**Regulatory Framework**

The regulatory framework for KYC in web3 is still developing. Some countries have started to implement regulations specific to web3 technologies, while others have issued guidance or are in the process of developing regulations.

The European Commission has passed regulations (MiCA, TRF and AMLD7) requiring all Virtual Asset Service Providers (VASPs) to undergo customer due diligence and comply with Financial Action Task Force (FATF) requirements.

In the United States, the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) have issued guidance and proposed bills related to digital assets and web3 technologies.

Other countries and districts, such as Switzerland, the United Kingdom, Hong Kong, Singapore, and Japan, have or are about to implement regulations specific to web3.

# EU - MiCA/TFR Regulations

The European Union has enacted a new law called the Markets in Crypto-Assets (MiCA) regulations, which aims to make Europe a hub for digital assets. The law was drafted in 2020, passed by the European Parliament in April, and officially signed into law on May 31, 2023. The law defines a crypto asset and provides guidelines for crypto asset service providers (CASPs) and crypto asset issuers, requiring them to adhere to certain standards and regulations, such as Anti-Money Laundering rules.

MiCA establishes CASPs as separate legal entities that can obtain a license in any of the 27 EU member states. Stablecoin service providers are required to provide a white paper containing key details about the product and the key players involved. The law, however, does not cover nonfungible tokens (NFTs) or central bank-issued digital assets.

The law is considered a significant step forward for the crypto community, providing a uniform framework for all EU member states. It is hoped that the rest of the world will take note and consider adopting similar regulations. With the clarity that MiCA provides, Europe is positioned to become a more dominant player in the global crypto scene.

## What are the key requirements for crypto service providers under the MiCA regulations?

The Markets in Crypto-Assets (MiCA) regulations set forth several key requirements for crypto asset service providers (CASPs) within the European Union:

**Legal Status**: CASPs are established as separate legal entities under MiCA. This means that a CASP must be a legally recognized entity within one of the 27 EU member states.

**Licensing**: CASPs can obtain a license in any of the 27 EU member states. Once licensed, they're authorized to conduct business in the region.

**Security Measures**: CASPs are required to adopt certain security measures to protect the assets they handle and to ensure the integrity of their operations.

**Anti-Money Laundering (AML) Compliance**: CASPs must adhere to established Anti-Money Laundering regulations. These measures are designed to prevent the use of cryptocurrencies for illegal activities, such as money laundering or financing terrorism.

**Market Manipulation and Abuse**: Service providers must have measures in place that prevent market manipulation and abuse. This includes monitoring transactions and reporting suspicious activities to relevant authorities.

**Regulatory Supervision**: CASPs will be under the supervision of regulatory authorities, such as the European Banking Authority. This ensures they comply with the regulations and maintain the required standards.

**Disclosure and Transparency**: CASPs are required to provide complete and transparent information about the crypto assets they handle. This can include details about the asset's issuance, its nature, the rights it confers, and any associated risks.

**Stablecoin Rules**: For CASPs dealing with stablecoins, a white paper detailing key aspects of the product, the involved parties, terms of the public offer, blockchain verification mechanism, rights associated with the crypto assets, and the main risks for investors, among other details, must be provided.

# UK - Crypto Regulations

### Who is the regulator?

The Financial Conduct Authority (FCA) is the main financial regulator in the UK. It regulates crypto asset providers to ensure that they implement effective Anti-Money Laundering and Countering Terrorism Financing (AML/CFT) policies and procedures.

The FCA maintains a register of crypto asset providers that fall under UK money laundering regulations (MLR 2017 with amendments) and issues guidelines. When it comes to assets, security tokens are the only ones regulated by the [FCA](https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-bill-2022-factsheets/fact-sheet-cryptoassets-technical).

