BIS

BIS Bulletin

No 111

An approach to anti-money laundering compliance for cryptoassets

Iñaki Aldasoro, Jon Frost, Sang Hyuk Lim, Fernando Perez-Cruz and Hyun Song Shin

13 August 2025

BIS Bulletins are written by staff members of the Bank for International Settlements, and from time to time by other economists, and are published by the Bank. The papers are on subjects of topical interest and are technical in character. The views expressed in them are those of their authors and not necessarily the views of the BIS. The authors are grateful to Rebeca Anguren, Raphael Auer, Maha El Dimachki, Marc Farag, Pablo Hernández de Cos, Friedrich Klinger, Ulf Lewrick, Noel Reynolds, Peter Wierts and Phil Wooldridge for helpful comments and suggestions, Giulio Cornelli for excellent research assistance, Emma Claggett for editorial review and Nicola Faessler and Danielle Ritzema for administrative support.

The editor of the BIS Bulletin series is Hyun Song Shin.

This publication is available on the BIS website (www.bis.org).

ISSN: 2708-0420 (online)
ISBN: 978-92-9259-881-5 (online)

Iñaki Aldasoro Inaki.Aldasoro@bis.org
Jon Frost Jon.Frost@bis.org
Sang Hyuk Lim Sanghyuk.Lim@bis.org
Fernando Perez-Cruz Fernando.Perezcruz@bis.org
Hyun Song Shin Hyunsong.Shin@bis.org

An approach to anti-money laundering compliance for cryptoassets

Key takeaways

- Existing anti-money laundering (AML) approaches relying on trusted intermediaries have limited effectiveness with decentralised record-keeping in permissionless public blockchains.
- The public transaction history on blockchains can enable AML and other compliance efforts, such as FX regulations, by leveraging the provenance and history of any particular unit or balance of a cryptoasset, including stablecoins.
- An AML compliance score based on the likelihood that a particular cryptoasset unit or balance is linked with illicit activity may be referenced at points of contact with the banking system ("off-ramps"), preventing inflows of the proceeds of illicit activity and supporting a culture of "duty of care" among crypto market participants.

Cryptoassets circulating on permissionless public blockchains have grown in heft rapidly and are becoming increasingly integrated with the mainstream financial system. As their usage expands, concerns about illicit activity have also grown. Since 2022, stablecoins have overtaken bitcoin as the asset of choice among criminals using crypto, and as of 2024 accounted for approximately 63% of all illicit transactions (Chainalysis (2025); TRM Labs (2025)).[1] With growing interconnections between the crypto world and the traditional financial system, strengthening the integrity of payment activity – by guarding against money laundering and other forms of illicit activity – has become more urgently necessary.

Currently, rules to ensure anti-money laundering (AML) compliance rely on regulated financial intermediaries, especially the banking sector. In an intermediary-based monetary system, a payment is executed by debiting the sender's account and crediting the receiver's account. Customer checks can be conducted at the time of account updates, and the duty to perform them falls on the intermediary. This principle applies both domestically and to international payments through the correspondent banking network (CPMI (2016); BIS (2025)).

Existing international standards for AML compliance for cryptoassets attempt to apply the intermediary-based principles for AML compliance to the crypto world.[2] However, there are clear limits to such an approach. Permissionless public blockchains rely on the operation of decentralised consensus mechanisms sustained by a dispersed set of self-interested "validators" who jointly maintain the records of transfers between addresses on the blockchain in a decentralised way. No individual intermediary may be held accountable for the account update. While customer verification can be performed at points of contact with the conventional monetary system (eg by crypto exchanges) at the time of fund transfers into

[1] The estimated volume of cryptocurrencies used in illicit activities reached $51.3 billion in 2024. These figures are probably a lower bound as they exclude cryptoassets used for money laundering in non-crypto-related crimes (eg drug trafficking) and only count known illicit addresses.

[2] The Financial Action Task Force (FATF) standards require virtual asset service providers and financial institutions to obtain, hold and transmit specific originator and beneficiary information when transferring virtual assets (FATF (2025)), ie the "travel rule".

and out of the exchange, once claims move to unhosted wallets on the permissionless blockchain itself, the transactions are out of the reach of conventional forms of intervention.[3] While stablecoin issuers have frozen balances at authorities' request in high-profile cases of financial crime, such an approach is unrealistic to cover billions of day-to-day transactions.

