KYC Levels

What is Know Your Customer (KYC)?

KYC is a regulatory requirement for financial institutions to verify the identity of their customers.

It is a crucial part of anti-illegal activity measures and helps prevent illegal activities like fraud and illicit fund transfers.

In the digital asset industry, KYC is used by platforms to establish the identity of their users and understand their activities.

What is KYC and its Purpose?

Know Your Customer, often abbreviated as KYC, is a regulatory requirement for financial institutions to verify the identity of their customers. This process is a crucial part of anti-illegal activity measures and is designed to prevent illegal activities such as fraud, illicit fund transfers, and financing of terrorism.

KYC procedures involve collecting and verifying a customer's personal information, such as their full legal name, date of birth, and address. This information is usually verified using government-issued identification like a passport or driver's license. The objective of KYC guidelines is to prevent financial institutions from being used, either intentionally or unintentionally, by criminal elements for illicit activities.

KYC in the Digital Asset Industry

In the digital asset industry, KYC procedures are employed by platforms to establish a user's identity. This is usually done by requiring identifying information, which can include a user's full legal name, date of birth, and address, among other pertinent and verifiable data.

As the digital asset industry grows, global and national financial regulators are putting more pressure on platforms that offer digital asset services to comply with the same

rules that regulate traditional banks. Proper KYC measures help to prevent the illegal use of digital assets.

The Importance of KYC for the Digital Asset Industry

The importance of KYC in the digital asset industry cannot be overstated. In 1970, the US passed the Bank Secrecy Act (BSA) to help guard against illicit fund transfers, tax evasion, or other criminal activities. It requires financial institutions to keep records of transactions, file reports of transactions, and report suspicious activity.

KYC standards evolved from this, particularly when the Financial Crimes Enforcement Network (FinCEN) formed in April 1990. FinCEN, a regulatory authority of the US Department of the Treasury responsible for monitoring KYC and anti-illegal activity regulations, was created to support local, state, federal, and international law enforcement by gathering and analyzing information about financial transactions to combat domestic and international financial crime activities falling under the BSA.

Can Users Acquire Crypto Without KYC?

Decentralized applications are not required to run KYC on their users under most countries' existing laws because these protocols are not considered financial intermediaries or counterparties. Users trade directly with one another (peer-to-peer) by leveraging smart contracts. Acquiring crypto requires using funds from a regulated financial institution — which require KYC procedures.

How KYC Works

The KYC process starts by asking customers to provide a range of basic information, which can include a user's name, date of birth, and address (amongst other pertinent and verifiable data), which is supplemented with government-issued documentation. Once the KYC process has started, financial institutions cross-reference a user's information, usually involving any or all of the following processes:

Establishing a user's identity.

Understanding and verifying the user’s activities and the legitimacy of their source(s) of funds.

Establishing a risk profile for the customer based on key anti-illegal activity factors like their activities and location.

Accepted identity documents

Supported identity documents	Supported proof of address documents, issued within the last 3 months	Special considerations
• Driver’s license • Passport •National ID card • Foreign ID	• Bank statement • Credit card statement • Utility bill	An ID with an address is required to complete verification.