Bitstamp

A Guide to Crypto Regulations and Compliance

Bringing clarity over complexity around the world.

Table of Contents

Introduction

As mainstream financial institutions enter the cryptocurrency space, many new players are seeking clarity on exactly how this asset class is regulated. They want assurance that their crypto assets—and those of their customers—have protection from fraud and cybercrime, and they want to know about the regulatory requirements that they must meet.

by The Bitstamp Compliance Team

In this guide, we'll provide:

- A broad overview of how crypto regulation has developed over time,
- How it compares to traditional finance regulation and
- The basic elements of a sound crypto compliance program

We'll then cover regulatory developments in key markets worldwide including the **United States, Europe, Asia-Pacific and Latin America.**

An Evolving Regulatory Landscape

Many people who aren't familiar with cryptocurrency assume that it is lightly regulated or even unregulated but this is not the case. **In many jurisdictions, cryptocurrency exchanges are subject to the same anti-money laundering (AML) and know your customer (KYC) requirements as traditional finance institutions** and, due to the novel characteristics of blockchains and crypto assets, may have unique or more effective tools to meet those requirements.

But though the rules are in many cases the same as for traditional assets, the nature of cryptocurrency adds complexity. Cryptocurrency is transacted in a borderless, electronic environment. Wallets aren't bound by geographic location, and as a result many cryptocurrency companies have customers from all over the world. By contrast, traditional finance developed in the pre-digital age when customers were more likely to patronize financial institutions close to them; financial institutions naturally concentrated their activities in certain geographic areas.

Cryptocurrency exchanges often serve customers in many jurisdictions where cryptocurrency regulation can vary significantly. For instance, Canada applies many typical securities regulations to cryptocurrency trading, which means that a suitability standard is often applied to purchases of these assets. The Monetary Authority of Singapore (MAS) has issued guidelines for advertising in the crypto industry, which state that companies are discouraged from marketing or advertising their services to the general public. The guidelines are aimed at ensuring that advertising materials related to crypto products or services are not misleading or deceptive and provide accurate and balanced information to consumers.

The U.S. regulatory framework is unique in that commodity-derivatives trading is regulated by the Commodities Future Trading Commission (CFTC) while securities trading is regulated by the Securities and Exchange Commission (SEC). This is in addition to the differing regulatory treatment of cryptocurrency by individual state regulators. That's complicated enough on its own but additionally there is still uncertainty about how these regulations should be applied to digital assets. It's not entirely clear, for instance, what should be classified as a commodity and what should be classified as a security.

Cryptocurrency has unique features and functionalities that make it difficult to categorize—as a commodity, a security or a digital currency. Different countries may classify it differently too, creating additional complexity. There isn't any single cohesive regulatory scheme, although this may be changing as the market evolves to serve a growing number of traditional finance institutions.

The Core Components Of Crypto Compliance

Most established crypto companies have compliance programs in place which typically include:

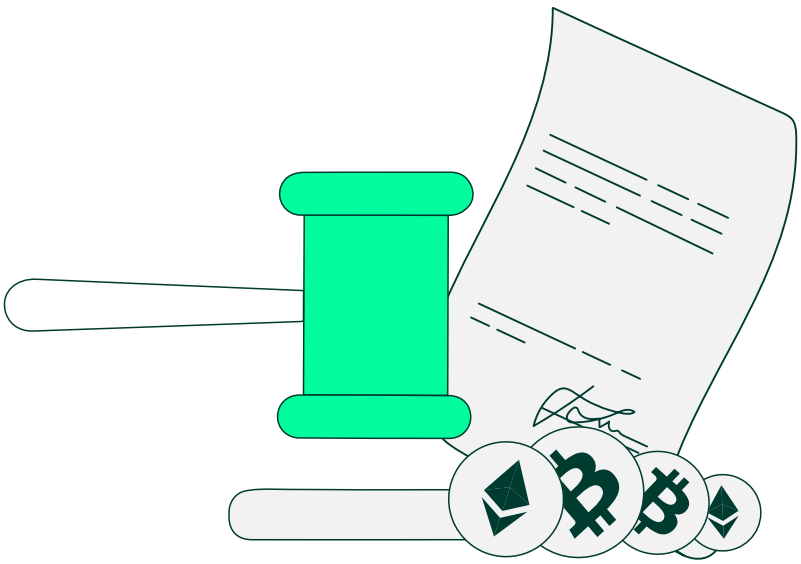
A chief compliance officer with broad authority and high visibility among the company's senior leadership team.

