RESEARCH
by COINTELEGRAPH

NEW CRYPTO EXCHANGE STANDARDS

A comparison of crypto exchanges
in a globalized world

INTRODUCTION

Decoupling money from the government has been at the very core of crypto's philosophy. This is why many ideological streams within the community are outright hostile toward any attempts to comply with governments and regulators. However, some may argue that this lax attitude has given bad actors free reign. The use of non-compliant offshore exchanges is normalized among the crypto community on YouTube and X. The resulting business has encouraged bad business practices on these exchanges to run rampant, putting customer funds at risk.

It is no wonder that the crypto industry had to undergo lessons that traditional finance has already learned. The year 2022 saw a historic breakdown of users' trust in exchanges and other crypto service providers. Previously, many implicitly assumed that large corporate entities would always honor common-sense fiduciary duties toward their customers. However, the prominent collapses of FTX and Celsius proved that bad business practices can happen in corporations of any size. A sleek website, high trading volume or prime-time television ads are no guarantee that customers' savings will be safe.

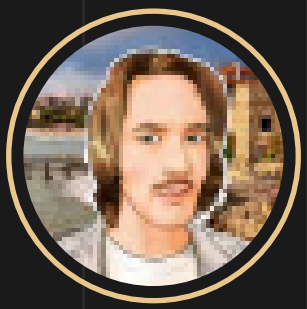
To achieve true mass adoption, crypto needs to be brought into regulatory frameworks. This doesn't mean giving up on the principles of decentralization and privacy, but rather finding a balance where these principles can coexist with legal and financial safeguards.

Regulatory clarity and compliance, especially those directed to protect customers, would increase trust among potential users and open opportunities for institutional investors and businesses to enter the crypto space. We ought to create an ecosystem where the benefits of crypto are accessible to everyone while minimizing the risks of fraud, money laundering and bad business practices that might put your cryptocurrencies in jeopardy.

This report was written to compare centralized exchanges in the retail space and assess how well they align with this objective. It is motivated by the goal of increasing users' financial literacy with respect to the products and services they use, including on- and off-ramps, spot trading, derivatives and earn products. Our report provides an overview of how these popular products work and, correspondingly, what their risk profiles are.

Furthermore, we compare jurisdictions according to the protections they afford to domestic and overseas customers. This includes information of special interest to risk-averse spot customers, namely evidence for segregated funds, custody solutions, cybersecurity, crypto reserve audits and insurance coverage. The centerpiece of our analysis is several comparison tables highlighting our key findings for nine popular exchanges: Binance, Bit2Me, Bitfinex, Bitstamp, Bybit, Coinbase, HTX, Kraken, OKX.

AUTHORS



Ilya Lazarev
Research Analyst

Nikita Malkin
Senior Researcher

Exchanges	Binance	Bit2Me	Bitfinex	Bitstamp	Bybit	Coinbase	HTX	Kraken	OKX
	Legal protections for customers								
Jurisdiction of corporate headquarters	Cayman Islands	Spain	Hong Kong	U.K.	UAE	U.S.	Seychelles	U.S.	Seychelles
Headquartered jurisdiction in tax haven	Yes	No	Yes	No	Yes	No	Yes	No	Yes
Pro-customer jurisdiction score	2	5	3	5	3	4	1	4	1
Does it have KYC?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Security of Assets								
Cybersecurity Score (out of 10)	6,25	8	5.75	6.75	7.5	7.5	5	8	5.5
Custody provider (for crypto holdings)	Ceffu (Former Binance Custody)	Ledger enterprise	Zodia Custody	BitGo	1st Party	Coinbase Custody	HTX Custody	1st Party	Komainu (Instituional)
Insurance coverage of assets	>$1 billion SAFU fund	150M euros (on custodian side)	No	$250M (on custodian side)	No	No	SAFU fund (recently launched)[1]	No	No
Proof of reserves or equivalent	Merkle tree, zk-SNARK(Mazars Company till 2022)	Merkle tree (Hacken)	None (only published wallets on github)	N/A, but audited by Ernst & Young	Merkle tree (no third party named)	Merkle tree N/A, but audited by Deloitte	Merkle tree (no third party named)	Merkle tree (Armanino LLP)	zk-STARK(no third party named)
Fiat deposit coverage (EUR)	Uncertain	100% of money deposited	100% of money deposited	100% of money deposited	100% of money deposited	100% of money deposited	Uncertain (insufficient data)	100% of money deposited	No fiat deposits
	User Experience								
Interface Friendliness Score (A to D)	C	A	D	B	B	C	C	A	B
Customer Support Score (out of 10)	4	8	6	5	5	3	3	5	3
Tax Reporting Tool	Yes	Yes + online consultant	Yes	Yes	Yes	Yes	No	Yes	No
	Products and services								
Serves Institutional or Business customers?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Asset support	350+	240+	170+	80+	888	150+	700+	200+	320+
Product range (out of 8 products)	7	6	6	3	8	6	7	4	7
Number of fiat currencies supported	11	2	4	3	6	3	12	7	N/A

[1]Audit results will be published in December, 2023

TABLE OF CONTENTS:

A Comparison of B2C and B2B Exchanges in a Globalized World 1

INTRODUCTION

1. LEGAL PROTECTIONS FOR CUSTOMERS 5

1.1 Pro-Customer Jurisdictions: 5
1.1.1 Security of Personal Data
1.1.2 Customer Protection Laws and Financial Transparency
1.1.3 Tax Haven Status
1.1.4 License for Promoting or Servicing Cryptocurrency

1.2 Exchange KYC 10
1.3 History of Legal and Regulatory Disputes

2. SECURITY OF CUSTOMER FUNDS 14

2.1 Crypto Assets 14
2.1.1 Crypto Reserve Audits
2.1.2 Crypto Custody Providers and Insurance of Crypto Assets

2.2 Fiat Deposits 16
2.3 Cybersecurity 18

3. USER EXPERIENCE: INTERFACE / CUSTOMER SERVICE / TAX REPORTING 20

3.1 Interface 20
3.2 Customer Service 21
3.3 Tax Reporting Tools 22

4. GENERAL OVERVIEW: ASSET SUPPORT AND PRODUCT COMPARISON 24

4.1 Product Range 24
4.2 Spot Trading 25
4.3 Derivatives and Their Risks 25
4.4 P2P Trading 25
4.5 Launchpad 26
4.6 Crypto Lending 26
4.7 Staking Services 27
4.8 Institutional or Business Customers Services 27

5. CONCLUSIONS 28

1. LEGAL PROTECTIONS FOR CUSTOMERS

1.1 Pro-customer Jurisdictions:

Which jurisdiction a crypto exchange is registered in holds great significance and ought to be one of the primary concerns of users when choosing where to open an account. There are broadly two reasons for this. Firstly, more thorough regulation for virtual asset service providers encourages platforms to build a more customer-centric and low-risk environment around crypto assets, even if this comes at the cost of offering fewer products. Secondly, there may be existing laws that are not specific to crypto businesses but still protect customers against bad business practices. The second aspect is of special importance at a time when specific crypto regulation is still in its infancy.

Much like the banking industry in the late 19th and early 20th centuries, cryptocurrency exchanges started as relatively unregulated businesses. However, this does not mean their customers were left completely unprotected. Most jurisdictions have laws that ensure financial transparency and protect users against various bad business practices, fraud and a lack of data protection. These laws and protections vary widely among countries. Therefore, without a comprehensive, global regulatory framework for cryptocurrency exchanges, customer protection as it relates to crypto exchanges heavily depends on the individual jurisdiction.

In some countries, exchanges can move their clients' assets into high-risk investments without minimum capital requirements or make trades against their users without repercussions. In others, the basic customer protection laws for financial services and basic financial transparency guard users against this. They may also prevent various kinds of fraudulent activity and subject businesses to regular audits to curtail malfeasances.

Despite this, basic provisions are insufficient to specifically protect crypto customers in some respects. This is why many regulators around the world, especially in the European Union, have started to move beyond ensuring basic user rights and Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) policies. There is an increasingly strong emphasis on the idiosyncrasies of cryptocurrency and its convergence with other regulations.

While comprehensive laws are still outstanding on a global scale, it is helpful to categorize jurisdictions according to whether they follow a pro-customer approach to legislation or are skewed toward the interests of companies. The following criteria are important to take into consideration.

1.1.1 Security of Personal data

Several jurisdictions have comprehensive frameworks for this, such as the General Data Protection Regulation (GDPR) of the EU or the Data Protection Act (DPA) of the United Kingdom. All of these are applicable to crypto exchanges as fintech companies. A number of jurisdictions also have similar legislation, but its structure and requirements may not be as comprehensive as those in the EU and the United Kingdom. Both Hong Kong's Personal Data (Privacy) Ordinance (PDPO) and the UAE's Personal Data Protection Law (PDPL), for example, have no principle of accountability and do not mandate privacy management measures, while the Personal Information Protection Act (PIPA) of South Korea has less clear and defined requirements for data processing compared to GDPR.

However, two jurisdictions in which exchanges are commonly located have no personal data provisions whatsoever. The Seychelles currently lacks any separate legislation on user data protection. In the United States, data protection regulation is handled on a state-by-state basis with laws like the California Consumer Privacy Act (CCPA). In states other than California, U.S. data protection is considerably weaker than its analogue in the European Union.

1.1.2 Customer Protection Laws and Financial Transparency

Protecting customers' rights and ensuring financial transparency are key objectives that a legal system needs to fulfill to keep companies in check. The laws that achieve this are generally not specific to virtual asset service providers but apply to all businesses. Nonetheless, they have special importance in an industry where people's savings are at risk.

Customer protection laws denote legislative measures that guard consumers from fraudulent business practices, defective products, dangerous goods and services, and breaches of contract. Rules like these form the bedrock of a reliable economy by enforcing basic standards of honesty in contractual dealings. They usually mandate a point of contact for the customers to file complaints and include basic provisions in the case of bankruptcy. Some laws on consumer rights also prohibit false advertising and various other fraudulent activities that are not already covered by criminal law.

1. LEGAL PROTECTIONS FOR CUSTOMERS

While most countries, with the exception of a few developing nations, have basic provisions for this in place, some legal frameworks are younger and less mature. For example, the Seychelles and the Cayman Islands only had dedicated customer protection acts introduced in 2022. However, general purpose consumer protection laws are still being used, mostly for offenses related to fraudulent advertising and ordinary scams. For example, in Italy, the eToro crypto platform was fined 1.3 million euros for providing consumers with misleading information about the cost of its services, while Spain and France even introduced dedicated requirements for social media influencers. This was in response to misleading advertising for crypto projects.

