DIGITAL
ASSET
RESEARCH

Exchange Vetting Methodology v2.9 Q4 2023

Table of Contents

1. Overview

1.1 Introduction

The Digital Asset Research (DAR) Exchange Vetting Methodology is designed to provide market participants with a transparent view of the objective process followed to evaluate the largest digital asset exchanges by reported volume. This process aims to identify trustworthy exchange platforms and encourage best practices by gathering, recording, and comparing a series of quantitative and qualitative data points.

DAR's team of researchers and technical experts work closely with exchanges, regulators, and investors to collect public and non-public data points that are used to reach a reasoned determination on each of the methodology's criterion. DAR regularly reviews each exchange using the vetting criteria described herein to ensure its conclusions remain reflective of the market.

DAR uses the Exchange Vetting Methodology to select data providers for its Digital Asset Research Reference Price. However, DAR also works with clients to ensure selected data providers meet their specific needs and can collaborate to create a bespoke methodology based on geography, liquidity, or other requirements.

The Exchange Vetting Methodology is reviewed quarterly and updated as required to reflect the maturing digital asset marketplace and the needs of its participants.

1.2 Process

During the Exchange Vetting process, DAR performs the following assessments:

- Regulatory Assessment
- Governance and Institutional Factors Assessment
- Technical Assessment
- Data Science Assessment

Each assessment is divided into factors that are determined to be essential, and these factors are individually scored as "Met", "Provisional" (partially passing or passing for less than the required time period), "Not Met", or "Not Applicable" ("N/A"). Unless otherwise noted, an assessment evaluation can only change from "Not Met" or "Provisional" to "Met" after an exchange has met the requirements of the relevant factor(s) for at least 6 months. Assessment results are compiled to form a comprehensive evaluation of each exchange.

To determine which exchanges should be vetted, DAR collects information on exchanges that report a minimum of $5 million USD in daily volume. These exchanges are then evaluated against a series of preliminary criteria, which are detailed below, including a liquidity check, capital control requirements, API availability, and data science tests. Exchanges that pass all preliminary checks are placed on the DAR Exchange Watchlist.

Exchanges on the Exchange Watchlist are then vetted under the comprehensive criteria and must receive a designation of “Met” or “N/A” for all mandatory factors to pass vetting and be added to the DAR Vetted Exchanges List. DAR engages with each exchange on the Exchange Watchlist to help them understand the steps needed to move towards promotion and encourage best practices.

Assessment results are reevaluated quarterly and updated as needed to maintain current and accurate vetting. When reevaluating results, the last weekday of the quarters ending in March, June, September, and December serves as the data cut-off date for the vetting process. Exchanges are added to and removed from the Vetted Exchanges List and Exchange Watchlist as a result of the quarterly vetting process. Each list is updated no later than 5 business days after the start of the new quarter and/or prior to any reconstitution or rebalance required by the most recent version of the DAR Reference Price Methodology.

1.3 Penalty List

An exchange that fails certain vetting criteria, including preliminary data science tests, is placed on the Penalty List. To be removed from the Penalty List and added to the Vetted Exchanges List:

- One year must pass from the date on which the exchange was placed on the Penalty List
- The exchange must pass the Exchange Vetting Methodology criteria that is current at that time
- The exchange must provide satisfactory answers to the Due Diligence Questionnaire that is current at that time
- The exchange must be approved by the Review Committee, which is described in the subsequent section

At the discretion of the Review Committee, an exchange removed from the Penalty List may be placed on Enhanced Review status. Exchanges with the Enhanced Review Status are vetted on a monthly basis and reevaluated by the Review Committee on a quarterly basis.

1.4 Review Committee

In the following exceptional cases, a Review Committee, comprised of executive members and advisors from DAR and governed under the DAR Review Committee Charter, will determine an exchange's eligibility based on the totality of circumstances involved:

1. An exchange that failed any of the preliminary criteria in the Data Science assessment may only be added to the Vetted Exchanges list after:
    a. Waiting a period of one year from the date of the failure
    b. Passing a subsequent Exchange Vetting review
    c. Giving satisfactory answers to the Due Diligence Questionnaire that is current at that time
    d. Achieving a positive determination by the Review Committee

2. A qualitative assessment that produces conflicting information requires thorough review and is therefore subject to Review Committee approval. Issues related to specific qualitative criteria (which are noted in this methodology), including those related to regulatory misconduct, will always require Review Committee approval.