Documented policies and procedures on how to handle matters across every aspect of compliance, from customer onboarding, to AML, sanctions, transaction monitoring, anti-market manipulation, customer complaints, regulatory exams and audits.

A risk-based approach which identifies the highest compliance risks to the organization and focuses controls, policies and procedures on managing these risks.

Regular reporting and monitoring with well-defined procedures for sharing information with regulators, law enforcement and tax authorities.

Certified compliance officers with accreditation such as the Association of Certified Anti-Money Laundering Specialists (ACAMS) or Certified Regulatory Compliance Manager (CRCM) designations.



Transaction Monitoring And Blockchain Forensics

One common misconception about cryptocurrency is that transactions are completely anonymous, making it difficult to know where funds are coming from or whether they have been involved in criminal activity. But in fact, for most blockchains, transaction data is publicly visible which provides unique insight into the entire history of a cryptocurrency wallet or movement of funds. This is a unique advantage of cryptocurrencies and can be extremely helpful in structuring all kinds of compliance functions, including AML, KYC, sanctions compliance and counter-terrorism programs.

In recent years, the increasing effectiveness of these transaction monitoring tools has made hacking less profitable for criminal organizations. Illicit activity in cryptocurrency has continued to grow in absolute terms but in 2022 it accounted for a very small portion of total crypto activity, representing just 0.24% of all transactions.[1]

Blockchain analytics can help companies identify and freeze stolen cryptocurrency, so that the criminals can no longer withdraw it from their platforms. In some cases, white hat hackers, individuals who use their hacking skills ethically to help identify security vulnerabilities, will unlock these assets and return them to their rightful owners for a modest reward. In other instances, the hackers themselves may return all or part of the assets they have stolen in exchange for a reward once they realize these assets have been frozen.

In August 2021, for instance, a hacker stole $600 million worth of cryptocurrency from the Poly Network platform, then returned all of it within a few weeks.[2] In another major case, the U.S. government was able to retrieve half, or $2.3 million, of the ransom paid in the Colonial Pipeline attack, which shut down gas stations all over the southeastern United States in 2021.[3]

While transaction monitoring tools cannot identify individuals on the other end of a transaction, they can help make it possible to determine whether a transaction is coming from a criminal entity or whether it is going to sanctioned organizations. By looking at both the source and destination of funds for various wallets, they can identify suspicious patterns that can indicate potentially risky or illicit activity. Due to these tools and a coordinated effort among companies in the cryptocurrency space, it has become increasingly difficult for criminal networks to cash out and benefit from the proceeds of their criminal exploits. Tellingly, many continue to favor physical cash for their exploits. A 2020 report from Europol noted that while criminals do use cryptocurrency for a variety of illicit activities, "Criminals and criminal networks involved in serious and organized crime also continue to rely on traditional fiat money and transactions to a large degree."[4]

[1] 2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking" Chainalysis, January 12, 2023.
[2] "Hacker behind $600 million crypto heist returns final slice of stolen funds," CNBC, August 23, 2021.
[3] "How A New Team Of Feds Hacked The Hackers And Got Colonial Pipeline's Ransom Back," NPR, June 8. 2021.
[4] "Cryptocurrencies: tracing the evolution of criminal finances," Europol, January 26, 2022.

AML & KYC

In many jurisdictions, cryptocurrency service providers are subject to the same AML and KYC regulations as traditional finance organizations. In broad terms, cryptocurrency exchanges must maintain a record of who their customers are and monitor transactions for suspicious activity, just as banks and brokerage firms do. That includes ensuring that their customers are not engaged in money laundering.

Consider that money launderers using cryptocurrency often move funds rapidly through hundreds of wallets when trying to obscure the origins of illicit funds. Blockchain forensics provide access to a record of the cryptocurrency's history and can flag problematic transactions that originate in likely criminal addresses.

When this occurs, cryptocurrency exchanges, just like traditional finance institutions, are required to file Suspicious Transaction Reports (STRs) or Suspicious Activity Reports (SARs) to notify government financial intelligence units (FIUs) of unusual transactions.