Financial transparency requirements are another tool used to protect customers. In the EU, UAE, Seychelles and the U.K., all companies, whether public or private and regardless of their size, have the obligation to prepare annual financial statements and file them with the relevant national business register. These financial statements must include the company's balance sheet, profits and losses, and addenda, such as details about long term debt commitments or possible liabilities not included on the balance sheet. In Europe, mid- and large-sized companies must further publish management reports that publicly display their management team, ownership structure and yearly operations.

In the U.S., on the other hand, only publicly listed companies are required to publish these financial statements, which means only Coinbase has the transparency that businesses in Europe, the U.K. or the UAE have by default.

In Hong Kong, companies, both private and public, must file annual financial statements. These statements must comply with the Hong Kong Financial Reporting Standards (HKFRS) issued by the Hong Kong Institute of Certified Public Accountants (HKICPA) and have to include a balance sheet, income statement, changes in equity, cash flow and accounting policies.

Moreover, the financial report must be audited before being filed in the company registry. In the Cayman Islands, financial reporting is required only for companies on the regulated sector list. This includes virtual asset service providers (VASPs). However, since the law on VASPs was passed very recently, the exact list of required financial statements is not yet fully defined and currently includes only an annual AML survey. In practice, financial statements are commonly prepared in accordance with generally accepted accounting principles (GAAP) or international financial reporting standards (IFRS) due to the international focus of business operations in the Cayman Islands.

Only three of the companies examined in this report have been audited: Coinbase, as its status as a public company requires it to be, and Bit2Me, which, from 2018 to 2021, voluntarily opted to be audited by RSM (in the Top 10 Firms by the International Accounting Bulletin 2023), despite this not being a legal requirement. In addition, Bitfinex was audited by Ernst & Young. Therefore, these three exchanges offer superior financial transparency over the others.

Exchanges	Binance	Bit2Me	Bitfinex	Bitstamp	Bybit	Coinbase	HTX	Kraken	OKX
HQ Jurisdiction	Cayman Islands[1]	Spain	Hong Kong	U.K.	UAE	U.S.	Seychelles	U.S.	Seychelles
Official name	Binance Holdings Limited	Bitcoinforme S.L.	iFinex Inc	Bitstamp Limited	Bybit FinTech FZE	Coinbase	Huobi Global Limited	Payward Ventures, Inc	Aux Cayes FinTech Co. Ltd
Public Financial Statements	Not found	Yes	Yes	Yes	Yes	Yes	Yes	Not found	Not found
Management Report	No	Yes	No	No	No	No	No	No	No
Audit	No	Yes, Voluntary (RSM)	No	Yes (E&Y)	No	No	Yes (Deloitte)	No	No

[1]Binance's exact headquarters location is currently undisclosed. CoinGecko lists the Cayman Islands as its jurisdiction of registration.
Source: ***CoinGecko, Coin Bureau***

1. LEGAL PROTECTIONS FOR CUSTOMERS

1.1.3 Tax Haven Status

If an exchange is headquartered in a tax haven, this can indicate that it is seeking out an environment with less financial transparency and does not follow a pro-customer approach to regulation. This sometimes allows such exchanges to provide a wider range of products and assets for trading, but the financial security of customers is generally at greater risk. International organizations such as the European Union, the International Monetary Fund (IMF), the Financial Action Task Force (FATF) and the Oxford Committee for Famine Relief (Oxfam) compile lists of tax haven countries.

The approach to classification differs from organization to organization and is sometimes influenced by geopolitical considerations. Nevertheless, the inclusion of a jurisdiction on these organizations' lists may indirectly suggest that the country's regulatory system may favor businesses over consumers.

Signing up to an exchange in a poorly regulated, overly business-centric jurisdiction can draw negative attention from domestic law enforcement or lead to account closures. It may also result in scenarios where business partners terminate their collaboration due to compliance concerns and suspicion of their offshore business partner.

Examples of such incidents abound. Recent regulatory pressure led Binance.US' banking partners to terminate their relationship with the exchange.

The customers who did not withdraw their U.S. dollar deposits in time faced a forced conversion to USD stablecoins. A similar event occurred for the European customers of the exchange, who were once urged to convert their EUR deposits to Tether (USDT) because of Binance's difficulty finding a new banking partner.

However, Binance is not the only crypto exchange that has struggled. Recent rule changes by the Financial Conduct Authority (FCA) in the U.K. also forced popular offshore derivatives exchange Bybit to shut its doors to U.K. customers and force the settlement of open derivatives contracts on the platform after a short notice period. For users, an unexpected termination of services is a severe nuisance at best and can result in stuck funds at worst. The table below provides an overview of which of the examined exchanges are in a tax haven under various classifications.

Exchanges	Binance	Bit2Me	Bitfinex	Bitstamp	Bybit	Coinbase	HTX	Kraken	OKX
HQ Jurisdiction	Cayman Islands[1]	Spain	Hong Kong	U.K.	UAE	U.S.	Seychelles	U.S.	Seychelles
Tax Haven?	FATF, IMF, Oxfam	No	Oxfam	No	FATF	No	IMF	No	IMF
Pro customer or pro company jurisdiction?	Pro company	Pro customer	Pro customer	Pro customer	Pro company	Pro customer	Pro company	Pro customer	Pro company

1.1.4 License for Promoting or Servicing Cryptocurrency

In recent years, many countries have formalized licensing processes for crypto exchanges and have thus set minimum standards for compliance. A license from the official financial authorities of a country with well-developed cryptocurrency legislation is a first — albeit non-exhaustive — indicator of its reliability.

The process of obtaining a VASP license to operate an exchange in well-developed European jurisdictions involves obtaining central bank registration, registering a legal address in the country, having a detailed business plan, as well as having AML staff and a full compliance team.

[1]Binance's exact headquarters location is currently undisclosed. CoinGecko lists the Cayman Islands as its jurisdiction of registration.
Source: ***CoinGecko, Coin Bureau***

1. LEGAL PROTECTIONS FOR CUSTOMERS

The most extensive licensing requirements are outlined in the previously mentioned MiCA Regulation, which is progressively being rolled out in the European Union. Under the new law's provisions, European crypto asset service providers (CASPs) will be required to acquire a distinct license and adhere to new regulatory obligations akin to those imposed on conventional financial service providers.

Other jurisdictions included in the comparison also impose their own set of requirements, except for the Seychelles, which has not yet implemented specific licensing regulations for crypto firms. Comparing the licensing processes is challenging due to varying legislative approaches and external factors. Nonetheless, it's feasible to pinpoint some common requirements for nearly all crypto licenses, such as central bank authorization, minimum capital requirements and AML/CFT procedures.

Of the jurisdictions surveyed, the most detailed measures to protect crypto customers, specifically, are presented in the EU's MiCA Regulation. Existing laws in EU countries already protect customers to a certain extent, but MiCA offers a stabler basis for this by making exchanges liable for damages and losses caused to their customers as a result of hacking or operational problems that need to be avoided.

In the case of cryptocurrencies, exchanges would be required to provide a white paper and take responsibility for any misinformation provided. In the U.K., some positive initiatives from the consumers' point of view are of note.

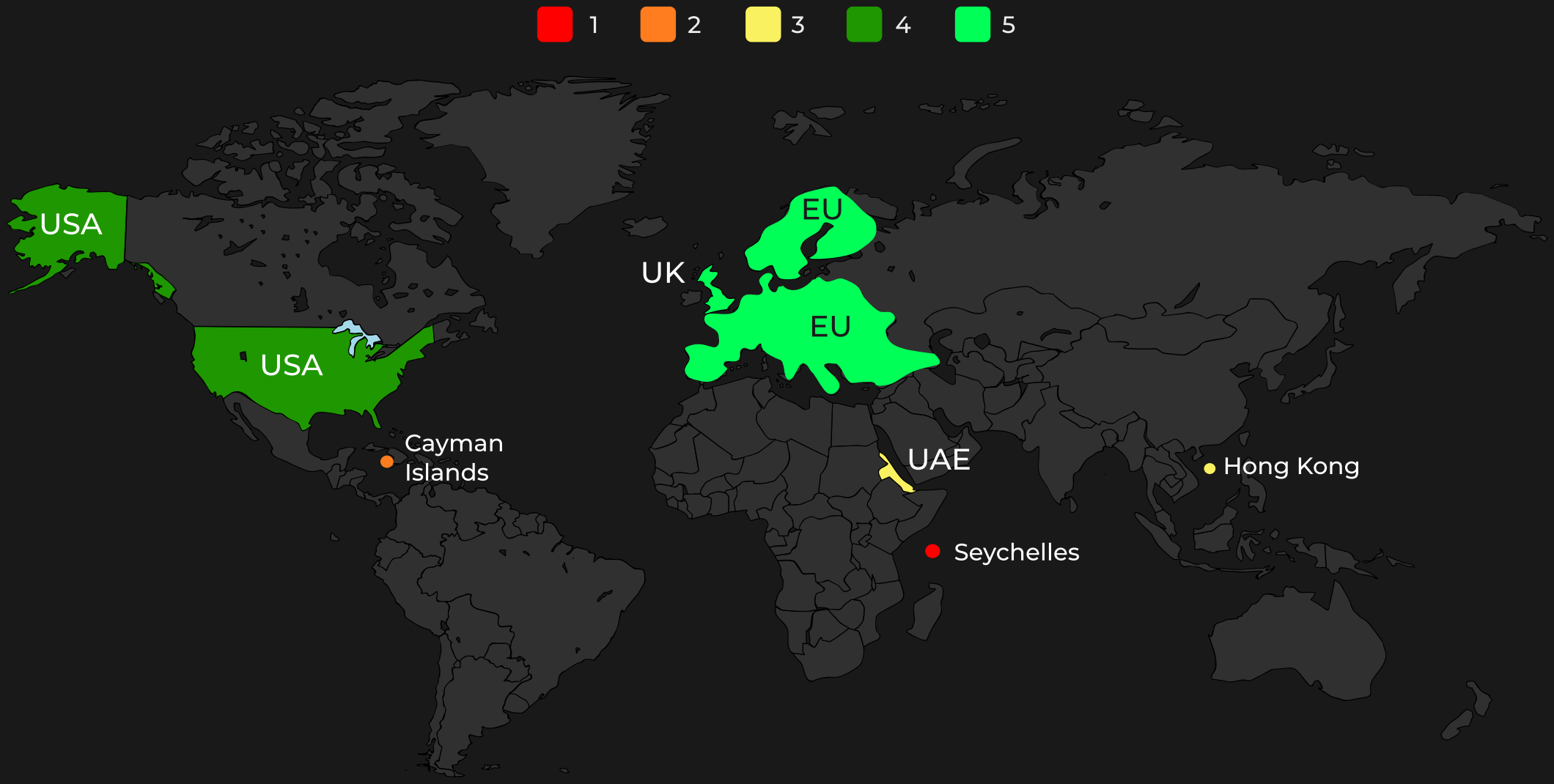
For example, the "Financial Promotion of Cryptoassets Regulations," introduced by the British Financial Conduct Authority (FCA), set strict requirements for the advertising of cryptocurrency-related products. In contrast, recent crypto legislation in the U.S. has demonstrated a greater emphasis on expanding the authority of regulatory bodies like the Commodities Futures Trading Commission (CFTC) and Securities and Exchange Commission (SEC).