This Bulletin explores an alternative approach to AML compliance in permissionless blockchains which utilises the very features that make them impervious to traditional approaches. As the full history of transactions on the blockchain is publicly available, it could inform an assessment of how closely a particular unit of a cryptoasset is associated with past or current illicit activity. A diagnostic "AML compliance score" could be referenced in any further interventions by authorities when cryptoassets (including stablecoins) are presented for conversion to fiat currency at the "off-ramps" – notably, at the point of contact with the banking system.

The specific criteria for assessment could vary across jurisdictions. For instance, for those that maintain foreign exchange regulations, the definition of illicit activity could encompass transactions that violate those regulations. Given the widespread cross-border use of stablecoins, such safeguards could help to slow the erosion of monetary sovereignty and maintain the effectiveness of monetary policy.

This Bulletin presents a range of options in implementation and the possible broader impact on the crypto ecosystem, including endogenous changes in the behaviour of illicit actors and associated shifts in the allocation of the "duty of care" between crypto users and authorities.

Record-keeping and cryptoasset transfers on permissionless blockchains

Cryptoassets that circulate on permissionless public blockchains repudiate trusted intermediaries such as central banks and commercial banks. Instead, permissionless blockchains rely on a dispersed network of self-interested record-keepers – "validators" or "miners" – who update and maintain a record of transactions in a decentralised way. The system can select a validator at random to append a new block of transactions to the chain of past blocks of transactions, where the record-keeping is a matter of consensus among the network of validators. The consensus mechanism is decentralised in the sense that each validator has an incentive (through rewards and fees) to follow the consensus protocol provided other validators do so (Auer et al (2025)). Hence, once the consensus mechanism is established the system is self-sustaining. In a permissionless public blockchain, the entire history of transfers on the blockchain serves as a "master ledger" and as a substitute for having intermediaries that maintain account balances.

One example of this decentralised model of record-keeping is the Bitcoin blockchain, which follows the unspent transaction output (UTXO) model.[4] The holding and transferring of bitcoin are defined entirely by the history of UTXOs, effectively functioning as a master ledger where money serves as memory.[5] This system does not record account balances in the way that intermediaries like banks do. Instead, the bitcoin in a user's wallet represents a collection of unspent records from previous transactions. Each transaction references these records to generate a new one. For example, the recipient's UTXO references the amount of bitcoin being bought, and the sender's UTXO the difference between the input UTXO and the amount

[3] Unlike hosted wallets, which are offered by a crypto exchange that does know-your-customer checks, unhosted wallets allow users to transact without identification.

[4] On blockchains like Bitcoin, a UTXO represents a given amount of cryptocurrency that has been authorised by a sender and has not yet been spent by a recipient (Antonopoulos (2017)).

[5] Economic theorists have explored how the convention of money resembles a record-keeping device that records all past transactions. Once the convention has taken root, holding money is evidence that the holder acquired money by providing goods and services in the past (Kocherlakota (1998)). While this was originally a theoretical fiction, the advent of crypto has made such a master ledger a realistic proposition.

being paid minus the fee taken by the miner.[6] As a result, users can trace these records all the way back to the original minting of the bitcoins.

Stablecoins follow an "account-based" token standard on programmable blockchains (eg Ethereum or Tron), which record balances as account updates. For this reason, once a unit of a stablecoin enters a wallet, it is indistinguishable from other units in that wallet. This differs from Bitcoin, in which the UTXOs in a wallet remain unmixed and individually traceable. Stablecoins circulate on these blockchains because they allow greater programmability features, a higher number of transactions per second and lower fees. In the case of account-based blockchains, tracking the individual token or UTXO is not possible. However, stablecoins also allow for some degree of transaction traceability, as it is possible to map the wallet addresses that have transacted previously on the public blockchain. Moreover, the stablecoin market is dominated by centralised fiat-backed stablecoins, whereby only the issuer can mint new coins when they receive the fiat currency and burn the stablecoins when they pay out. The tree of wallets for any stablecoin can be traced back to its minting origins until it is burned. This centralised property also allows the stablecoin issuer to freeze the stablecoins in a wallet or deny their conversion to fiat currency.

AML compliance scores for cryptoassets

The attributes of permissionless public blockchains described above suggest that a system of summary scores could be the basis of diagnostic tools and AML compliance scoring mechanisms at points of contact with the conventional monetary system. In particular, an AML compliance score that references the UTXOs for bitcoins or wallets for stablecoins could use the information on the blockchain, including the full history of transactions and the wallets they have passed through.[7] A higher value (eg maximum 100) would denote relatively clean funds, coming mostly from "allow-listed" wallets, while a lower value (eg minimum zero) would denote funds that are tainted by being associated with one or more wallets known to be on a "deny list" (Graph 1).[8] The AML compliance score for such wallets can then be assessed against a threshold value chosen by authorities following jurisdictional considerations to determine whether off-ramp transactions with that wallet are allowed or denied. Crypto exchanges, stablecoin issuers and banks could apply safeguards by considering minimum AML compliance score requirements for cashing out crypto coins, helping to prevent funds from illicit activities from entering the conventional monetary system.