Controls on how much customers can deposit or withdraw within a set time period can also help limit the damage from bad actors. Deposit limits make it harder to launder money into clean accounts. Withdrawal limits slow losses from fraud and hacking.

Compliance professionals at cryptocurrency exchanges often have decades of experience in the traditional finance world and are able to apply this knowledge and expertise to building out proper AML and KYC policies and procedures.

Sanctions And Counter-Terrorism Measures

AML compliance slows the flow of illicit funds into the financial system. Sanctions and anti-terrorism regulations stop flows going in the other direction, from the financial system to illicit organizations. In both cases, cryptocurrency organizations follow the same rules as traditional finance organizations.

Regarding sanctions, for instance, in the U.S., the Office of Foreign Asset Controls (OFAC) publishes a continually updated Specially Designated Nationals and Blocked Persons list. OFAC prohibits U.S. institutions and individuals from transacting business with any entity on this list, whether in fiat currency or cryptocurrency. OFAC also now sanctions specific wallet addresses known to be controlled by sanctioned entities. In September 2022, OFAC added to their SDN list the cryptocurrency addresses of a suspected Iranian-based ransomware group believed to be behind ransomware attacks on a children's hospital, a utility company, and the infrastructure of a city in the U.S. state of New Jersey.

The Council of the EU also has broad power to issue sanctions, most recently in 2022 acting to place restrictions on transactions involving entities in Russia and the Russia-controlled regions of Ukraine, including both traditional assets and cryptocurrency.
Financial institutions globally must follow anti-money laundering regulations that require them to assess their risk and exposure to financing terrorism, monitor suspicious transactions and identify and exclude entities affiliated with terrorist activity from their customer base.

Examples of how cryptocurrency exchanges apply these rules include the possibility to block customers. For instance, they can block customers from jurisdictions that are sanctioned or suspected of funding or otherwise aiding terrorism by screening for IP addresses and identify users who are trying to get around those blocks. Going further, blockchain analytic tools can help identify customers who are not sanctioned themselves but have potential exposure to sanctions. These tools can look through rapid bursts of transactions—sometimes dozens within minutes and all by the same entity—to find links to illicit addresses.

Cryptocurrency firms also work collaboratively with law enforcement and government FIUs, reporting on any entities that they have blocked due to sanctions and terrorism controls. This provides authorities with additional information about how sanctioned entities operate and manage their cash flows.

Cybersecurity

Financial institutions in the crypto space have a responsibility to protect their customers from hacks, malware, and other criminal attacks. Preventing theft and fraud is especially important in the cryptocurrency space because it is effectively impossible to reverse transactions. Cryptocurrency is similar to a "digital bearer" asset, so if funds are stolen, legal routes are available but there is often limited recourse.

To help customers protect their assets, robust cybersecurity practices, including two-factor authorization, can prevent hackers from gaining access to their information or accounts.

Customer education is equally important and crypto firms have invested in providing detailed information to the public about how to recognize and prevent cyberfraud.

The Travel Rule

To combat fraud, money laundering and terrorism financing, the Financial Action Task Force (FATF) adopted the Travel Rule specifically for cryptocurrencies in 2019. This rule states that FATF member countries (i.e., G-7 and about 30 other countries) must require crypto companies in their jurisdictions to provide information to their transaction's counterparty institution on any party that sends or receives crypto assets above a certain threshold. This information is recommended to include inter alia the names of the sender and the recipient, the address of the sender, and the account numbers of both the sender and the recipient. FATF member countries are able to interpret the guidance and implement rules specific to their jurisdiction.

The rule essentially subjects crypto transfers to the similar rules that for years have been in place for other types of funds transfers, for example wires. Because cryptocurrencies can be sent from a user's account at an institution to a wallet managed by an individual and vice versa, the practicalities of sending recipient or sender information are more challenging. This information cannot be added to the transaction record on the blockchain itself. Adding this information to the transaction record also creates privacy concerns. However, specialized firms have developed solutions to help cryptocurrency exchanges comply with the Travel Rule.

Anti-Market Manipulation

In a still developing area of cryptocurrency compliance, regulators have recently shifted their focus to developing and implementing anti-market manipulation rules. These requirements for surveillance and controls are designed to ensure market integrity and prevent many of the same manipulation techniques used in traditional financial markets, such as spoofing, pump and dumps, wash sales and other schemes, designed to fraudulently influence the value of assets. The EU's Markets in Crypto Assets (MiCA) framework includes specific provisions around consumer protection and market integrity. Similarly, in the United States, various proposals such as the Digital Commodity Exchange Act seek to clarify legal and regulatory requirements to strengthen market integrity.