This shift is evident in the legislative priorities. Regulatory agencies are being granted additional oversight and enforcement capabilities, whereas the development of comprehensive consumer protection measures has received comparatively less attention. A notable example of this trend is the Digital Asset Anti-Money Laundering Act recently discussed in U.S. Congress, which has received a portion of criticism from U.S. crypto-activists for potentially hindering the growth of the digital asset industry and forcing operations to jurisdictions with less security and regulation.

The expansion of consumer protection measures in the UAE and Hong Kong is under active discussion, but such laws are mostly in their draft stages. Given that both jurisdictions seek to position themselves as prominent crypto hubs, future measures will tend to be pro-business while having to avoid damaging the reputation of the jurisdiction for consumers.

Jurisdiction	User data protection measures	Customer protection measures	Financial transparency measures	License requirement	Is on tax haven lists?	Pro Company/ pro Customer Score (1 to 5)
Cayman Islands	+	-	-	+	FATF, IMF, Oxfam	2
EU	+	+	+	+	No	5
UK	+	+	+	+	No	5
Hong Kong	+	+	-	+	FATF	3
Seychelles	-	-	-	-	IMF	1
UAE	+	-	+	+	FATF	3
USA	-	+	+	+	No	4

Pro Company/ Pro Customer Score (1 to 5)



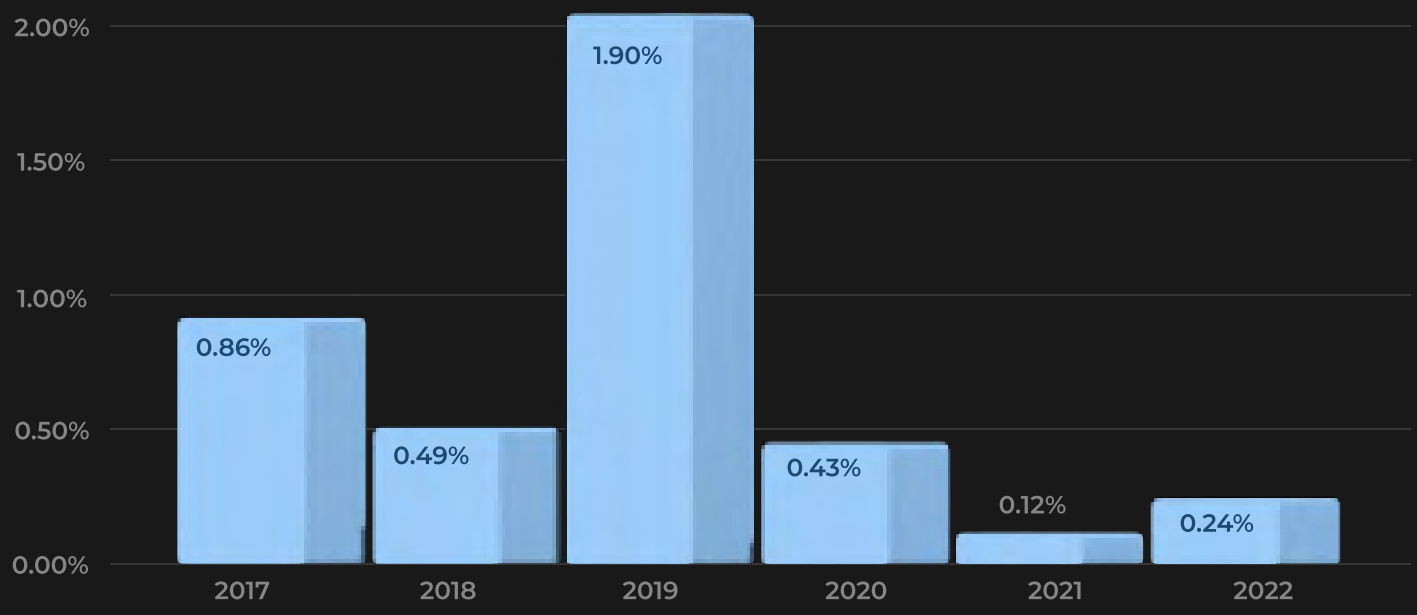
1. LEGAL PROTECTIONS FOR CUSTOMERS

1.2 Exchange KYC

Virtually all exchanges that have fiat on- and off-ramp features now implement KYC to avoid involvement in the financing of terrorism and money laundering. The crypto industry has often been accused of being a hotbed for these activities.

Taking steps to prevent them is integral to making investments in crypto assets ethical and to avoiding users inadvertently providing liquidity for criminals. Blockchain analytics firm Chainalysis estimated that 0.24% of transactions on cryptocurrency blockchains were still illicit in 2022.

Illicit share of all cryptocurrency transaction volume, 2017-2022



Data Source: Chainalysis, The 2023 Crypto Crime Report

To prevent illegal activities such as money laundering, fraud and terrorism financing, exchanges often collaborate with third-party companies that specialize in identity verification. These partnerships allow them to leverage the expertise and technology of the verification providers to streamline the onboarding process and ensure that regulatory requirements are met. However, this also means that an additional third party is involved in accessing and processing user data.

Arguably, there is tension between KYC requirements and data protection. As the former has become mandatory, it is vital that users take the time to understand the process and the implications that it carries for their privacy. KYC requires sensitive personal information, including government-issued identification, address details and sometimes even biometric data.

The table below shows how each of the exchanges we examined handles KYC and will include a link that leads to the relevant terms and conditions and the respective privacy policy.

Having to complete KYC can seem like an intrusive nuisance to the consumer; however, it is not only law enforcement and businesses but also ordinary customers that can benefit from KYC requirements. Exchanges that do not have KYC put the user's assets at risk if the platform is prosecuted for money-laundering or customers attract the attention of law enforcement with tainted cryptocurrency.

A lack of KYC incentivizes criminals to try and deposit cryptocurrency with an exchange because law enforcement will not have sufficient information to apprehend them if a transaction is flagged. Consequently, ordinary users on non-KYC-compliant platforms have a greater risk of receiving tainted funds with their withdrawals. This will cause their cryptocurrency to be classified as higher risk when later deposited with another service.

1. LEGAL PROTECTIONS FOR CUSTOMERS

The result may be the freezing of their crypto assets in the absence of additional documentation. In more extreme cases, platforms used for international money laundering and sanctions evasion, such as the Russian exchange BTC-e, have been entirely shut down by U.S. law enforcement.

In the case of BTC-e, some customer funds were seized by the U.S. government. The successor exchange, WEX, initially promised to make customers whole again but allegedly lost control of their funds.

Exchanges	Binance	Bit2Me	Bitfinex	Bitstamp	Bybit	Coinbase	HTX	Kraken	OKX
KYC Provider	Refinitiv	Jumio	Bitfinex (Internal)	Prove Identity	SumSub	Jumio (U.K.), Onfido, SolarisBank (Germany), Plaid (U.S.)	Jumio	Kraken (Internal)	OKX (Internal)

1.3 History of Legal and Regulatory Disputes

Exchanges	Binance	Bit2Me	Bitfinex	Bitstamp	Bybit	Coinbase	HTX	Kraken	OKX
Has it been involved in litigation with regulators?	Has been previously prosecuted in multiple jurisdictions and is currently in a lawsuit	No history of conflicts with regulators	Has been fined by regulators	No history of conflicts with regulators	Has been fined and banned from offering services in numerous jurisdictions	Has a vast history of issues with regulators	Hasn't been prosecuted but has been involved in lawsuits	Has been fined by regulators	No history of conflicts with regulators
Was it forced to cease operations in a jurisdiction due to problems with regulators?	Yes (U.K., Canada, Australia, Netherlands, Italy, Belgium)	No	Yes (U.S., Canada)	Yes (Canada[1])	Yes (U.K., Canada, France)	Yes (Japan, India)	Yes (Singapore, Malaysia)	No	Yes (Canada)
Has it ever been forced to remove products due to legal constrain ts?	Had to remove products in multiple jurisdictions and faced partnership terminations	No	Had to remove staking in the U.S.	No	Had to remove brokerage in Brazil	Had to remove loan services globally and staking in 4 U.S. states	No	Had to remove staking in the U.S.	Had to remove derivatives in the U.K.

[1]*Bitstamp will officially discontinue its services to customers in Canada starting Jan. 8, 2024. Source: Cointelegraph*

The way exchanges brand themselves publicly can be misleading. Bad business practices can happen in corporations of any size regardless of the image they outwardly display. The events of 2022 have provided salient examples of this in the cryptosphere with the collapses of FTX and Celsius.

While these two corporate meltdowns came unexpectedly, negative press coverage on hacks and legal disputes can be an early indicator that an exchange may engage in malpractice despite being outwardly trustworthy. The public track record of a business is even more important than the information it voluntarily provides. Naturally, this disadvantages larger exchanges that have a long history.

1. LEGAL PROTECTIONS FOR CUSTOMERS

Of the exchanges compared, Bit2Me and Bitstamp appear to have no publicly known conflicts with regulators. HTX has also maintained a relatively clean record within its jurisdictions of operation, apart from a copyright lawsuit initiated by one of its co-founders. OKX managed to avoid major problems but nonetheless had to leave Canada in 2023 due to the new requirements of Canadian lawmakers.