Importantly, AML scoring can be designed to reflect compliance with various existing rules. For example, adherence to foreign exchange regulations may be relevant for some economies. By incorporating jurisdiction-specific requirements, the scoring system can reference local rules and adapt to the specific regulatory needs of different jurisdictions. Leveraging the traceability of records, these compliance scores could further address criteria such as taxation and consumer protection. As a result, compliance scores could vary depending on the type of rules applied, ensuring the scoring system remains relevant and effective across diverse regulatory environments.

At its most basic, the approach could range from stringent to permissive. At one end, the strongest form of AML compliance would require off-ramps to accept tokens for conversion only if they have passed through addresses that have met KYC compliance checks – ie wallets that are on an "allow list" (Graph 2). This stringent version of the AML test implies that all users (including those operating unhosted wallets)

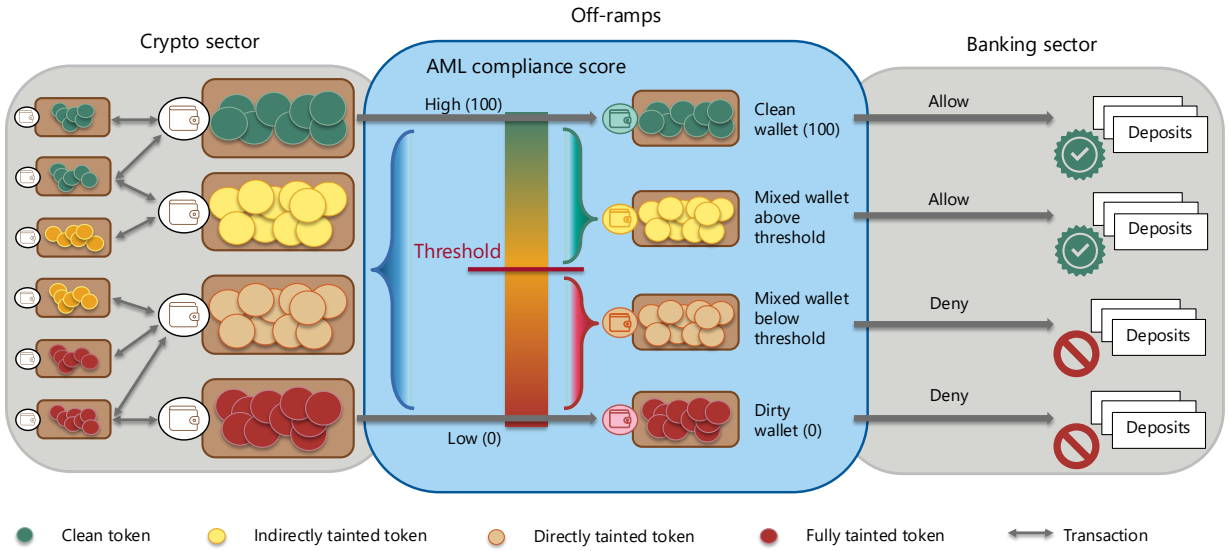
[6] A miner can also combine several UTXOs to make a single larger payment. The Satoshi (the smallest unit of bitcoin) in each UTXO can be traced back to the original minting of the coins (ie it is possible to know all the UTXOs and wallets where the Satoshi in a UTXO has previously been). If a UTXO results from the combination of several UTXOs, the Satoshi in it would have different, indistinguishable origins; however, all the histories are traceable.

[7] For an early statement of similar ideas in terms of risk scoring of bitcoin transactions, see Möser et al (2014).

[8] An endogenous response whereby illicit activities move to alternative wallets is to be expected. This could include the use of so-called mixers or unregulated exchanges that perform off-chain transactions between their clients. However, systematic efforts to circumvent rules could be also observed and taken into account in the AML scoring at the off-ramps.

would have to undergo KYC checks, just as all clients of banks must do when opening an account today. Using smart contract functionalities, crypto exchanges and other wallet providers could be required to block any transactions from or to addresses that are not on the allow list.

