With the pseudo-anonymity offered by cryptocurrencies, it has become seemingly easier for criminals to engage in illicit activities. But as the industry matures, regulatory authorities have brought obligatory KYC / AML procedures to the table to combat these risks. In this article, we will delve into how KYC works for crypto, for what crypto firms it’s a must, and how to implement it if you’re up to this challenge.

What is KYC at a glance?

KYC stands for "Know Your Customer" and refers to a process used by financial institutions to verify the identities of their customers. The goal of KYC is to prevent money laundering, financing of terrorism, and other forms of financial crimes by ensuring that customers are who they claim to be. The trigger for the development and widespread implementation of KYC was the events of 9/11 in the U.S.

The procedure isn’t something specific to the crypto industry. Originating as a regulation for traditional financial organizations, e.g. banks, it’s now a way to bring crypto out of the shadows and make it more transparent and secure.

The KYC process typically requires customers to provide personal information, such as their name, address, date of birth, and a government-issued ID. This information is then verified using various methods, such as performing document authentication, running biometric checks, and comparing the provided information to public records. Once the customer’s identity has been verified, they will be allowed to use the services they applied for: e.g., buying, selling, withdrawing, and/or lending cryptocurrencies.

It’s important to note that KYC is a legal requirement in many jurisdictions. Failure to comply with KYC regulations may lead to penalties for a business, a complete ban on activities, and even criminal prosecution.

What crypto services require KYC?

The range of services that may require KYC include exchanges, custodial crypto wallets, and peer-to-peer (P2P) marketplaces. Some other examples of cryptocurrency service providers that may require KYC can also include:

* OTC (over-the-counter) trading services. These platforms allow you to execute orders, mostly for larger sums, directly with a counterparty through an OTC desk, as opposed to placing it on auction open for everyone.
* Crypto lending platforms. Such platforms allow users to access loans using cryptocurrency as collateral.
* Payment processors. These services let merchants accept cryptocurrency payments for their goods and services.
* Token sale platforms. These are platforms that allow companies related to cryptocurrency to raise funds by offering interested investors their crypto tokens at early stages.

However, it’s not the specific type of service the company provides that obliges it to comply with KYC. The two main factors are:

1. **The jurisdiction** in which a crypto firm wants to operate;
2. **The volume of funds** it operates.

Let’s dive a bit deeper into those.

Geography of operation

In many jurisdictions, it’s not legal for a crypto firm to operate without implementing some form of KYC process. For example, the EU countries and the United States, being appealing affluent markets, are at the same time significantly regulated.

In the U.S., crypto assets fall under the Bank Secrecy Act (BSA). All cryptocurrency exchanges must register with [FinCEN](https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf) and require users to verify their identities to comply with AML and combating the financing of terrorism (CFT) regulations. Also, the IRS is one of the main regulators lobbying identity verification in the U.S. Crypto service providers are [obliged to report](https://www.irs.gov/newsroom/irs-announces-delay-for-implementation-of-600-reporting-threshold-for-third-party-payment-platforms-forms-1099-k) users’ earnings on crypto of over $600 as income. The latter have to pay taxes regardless of the sum.

A vivid example of challenges for crypto firms in the North American market is Binance US. In 2019, Binance had to launch a separate exchange platform to comply with all the requirements (read: continue serving the US market).

The EU is also an intensively regulated market where the screws will only be tightened. To date, there have been several important initiatives that affect KYC. First is the [5th Anti-Money Laundering Directive](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843) (AMLD5), which came into effect in early 2020 and made all crypto-related companies “Mandatory Entities.” Second, there’s the more recent [AMLD6](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L1673), which focused on sanctions for non-compliance. In addition, there are provisional agreements reached in June 2022 on two more regulatory initiatives:

* The so-called [“Travel rule”](https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/) obliges crypto asset service providers to collect and make accessible information about the originator and the beneficiary of the transfers to ensure traceability.
* Also, there’s [MiCA](https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/" \t "_blank), the Markets in Crypto-Assets regulatory framework, according to which crypto-asset service providers will need authorization to operate within the EU.

