The new frontier

Applying AML compliance to cryptocurrencies

kpmg.com

A KPMG publication coauthored with Chainalysis, Inc.
Cryptocurrencies allow parties to transact directly without the need for a third party to verify the transactions. The cryptographic nature of the transaction allows for the entire cryptocurrency community to both view and verify the transaction, removing the need for an intermediary. The cryptography also allows for a degree of privacy, so the transaction is made public, but the details and parties involved remain private. However, like with all cryptography, since some information is known, there is not true anonymity.

This unique aspect of transacting “pseudonymously” has resonated with an ever-increasing multitude of consumers, merchants, investors, government regulators, and, unfortunately, criminals. This last category of less ethical actors has increased suspicion in market stakeholders, as well as regulators due to the ease and speed with which certain illicit activity can be conducted through cryptocurrencies.

Knowing the anti-money laundering (AML) regulations for a cryptocurrency business is essential to developing an AML compliance program. Understanding the nuances of the market, the need for a robust compliance program, and leading practices around specific control implementation can help reduce exposure to high-risk activity involving cryptocurrencies.

What makes cryptocurrencies “pseudonymous”?
Certain cryptocurrencies (e.g., Bitcoin) are “pseudonymous,” meaning that a transaction is displayed as a seemingly random collection of characters, rather than identifiable information, such as a name or address. However, the transactions are logged in a public “blockchain,” which is a decentralized ledger system in which anyone can view records of every transaction ever made. This provides a much more transparent view than current market systems, even if the exact parties’ information is indiscernible.
Cryptocurrency businesses are all looking to capitalize on the demand of this emerging market. It’s no wonder that business models such as cryptocurrency exchanges, as well as traditional financial institutions (FIs), and even the retail industry, are trying to capitalize on the opportunities. Various offerings are being introduced into the cryptoasset ecosystem to meet a demand that could not previously be filled, such as stablecoins, security tokens, and utility tokens.

It is important that all businesses dealing in cryptocurrency fully understand, and mitigate, the inherent risks associated with their crypto-offerings, as well as develop a regulatory change management framework to comply with all statutory and regulatory requirements to which they may be subject. Perceived anonymity of cryptocurrency, use of cryptocurrency by bad actors, and regulatory requirements and expectations all necessitate an ongoing effort to address the concerns of customers, as well as protect them.

For those required to comply with the Bank Secrecy Act (BSA), a robust AML compliance program needs to be implemented up-front, so as to effectively manage the following risks:

— Regulatory enforcement action(s)
— Reputational damage
— Disruption in business continuity
— Loss of potential cryptocurrency market penetration or existing market share.

Effective management of BSA/AML compliance risks should not be overlooked by businesses dealing in cryptocurrency. Enforcement actions for willful or neglectful violations of BSA requirements have been occurring since 2015, resulting in civil money penalties of up to $110 million, as well as criminal indictments.

There are a number of considerations that should be taken into account to mitigate the above risks, but understanding the systemic and business challenges is key.
Systemic challenges

The lack of visibility into cryptocurrency transaction data, due to the inability to identify the underlying parties to a transaction, is a fundamental systemic challenge to the application of a traditional compliance framework. For example, cryptocurrency is exchanged between digital wallets/addresses, often without adequate customer identification data present, at least with respect to the third-party address. Consider the following:

Limitless “address” usage

There is no limit to the number of “addresses” a single wallet can produce. At present, linking a single user to specific addresses is difficult. While techniques exist to account for the proliferation of multiple cryptocurrency addresses, attributing them to real-world entities or individuals using only publicly available data is extremely labor-intensive, and even then, is an incomplete and inexact process of performing cryptocurrency address reconciliation.

Attempts to anonymize

There is a certain set of cryptocurrency users for whom privacy is extremely important. Some of those users value that privacy because it serves to obfuscate illicit purposes, others value that privacy for ideological reasons, and still others may be day traders who simply don’t want outsiders to see their transactions. A few different services exist to meet that demand, including mixers (or tumblers) and “privacy coins,” which are cryptocurrencies with enhanced privacy features baked into their code.

Mixing services are the digital equivalent of mixing names together in a hat for a raffle. An algorithm joins a group of transactions together so that nobody can guess what comes out the other side. These services are successful at obfuscating beneficial ownership to a certain degree, but specialized blockchain analysis software can show cryptocurrency businesses and financial institutions that a given entity has been transacting with a mixing service. Depending on the perspective, this may be seen as high-risk exposure.