3. An exchange that has passed full vetting may be placed on Enhanced Review status if subsequent diligence reveals conflicting or new information. Vetted Exchanges placed on Enhanced Review status are vetted on a monthly basis and are subject to review by the Review Committee to determine whether they will remain on the Vetted Exchanges list.

For additional information on the Review Committee, please see the Digital Asset Research Review Committee Charter.

1.5 Auxiliary Factors

DAR regularly engages with global regulators and market participants to discuss the behaviors an exchange must adopt to meet regulatory requirements and investor needs. Under each assessment, DAR also tracks Auxiliary Factors which have been cited by regulators, investors, and financial institutions as best practices in a maturing digital asset marketplace. Auxiliary Factor items are not currently mandatory under the Exchange Vetting Methodology because this information is often unavailable, incomplete, or the related policies and procedures are in varying states of implementation.

DAR gathers information about an exchange's current practices and future plans through a Due Diligence Questionnaire process and other direct communication. Auxiliary Factor items will be

added to the Exchange Vetting methodology as they are deemed necessary or appropriate based on market conditions or regulator guidelines.

2. Regulatory Assessment

During the Regulatory Assessment, DAR reviews the regulatory landscape in the jurisdiction where an exchange is domiciled, including the country's attitude toward digital assets, capital control requirements, and the regulatory framework. The assessment also looks at any licensing or registration requirements an exchange is subject to based on the location of its users.

2.1 Mandatory Factors

2.1.1 Capital Controls (Preliminary Criteria)

The Capital Controls factor reviews any capital control requirements in place in the country where an exchange is registered as a legal entity.

To meet the requirements of the Capital Controls factor, an exchange must be registered in a country which does not restrict the ability of domestic investors to acquire foreign assets or the ability of foreign investors to buy domestic assets. This requirement exists because an exchange located in a country that restricts the flow of domestic or foreign assets may have prices that reflect this constraint and are therefore not inline with the larger market.

An exchange's registration documentation and the capital control rules in the country where it is registered are reviewed when determining whether an exchange meets the requirements of the Capital Controls factor. An exchange will be given a designation of "Not Met" if it is registered in an excluded jurisdiction or if the name of its legal entity and/or registration location cannot be determined.

DAR maintains a list of countries that do not meet the Capital Controls requirement; this list is updated quarterly.

2.1.2 Regulatory Compliance

The Regulatory Compliance factor examines an exchange's compliance with the regulatory framework in the jurisdictions where it is domiciled.

When evaluating whether an exchange meets the requirements of the Regulatory Compliance factor, the jurisdictions where an exchange is headquartered, maintains an office, or is registered are determined. Local and federal regulations in each of those jurisdictions are then reviewed and compared against the exchange's licenses, registrations, and behaviors.

DAR continually monitors the evolving global digital asset regulatory landscape. Information on proper registrations and licenses in a jurisdiction is sourced from an exchange's website, as well as regulator and governmental registration databases. Third-party media sources are also monitored for reports of exchange behavior that is counter to these requirements.

To achieve a designation of "Met", an exchange must comply with all regulatory requirements in the jurisdictions where it is domiciled.

An exchange will be given a designation of "Not Met" if:

- it is confirmed the exchange does not comply with a regulatory requirement;
- the exchange is subject to legal action or substantial investigation by a regulatory body in a jurisdiction where is domiciled; or
- its country of registration cannot be determined.

2.1.3 Differentiation of Users Based on Geolocation

Many jurisdictions require an exchange to hold specific licenses or registrations prior to allowing users based in that jurisdiction to trade on an exchange. These rules vary widely by regulator and jurisdiction, and often include separate requirements for buying, selling, and converting digital assets.

To measure whether an exchange is attempting to comply with jurisdictional requirements, DAR reviews whether the exchange differentiates users based on geolocation. An exchange's terms of service or terms of use are reviewed to ensure the exchange specifiies in which countries or states its users may be located and restricts users in jurisdictions in which it does not hold proper licenses. DAR further confirms compliance by registering for the exchange and noting how the exchange verifies, or does not verify, user location prior to allowing trading.

An exchange achieves a designation of "Met" for this factor if it has a stated policy or protocol that restricts trading to users in specific jurisdictions. Exchanges that do not have a policy or protocol that restricts trading to users in specific jurisdictions are assumed to be non-compliant with these regulatory requirements and are given a "Not Met" designation.

3. Governance and Institutional Assessment

The Governance and Institutional Assessment looks at the governance and institutional factors in place at an exchange, including a review of know your customer (KYC)/anti-money laundering (AML) policies, exchange transparency, and the exchange leadership team.

