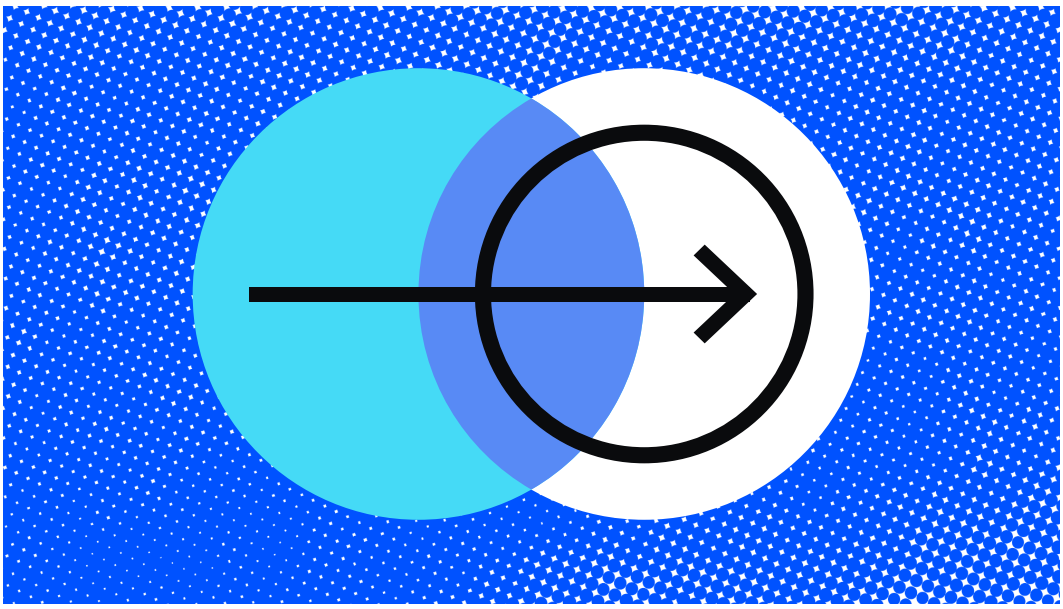
Crypto Innovation is Essential to Curtailing Illicit Finance



Tl;dr:

The United States has a significant opportunity in the coming years to lead the world in digital asset innovation, which will better prepare it to combat financial crime and protect national security. But this leadership depends on a U.S. regulatory landscape that holds bad actors to account while fostering private innovation. As explained in Coinbase's recent response to the U.S. Treasury Department's request for comment on "Ensuring Responsible Development of Digital Assets," the U.S. government should focus on facilitating the use of blockchain and other new technologies that provide unique opportunities to track and disrupt illicit finance.

Note: The views and opinions expressed herein are those of the authors and do not necessarily reflect the views of Coinbase or its employees and summarizes information and articles with respect to cryptocurrencies or related topics that the author believes may be of interest. This material is for informational purposes only, and is not (i) an offer, or solicitation of an offer, to invest in, or to buy or sell, any interests or shares, or to participate in any investment or trading strategy, (ii) intended to provide accounting, legal, or tax advice, or investment recommendations or (iii) an official statement of Coinbase. No representation or warranty is made, expressed or implied, with respect to the accuracy or completeness of the information or to the future performance of any digital asset, financial instrument or other market or economic measure. The information is believed to be current as of the date indicated on the materials. Recipients should consult their advisors before making any investment decision.

Part 1 Digital Assets and Illicit Finance

Digital assets play an increasingly important role in our global financial system. With a worldwide market cap of over $870 billion, these assets offer increased security, privacy, transparency, and specific gains like decreased settlement time and risk. But with these benefits comes concern about the use of digital assets for illicit finance. Specifically, the U.S. government has raised concerns about the use of crypto in "money laundering, terrorist and proliferation financing, fraud and theft schemes, and corruption." The U.S. Department of Justice has also noted the direct link between illicit finance and national security, emphasizing that the U.S. must work "to prevent and disrupt the exploitation of [digital asset] technologies to facilitate crime and undermine our national security."

This paper explores the use of existing regulatory regimes and digital asset technology to combat illicit finance, noting the key role of blockchain technology in enforcing compliance, and the need for public-private collaboration to facilitate the use of new technologies.