It also barely escaped prosecution in the U.K. when launching an advertising campaign for derivative products banned in the country. In contrast, all the biggest names in the crypto exchange market have faced serious regulatory challenges.

All of the remaining exchanges in the comparison were subject to recent court cases or regulatory fines in North America. Two of the examined exchanges were prosecuted for violations of commodities or banking regulations. In 2021, Bitfinex was fined $1.5 million by the CFTC for "illegally facilitating off-exchange retail commodity transactions in digital assets with U.S. citizens" and for operating as an unregistered futures commission merchant.

In early 2023, Coinbase paid one of the crypto industry's largest fines of the year after failing to comply with New York's financial services and banking laws. This resulted in a $50-million payment, and it was mandated that Coinbase invest a similar amount in its compliance program. In addition to this large fine, Coinbase had to suspend its Bitcoin-backed loan service globally after receiving a Wells notice from the SEC. It also had to pause staking services in a number of U.S. states.

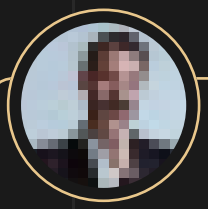
Due to the lack of regulatory clarity on securities classifications, legal proceedings in this area are even more common and have affected Bybit, Kraken and Binance's U.S. division. Bybit was fined $2.4 million for securities law infringement after not complying with registration requirements by the Ontario Securities Commission (OSC) in Canada.

It was also banned from offering securities in Brazil by the Brazilian Securities and Exchange Commission. Crypto exchange Kraken was subjected to prosecution by the SEC for failing to register its staking service, resulting in the discontinuation of Kraken's staking program for U.S. customers. It paid a total of $30 million in disgorgement, prejudgment interest and civil penalties.

Amid all these lawsuits, the ongoing battle between the SEC and Binance's U.S. division, which commenced in mid-2023, stands out.

Binance.com and its affiliated entities, Binance.US and BAM Trading, failed to register as clearing agencies, broker-dealers and exchanges, respectively. The proceedings have allegedly been held up by the company's failure to cooperate with formal requests.

The fallout from this lawsuit is causing great inconvenience to the platform's users. Binance.US users had to face the suspension of direct USD withdrawals. As a result of Binance's continuous compliance issues, Mastercard and Visa terminated their collaboration with the exchange for its debit card in Latin America and the Middle East. Card issuer Finansinės Paslaugos announced the termination of its issuance of Visa cards for Binance in the European Economic Area (EEA) by December 2023.



Sebastien Badault,
VP of Enterprise Revenue at Ledger

The past year has highlighted more than ever the need for self-custody for everyone, not just retail investors, but for institutions as well. Bank runs are becoming all too common. Realistically, every business should have at least 3 months of payroll in crypto in self-custody.

That can be done by the institution themselves or through a regulated custodian. While we all know self-custody is the best option for security, provided it is paired with a modern, auditable governance layer, we must ensure self-custody can serve the needs of traders.

Building robust, cross-platform networks such as Ledger Enterprise Tradelink is essential for ensuring institutions can reap the benefits of self-custody while minimizing friction in the trading process." - Sebastien Badault, VP of Enterprise Revenue at Ledger.

Enterprise
Tradelink

Build your own Trading Network.

Ledger Enterprise TRADELINK is a revolutionary trading and settlement network technology. Fully customizable, It empowers you to build your own trading network for unmatched control over your digital assets.

Learn more by visiting enterprise.ledger.com/tradelink

0

Transaction charges

Ledger does not charge on transactions

+400%

Trade swiftly & efficiently

Skip complex and repetitive operations

2. SECURITY OF CUSTOMER FUNDS

2.1 Crypto Assets

2.1.1 Crypto Reserve Audits:

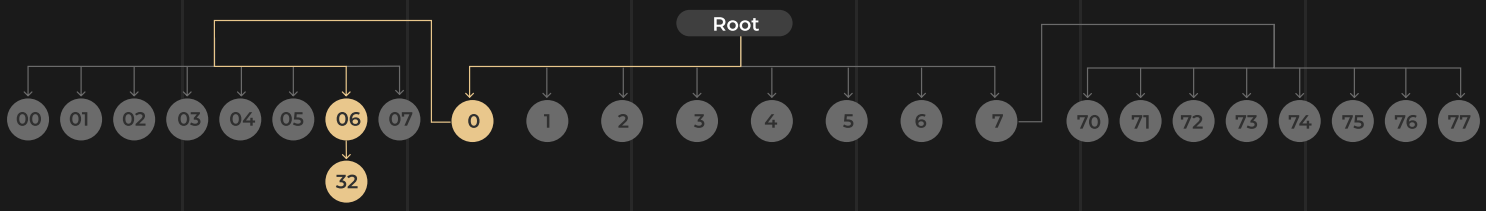
There are different ways exchanges can credibly demonstrate that they back their users' holdings of crypto assets sufficiently. The most complete showcase of this would be a full third-party financial audit, which includes crypto reserves, customer deposits and other liabilities. Alas, big, reputable accounting firms are often reluctant to publicly certify crypto businesses. The only exchanges that have received such an audit at the time of writing are Coinbase, which was fully audited by Deloitte, and Bitstamp, which has undergone an Ernst & Young audit.

However, there are so-called proof-of-reserves (PoR) audits, which at least certify that crypto deposits are backed by crypto reserves, even if they may not take into account other liabilities on the balance sheet. It is preferable for these audits to be fully published and to be independently conducted by a third party.

PoR is an auditing method used to demonstrate cryptographically that cryptocurrency holdings match user deposits.

It is designed to increase confidence in the financial stability of the exchange both for users and investors by showing that an exchange's holdings in cryptocurrency match or exceed the value of assets deposited by users.

Structure of a Merkle tree



The widespread use of proof-of-reserves audits by exchanges is a recent phenomenon that is the result of major bankruptcies in the industry. The most popular method for performing a PoR audit is using Merkle trees to create a cryptographic record of liabilities — i.e., deposits — and then demonstrate control of the funds required to back these liabilities.

Merkle trees are simply a way of structuring a database to ensure its integrity. Every node in the tree is a cryptographic hash that is derived from the hashes of its children. So-called leaf nodes are the hashes at the bottom of the tree that link to the packets of data that are being secured. The topmost hash is called the root hash, which is the part of the audit that would usually be published.

If a user wants to verify that their account is included in the Merkle tree that records liabilities, they can create a hash of their account number and the deposits they hold. It is then possible to check cryptographically if this hash is one of the leaves belonging to the published root without knowing the rest of the tree. This keeps other user's balances private but allows everyone to check if their accounts were included in the public audit. However, there is no way of checking the total sum of all the liabilities based on a Merkle root.

This is where the involvement of a third-party auditor in creating a Merkle tree PoR is essential. They need to certify what number the user balances in the Merkle tree adds up to.

The exchange can then submit additional cryptographic proof that shows they have the required crypto assets to back these deposits. Some have proposed using Merkle sum trees that track the cumulative balance of each node, but these come with privacy concerns and can be manipulated by including fake accounts with a negative balance. More advanced PoR schemes have started employing zero-knowledge (ZK) proofs (in particular zk-SNARKs and zk-STARKs) to mathematically verify certain properties of the leaf node set without the risk of revealing individual balances. This can include the absence of negative balances and the sum of all balances.

However, even if a ZK-proof is used or the auditor certifies the proof of liabilities correctly, there is no way of knowing whether the exchange used borrowed funds to demonstrate reserves. It also does not take into account liabilities other than user deposits that the exchange may have, such as loans.

PoR audits, therefore, have clear limitations. They are not in themselves sufficient to fully certify the financial health of an exchange. They are also usually not provided in real-time but only capture a snapshot at a specific moment that may not reflect the current state of assets and liabilities. Until traditional auditing firms become more willing to certify cryptocurrency service providers, some uncertainties about the financials of major exchanges will remain.

2. SECURITY OF CUSTOMER FUNDS

With respect to the remaining exchanges, we regard a self-attested Merkle tree proof-of-reserves and liabilities as insufficient to prove that deposits are sufficiently backed. Without a third-party auditor or a ZK-proof, these kinds of audits are easily manipulated. Bybit, Bitstamp and Bitfinex can, therefore, not demonstrably show that their deposits are backed.

Bit2Me, Kraken, Binance and OKX, on the other hand, have either a ZK-proof or an external auditor as part of their PoRs.

Exchanges	Binance	Bit2Me	Bitfinex	Bitstamp	Bybit	Coinbase	HTX	Kraken	OKX
Proof-of-reserves or equivalent	Merkle tree, zk-SNARK(Mazars Company till 2022)	Merkle Tree (Hacken)	None (only published wallets on github)	N/A, but audited by Ernst & Young	Merkle tree (No third party named)	N/A, but audited by Deloitte	Merkle tree (No third party named)	Merkle tree (Armanino LLP)	zk-STARK (No third party named)
Publicly viewable	Public	Not currently publi[1]	N/A	Not public	Public	Not public	Public (for users)	Public (for users)	Public

[1]*Bit2Me plans to publish at the end of December, 2023*

2.1.2 Crypto Custody Providers and Insurance of Crypto Assets:

Crypto custody is a critical aspect of the operations of a centralized exchange. The term custody denotes the secure storage of assets and their management. Most exchanges employ a mix of hot and cold storage methods to safeguard against theft, hacking and other potential threats. While cold storage is generally securer, it is more difficult to retrieve funds. This makes cold storage unsuitable for trading.

Large crypto exchanges commonly adopt either in-house (first-party) custody solutions or opt to delegate these responsibilities to external custody providers, entrusting them with the safeguarding of users' assets.

The terms governing how the provider organizes this process are usually established through service-level agreements (SLAs).

Consequently, the choice of provider often hinges on the storage conditions of interest to the exchange and the jurisdiction of the provider company. Utilizing the services of a reputable third-party custodian that complies with regulatory requirements reduces the risk of the exchange misusing user funds. However, old exchanges, such as Kraken, often have mature in-house solutions that are equally as trustworthy. Only Bybit appears to have a concerning lack of transparency about how or with whom they store user funds.