Customer Protection And Education

Disclosure of the unique characteristics and risk of cryptocurrency are an important part of compliance. For instance, regulators require that cryptocurrency firms disclose to customers that cryptocurrency transactions may not be reversible. Customer education can go hand in hand with these minimum requirements to help customers understand more about how cryptocurrency works and how they can keep their assets safe.

Crypto firms have developed resources to address this need, from introductory materials focused on concepts at a broad level to detailed explainers specific to certain technologies and trends. Bitstamp, for instance, maintains a Learn Center consisting of guides, how-to articles, and videos on a wide array of crypto topics.

An Overview Of The Regulations Around The World

We've discussed basic elements of cryptocurrency compliance that are common to most jurisdictions. Now we'll look at how the regulatory landscape is evolving in major financial markets around the world.

The United States

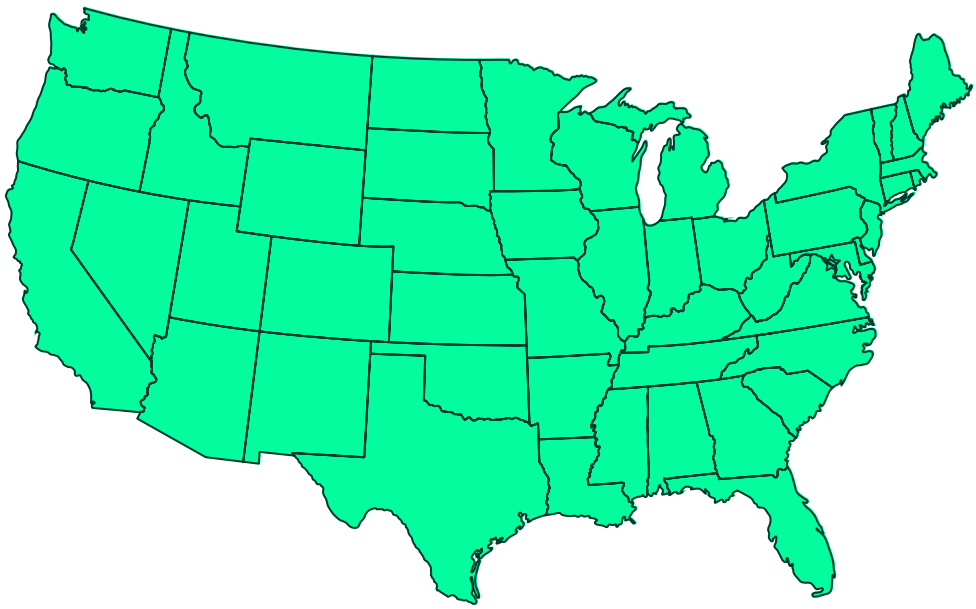
President Joe Biden's Administration focused its attention on cryptocurrency regulation in the U.S. with its March 9, 2022 "Executive Order on Ensuring Responsible Development of Digital Assets." The Executive Order requested input from regulators on how to enhance cryptocurrency market safety and transparency. The Administration released a framework for regulating cryptocurrency in September 2022, as well as plans for working with other governments to align on rules globally.[5] However, the framework was short on actionable policy items and much further work remains to be done.

Clearer rules may well come from a variety of Senate bills that were introduced the same year. The Responsible Financial Innovation Act, sponsored by Senators Cynthia Lummis (R., Wyo.) and Kirsten Gillibrand (D., N.Y.) would significantly clarify regulations around cryptocurrency in the U.S.[6] The bill would give the CFTC a primary role in overseeing cryptocurrency. It would also, for the first time, define which types of digital assets are commodities and under the CFTC's purview, and which are securities and regulated by the SEC. This would provide cryptocurrency market participants with an enhanced ability to understand and fulfill their regulatory obligations.

[5] "Treasury Outlines International Engagement on Digital Asset Regulations," WSJ.com, July 8, 2022.