An AML compliance score using transaction history and token provenance Graph 1



Indirectly tainted token = indirectly associated with addresses on the deny list through intermediary addresses or multi-step transactions; directly tainted token = directly linked to addresses on the deny list.

Source: Authors' elaboration.

At the other end of the spectrum, a permissive form of AML compliance is to check whether a coin has passed through an address known to be associated with illicit activity – ie on a deny list. For bitcoin, it is possible to assess whether a UTXO (or part of it) has *ever* passed through such an address. For stablecoins, it would not be possible to track the full provenance of specific coins, but transactions directly from or to illicit addresses (or to addresses that have directly transacted with addresses on the deny list) could be identified for intervention by authorities at the off-ramp.[9]

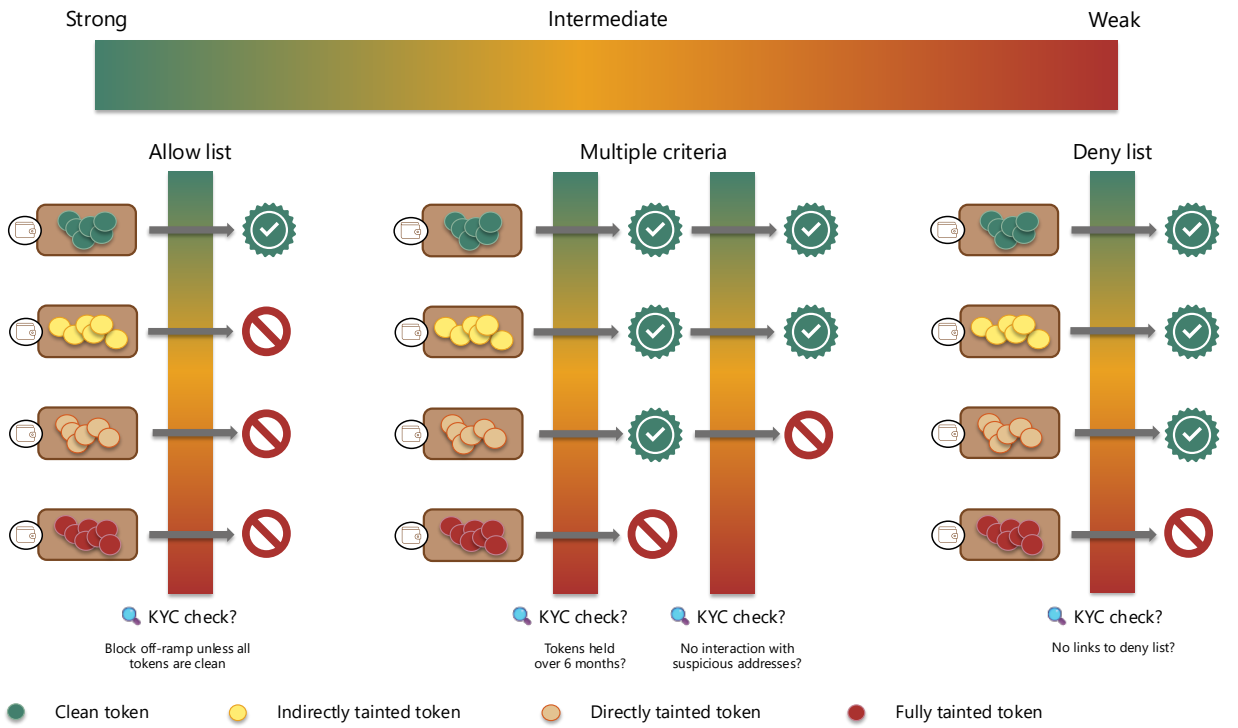
Between these two extreme cases lie a range of intermediate levels of stringency. Considering the potential for regulatory circumvention and money laundering through mule or dormant wallets, multiple criteria and patterns of fund transfers could be considered. For example, conditions could include requiring that the most recent recipients of a UTXO or wallet addresses are on an allow list, that a specific address has not transacted with deny list addresses, that the UTXO or funds in a wallet have remained on an allow list for a certain period, or differentiating allowable transfer amounts based on AML compliance score ranges. A history of transactions with protocols known to be used to facilitate money laundering could raise red flags for further scrutiny.