Exchanges	Binance	Bit2Me	Bitfinex	Bitstamp	Bybit	Coinbase	HTX	Kraken	OKX
Proof-of-reserves or equivalent	Ceffu (Former Binance Custody)	Ledger enterprise	Zodia Custody	BitGo	1st Party	Coinbase Custody	HTX Custody	1st Party	Komainu (Institutional)

Insurance funds protect users against unexpected losses due to operational failures, cyber theft or other forms of compromise. Some exchanges choose to allocate a portion of their trading fees to such a fund. After the FTX collapse and multiple hacking incidents, Binance and HTX decided to create special secure asset funds for users, or SAFU, that would compensate users in the case of misuse, theft or hacking of funds.

Bitstamp and Bit2Me achieve the same through a different approach. They have third-party custodial providers, namely BitGo (Bitstamp) and Ledger (Bit2Me), which provide insurance coverage of $250 million and $150 million, respectively. Most exchanges, however, including Kraken and Bybit, have no such insurance. The funds that do exist are only there to cover losses incurred in the case of trading defaults, but not to insure assets from theft or hacks.

Exchanges	Binance	Bit2Me	Bitfinex	Bitstamp	Bybit	Coinbase	HTX	Kraken	OKX
Theft insurance	>$1 billion SAFU fund	$150M (On custodian side)	No	$250M (On custodian side)	No	No	SAFU fund (recently launched)	No	No

2. SECURITY OF CUSTOMER FUNDS

2.2 Fiat Deposits

Centralized cryptocurrency exchanges typically facilitate fiat currency transactions and offer users the ability to deposit, withdraw and hold various currencies. The protection of these fiat balances is of critical concern. Unlike cryptocurrencies, fiat holdings within these platforms are subject to extensive global regulatory frameworks that safeguard the funds and ensure they are managed appropriately.

Apart from the exchange itself, the bank at which accounts are ultimately held presents a potential risk factor. In the EU and U.S., strong minimum reserve requirements and deposit insurance for the clients of commercial banks exist. The Federal Deposit Insurance Corporation (FDIC) covers funds of up to $250,000 per individual, and the Deposit Guarantee Scheme (DGS) offers insurance of up to 100,000 euros.

Nevertheless, the coverage offered by such regulatory protections typically applies on a per-account basis, as evidenced by cases such as that of Silicon Valley Bank. Given the large clientele of exchanges, which ranges from thousands to millions of users, providing equivalent security to the underlying bank would necessitate separate bank accounts for each client. This requirement presents a logistical challenge that is often impractical or unfeasible, and as such, is generally not standard practice within the industry.

The predominant approach is to leverage the services of an electronic money institution (EMI) or to acquire such a license directly. EMIs operate under regulatory conditions akin to traditional banks, which allows them to accept deposits and issue payment instruments such as cards.

A crucial stipulation for EMIs, however, is that customer funds must remain untouched, prohibiting lending or other uses of these deposits. Consequently, customer funds are held in segregated accounts with full reserve backing. This substantially reduces the risk of a financial loss due to bankruptcy and provides an additional layer of security even in instances where the custodial bank — separate from the exchange itself and from the EMI — encounters financial difficulties.

The specific protections and legislative measures can differ significantly across different jurisdictions, reflecting the diversity of regulatory environments that exchanges must navigate. For a detailed and uniform comparison, it is better to focus on a single regulatory zone. The European Union stands out in this context, offering a transparent and well-defined set of rules connected with fiat deposits. Consequently, the forthcoming analysis and comparison will specifically examine how different cryptocurrency exchanges manage euro deposits within their platforms.

Exchanges	Binance	Bit2Me	Bitfinex	Bitstamp	Bybit	Coinbase	HTX	Kraken	OKX
Currency	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR
FIAT custody	Uncertain	E-money institution	E-money institution	Payment institution	E-money institution[1]	E-money institution	No information	E-money institution	No fiat deposits
Provider	Multiple	Pecunia	OpenPayd	Self-provided (according to the payment institution license in Luxembourg)	UAB Onlychain and EasyEuro (Kitakami Ltd)*	Self-provided (according to e-money license in Ireland)	Multiple	Self-provided (according to e-money license in Spain)	No fiat deposits
Coverage	It is said that EUR deposits are insured according to EU laws, though insufficient proof	100% of money deposited	100% of money deposited	100% of money deposited	100% of money deposited	100% of money deposited	Uncertain (insufficient data)	100% of money deposited	No fiat deposits

*[1]UAB Onlychain is offering e-wallet and fiat payment services in collaboration with EasyEuro, a third-party exchange operated by Kitakami Ltd — an **electronic money institution** licensed and regulated by the U.K. Financial Conduct Authority (FCA) under EMI license number 900914.*

Europe's most trusted exchange to manage your crypto

bit 2 me

Prepared for the arrival of MiCA in 2024. The team is working alongside regulators and academics.

2023-2025

Compliance team of the year by Iberian Lawyer Against some of the Top 10 European banks.

VIII EDICIÓN PREMIOS Expansión

Compliance SME of the year award by Top News outlet in Spain.

NOVEMBER 2023

Bank of Spain approves Bit2Me as country's **first crypto services provider.**

MARCH 2023

Spanish Government **trusts in Bit2Me.**

MAY 2022

FEBRUARY 2022

Backed by: Google Telefónica invenready INVESTCORP

LEARN MORE

2. SECURITY OF CUSTOMER FUNDS

2.3 Cybersecurity

The nature of cryptocurrency exchanges, which involves the management and transfer of digital assets, makes them a prime target for cyberattacks. As a result, exchanges invest significantly in cybersecurity measures to protect both their assets and their users. All exchanges of note use two-factor authentication, data encryption both at rest and in transfer, and perform regular backups. However, naturally, cybersecurity is significantly more complex than this, and differences manifest in the details.

Penetration testing and bug bounty programs

Penetration testing involves simulating cyberattacks on an organization's systems to identify vulnerabilities before malicious actors can exploit them. Exchanges often conduct periodic penetration tests, employing either internal teams or third-party experts, to assess their defenses.

After that, vulnerabilities are patched and the systems reinforced.

Bug bounty programs are initiatives that incentivize security researchers and white hat hackers to report potential security vulnerabilities and breaches in the exchange's systems. In return for their findings, participants are usually rewarded. The remuneration depends on the severity of the vulnerability.

Crypto exchanges widely promote their bug bounty programs to attract skilled security professionals and demonstrate their commitment to maintaining robust security measures. Either these programs are run by the exchanges themselves or by partnering with third-party service providers such as HackerOne, Bugcrowd, etc. The following lists the bug bounty programs and their sizes for the examined exchanges:

Exchanges	Binance	Bit2Me	Bitfinex	Bitstamp	Bybit	Coinbase	HTX	Kraken	OKX
Bug bounty provider	Bugcrowd	Internal	Internal	Bugcrowd	Internal	HackerOne	Hacken Proof	Internal	Hacker One
Bug bounty size	BugcFrom $200 up to $100,000	From 50 EUR up to 5,000 EUR	From $10 up to $10,000+	From $100 up to $100,000	From $50 up to $4,000	From $200 up to $1M	From $100 up to $10,000	From $500 up to $100,000+	From $200 up to $1M

Having periodic "pen tests," alongside bug bounty programs, helps to enhance the cybersecurity of the exchange and protect users' funds and personal information.

ISO certifications

The International Organization for Standardization (ISO) provides globally recognized standards for various industries, including information security. Among many certifications, the main ones that we consider relevant qualifications for the operators of crypto exchanges are as follows:

1. The term information security management systems (ISMS) encompasses all provisions against information risks, such as cyberattacks, data leaks or the discovery of vulnerabilities. ISO/IEC 27001 is a widely recognized standard for ISMS. It offers a systematic approach to managing sensitive company information, ensuring its confidentiality, integrity and availability. Many leading crypto exchanges aim for **ISO/IEC 27001** certification to demonstrate the robustness of their security protocols. It is held by all exchanges on our list. In the same family of ISO/IEC 27001, there are two more advanced certifications:

   a) **ISO/IEC 27701** is a standard for structuring the information privacy management processes within an organization.

   b) **ISO/IEC 27018** is a set of guidelines intended to enhance the protection of personally identifiable information (PII) processed by public cloud service providers.

2. Business continuity management systems (BCMSs), on the other hand, are focussed on mitigating the disruption that a cybersecurity or other incident might cause. It should ensure the continuity of business operations in case of such an event. The corresponding international standard for certifying BCMSs is **ISO 22301.**

Transparency of cybersecurity assurance

In the realm of cybersecurity, the escalation of numerous threats necessitates an elevated level of trust and assurance in security practices, with transparency serving as one of the key elements. Mere declarations or visually appealing marketing efforts fall short of instilling this trust, while direct transparency is pivotal.

2. SECURITY OF CUSTOMER FUNDS

Most crypto exchanges choose not to disclose the scope of their cybersecurity measures even if they have been certified and are known to comply with industry standards. Notable examples here could be Binance and HTX. Some companies, however, pursue a more transparent approach and publish cybersecurity information on the website to reassure the user and help them choose an exchange.

Coinbase, OKX and Bybit have taken steps toward this. Bitfinex and Bitstamp achieved a significant level of transparency but lacked some detailed information. However, Bit2Me and Kraken are the most transparent. They have special menus or portals with detailed information on the exchange's security measures. Bit2Me has the best information, with a dedicated security portal that offers real-time insights into audit activities and allows access to its certifications.

Exchanges	Scoring Weight	Binance	Bit2Me	Bitfinex	Bitstamp	Bybit	Coinbase	HTX	Kraken	OKX
History of hacking + date of latest hack + amount of hacks	0 if multiple hacks within 5 years 1 if single hack within 5 years 2 if there was 1 hack more than 5 years ago 3 if there were no hacks	$40M[2] (2019)	None	$72.5M (2016) (2 hacks)	$5M (2015)	None[1]	None[1]	$8M (2023)	None[1]	$8.6M (2020) (2 hacks)
Bug bounty program	1 if Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Penetration tests	1 if privately audited, 2 if publicly audited	Yes (public)	Yes (private)	Yes (public)	Yes (public)	Yes (public)	Yes (public)	Yes (public)	Yes (public)	Yes (public)
ISO 27001 (information security managem ent systems)	1 if 27001 Certificate 2 if extension to 27001 Certificate	Yes[3]	Yes	Yes[5]	Yes	Yes	Yes	Yes	Yes	Yes[3]
ISO 22301 (business continuity managem ent system)	1 if Yes	No	Yes	No	No	No	No	No	No	No
Transparency of cybersecurity assurance	Score in brackets	Accessible through direct search request (0.25)	Easily and fully accessible (1)	Easily and almost fully accessible (0.75)	Easily and almost fully accessible (0.75)	Not easily but almost fully accessi ble (0.5)	Easily but not fully accessible (0.5)	Not easily and not fully accessi ble (0)	Easily and fully accessi ble (1)	Easily but not fully accessi ble (0.5)
Total final score	Sum (max. 10)	6.25	**8**	5.75	6.75	7.5	7.5	5	**8**	5.5

[1] Accounts can be compromised, though centralized hacks haven't occurred.
[2] There was also a BNB Smart Chain hack worth $570 million, though it was connected with the blockchain rather than an exchange.
[3] Also has the 27701
[4] Also has the 27018
[5] Public audit with Hacken to be conducted

3. USER EXPERIENCE: INTERFACE / CUSTOMER SERVICE / TAX REPORTING

3.1 Interface:

The user interface of a cryptocurrency exchange can significantly affect the user experience. A good UI is characterized by simplicity, intuitive design and usability. It should have a clear and organized structure that allows users to easily navigate the platform, execute trades, and manage their accounts. Quick access to basic information such as account balances, open orders and trading pairs is desirable. In addition, advanced users benefit from trading tools such as technical analysis charts, order types and real-time market data.