Part 2 Most Illicit Finance Takes Place Via Noncompliant Institutions

Most illicit finance involving crypto relies upon a very small number of noncompliant crypto exchanges. This is because illicit actors such as ransomware groups, sanctioned entities, and scammers consistently seek out noncompliant institutions to exchange crypto for fiat or other crypto. A 2021 report by Chainalysis, a leading blockchain analysis firm, found that cybercriminals "rely on a surprisingly small group of service providers to liquidate their crypto assets," including "money services businesses with lax compliance programs." Similarly, blockchain analytics firm Elliptic has found that "[c]riminals deliberately seek out exchanges they know they can exploit with little or no obstruction," whether moving money between crypto and fiat or among different types of crypto.

The U.S. Treasury Department recognized this tactic in its recent report on illicit finance, identifying the use of noncompliant virtual asset service providers, or "VASPs," as a "primary concern." And the U.S. Justice Department recently cautioned that "criminals continue to take advantage of noncompliant actors … including noncompliant cryptocurrency exchanges … to exchange their cryptocurrency for cash

or other digital assets without facing rigorous [regulatory] scrutiny." In sum, one of the most effective ways to combat illicit finance is to disrupt the ability of noncompliant VASPs to liquidate and conceal criminal proceeds, thereby making it much harder for criminals to profit from their behavior.

Fortunately, the U.S. government already has the tools to address much of this illicit finance risk. The U.S. Treasury Department has the authority to bring enforcement actions against noncompliant VASPs located anywhere in the world, as long as these institutions do business in the United States or substantially service U.S. customers. Globally, however, there remain large gaps in enforcement efforts. Some bad-faith providers take advantage of these gaps by engaging in jurisdictional arbitrage—providing crypto services to global customers located in countries with weak or non-existent anti-money laundering (AML) controls, with the expectation that regulators will not hold them accountable.

Part 3 Blockchain Technology Can be a Powerful New Tool for Combating Illicit Finance

The emergence of crypto over the past decade has also given institutions a powerful new set of tools that can radically enhance their ability to identify and disrupt illicit finance. These tools harness the public and transparent nature of blockchains – public, immutable ledgers that maintain a record of all transactions, including crimes such as crypto thefts and laundering by ransomware actors.

Tracing Financial Crimes on the Blockchain

The ease of tracing transactions on the blockchain offers significant benefits to law enforcement, allowing them to detect and disrupt illicit activity by mapping specific transactions to illicit actors. They can then trace the transfer of ill-gotten funds through different digital wallet addresses, and seek to connect those addresses to specific individuals. Recent high-profile arrests underscore the success of these government mapping efforts. In 2020, the IRS dismantled three online terrorist financing campaigns that had solicited donations in crypto. Despite the terrorist group's boast that "bitcoin donations were untraceable," FBI agents tracked and seized millions of dollars' worth of crypto from over 300 accounts related to the campaigns. Similarly, authorities were able to trace and recover many of the lost funds from a

Russia-linked ransomware attack on the critical Colonial Pipeline in 2021. Moreover, the federal government recently recovered over $3.5 billion worth of crypto in the "largest financial seizure ever" after the hackers were unable to launder the money.

As an official at the Commodity Futures Trading Commission recently noted, it "is easier for law enforcement to trace illicit activity using Bitcoin than it is to trace cross-border illegal activity using traditional banking transactions, and far easier than cash transactions."

From KYC to KYT: Using Blockchain Technology to Enhance Compliance

Blockchain technology can also enable service providers to better combat money laundering. All U.S. financial institutions, including those that custody virtual assets, are required by the federal Bank Secrecy Act (BSA) to guard against financial crimes by implementing programs aimed at combating money laundering. These AML programs require institutions to collect identifying information and perform a basic risk assessment before onboarding new customers – a process known as "know-your-customer," or KYC. The BSA also requires institutions to monitor transactions, file Suspicious Activity Reports (SARs) in certain circumstances, and train employees on compliance. Each of these requirements applies equally to traditional banks and to VASPs.

Compliance measures have historically been limited, however, by the reliance of traditional financial institutions on their own private and opaque ledgers, which creates a significant risk of blind spots. In short, a traditional institution cannot fully monitor transactions that take place outside its specific platform. For example, if a client wants to deposit funds into her bank account, the bank must rely on information provided by the customer about the source of those funds.

The blockchain can greatly enhance these compliance measures by allowing VASPs to track the flow of assets beyond their individual platforms. This tracking gives financial institutions a far deeper and richer understanding of the risks posed by specific transactions and customers. In the case of a customer wishing to deposit funds, the blockchain would let institutions independently – and instantly – analyze the full history of those funds by reviewing a complete and public record of transactions. This additional data could let VASPs conduct sophisticated analyses to determine the risk of a specific transaction or asset, using tools and methods broadly referred to across the crypto ecosystem as know-your-transaction, or "KYT."