Another bill, The Digital Commodities Consumer Protection Act, emerged out of the Senate Agriculture, Nutrition and Forestry Committee. Sponsored by Senators Debbie Stabenow (D., MI) and John Boozman (R., AR), this bill would give the CFTC sole oversight over crypto market regulation.[7] The bill raised questions among cryptocurrency industry veterans pertaining to the treatment of software application developers and other participants for whom the definition of "broker" does not apply. The Senate Committee held additional hearings on the bill after the collapse of cryptocurrency exchange FTX, whose founder and CEO was a vocal proponent of the bill; the committee has considered additional conflict of interest and financial disclosure provisions to prevent future market failures.[8]

Digital currencies are also regulated at the state level. Cryptocurrency businesses located or conducting business in New York State, for instance, must obtain a BitLicense. The state of Louisiana is the most recent to require crypto businesses to obtain virtual currency business licenses. Major states, such as California, are pushing for laws to regulate crypto exchanges and more states are expected to follow suit. In addition, most states require crypto businesses to obtain money transmitter licenses, currently the main state level regulatory regime for virtual currency activity.



[6] "Lummis-Gillibrand Responsible Financial Innovation Act Section-by-Section Overview," Office of Kirsten Gillibrand, July 28, 2022.
[7] "The Digital Commodities Consumer Protection Act Closes Regulatory Gaps," U.S. Senate Agriculture, Nutrition and Forestry Committee
[8] "CFTC chairman urges strengthening conflict-of-interest part of Senate crypto bill," Roll Call, December 1, 2022.

Europe

In European Union (EU) the Markets in Crypto Assets (MiCA) is expected to enter into force in April 2023, providing for the first time a unified European market with consistent rules across countries and jurisdictions.

New rules will require stablecoins like Tether and USDC to maintain sufficient liquidity to meet redemption requests. The legislation also gives the European Securities and Markets Authority the power to ban or restrict cryptocurrency platforms that don't properly protect investors or that threaten market integrity or financial stability.

The main benefit of MiCA, however, will be in creating a broad, well-regulated market for cryptocurrencies, with consistent, predictable requirements. This added stability will enable additional innovation in the cryptocurrency markets.

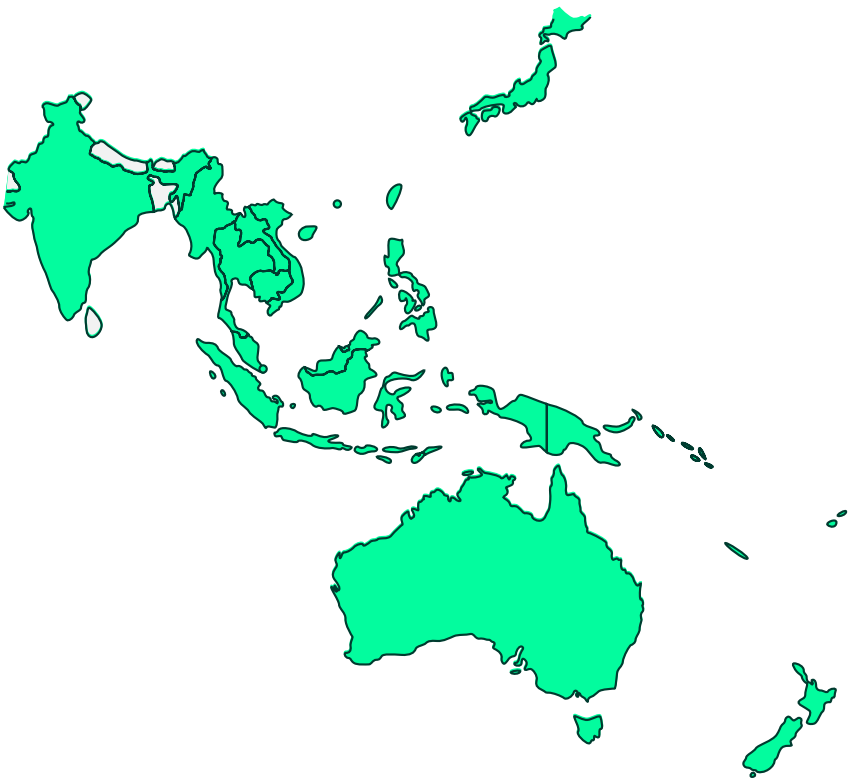
Asia-Pacific

Asia encompasses a wide range of regulatory regimes from China's outright ban on crypto transactions and crypto services, to accommodative jurisdictions like the Philippines, which has gone as far as recognizing cryptocurrency as legal tender.