Crucially, these approaches would require defining which actor is responsible for preventing illicit flows. This could be the individual user, the crypto intermediary (crypto exchange or virtual asset service provider) or other parties such as a system of clearing houses that convert stablecoins into fiat money. A pragmatic approach is to rely on the points where cryptoassets and stablecoins are converted into fiat currency. Imposing a duty of care on these entities would incentivise them to avoid accepting or paying

[9] If AML approaches were widely adopted, the risk of seizure for token recipients could be mitigated. An alternative would be to treat tokens like banknotes, and thus to explicitly indemnify recipients against any risk of seizure (Jeng (2025)). This approach could, however, undermine the duty of care and incentivise (known) illicit activity.

out tainted coins, as failure to comply could result in fines or other penalties. Individual holders could also face specific requirements. Given the public nature of blockchain transactions, more third-party service providers could also be expected to enter the market for compliance services. While some users may reasonably claim to have received a tainted token in good faith if information on illicit use is scarce, such an argument would be less persuasive if there were widespread and affordable compliance service providers. In such a setting, users could reasonably be expected to exercise a duty of care in transacting with crypto tokens by checking beforehand if a crypto coin is known to be compromised. Approaches that clearly define responsibility create incentives for good actors to seek out illicit activity and report it to authorities.[10]

The spectrum of AML compliance stringency Graph 2



Indirectly tainted token = indirectly associated with addresses on the deny list through intermediary addresses or multi-step transactions; directly tainted token = directly linked to addresses on the deny list.

Source: Authors' elaboration.

Broader policy considerations

Crypto and stablecoins pose challenges to existing regulatory frameworks. These risks differ from those of traditional financial instruments, meaning the principle of "same risk, same regulation" does not apply (Aldasoro et al (2025)). An approach that takes account of the unique features of crypto and stablecoins and uses them to enhance regulation emerges as a promising avenue to close regulatory gaps.

[10] There are even proposals for a "bounty hunter" approach to compliance, whereby licensed firms could receive compensation for reporting suspicious activity to regulators (Kellerman (2025)). This can be compared with "bug bounties" that are paid for successfully finding cyber vulnerabilities.

Incorporating the provenance of crypto coins into regulations could support AML / countering the financing of terrorism (CFT) efforts and strengthen financial system integrity. Differentiating stablecoins by their provenance would mean that histories would enter as an essential attribute. For instance, stablecoins that had passed through wallets with a chequered history could trade at a higher discount relative to others with no such history. This property is an instance of the idea from economic theory that the value of goods varies with time, place and circumstances (Debreu (1959)).

Compliance scores of the type described here could also generate incentives to support better outcomes in terms of overall compliance. They could not only be used at the off-ramps from the crypto ecosystem to the conventional monetary system, but also accompany the token as it moves within the permissionless blockchain – embedding the score into the UTXO or wallet itself. A duty of care among users would thus be established, potentially influencing behaviour even among those transacting solely through unhosted wallets. If such duty of care took hold, there would be an incentive to transact with clean allow-listed wallets that could generate a positive feedback loop in terms of compliance.

International cooperation across jurisdictions would significantly improve regulatory outcomes. Cryptoassets straddle borders and hence pose unique policy challenges that require effective cooperation. Jurisdiction-level rules could allow greater scope for international cooperation at subsequent stages of rule development.

References

Aldasoro, I, M Aquilina, U Lewrick and S H Lim (2025): "Stablecoin growth – policy challenges and approaches", *BIS Bulletin*, no 108, July.

Antonopoulos, A (2017): *Mastering Bitcoin: programming the open blockchain*, O'Reilly Media, 2nd ed.

Auer, R, C Monnet and H S Shin (2025): "Decentralised ledgers and the governance of money", *Journal of Financial Economics*, vol 167, 104026, May.

Bank for International Settlements (BIS) (2025): "The next-generation monetary and financial system", *Annual Economic Report 2025*, Chapter III, June.

Chainalysis (2025): "The 2025 crypto crime report", February.

Committee on Payments and Market Infrastructures (CPMI) (2016): *Correspondent banking*, July.

Debreu, G (1959): *Theory of value: an axiomatic analysis of economic equilibrium*, Yale University Press.

Financial Action Task Force (FATF) (2025): *Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers*, June.

Jeng, L (2025): "Stablecoins should be treated as currency", *Financial Times*, 7 May.

Kellerman (2025): "Licensed detection agents: the case for financial crime bounty hunters", available at SSRN: https://ssrn.com/abstract=5106992 or http://dx.doi.org/10.2139/ssrn.5106992.

Kocherlakota, N (1998): "Money is memory", *Journal of Economic Theory*, vol 81, no 2, pp 232–51.

Möser, M, R Böhme and D Breuker (2014): "Towards risk scoring of bitcoin transactions", mimeo.

TRM Labs (2025): "2025 crypto crime report", February.