KYT is groundbreaking for compliance because the data received by institutions is:

- **Immediate** – available as soon as the transaction happens;
- **Independent** – derived from a source other than the customer, and tamper-proof; and
- **Dynamic** – can be constantly reevaluated based on new information.

For example, KYT can be directly incorporated into transaction monitoring tools, alerting a VASP whenever a customer engages in risky transactions, whether on or off its platform and with a hosted or self-hosted wallet, as discussed below. Many factors can trigger alerts, including indications of money laundering and contacts with high-risk actors and platforms. Once an alert is triggered, VASPs can carry out additional diligence on the customer, potentially file a SAR, or take other measures.

VASPs can also dynamically incorporate KYT into a customer's risk rating. While initial risk ratings are static because they are based on KYC information collected when an account is opened, KYT data can leverage the blockchain to dynamically adjust a customer's risk rating. If the rating rises to a certain level, VASPs can take further action, such as conducting enhanced diligence reviews, closing the account, or filing a SAR.

KYT also creates an enhanced approach to sanctions compliance. It allows VASPs to directly screen for crypto addresses identified by the the U.S. Treasury's Office of Foreign Assets Control (OFAC) and then proactively build out larger networks of high-risk addresses. Before the advent of crypto, OFAC was limited to putting static, traditional identifiers—such as names and addresses—on its Specially Designated Nationals List. But with blockchain technology, sanctions compliance can be based on transactional data, not just personal identifying information. Using blockchain analytics, VASPs can use addresses provided by OFAC to build out and identify much larger networks of high-risk counterparties using blockchain heuristics. And they can do this by leveraging immutable transactional data on the blockchain that is unrestricted by private ledgers and provides information on common ownership. Indeed, in recent years, an entire industry of blockchain analytics firms has developed to assist VASPs (and law enforcement) in utilizing the treasure-trove of data held in blockchains.

Case Study

Self-Hosted Wallets

A "self-hosted," or "self-custody" wallet is essentially an app or browser extension that functions as a digital wallet where users can buy, sell, and manage their crypto. Unlike a hosted, or custodial wallet, self-hosted wallets are managed solely by the individual user, not by a third party. These wallets are an important part of the crypto ecosystem because they allow users to directly participate in a developing universe of internet services built on blockchain technology. They also demonstrate the sufficiency of current regulations, in partnership with blockchain analysis, to precisely and dynamically address potential illicit finance risks.

Because users with self-hosted wallets can transfer crypto directly peer-to-peer without relying on a regulated financial intermediary, they sometimes raise concerns about criminal use. But recent reports have found no evidence that self-hosted wallets pose an inherently high risk. The Financial Action Task Force, the international body tasked with analyzing illicit finance and setting global AML standards, has extensively studied self-hosted wallets and was unable to identify them as categorically high risk. Similarly, in a recent report, the UK Treasury concluded that "there is not good evidence that self-hosted wallets present a disproportionate risk of being used in illicit finance," noting that many people "who hold [crypto] for legitimate purposes use unhosted wallets due to their customizability and potential security advantages."

Nevertheless, concerns over potential illicit uses of self-hosted wallets have led to some calls for preemptive, heightened regulation, such as a recent proposal by the U.S. Treasury Department that would require VASPs to collect counterparty information on all transactions with self-hosted wallets over $3,000, and to file suspicionless reports on those greater than $10,000.

Institutions are already obligated to carry out traditional compliance measures on transactions involving self-hosted wallets, as described above, including filing SARs, risk-rating customers, and carrying out additional diligence when warranted. Imposing an additional data collection requirement would be highly ineffective because such bulk collection – in contrast to blockchain analysis – is imprecise, static, and unverifiable.

First, when conducting bulk data collections, VASPs must rely on counterparty information provided by customers. But there is no guarantee that customers can accurately and precisely collect this information; for example, customers have no direct relationship with many counterparties, such as merchants. Further, in a bulk-collection scenario, VASPs may have no way of verifying counterparty information. Bad actors could simply provide false information about their counterparties, leading to bad data both coming in and going out in the form of inaccurate SAR filings and data sharing.

Instead, VASPs can look to blockchain analytics to identify potentially risky self-hosted wallet counterparties. The blockchain allows VASPs to precisely and dynamically understand the risk posed by a counterparty in a crypto transaction based on verifiable and independent data, even when the counterparty is a self-hosted wallet.