As their name suggests, privacy coins are cryptocurrencies designed to enhance the privacy of transactions. They employ a variety of technologies to accomplish this, all of which typically involve some trade-off between privacy and transaction throughput: the more private, the slower and more costly the transaction. Dash is a privacy coin that uses a methodology conceptually similar to mixing, where transactions are grouped together in order to obfuscate individual participants’ identities. Monero is a privacy coin that goes a step further, using “ring signatures” to obscure the sender, “confidential transactions” to obscure the amount, and “stealth addresses” to obscure the recipient. Z-cash is yet a third privacy coin that uses an entirely different technology called “zk-SNARKs,” which is an example of a zero-knowledge proof. Zero-knowledge proofs have the same obfuscating effect as the other privacy technologies listed and come at the same cost to transaction speed and efficiency.
Compliance program processes and controls

Although data contained within the blockchain is insufficient to determine real-world identities, cryptocurrency trading platforms, or cryptocurrency businesses that meet the Financial Crimes Enforcement Network (FinCEN) definition, are nonetheless mandated to maintain a robust AML program. Regulatory mandates, and leading practices, order that they are essentially obligated to:

— Verify their customer’s identity prior to onboarding via Know Your Customer (KYC) processes
— Monitor customer transactions to screen for suspicious transactions via transaction monitoring and filtering
— Adhere to reporting and record-keeping requirements, among other requirements.

While some components of a cryptocurrency business’s program can be satisfied by processes that attempt to mirror those implemented by traditional FIs, other components require industry-specific solutions to satisfy regulatory requirements. Specially, the following AML compliance program processes and controls should be assessed.

KYC and customer onboarding
Customer onboarding and KYC require obtaining, verifying, and screening customer information so that a business can know its customer base. Tailoring of customer due diligence programs to the cryptocurrency market will be essential to effectively detect real suspicious activity while avoiding inefficiencies and compliance fatigue. At a traditional FI, customers are typically required to be physically present and provide documentation to prove their identity and their address.

In the cryptocurrency market there is not usually physical human interaction, which can create unique challenges for onboarding and other core AML components. There are some innovative approaches to this problem, which involve the collection of KYC data through entirely remote processes, such as a copy of a government-issued identification document (e.g., driver’s license or passport) submitted via electronic means (i.e., e-KYC). However, this would not prevent someone from providing false or fraudulent identification. Therefore, a multistep approach to verify the customer’s identity must be used, which entails cross-referencing the copy of the identification document with other identifiable and verifiable forms of information. It is incumbent upon cryptocurrency businesses to evaluate their customer identification processes carefully, so as to identify potential loopholes or gaps that regulatory examiners will find unacceptable and verify that e-KYC is permissible in their jurisdiction in the first place.

Cryptocurrency businesses can implement controls to mitigate KYC risk by incorporating the collection and screening of customer cryptocurrency addresses into the onboarding process. Screening known customer addresses with blockchain analysis software allows a cryptocurrency business to see a potential customer or counterparty’s entire transaction history. The ability to see transaction history and follow any suspicious flows gives a compliance team a thorough, up-front assessment of KYC risk. That level of transparency isn’t available in other asset classes and is one of the key opportunities presented by cryptocurrencies.

As an onboarding leading practice, cryptocurrency businesses should use blockchain analysis software to identify their customer’s known cryptocurrency transaction exposure and use those results in the decision-making process. When the customer is onboarded, cryptocurrency businesses should use the same software to maintain consistency of analysis between transaction and customer risk rating. This establishes a baseline customer risk rating, in order to perform the following sanctions screening, transaction monitoring, and reporting requirements.

Sanctions screening
In November 2018, the U.S. Department of Treasury’s Office of Foreign Assets Control (OFAC), after asserting that they may include specific digital currency addresses associated with blocked persons on its List of Specially Designated Nationals (SDN List), added the first two digital currency addresses to the SDN List. This has begun the necessity of screening cryptocurrency transactions against the SDN List and reporting or blocking flagged transactions, as is done with names of individuals and entities. This OFAC regulation applies, for example, to an individual from a foreign government that is under OFAC sanctions. If the individual happens to be an active customer of a cryptocurrency business and one of his or her addresses gets published on the SDN List, that business may be violating sanctions particularly if they are unable to identify that address as connected to that user.

1 FIN-2013-G001, “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,” March 18, 2013
2 Ibid.
3 U.S. Department of the Treasury OFAC Resource Center—OFAC FAQs: Sanctions Compliance, Questions on Virtual Currency, FAQs 559-63
4 U.S. Department of the Treasury website: November 28, 2018 Press Release
Cryptocurrency businesses should ask the following of their sanctions compliance program and seek to implement appropriate solutions or controls:

— How can our interdiction software incorporate new data points and regulatory procedures to efficiently comply with sanctions requirements in the jurisdiction in which we operate?

— How will our program stay relevant and up-to-date and ensure that updates to the SDN List and our transaction filtering process are put into effect in a timely manner, in accordance with regulatory requirements or expectations?

— Are our sanctions filters appropriately set to comply with regulatory requirements?

— Are we ensuring that our sanctions processes and controls are calibrated to align with any new and/or updated business products and services that could pose sanctions risks?