Other UK institutions that regulate crypto include:

* HM Treasury
* The Bank of England

### What are the main regulations?

Crypto companies in the UK have comply with the following to meet AML/CFT requirements:

* ​[The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017](https://www.legislation.gov.uk/uksi/2017/692/), or simply MLR, which is the main regulation that outlines all the AML requirements and registration requirements. It has been amended several times since its original publication to [implement](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/860279/Money_Laundering_and_Terrorist_Financing__Amendment__Regulations_2019.pdf) the EU’s AMLD5 in 2019 and [the Travel Rule in 2022](https://www.legislation.gov.uk/uksi/2022/860/contents/made).

Depending on the nature and type of assets a crypto firm deals with, the following laws and regulations can also apply:

* The Financial Services and Markets Act 2000 (“FSMA”) and the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (“RAO”)
* Electronic Money Regulations 2011 (“EMRs”) or the Payment Services Regulations 2017 (“PSRs”)

### Who is affected?

Affected companies can be separated into two types, according to the MLR 2017 and its amendments. The first are “crypto asset service providers,” which include companies that conduct either of the following:

* “Exchanging, or arranging or making arrangements with a view to the exchange of, crypto assets for money or money for crypto assets,
* Exchanging, or arranging or making arrangements with a view to the exchange of, one crypto asset for another, or
* Operating a machine which utilizes automated processes to exchange crypto assets for money or money for crypto assets.”

The second are “custodian wallet providers,” which provide services to safeguard and/or administer crypto assets—or private cryptographic keys for holding, storing, or transferring crypto assets—on behalf of customers.

### Who needs to register with the FCA?

Companies that deal with security tokens must register with the FCA because they are considered “regulated tokens”. Meanwhile, companies that deal with exchange and utility tokens do not have to register.

### How to register with the FCA

Before registering with the FCA, companies should answer the [following questions](https://www.fca.org.uk/publication/documents/cryptoasset-registration-flowchart.pdf):

* Does the company advertise or act in a way that suggests it’s providing crypto asset services by way of business?
* Does the company receive direct or indirect benefit from this service?
* How significant is the activity to the business’ other activities (crypto asset activities may be only part of the business)?
* Does the frequency of the activity suggest that it is being carried on as a business?
* Does the company have a registered or head office in the UK\* and does the company carry on day-to-day management of these activities from this office, irrespective of where, geographically, the crypto asset activity is conducted?
* Does the company operate one or more ATMs in the UK?
* Does the company have any UK presence that is engaged in or facilitates crypto asset activities?

\*If there is no UK office or other activity in the UK, beyond having a client in the UK, the FCA is likely to consider that the company is not conducting UK business.

If a company answers positively to some of these questions, then registration with the FCA is likely to be required.

The full requirements for registration can be found on the [FCA website](https://www.fca.org.uk/firms/cryptoassets-aml-ctf-regime/registering).

### AML requirements

Companies should take AML requirements very seriously, as failure to comply may lead to severe penalties.

To stay compliant with the AML requirements introduced in the MLRs in 2017, companies have to implement a clear set of procedures. This includes at least the following:

* Appointing a Money Laundering Reporting Officer (MLRO)
* Staff training
* Risk assessment
* Conducting Customer Due Diligence (CDD), Simplified Due Diligence (SDD) and Enhanced Due Diligence (EDD)
* Screening for persons on sanction lists, Politically Exposed Persons (PEPs) lists
* Transaction monitoring
* Ongoing monitoring of customer behavior and transactions
* Recordkeeping for at least five years from the date of the end of a business relationship or final transaction
* Reporting suspicious activity to the National Crime Agency

At the onboarding stage (KYC), at least the following information should be collected from users for verification:

* Full name
* Birth date
* Address

As a rule, such data is collected from government-issued documents. Proof of address documents can include current bank statements or credit/debit card statements issued by a regulated financial sector firm in the UK, in addition to utility bills.

### UK Crypto Travel Rule

The UK recently has adopted the Travel Rule requirement to its regulation of crypto asset service providers. The Travel Rule requires crypto companies to obtain information from the sender and receiver of crypto assets and share it with counterparty crypto asset service providers. The requirement comes into force on September 1, 2023.