Some other countries may be smaller in market volume but offer crypto-related firms a milder climate.

The UAE, [the fastest-growing market](https://www.pwc.com/m1/en/publications/documents/uae-virtual-assets-market.pdf) in the Middle East, is an excellent example of a crypto-friendly regulatory regime. Its Securities and Commodities Authority [is reportedly](https://www.bnnbloomberg.ca/uae-readies-national-crypto-licensing-in-push-to-embrace-fintech-1.1724751) in the final stages of finalizing country-wide crypto legislation and is preparing to issue federal licenses. Some parts of the country have already taken steps towards this. The Emirate of Dubai, for example, has established the Virtual Assets Regulatory Authority (VARA), which has already issued its [Virtual Assets and Related Activities Regulations 2023](https://www.vara.ae/media/Virtual%20Assets%20and%20Related%20Activities%20Regulations%202023.pdf).

Unfortunately, there’s no universal list of requirements that would fit every jurisdiction, so you’ll inevitably face the need to evaluate it case by case when choosing your target geography.

Trade volume

The bigger the player is, the more attention and questions it naturally gets from regulators. Binance, the whale among crypto exchanges, is trying to keep everything as compliant as possible, so they only allow new users to access their services through KYC.

Other exchanges or services that aren’t that big can afford to check users less strictly, for example, upon reaching a certain threshold. KuCoin, for example, [allows unverified users](https://www.kucoin.com/support/360015102254) to trade crypto with just an email address. However, the withdrawal per day is limited to 1BTC.

In fact, the industry standards for initiating KYC are still drifting, so just like with varying jurisdictions' requirements, there’s no ready-made one-size-fits-all approach.

Can a crypto service go without KYC?

The ubiquitous implementation of KYC by crypto services has raised questions about how it impacts the industry. When Binance introduced KYC, [over 96%](https://www.cointribune.com/en/binance-loses-3-of-clients-after-kyc/) of its users complied. For ShapeShift, however, [KYC cost 95%](https://www.coindesk.com/markets/2020/02/18/erik-voorhees-within-five-years-there-will-be-a-major-financial-meltdown-and-crypto-will-be-ready/) of its user base, which made the platform pivot their business model to stay afloat.

On the one hand, KYC procedures provide more security for the general public. This leads to a better reputation for the industry and higher adoption of cryptocurrencies by a wider community. By verifying the identity of customers, crypto services mitigate the risk of fraud and identity theft, and ensure that only legitimate users have access to their platform and funds.

On the other hand, KYC can repel users who value cryptocurrency for privacy and anonymity above everything else. The very nature of cryptocurrency was initially designed to provide users with a decentralized, anonymous way to conduct financial transactions without oversight by centralized authorities. For these users, KYC procedures are seen as intrusive and go against the core principles of the crypto world.

This clash of philosophies has created tension in the industry between those who believe in the importance of KYC for security and those who value privacy. Luckily, there are options for both parties.

CEX vs. DEX

The principle of how transactions in a crypto service are performed is an essential fundamental point. There are centralized and decentralized exchanges.

**A centralized exchange (CEX)** largely resembles traditional stock exchanges that facilitate trades between buyers and sellers. A CEX is the easiest and fastest way to start buying and selling crypto. With a minimal learning curve, a new user can become a crypto trader in no time. However, convenience, a smooth user experience, and support in case of issues have their price.

The crypto assets in CEXs are kept off-chain—on centralized servers where these funds are associated with users’ identities. A CEX acts as a custodian that has taken on the obligation to hold users’ funds. That leads to two natural consequences:

* CEXs require all users to register to associate their funds with their identities.
* Users don’t have guaranteed real-time access to their funds and the ability to withdraw them, as would be the case with blockchain storage. Access can be frozen in a snap in case of any issues related to their identity or other reasons.

The most popular CEX is Binance, which we’ve mentioned multiple times in this article.