Furthermore, cryptocurrency businesses need to assess whether screening filters need to be adjusted to better align with the businesses’ risk profile, based upon the number and quality of alerts generated through the screening process. Too few or too many alerts could be indicative of threshold rules, scenarios, and algorithms set within the screening software as being inadequate. Beyond the use of interdiction software, cryptocurrency businesses should ensure that a robust, risk-based due diligence methodology is established for purposes of reviewing and dispositioning sanctions alerts.

**Transaction monitoring**

Under the BSA and applicable state law(s), cryptocurrency businesses are required to maintain a transaction monitoring system (TMS) that monitors customer transactions for suspicious activity. The inherent pseudonymity of cryptocurrency presents a unique challenge as businesses are required to maintain the ability to identify and monitor the provenance of customers’ cryptocurrency assets as well as their overall cryptocurrency transaction activity. TMS/AML detection scenario logic that is aligned with leading market monitoring practices is a critical component of an effective transaction monitoring system. Common examples specific to cryptocurrency businesses include transactions to/from darknet markets, illegal Initial Coin Offerings (ICOs), and unregulated exchanges.

Currently, most traditional third-party tools that are leveraged to track cryptocurrency transactions and potentially identify transactional history do not provide adequate solutions for all cryptocurrencies, nor do they have the capability to track “off-chain” transactions. Thus, cryptocurrency businesses should ask the following of their TMS compliance program(s), and either assess the adequacy of existing controls in place or look to implement appropriate controls:

— How can we leverage both internal and third-party solutions for identifying and monitoring suspicious transactions?

— What methodologies can be leveraged to develop detection scenarios aligned to particular risks posed by cryptocurrency transactions?

— What KYC attributes or transaction monitoring data points are necessary to measure the AML risks?

— Is the TMS data available and accurately mapped?

— Is the data complete and reliable?

— How is the data mined, converted, and processed into various compliance systems for the duration of the customer transaction lifecycle?

Developing an action plan around these touchpoints is key to the implementation of an effective TMS and its alignment to a robust cryptocurrency-specific risk assessment. Blockchain analysis solutions can be leveraged to support effective TMS scenario logic/rules that are critical to an effective transaction monitoring compliance program. In addition to identifying high-risk transactions (HRTs) as a stand-alone TMS rule, blockchain analysis solutions can greatly enhance existing TMS scenario logic by assisting in customer segmentation e.g., customers linked to HRTs via analysis can more effectively be segmented into High-Risk Customer (HRC) segments.

As a leading practice, cryptocurrency businesses should be able to create and automate an ongoing monitoring process for each customer profile established during onboarding. Such monitoring can take into consideration cryptocurrency transactional exposure to illicit sources, anomalies in transactional behavior from the baseline customer profile, and/or fiat transactional exposure to other cryptocurrency-related businesses that may not be well-known.

---

5 In accordance with U.S. regulations codified under 31 CFR Chapter X (FinCEN’s Customer Due Diligence Requirements for Financial Institutions); see 31 CFR 1022.210 (Anti-Money Laundering Programs for Money Services Businesses); 31 CFR 1022.320 (Reports by Money Services Businesses of Suspicious Transactions); 31 CFR 1022.210 (d)(3); OFAC Resource Center, OFAC FAQs: Sanctions Compliance, Questions on Virtual Currency, FAQs 559-63; For example(s) of applicable state law, see NYDFS Part 504 (New York Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications)

6 Note that off-chain transactions do not happen on the blockchain and are not available for public analysis. It is possible for even the operators of the exchange itself not to be able to determine who participated in an “off-chain” transaction.
Conclusion

Understanding the need for AML compliance and specific control implementation leading practices can help reduce exposure to high-risk activity involving cryptocurrencies and is critical to overcoming the compliance challenge. Failure to choose an adequate solution can result in expensive, inefficient, and extremely manual processes that will ultimately fail to properly mitigate significant risk factors. The quality of AML data is vital in understanding risks, developing effective controls to mitigate the risks, and executing effective risk assessment and risk management.

Cryptocurrency blockchains are able to be made more transparent by identifying known dark markets, regulated exchanges, mixing sites, mining pools, etc. A significant understanding of cryptocurrency activity over time also requires additional context on cryptocurrency addresses for each service. Through a reference data set for linking real-world services to cryptocurrency transactions and addresses, and the visualization capabilities offered by some entities to easily understand this activity on the blockchains, it is possible to follow the flow of funds.

Businesses engaged in cryptocurrency should seek out specialized solutions that combine a deep understanding of, and expertise in, cryptocurrency technology. Technology with regard to making the blockchain more transparent, verifying customer information, and ensuring sanctions compliance have become necessary. While many AML regulations in the cryptocurrency industry parallel those of traditional FIs, the means by which to abide by them, and controls needed to defend against risks, can be vastly different. The quality of AML data is vital in understanding the risks, developing effective controls to mitigate the risks, and executing an effective risk management program.
Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

special thanks to Silvia Lacayo, Zachary Nusbaum, and Jeffrey Billingham from Chainalysis, Inc.

KPMG.com/socialmedia