A poorly designed user interface, on the other hand, can be frustrating and negatively impact the user experience. Cluttered screens, confusing navigation and a lack of customization options can make it difficult to find the required information. Inefficient order placement and execution processes, slow loading times or frequent system crashes can also hinder trading activity.

Despite these universal requirements, evaluating a user interface is fundamentally subjective. How long the user has been using the platform plays an important role in their perception. Some platforms may emphasize the accessibility of the interface to new users, while others tend to cater more to audiences who already have trading experience.

The following table presents a comparison of exchanges based on key aspects of the user interface. It focuses on the overall appearance, the clarity and transparency of the products offered, the user-friendliness of customer support features, the presentation of trading information, and the availability and comprehensiveness of educational materials.

Factor of comparison	Bit2Me	Kraken	Bitstamp	Bybit	OKX	Coinbase	HTX	Binance	Bitfinex
Main interface convenience	The interface is designed with user-friendliness in mind. Each page has a mini-introduction for the available options.	The interface is intuitive, with clear descriptions for each option, including a pro version for experienced users.	Basic and Pro versions are available. The Basic interface is intuitive, while the Pro version optimizes menus for trading.	The interface is logically structured. Products and options are grouped in their respective sections.	The interface is adequately organized, with features and options in their respective sections.	The interface is intricate, but the placement of some options may not be evident to new users	The interface is generally intuitive, with transparent and well-visualized menus.	The interface is well-executed, yet lacks transparency for certain options and features.	The interface appears to be quite generic and resembles that of lower-tier exchanges.
Accessibility of products	All of the products are grouped together within a dashboard, making it convenient to locate and access them.	The available products are conveniently and concisely grouped in a single section of the menu.	The basic version allows deposits and withdrawals, while some assets are exclusive to the advanced trading version.	All products are listed transparently in their respective sections	Products primarily in one section with several in the other sections but quite intuitively sorted	Access to some of the products offered by the exchange is not very clear and generally lacks transparency.	All products are listed transparently in their respective sections	The products are divided into sections, but the division may seem unintuitive to fresh users.	All trade products and tokens are available via the sidebar and dashboard, but are barely sorted.
Accessibility of customer support	Contact form and phone numbers for support, with language preference selection, accessible from any page.	Accessible from the main menu, customer support offers integrated LiveChat and prompt assistance options.	The 'contact support' button is at the very bottom. Features FAQ, email tickets, and three phone numbers.	The support box on the main page includes FAQs but lacks adequate contact options.	Support box on the main page with a chatbot and then you can choose to contact via email.	The tech support contact button is at the bottom; accessing support involves navigating through intermediate pages.	Customer support is available via a block on the homepage, but is more like FAQ with an option to create a ticket via email.	Main page features a support box with FAQ links, requiring scrolling to access the email feedback function.	The support contact button is at the site's bottom, has live chat and the option to submit detailed tickets on a wide range of topics.
Visualization of trading data	Each token page includes price charts, purchase options, and details, featuring Simple and Pro chart versions.	Every token page includes a price chart, description and purchase method.	The trading data is available in simplified and detailed form.	Every token page comes with a price chart, trading options, and descriptions.	Not conveniently located, has price charts and descriptions, but less overall data and no purchase options.	All popular visualization options are available, along with aggregated news and additional token information.	Not beginner-friendly, with technical graphs and order books, lacks descriptions and basic visualization.	Each token page includes a price chart, description, and purchase options, though it opens in a separate tab, which might not be very convenient.	Like other exchanges, main visualization is provided through TradingView; no simplified chart option.
Learning center & tutorials	One of the most comprehensive learning centers, easily accessible from the main dashboard.	The learning center offers basic articles on tokens and crypto, but lacks convenient organization.	Features a comprehensive crypto learning section with various topics.	Has a vast number articles but lacks proper grouping, leading to somewhat chaotic arrangement	Located as a separate option in the main menu, though learning center is not very informative and conveniently organized	Accessible from the main menu, there are basic tutorials and articles covering crypto trading, although not very in-depth.	Offers comprehensive, easily accessible tutorials with varying levels of detail, including text and video tutorials.	The learning center contains a variety of comprehensive materials, tutorials, and also includes a reward hub.	Tutorials and option overviews are found on the Bitfinex blog and a dedicated page, but there's no direct access from the main page.
	A		B			C			D

3. USER EXPERIENCE: INTERFACE / CUSTOMER SERVICE / TAX REPORTING

3.2 Customer Service:

Support is one of the most important components of the user experience. It ensures that customers are not left to fend for themselves when they face unusual circumstances or struggle to understand the terms of a product. Given the global reach of cryptocurrency exchanges and the diverse user base they cater to — often spread across several geographic regions — the task of delivering efficient customer support can be challenging. Our investigation underscores that email and in-app ticketing systems represent the primary and most widely accessible means of customer support across exchanges. However, some choose to extend their support services to dedicated X (formerly Twitter) accounts, or even phone-based assistance.

By analyzing user ratings and reviews on popular company rating platforms, such as TrustPilot, and general customer feedback on sites such as Reddit, we came to broad conclusions about the quality of customer support across the compared exchanges. Looking at the overall scores, users express higher satisfaction with the support provided by Bit2Me and Bitfinex, whereas on other platforms, users frequently face issues related to slow response times or inability to resolve issues customers face.

Exchanges	Binance	Bit2Me	Bitfinex	Bitstamp	Bybit	Coinbase	HTX	Kraken	OKX
Does it have integrated support?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
In what countries is customer support available by phone?	No	EU (France, Poland, Portugal, Spain), U.K., Argentina, Brazil, Chile, Colombia, Mexico, Panama	No	U.S., EU (Luxembourg), Global[1]	No	U.S., Canada(Automatic response only)	No	U.S., Canada, EU (Ireland)	No
Does it have a support channel on X?	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Is support available through email?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Does it offer support on WhatsApp?	No	Yes	No	No	No	No	No	No	No
Languages supported for text inquires	English, German, French, Italian, Polish, Turkish, Russian, Arabic, Chinese, Indonesian, Spanish, Filipino, Portuguese, Romanian, Vietnamese, Ukrainian, Japanese, Korean	Both text messages and phone calls available in English, Spanish, French, Portuguese, German, Italian, Romanian, Polish, Bulgarian	English, Russian, Chinese (Simplified and Traditional), Spanish, Portuguese, Vietnamese	English, German, Slovenian	Chinese (Simplified and Traditional), English, Japanese, Korean, Portuguese, Russian, Spanish, Turkish, Ukrainian, Vietnamese	German, English, Portuguese, Spanish, French, Japanese, Italian, Dutch, Polish, Russian, Thai	English, Chinese, Russian, French, Spanish, Turkish, Vietnamese, Japanese, Portuguese, Italian, Ukrainian, Indonesian	Chinese, English, Filipino, French, Italian, Japanese, Portuguese, Russian, Spanish, Turkish, Ukrainian, Vietnamese	English, Russian, Turkish, Spanish, Hindi, Portuguese, Ukrainian, Indonesian, Thai, Vietnamese, Filipino, Japanese, Korean
Languages supported for phone calls	N/A		N/A	English	N/A	English	N/A	English, Spanish, French	N/A
Total support rating based on user feedback (out of 10)	4	8	6	5	5	3	3	5	3

[1]*Bitstamp has a phone number with the U.K. country code listed as its global customer support number.*

3. USER EXPERIENCE: INTERFACE / CUSTOMER SERVICE / TAX REPORTING

3.3 Tax Reporting Tools:

In the vast majority of countries, a user's activities on a crypto exchange are subject to capital gains taxes. This makes the ability to quickly download transaction data for tax reporting an undeniable advantage. The reports issued for this purpose are usually available from exchanges upon request and provide users with a complete overview of their cryptocurrency transactions for the tax year. This includes information such as transaction dates, cryptocurrency quantities acquired, sold or transferred and corresponding transaction fees. In ideal cases, a corresponding calculation of capital gains or losses and the resulting tax liabilities is included.

However, it should be noted that not all exchanges offer this service. For example, Bitstamp provides only taxation forms 1099-K and 1099-MISC, and Kraken provides 1099-MISC and 1099-INT for U.S.-based users. OKX and HTX do not have any in-house tax report generating system. This limits users to using tax reporting services from external providers such as Koinly and CoinLedger. However, the vast majority of exchanges have integrated tax tools for major jurisdictions at this point. Bit2Me even has an online consultant that can help users build a proper tax report.

Tax Reporting Tool Availability by Exchange

Exchanges	Binance	Bit2Me	Bitfinex	Bitstamp	Bybit	Coinbase	HTX	Kraken	OKX
Tax reporting tool	Yes	Yes + online consultant	Yes	Yes	Yes	Yes	No	Yes	No
Availability	Worldwide	Worldwide	Worldwide	Only U.S.	Worldwide	Worldwide	External providers	Only U.S.	External providers

Evolution of Crypto Exchanges Security

2014

850,000 btc stolen in Mt. Gox hack revealing centralization risks

First Proof of Reserves

2017

ICO & CEX boom

Hacken launch & first smart contract audits.