Part 4 Public-Private Collaboration is Essential

To maintain American leadership in technology while protecting against emerging threats, the U.S. government must partner closely with the private sector. Industry stakeholders on the front lines of compliance are often the first to recognize emerging threats to the financial system, and to identify effective responses. Here, collaboration can help develop regulation and tools to support a promising new form of identity verification known as "decentralized identity."

Decentralized Identity

Traditional KYC mechanisms were developed in the context of transactional ledgers and customer records maintained and accessed solely by one firm. As a result, firms today rely largely on their own identity-verification processes rather than capitalizing on verification work already done by others. This in turn requires customers to provide their personal information to each and every financial institution where they wish to have an account.

A new form of identity verification and management, decentralized ID (DID), simplifies this process by harnessing the unique advantages of the blockchain and sophisticated forms of encryption. The U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) recently promoted the development of novel identity tools, noting the potential for digital identity proofing to reduce money laundering and terrorist financing.

DID lets users securely and simply confirm their identity to various institutions, at times without even having to disclose their actual personal information. For example, suppose that Hal wants to build a digital identity profile that he can store on his phone in a digital "wallet" that he controls. First, Hal requests that a trusted entity, such as a financial institution, verify certain information, such as his birthdate, social security number, or the fact that he has undergone full KYC as of a certain date. The trusted entity then issues an "attestation token" to Hal confirming that fact. As the token holder, Hal can use the token when interacting with other entities that need to confirm the same fact. For example, if his employer needs to confirm Hal's bank account number, Hal can present the attestation token to the employer without disclosing other sensitive information, such as his account balance or history. Similarly, a new financial institution opening an account for Hal could rely on his attestation token from a VASP that has already conducted his full KYC evaluation.

The ability to rely on an attestation token would greatly streamline the KYC process itself, in turn strengthening protection against financial crimes. Specifically, KYC analyses that rely on DID have the potential to be significantly more effective because they use data stored on the blockchain that, as described above, is immediate, independent, and dynamic.

Embracing the more efficient DID process would also free up compliance resources for other tasks, and could reduce customer onboarding costs up to 90%. These reduced costs could in turn "facilitate financial inclusion for otherwise excluded or under-served individuals."

Despite the many potential benefits of DID, its full adoption is currently limited by a lack of regulatory clarity. Under current law, financial institutions must take certain steps to verify customer identity and decrease AML risks. Specifically, banks are subject to the Customer Identification program (CIP) rule, which requires financial institutions to obtain basic customer information such as name, birthdate, and address, maintain records of this information, and compare it against government lists of known or suspected terrorists. But while the CIP rule allows banks to rely on "non-documentary methods" to verify customer ID, it is unclear whether this category would include DID methods such as attestation tokens.

A similar ambiguity surrounds whether a VASP – which is often registered as a money services business and must follow general KYC requirements – could rely on DID to help satisfy its compliance obligations. And while the CIP rule allows banks to rely on verifications provided by other financial institutions, it strictly limits which kinds of other financial institutions this includes. By restricting verifiers to a limited class of institutions, the rule excludes many money services businesses and other firms that could potentially provide DID services.

As a result of this lack of clarity, private industry has been hesitant to more fully embrace DID. Until the underlying regulations are modified, or FinCEN issues guidance clarifying how firms can meet their compliance obligations using DID, it is unlikely that industry will be able to fully integrate DID, and will continue to miss out on opportunities for enhanced compliance.

Part 5 Policy Recommendations

As set out in more detail in Coinbase's recent Response, the U.S. Treasury Department can take the following steps to ensure the responsible development of digital assets:

- Prioritize the enforcement of existing, robust AML regulations against noncompliant market participants. Most financial crimes involving crypto occur on a small number of noncompliant exchanges. The U.S. government has the authority to bring enforcement actions against such VASPs worldwide, as long as they do business in the U.S. or substantially service U.S. customers.

- Work with the crypto industry to unlock new compliance technologies in blockchain analytics and decentralized identity. The government could facilitate the use of groundbreaking new technologies by modifying federal regulations and/or issuing guidance to clarify how financial institutions can use blockchain analytics and decentralized ID to meet their compliance obligations.

- Reject proposals for bulk data collection. The Treasury Department's proposed rule requiring VASPs to bulk-collect counterparty information on transactions with self-hosted wallets would ultimately be ineffective. Instead, Treasury should make clear that VASPs may use advanced "KYT" technologies to facilitate precise and dynamic understandings of risk, even when the counterparty is a self-hosted wallet.