Suggested read: [What is the FATF Travel Rule? The Ultimate Guide to Compliance (2023)](https://sumsub.com/blog/what-is-the-fatf-travel-rule/)​

​[The Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulation 2022](https://www.legislation.gov.uk/uksi/2022/860/regulation/5/made) is the key law explaining the specifics of the Travel Rule in the UK. There is no information regarding the de minimis threshold, which means that certain information should be transferred regardless of the transaction amount.

For certain transactions equal or exceeding 1,000 euros, there are some additional requirements. This includes international transfers as well as transactions involving unhosted wallets.

As a rule, VASPs (cryptoasset exchange providers and a custodian wallet providers in the UK) have to take the following steps to comply with the Travel Rule:

1) In respect of an inter-cryptoasset business transfer, the originating VASP must ensure that the transfer is accompanied by the following information:

1. 1.

the name of the originator and the beneficiary

1. 2.

if the originator or beneficiary is a firm, the registered name of the originator or beneficiary (as the case may be), or if there is no registered name, the trading name

1. 3.

the account number of the originator and the beneficiary, or if there is no account number, the unique transaction identifier.

If the beneficiary VASP request additional information about the sender, the originating VASP should also transfer the following information within 3 days, provided each VASP is conducting business in the United Kingdom:

(a) if the originator is a firm—

* the customer identification number or
* the address of the originator’s registered office, or, if there is none, its principal place of business
* if the originator is an individual, one of the following—
* the customer identification number
* the individual’s address
* the individual’s birth certificate number, passport number, or national identity card number
* the individual’s date and place of birth.

If a VASPs is carrying out business outside the United Kingdom and the transaction is equal to or exceeding 1,000 euros in value, the originating VASP should ensure that the transfer is accompanied by all the information specified in paragraph 1 (clauses a, b, c + a or b).

2) Information relating to the originator must be verified by the originating VASP using documents or a reliable source independent of the person whose identity is being verified.

3) When a Beneficiary VASP receives a crypto-asset as part of an inter-cryptoasset business transfer it must, before making the crypto-asset available to the beneficiary, check whether —

(a) it has received the information required by regulation to be provided; and

(b) the information relating to the beneficiary corresponds with information verified by it during customer due diligence.

4) Where the Beneficiary VASP becomes aware that any information required by regulation to be provided is missing or does not correspond with information verified by it, it must—

* request that the originating VASP provides the missing information;
* consider whether to make enquiries as to any discrepancy between information received and information verified during the CDD process; and
* where the Beneficiary VASP becomes aware that any information required to be provided is missing or does not correspond with information verified during customer due diligence, it must consider whether—

(i)to delay making the cryptoasset available to the beneficiary until the information is received or any discrepancy is resolved; and

(ii)if the information is not received or if any discrepancy is not resolved within a reasonable time, to return the cryptoasset to the cryptoasset business of the originator.

5) The beneficiary VASP must report repeated failure by a crypto-asset business to provide any information required as well as any steps the crypto-asset business of the beneficiary has taken in respect of such failures to the FCA.

6) A crypto-asset business must respond fully and without delay to a request in writing from a law enforcement authority for any information in connection to these requirements.

Please check out [Sumsub’s Travel Rule guide](https://help.sumsub.com/products/united-kingdom) for the requirements in relation to the transfers with unhosted wallets and any further details.

### The future of crypto regulations in the UK

For the last several years, the UK has been working towards a more regulated crypto industry. The country’s latest [plans were announced](https://www.gov.uk/government/news/uk-sets-out-plans-to-regulate-crypto-and-protect-consumers) in February 2023, including:

* Strengthening rules for crypto trading platforms
* Creating a world-first regime for crypto lending
* Implementing new rules to protect customers from market manipulation (e.g., pump and dump schemes)

According to the “Future Financial Services Regime for Crypto Assets” [Consultation document](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1133404/TR_Privacy_edits_Future_financial_services_regulatory_regime_for_cryptoassets_vP.pdf), the UK plans to widen the scope of regulated crypto activities, including activities with stablecoins. This includes:

* Issuance
* Payment
* Exchange
* Investment and risk management
* Lending, borrowing, and leverage
* Safeguarding and/or administration
* Validation and governance

The proposed regulatory regimes will be divided into phases. To learn more, you can read pages 27-28 [here](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1133404/TR_Privacy_edits_Future_financial_services_regulatory_regime_for_cryptoassets_vP.pdf).

