: Functions and Financial Stability Implications*, BIS Papers No. 156, 2025; World Economic Forum, Decentralized Finance (DeFi) Policy-Maker Toolkit, 2021: https://www.bis.org/publ/bppdf/bispap156.pdf & International Monetary Fund, "The Crypto Ecosystem and Financial Stability Challenges," Global Financial Stability Report, 2023.: https://www.elibrary.imf.org/downloadpdf/display/book/9781513595603/ch002.pdf

2. Bains, Parma, Arif Ismail, Fabiana Melo, and Nobuyasu Sugimoto. "Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets." FinTech Notes 2022, no. 007 (September 26, 2022).:https://www.imf.org/en/publications/fintech-notes/issues/2022/09/26/regulating-the-crypto-ecosystem-the-case-of-unbacked-crypto-assets-523715

3. Financial Conduct Authority, *Cryptoassets Consumer Research 2023 (Wave 4)*, 2023; Bank of England, *Financial Stability Report*, 2023: .https://www.fca.org.uk/publication/research-notes/research-note-cryptoasset-consumer-research-2023-wave4.pdf & U.S. Department of the Treasury, Illicit Finance Risk Assessment of Decentralized Finance, 2023; Financial Crimes Enforcement Network, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," Notice of Proposed Rulemaking: https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf

4. Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (FATF, 2021): https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html?utm_source=chatgpt.com

5. Financial Conduct Authority, *Cryptoassets Consumer Research 2023 (Wave 4), 202 ; Bank of England, Financial Stability Report*, 2023.: .https://www.fca.org.uk/publication/research-notes/research-note-cryptoasset-consumer-research-2023-wave4.pdf

6. TRM Labs, 2024 Crypto Adoption and Illicit Exposure Report, 20244: https://www.trmlabs.com/reports-and-whitepapers/2024-crypto-adoption-and-illicit-exposure-report & International Monetary Fund and Financial Stability Board, *IMF-FSB Synthesis Paper: Policies for Crypto-Assets*(September 2023). https://www.fsb.org/2023/09/imf-fsb-synthesis-paper-policies-for-crypto-assets/

7. Kraken, Custodial vs Non-Custodial Wallets; Gemini, Crypto Wallets: Custodial vs Non-Custodial.: https://www.kraken.com/learn/custodial-non-custodial-crypto-wallet

8. Kraken, Custodial vs Non-Custodial Wallets; Coinbase, Custodial and Non-Custodial Wallets.: https://www.kraken.com/learn/custodial-non-custodial-crypto-wallet

9. Binance Academy, Custodial vs Non-Custodial Wallets; Trust Wallet, Web3 and Self-Custody Wallets.: https://www.binance.com/en/academy/articles/what-are-web3-wallets

10. CoinTracker, *Custodial vs Non-Custodial Wallets; Cobo, Custodial vs Non-Custodial Wallet Explained*.: https://www.cointracker.io/blog/custodial-vs-non-custodial-wallets

11. FATF, Targeted Report on Stablecoins and Unhosted Wallets (2026).: https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf

12. FATF, ***Virtual Assets and Virtual Asset Service Providers: Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs*** (2021): https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

13. FATF, Updated Guidance for a Risk-Based Approach to VA and VASPs (2021).: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

14. World Bank, Remittances (updated 18 September 2024).: https://www.worldbank.org/en/topic/migration/brief/remittances-knomad

15. FATF, Targeted Report on Stablecoins and Unhosted Wallets (2026).: https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf

16. FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs (2024/2025 updates).: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf

17. World Bank, ***Remittances Slowed in 2023, Expected to Grow Faster in 2024*** (26 June 2024).: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099714008132436612

18. TRM Labs, ***2026 Crypto Crime Report*** (2026): :https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report

19. BIS, Annual Economic Report 2025, Chapter III: "The next-generation monetary and financial system." : https://www.bis.org/publ/arpdf/ar2025e3.pdf

20. BIS, Annual Economic Report 2025.: https://www.bis.org/publ/arpdf/ar2025e.htm

21. TRM Labs, data provided to GDF for this report (2026). Analysis of 318,630 unhosted wallet addresses across five blockchains. See Appendix [X] for full methodology

22. HM Treasury, Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017: Response to the Consultation (June 2022).: https://assets.publishing.service.gov.uk/media/62aaf6148fa8f503af595b33/MLRs_SI_2022_-_Consultation_Response_final.pdf

23. Financial Action Task Force (FATF), *Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs* (2024).: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html

24. HM Treasury, *Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017: Response to the Consultation* (June 2022), p 29. :https://www.gov.uk/government/consultations/amendments-to-the-money-laundering-terrorist-financing-and-transfer-of-funds-information-on-the-payer-regulations-2017-statutory-instrument-2022

25. FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*(2025): https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf

CONTACT GDF:

hello@gdf.io

www.gdf.io

CONTACT BLOCK:

www.block.xyz

FOLLOW GDF:

@GlobalDigitalFi

Global Digital Finance

FOLLOW BLOCK:

@Blocks

Block