2018

Coincheck loses $500M in a first-ever organized black-hat hacking attack

Hacken launches CEX ranking platform CER.live and Web3 bug bounty platform HackenProof

2019

A series of high-profile attacks targeting 10 CEXs lead to $1B+ in losses

Trust in crypto undermined

2020

CoinGecko and CoinMarketCap integrate **Hacken** audits & security scores

Tangible improvements in CEX resilience; pentests and bug bounties at all-time high

2022

FTX imposition, Terra Luna crash

Hacken solves a critical bug in Binance's Proof of Reserves

2023 →

Biggest-ever push for CEXs to prove reserves

Rise of crypto security standards & regulations (C4, EEA)

HACKEN

Trusted security partner for 50+ crypto exchanges since 2017

bit2me OKX KUCOIN whitebit Gate.io MEXC HTX

Full Security Coverage

- Proof of Reserve
- Penetration Testing
- Bug Bounty
- dApp audit
- CCSS & ISO/IEC 27001 Audit

Request Services →

4. GENERAL OVERVIEW: ASSET SUPPORT AND PRODUCT COMPARISON

4.1 Product Range

Product	Description	Risk profile
Spot trading	This is the most basic type of trading. A cryptocurrency is bought or sold at its current market price. The transaction is settled immediately, "on the spot," by exchanging the underlying asset.	Lowest risk
Futures	Futures are derivative products that allow for buying or selling a cryptocurrency at a predetermined price at a specific future date. Perpetual futures allow traders to borrow funds to trade larger amounts of a cryptocurrency, potentially amplifying profits or losses. This is also called leverage trading.	Elevated market, liquidity and settlement risks
Launchpad	A launchpad is a platform provided by some crypto exchanges that allows new cryptocurrency projects to launch their token sales.	High market risk characteristic of low-cap projects
Crypto lending	Crypto lending platforms allow users to lend their cryptocurrencies to others in exchange for interest.	Risk profile depends on deposited collateral, custody, LTV ratio and re-hypothecation.
Staking services	Staking involves participating in the proof-of-stake (PoS) consensus mechanism of certain coins to validate transactions and create new blocks. This generates rewards in the process.	Low risk, unless regulatory situation is unclear as currently in the U.S.
P2P trading	Peer-to-peer (P2P) trading involves buying and selling cryptocurrencies directly between users at a fixed, predetermined price. This effectively bypasses the exchange and its spot market.	High counterparty risk
Debit or credit card	Some crypto exchanges partner with card providers, such as Visa or Mastercard, to allow their customers to pay using their crypto balances.	Low risk
Institutional/ business customers services	For institutional and business customers, cryptocurrency exchanges provide bespoke services such as deep liquidity pools for bulk transactions, priority customer support, profound trading infrastructure and comprehensive reporting tools. Some exchanges offer additional services for business integrations — i.e., payment provision, marketplace listings.	Varying

Comparison of All Exchanges by Types of Products and Their Availability

Type of product	Binance	Bit2Me	Bitfinex	Bitstamp	Bybit	Coinbase	HTX	Kraken	OKX
Spot trading	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Derivatives	Futures, options, perpetuals	No[3]	Perpetuals, indexes	No	Futures, options, perpetuals, leveraged	Perpetuals, futures, indexes	Perpetuals, futures, options	Futures, perpetuals	Futures, perpetuals, options
P2P trading	100+ currencies, 8 cryptos	No	11 currencies, 5 cryptos	No	50+ currencies, 4 cryptos	Yes, in Coinbase Wallet	80+ currencies, 6 cryptos	No	80+ currencies, 5 cryptos
Launchpad	Projects	Projects	No	No	Projects	No	Projects	No	Projects
Crypto lending	Lending/ borrowing	Lending/ borrowing	Lending/ borrowing	No	Lending/ borrowing	Stopped	Lending/ borrowing	No	Lending/ borrowing
Staking services	10 cryptocurrencies	38 cryptocurrencies	10 cryptocurrencies	2 cryptocurrencies	6 cryptocurrencies	67 cryptocurrencies	18 cryptocurrencies	16 cryptocurrencies	9 cryptocurrencies
Debit/credit cards	No[1]	Mastercard debit card	No	No	Mastercard debit card	Visa debit card only for U.S. customers	No[2]	No	No
Institutional/business customers services	Yes (has KYB form + crypto payment provider and lists businesses on its marketplace)	Yes (Has KYB form + crypto payment provider)	Yes (doesn't have special KYB)	Yes (has integrated KYB form)	Yes (has integrated KYB form)	Yes (Has KYB form + crypto payment provider)	Yes (Form in Google survey for verification)	Yes (has integrated KYB form)	Yes (Has integrated KYB form)

[1] The service will be shut down in December 2023. New cards are no longer issued.
[2] Partnered with Visa to launch a debit card. Service is not available yet.
[3] Derivatives trading is prohibited in the EU

4. GENERAL OVERVIEW: ASSET SUPPORT AND PRODUCT COMPARISON

4.2 Spot Trading:

As the primary interest of most users is simply to buy and sell cryptocurrency, spot trading is by far the most important product offered by exchanges. The name "spot trading" derives from the fact that transactions are settled "on the spot" — i.e., immediately. A spot trade always involves an exchange of the underlying asset instead of equivalent financial commitments denominated in a fiat currency, as is often the case for derivatives.

On many exchanges, holdings in a customer's spot account are backed 1:1 by the underlying asset.

Although this should intuitively be the default, not all exchanges have played by this principle in the past, and unlike for traditional banks, there is no comprehensive regulatory framework that sets minimum reserve requirements for such deposits. Spot customers should therefore do their own due diligence and not blindly trust exchanges with their spot deposits (see Section 2.1.1). The most independent way to store cryptocurrency in the long term is with a hardware wallet.

4.3 Spot Trading:

As the primary interest of most users is simply to buy and sell cryptocurrency, spot trading is by far the most important product offered by exchanges. The name "spot trading" derives from the fact that transactions are settled "on the spot" — i.e., immediately. A spot trade always involves an exchange of the underlying asset instead of equivalent financial commitments denominated in a fiat currency, as is often the case for derivatives.

Cryptocurrency derivatives are financial products that allow individuals to trade on the price movements of cryptocurrency without owning the underlying asset. There are various mechanisms that ensure that the price of an asset on the derivatives market closely tracks its price on the spot market. However, users should be aware that these mechanisms are not perfect and that derivatives markets can have additional volatility and deviate in the short term. There are several types of crypto derivatives:

- Futures are contracts that constitute an agreement to buy or sell a specific cryptocurrency at a predetermined price at a specified time in the future. They can be settled in fiat or the underlying asset. Binance offers futures derivatives on its platform.
- An option is a contract that gives the holder the right, but not the obligation, to buy or sell a specific amount of cryptocurrency at a predetermined price (strike price) before the contract's expiration date. There are two types of options: calls (buy) and puts (sell). Options tend to be more popular on the traditional financial markets.
- Perpetuals are a variation of futures contracts but without an expiration date, which can be held indefinitely. These are unique to the crypto market and are also the most popular kind of crypto derivative.

Types of derivatives in crypto

- Crypto futures
- Crypto options
- Perpetual contracts

As derivatives allow trading with leverage, it not only amplifies earnings but also carries significant risks:

1. **Market volatility:** Cryptocurrencies are known for being highly volatile, and prices on derivatives exchanges don't always reliably track the spot price, especially on shorter time frames. Mass liquidation events in which the price temporarily breaks out and makes users lose their position are common.
2. **Leverage risk:** Derivatives often involve leverage, meaning traders can lose more than the size of their position. While trading on a derivative account, traders should always remember that they may end up with a liquidated account.
3. **Regulatory risk:** The legal landscape for crypto derivatives is uncertain and can vary by jurisdiction. For example, most exchanges do not offer derivatives products to U.K. citizens due to regulatory requirements. The Spanish and Dutch governments also don't allow the offering of derivatives.
4. **Legal and tax implications:** Depending on the customer's country, the legal and tax treatment of crypto derivative transactions may be unclear or subject to change.
5. **Manipulation risk:** The cryptocurrency market has faced criticism for being vulnerable to market manipulations. Traders might encounter pump and dumps, insider trading or other manipulative schemes.

4.4 P2P Trading:

Peer-to-peer (P2P) trading on cryptocurrency exchanges represents a shift from traditional, centralized forms of trading. It makes trades more independent of particular payment providers and facilitates direct interaction between users. If users have the patience to find an attractive offer or wait for their offer to be accepted, P2P trading can offer more competitive conversion rates.

Exchanges usually provide escrow services to mitigate potential fraud, and the seller's cryptocurrency is only released once the buyer has acknowledged receipt of the payment. P2P trading is also a convenient choice for jurisdictions with political or economic instability, as it is resilient to regulatory changes.

4. GENERAL OVERVIEW: ASSET SUPPORT AND PRODUCT COMPARISON

There are almost no explicit prohibitions against P2P trading in place globally. Of course, some risks come with P2P trading, such as attempted scams, higher spread or lower settlement speeds. However, these are somewhat mitigated on reputable exchanges and platforms.

4.5 Launchpad:

Many cryptocurrency exchanges have expanded their services beyond simply providing trading instruments. Launchpads are a special platform on some exchanges that facilitates the launch and initial sale of new tokens to the public, often referred to as initial exchange offerings (IEOs). This allows blockchain projects to debut their tokens by selling them to the public, similar to an initial coin offering (ICO), but with the exchange acting as an intermediary.

Exchanges check and do due diligence on these projects to avoid future rug pulls and screen out otherwise illegitimate tokens. Hosting IEOs increases user engagement for the exchange and can attract new users from a project's community. Projects similarly benefit as they get immediate access to the exchange's user base, which often results in a more successful launch with significant liquidity.