The “Future Financial Services Regime for Crypto Assets” also specifies a primary aim to expand “specified investment”.

Moreover, the HM Treasury now proposes to monitor crypto asset activities in the United Kingdom. This would monitor activities provided by UK firms to persons based in the UK or overseas (natural and legal), as well as those provided by overseas firms to UK persons (natural or legal).

# US - Crypto Regulations

The US regulatory framework for cryptocurrencies is complex and still developing. Companies in this space need to stay updated with the latest developments and be ready to adapt to changes. A verification solution is crucial for compliance with regulations and preventing illegal activities.

**US Crypto Regulation Landscape**: The US is still in the process of creating an efficient set of digital asset regulations. The regulatory landscape is complex due to the involvement of multiple regulators with overlapping responsibilities.

**Regulators**: The main federal institutions regulating digital assets in the US include the Financial Crimes Enforcement Network (FinCEN), the Securities and Exchange Commission (SEC), and the Commodity Futures Trading Commission (CFTC). The specific regulator involved depends on whether a digital asset is classified as a money transmitter, security, or commodity/derivative.

**Who is Affected?**: Regulations apply to entities defined as "financial institutions" under the Bank Secrecy Act (BSA), which includes money services businesses, securities brokers/dealers, futures commission merchants, introducing brokers in commodities, and mutual funds. Several business models involving the transmission of digital assets are also considered regulated under certain circumstances.

**Regulations**: The Bank Secrecy Act, the US Patriot Act, and the Anti-Money Laundering Act provide the framework for regulation. There are also registration requirements under the Commodity Exchange Act and Securities Exchange Act for assets considered securities and commodities.

**Crypto Mining**: Mining cryptocurrency is legal in all US states, but some states may impose limits due to environmental concerns. For example, New York state introduced a temporary two-year moratorium on certain types of crypto mining.

**Compliance**: Companies dealing with digital currencies must comply with the BSA and be registered with FinCEN, SEC, and CFTC, depending on the nature of the assets. They also need to follow state-level regulations. In addition, companies must establish an Anti-Money Laundering (AML) program, a Customer Identification Program (CIP), and satisfy recordkeeping and reporting requirements.

**State Differences**: Each US state might have its own regulations and licensing procedures for digital assets, although cryptocurrencies are legal in all states.

## ZKP in DeFi

Zero-knowledge proofs can also enable a DeFi service user to confirm that their identity has been verified without revealing personal information.

— [Illicit Finance Risk Assessment of Decentralized Finance](https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf), U.S. department of the treasury, April, 2023

The [report](https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf), authored by the Treasury Department, pointed to the growing use of cryptocurrency to pay for goods and services as a threat to government attempts to limit money laundering and the financing of terrorism. Among a series of recommendations to prevent money laundering via crypto, one example was buried deep within the report: privacy-enhancing tech.

The authors wrote that “the U.S. government supports privacy enhancing technologies that simultaneously allow for or even promote compliance with AML/CFT obligations.” Still, it noted that “the use of non-public blockchains” by non-compliant entities “will heighten AML/CFT risks.”

Several pages later, the report notes that zero-knowledge proofs can be used to verify that someone has passed an anti-money laundering check without harvesting or broadcasting their personal information.

— [Treasury: ZK Proofs Can Be Boon Or Bane Of AML Compliance](https://thedefiant.io/treasury-defi-report), The Defiant, Aleksandar Gilbert April 07, 2023

<https://docs.zk.me/zkme-dochub/zkkyc-compliance-suite/regulatory-framework>