Singapore, which has long set a high bar for regulation in the Asia-Pacific region, said that it will not ban crypto investing for retail investors as it is not viable considering the borderless nature of crypto exchanges. However, the Monetary Authority of Singapore (MAS) is concerned that individual investors may not understand the risks inherent in trading digital assets. The MAS has recommended a qualifying test for individuals to demonstrate that they understand these risks—and is proposing a ban on credit card purchases of digital assets.[9]

Since 2018, Hong Kong's Securities and Futures Commission (SFC) has only permitted "professional investors," or individuals with more than $1 million in wealth, to invest in digital assets, but they have more recently considered enabling a broader range of retail investors to participate. Hong Kong developed a regulatory framework for its crypto market in 2019, which requires all exchanges to be licensed by the SFC.[10]

Australia has taken important steps towards creating a regulatory framework for cryptocurrency as well. In October 2021, the Australian government released recommendations including establishing a licensing regime for digital currency exchanges, developing standards for custody and depository institutions holding cryptocurrency assets, researching cryptocurrencies currently owned and traded in Australia, creating a standardized Decentralized Autonomous Organization (DAO) company structure and applying existing anti-money laundering, counter-terrorism and tax laws to digital assets.



[9] "Singapore may soon require retail investors to take test before trading crypto, prohibit credit cards," Tech Crunch, October 26, 2022.
[10] "Hong Kong Mulls Letting Retail Investors Trade Crypto, Removing 'Professional Investor-Only Requirement'" Bitcoin.com, October 20, 2022.

Latin America

Cryptocurrency has a strong appeal in underbanked Latin American economies, where foreign remittances play a key role. El Salvador made headlines in 2021 when it adopted Bitcoin as legal tender,[11] and many countries in the region regulate digital assets lightly, if at all.

That may be changing in Brazil, Latin America's largest economy. In April 2022, the Brazilian Senate passed its first bill governing cryptocurrencies, a significant step towards creating a regulatory framework for digital assets. The new bill gave oversight to the country's executive branch, which would be responsible for formulating rules and designating a regulatory body—either an existing one like the Securities and Exchange Commission or the Central Bank of Brazil or a new one created specifically for the cryptocurrency marketplace.[12]

Another major Latin American market, Mexico, has long prohibited cryptocurrency. However, lawmakers have more recently began exploring legislation similar to El Salvador's, which if adopted, would make Bitcoin legal tenderw.[13]

[11] "A year on, El Salvador's bitcoin experiment is stumbling," Reuters, September 7, 2022.
[12] "Brazil's Senate approves 'Bitcoin law' to regulate cryptocurrencies," Cointelegraph, April 7, 2022.
[13] "Mexican senator to propose crypto law: 'We need Bitcoin as legal tender,'" Cointelegraph, February 23, 2022.

How Experienced Teams Can Streamline Compliance

The cryptocurrency regulatory landscape is complex. It varies by jurisdiction and is always changing. Some market participants can handle these demands with their own team and resources. Others require varying levels of assistance and expertise.

Experienced cryptocurrency exchanges have been deeply familiar with compliance requirements and trends for many years, working closely with legislators and regulators to shape a regulatory environment that supports their clients' business activities. We've identified three key issues of focus:

Replicating best practices from traditional finance in key areas including AML, KYC, sanctions screening and CFT measures, as well as consumer protection operations.

Leveraging blockchain analytics for a deeper, more nuanced view of transactional activity—as well as combating fraud, criminal activity and sanctions evasion.

Educating and providing insight to clients about evolving legislation, shifts in transaction activity and new approaches to compliance.

At Bitstamp, we offer a modular cryptocurrency infrastructure service for firms looking to rapidly enter the space in response to demand from their own customers. **These sit within a Bitstamp as a Service solution** umbrella and range from a foundational crypto exchange platform where you perform all compliance operations, all the way to a full-service offering where we take care of compliance requirements including licensing, customer onboarding, and AML/CFT, in addition to providing first and second level customer support. You can choose the service module that fits your needs, with the confidence that our experts are keeping your infrastructure and compliance efforts current with an ever-changing regulatory and market landscape.

Get in touch

Let's talk!

Send an email to
partners@bitstamp.net

Find additional resources

Want to learn more?
bitstamp.net/institutional-trading/