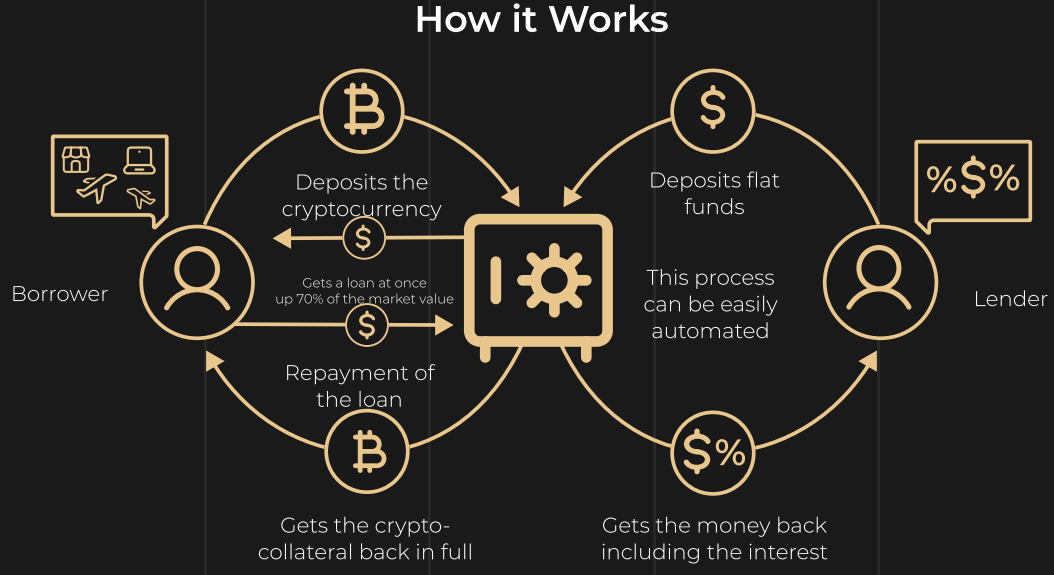
However, there are regulatory concerns, as IEOs fall into a gray area in many jurisdictions, with an ongoing debate over securities laws and how they apply to token sales. In the U.S., for example, if a token listed in an IEO is classified as a security, the exchange responsible for that offering must register with the SEC.

4.6 Crypto Lending:

Lending platforms allow users to earn interest on their assets by loaning them out. The interest rate can be fixed or variable, depending on the platform's model. Some exchanges also loan funds to their users against cryptocurrency as collateral. If the borrower does not repay a loan, the platform must enforce a collateral liquidation. Under volatile market conditions and a low loan-to-value (LTV) ratio, the lender's capital may be at risk.

The regulatory status of crypto loans is unclear in some jurisdictions, which poses risks for those involved in crypto lending operations. For example, the Thai SEC banned crypto lending and staking in the country in 2022. What's more, some exchanges, such as Binance and HTX, leave the right to use borrowers' collaterals for rehypothecation and other activities, which increases the exchange's returns but increases the risk for the user. Bit2Me and Bybit state that they do not rehypothecate loan collateral and should therefore be considered to have more secure lending features.

Exchanges	Binance	Bit2Me	Bitfinex	Bitstamp	Bybit	Coinbase	HTX	Kraken	OKX
Rehypothecation of loan collateral	Yes	No	No	N/A (No lending)	No	N/A (No lending)	Yes	N/A (No lending)	No



4. GENERAL OVERVIEW: ASSET SUPPORT AND PRODUCT COMPARISON

4.7 Staking Services:

Staking allows users who hold proof-of-stake (PoS) cryptocurrencies to earn passive income. Exchanges stake customer funds (lock them up) to participate in the respective PoS blockchain's consensus — i.e., to validate transactions and maintain the network's security. By doing this, they receive staking rewards.

While individuals can stake coins directly on a PoS blockchain, doing so requires maintaining a network node and has high capital requirements, which makes staking through an exchange a preferred option for many. While convenient, exchange-based staking is against the decentralization efforts of many blockchains, as exchanges control users' staked assets and can hence gain a say in the blockchain's operation and governance.

4.8 Institutional or Business Customers Services:

Crypto exchanges offer tailored services for institutional and business clients, providing advanced trading features, higher liquidity and dedicated support. These services often include over-the-counter (OTC) trading for large volume transactions, corporate accounts with enhanced security measures, API integrations for automated trading strategies, and customized reporting tools for compliance and auditing purposes. These products are designed to meet the requirements of professional investors and corporations, emphasizing security, regulatory compliance and operational efficiency. All the exchanges have additional verification processes for business accounts, ensuring the compliance and legitimacy of the client's business, known as KYB (Know Your Business).

However, certain exchanges, such as Binance, Bit2Me and Coinbase, go beyond these standard offerings. They provide institutional and business clients with additional services that facilitate sustained business operations on their platforms. This includes the provision of payment services, access to marketplace listings and other business-centric functionalities.

CONCLUSIONS

Users who want to choose the best cryptocurrency exchange for their personal needs should consider looking beyond widely advertised criteria, such as fees, trading volumes and signup bonuses. While the practical significance of these is easy to understand for retail users, factors that are just as important often remain hidden below the surface. This includes whether the company is located in a tax haven or in a pro-customer jurisdiction, how transparent their finances are, their customer support and interface, and how they ensure the user's assets are secure and well-handled. Our analysis of these criteria has found marked differences among the examined set of exchanges. To conclude the report, we will attempt to narrow down which of them manage to perform well in all areas under analysis.

Firstly, we considered which exchanges are based in first-tier jurisdictions, such as the European Union, the United Kingdom or the United States. These countries tend to prioritize the needs of consumers over the needs of businesses. They therefore extend comprehensive legal safeguards to the customers of exchanges located in their country – whether these rules are specific to crypto or fall under general consumer protection legislation. Exchanges who choose to headquarter their operations in a pro-customer jurisdiction often also follow a proactive approach and take protective measures that go beyond what is required by law. Of the exchanges examined, Bit2Me, Bitstamp, Coinbase and Kraken are located in what we consider pro-customer jurisdictions, which is why we will focus on them for the rest of the conclusion.

Our second level of analysis concerned the internal processes of companies to keep customers assets, be they fiat or crypto, safe. For crypto assets, Kraken and Bit2Me have third party Merkle tree PoR audits to prove that they keep sufficient reserves, while Bitstamp and Coinbase are audited by one of the Big Four accounting firms. Fiat custody on the other hand is handled through electronic money issuers by almost all exchanges, which offers strong protections. We did find differences in how cybersecurity is handled by various exchanges, with Bit2Me and Kraken being a step ahead of the rest.

Thirdly, user experience and customer support demonstrate how well an exchange can adapt to the needs of its customers and ensure consumer decisions are made with the best possible information. Here, Bit2Me and Kraken are again up to par — both have excellent interfaces; both have comprehensive customer phone support and tax reporting tools. However, Kraken seems to be more focussed on U.S. customers. It offers no local phone numbers in non-English speaking countries and only has U.S. tax reporting tools. Bit2Me on the other hand cannot currently serve U.S. customers but offers a high level of convenience everywhere else.

Although Bit2Me offers more products, staking assets and altcoins than Kraken, the latter has derivatives trading and strong features for English-speaking users. It supports currencies such as the Australian, Canadian and U.S. dollars alongside the British pound and the euro. This makes it the next-best option in those countries where Bit2Me cannot serve customers, such as the United States. However, generally speaking, derivatives trading tends to only be available in less regulated jurisdictions, and one should carefully evaluate its risk profile before engaging in it.

To conclude this report, for users who want to follow new industry standards and choose the most trustworthy exchange, Bit2Me and Kraken are prime candidates. Bit2Me is superior for those who value extra transparency, local phone support and a wide range of staking, assets and products. Meanwhile, Kraken is for those based in the U.S. or who want to engage in derivatives trading and value additional transparency over other exchanges that offer this product.

Disclaimer and Contacts

Cointelegraph Consulting is not an investment company, investment advisor or broker/dealer. This publication is for information purposes only and represents neither investment advice nor an investment analysis or an invitation to buy or sell financial instruments. Specifically, the document does not serve as a substitute for individual investment or other advice.

In no event shall Cointelegraph Consulting be liable to you or anyone else for any decision made or action taken in reliance on the information in this report or for any special, direct, indirect, consequential or incidental damages or any damages whatsoever, whether in an action of contract, negligence or other sort, arising out of or in connection with this report or the information contained in this report. Cointelegraph Consulting reserves the right to make additions, deletions or modifications to the contents of this report at any time without prior notice.

Readers should be aware that trading tokens or coins and all other financial instruments involve risk. Past performance is no guarantee of future results, and we make no representation that any reader of this report or any other person will or is likely to achieve similar results.

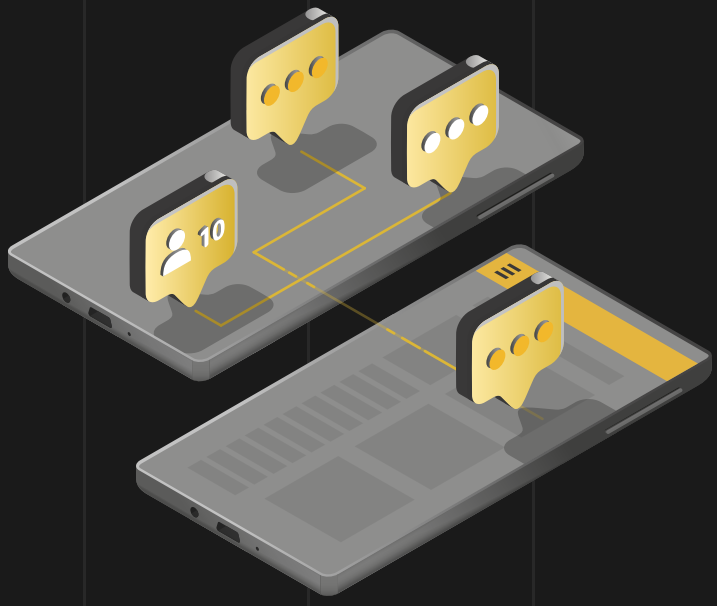
The statements contained in this publication are based on the knowledge as of the time of preparation and are subject to change at any time without further notice. The authors have exercised the greatest possible care in the selection of the information sources employed;
however, they do not accept any responsibility and neither does Cointelegraph Consulting for the correctness, completeness or timeliness of the information, respectively the information sources made available as well as any liabilities or damages, irrespective of their nature, that may result therefrom (including consequential or indirect damages, loss of prospective profits or the accuracy of prepared).

The value of cryptocurrencies can fall as well as rise. There is an additional risk of making a loss when you buy shares in certain smaller cryptocurrencies. There is a big difference between the buying price and the selling price of some cryptocurrencies, and if you have to sell quickly, you may get back much less than you paid. Cryptocurrencies may go down as well as up, and you may not get back the original amount invested. It may be difficult to sell or realize an investment. You should not buy cryptocurrencies with money you cannot afford to lose.

ADDITIONAL CONTACTS

Questions, Comments
or Customer Service

research@cointelegraph.com



This report was created in collaboration with and commissioned by Bit2me