**A decentralized exchange (DEX)**, as opposed to a CEX, preaches an on-chain approach. It doesn’t require users to disclose their identities, as they trade directly with one another by leveraging the smart-contract infrastructure provided by the DEX. By keeping funds on a blockchain, users keep all the control and can transact at any time. However, such freedom comes with responsibility, so users should be crypto-savvy to avoid making irreversible mistakes.

The sharper learning curve is the main stop factor for growing a user base for DEXs. While CEXs target a wider community of people who’d like to get started with crypto, DEXs mainly compete for a seasoned audience of people who are already in the field.

Some of the popular decentralized exchanges are Uniswap, PancakeSwap, and dYdX.

How does the KYC procedure work in crypto?

The approaches of different services may differ in detail, but generally, KYC in crypto involves three steps: collecting users’ personal information, identity verification, and due diligence.

Step 1: Collecting users’ personal information

A user creates an account and provides their personal information, such as name, phone number, address, date of birth, and government-issued identification. Some services offer to fill in some fields manually, but most often, this module is semi- or fully automated. For example, personal details can be fetched from an ID document. Note that a data entry automation solution for this purpose should [specialize in processing identity documents](https://regulaforensics.com/solutions/use-cases/data-entry-automation), as the cost of errors is high.

**Tools:**Data entry automation and extraction tools, OCR, biometric data capture module.

Step 2: Identity verification

Once the customer's information has been collected, it must be verified. Verification usually consists of two parts: ensuring the provided ID document is genuine and valid, and confirming that its presenter isn’t an imposter.

Usually, this is an iterative procedure that is conducted with the help of various software solutions. For example, the document verification process [powered by Regula technologies](https://regulaforensics.com/products/document-reader-sdk) includes automated recognition of document type and country of origin; reading and validating all the data, including the data encoded in machine-readable zones, barcodes, and RFID chips; and running cross-checks for the data from all the sources. When biometric verification is turned on, there’s also face matching and a liveness check.

**Tools:**Document verification software, facial recognition software, liveness check module.

Step 3: Conducting due diligence

The process of due diligence is initiated in case of any red flags detected in the previous steps, for example, if the user has been involved in fraudulent activities, and this fact is known. It can also take place when users exceed a certain amount of cryptocurrency and start to operate with more significant sums. This also requires additional checks that are often called KYC 2.

The process may involve comparing the information to public records, conducting background checks, and reviewing financial history, as well as manual verification methods, such as calling the customer to confirm their identity in a live conversation. One of the common ways to additionally anchor the user with their identity is asking for confirmation of the actual residence address. As a rule, this is confirmed by uploading paid bills for housing, electricity, etc.

**Tools:**Machine learning algorithms, risk assessment software.

Decision making

Based on the information collected and the risk assessment, the cryptocurrency service provider will decide whether to accept the customer. If the decision is positive, the customer can buy, sell, and trade cryptocurrency on the platform. If the decision is negative, the customer will be denied access to the platform.

Once a customer has been accepted, the cryptocurrency service provider will monitor their account for suspicious activity. This may involve monitoring transactions, reviewing customer behavior, and conducting periodic reviews of customer information to ensure it remains accurate.

How to implement the KYC procedure in crypto

While implementing KYC in crypto is an important and responsible task, it’s not unique. The market for KYC service providers is developed and competitive, so technically, adding a KYC module can be pretty straightforward.

The solution to this challenge will largely depend on your development ideology. You can opt to ally with a KYC service provider and integrate a ready-made module, or develop it in-house, purchasing various technologies as building blocks to accomplish the task.

If you choose the former, Regula is here to serve you as a reliable technology partner. Having over 30 years of experience in document and identity verification, Regula provides state-of-the-art technologies that let you set up custom verification workflows, ensure security, and instantly authenticate users without adding extra friction to the UX.

The technologies have been proven by border control authorities and businesses, including companies from the fintech and crypto sectors. One of the latest [success stories is LCX](https://regulaforensics.com/explore/customer-stories/lcx-ag), the Liechtenstein Cryptoassets Exchange, which uses Regula to integrate secure document verification in its biometric authentication process. Feel free to get in touch with us if you have any questions.

<https://regulaforensics.com/blog/kyc-crypto/>