3.1 Mandatory Factors

3.1.1 Liquidity (Preliminary Criteria)

To achieve a designation of “Met” for the Liquidity factor, an exchange must maintain a minimum average daily reported volume of $5M USD for 6 months prior to the assessment. This data is sourced from an exchange’s API and the daily average is calculated based on monthly totals.

3.1.2 Know Your Customer and Anti-Money Laundering

An exchange’s Know Your Customer and Anti-Money Laundering policies are collected from its website and reviewed when determining if the exchange meets this factor’s requirements. KYC and AML policies vary by exchange but generally require users to verify their identity by providing information such as an email address, phone number, bank account, government issued identification, or a user photo.

This assessment includes a review of whether, and to what level, an exchange requires a user to complete the KYC process prior to trading on the exchange or withdrawing funds, as well as any minimums a user can trade or withdraw without going through the KYC process. When made available during the confidential diligence process, DAR also reviews an exchange's full KYC policies to evaluate compliance with sanction list checks, politically exposed person (PEP) account monitoring, and other factors.

The robustness of an exchange’s KYC and AML policies determines whether an exchange is given a designation of “Met” for this factor.

3.1.3 Sanction Lists

An exchange’s official business entity name and registration name are collected from its website and reviewed against third-party sanction lists, including, but not limited to, the CFTC Red List and the ESMA sanctions database. If an exchange's official business entity name and registration name are not publicly available, DAR will review the exchange's known executives against OFAC's Specially Designated Nationals and Blocked Persons List (SDN) to determine the exchange's standing for this factor.

An exchange will fail this factor if it is listed on a sanctions list or if one of its executives is listed on the OFAC SDN list.

3.1.4 Fees

An exchange must operate as a centralized, for-profit business. An exchange's fee schedule, conversations with the exchange, and any relevant media are reviewed to determine whether the exchange meets this requirement.

To achieve a designation of "Met" for the Fees factor, an exchange must publicly list a uniform fee schedule and be determined to be a centralized, for-profit business.

3.1.5 Leadership Team

When reviewing an exchange's leadership team, two inquiries are made:

1. Can a C-level executive or equivalent be identified? DAR reviews whether the exchange has a transparent and accessible leadership team by reviewing public information, including the exchange's website, LinkedIn site, and regulatory filings.

2. Are there any known charges of a felony or other criminal activity which involves an element of fraud, or a finding of a willful violation of a regulatory requirement against any member of the leadership team? To make this determination, relevant media sources are monitored, including Google alerts, third-party news sources, and social media sites, such as Twitter and Reddit. Any reports of criminal or regulatory misconduct are verified by reviewing primary sources, including any available official documents.

To achieve a designation of "Met" under the Leadership Team factor, at least one member of the leadership team must be identified and no known member of the leadership team may have felony charges or any charges of criminal activity involving fraud or regulatory misconduct in the 12 months prior to the assessment.

A designation of "Not Met" due to criminal or regulatory misconduct by a member of the leadership team can only be overcome by removal of the offender or a resolution of the matter in compliance with the charging authority at least 6 months prior to a change in designation.

3.1.6 Accessible Support Team

To achieve a designation of "Met" for the Accessible Support Team factor, DAR must be able to reach an exchange's support team via email or other means that is not social media, and support team contact information must be available on the exchange's website.

3.1.7 No Criminal or Regulatory Misconduct

Under the No Criminal or Regulatory Misconduct factor, any charges, investigations, and findings against an exchange by a criminal or regulatory authority are reviewed. Third-party media is continually reviewed for information related to any such investigation or charge.

Upon finding an exchange is subject to an investigation or charge of misconduct, primary sources are reviewed to answer the following inquiries:

1. Has the exchange been found guilty of criminal activity or to have knowingly engaged in regulatory misconduct? If the answer to this inquiry is yes, the exchange is given a designation of “Not Met” for this criterion. If the answer is no, the assessment continues to the next inquiry.

2. Has the exchange complied with requests from the relevant criminal and/or regulatory authorities by taking actions such as responding to requests for information in a timely manner, ceasing operations in jurisdictions as ordered, and making operational or personnel changes required to correct offending behaviors? If the answer to this inquiry is yes, the exchange is given a designation of “Met” for this criterion. If the answer is no, the exchange is given a designation of “Not Met”. All determinations are made after a Review Committee review of the circumstances.

3.2 Auxiliary Factors

3.2.1 Market Surveillance Software

Market surveillance software monitors trading and assists in deterring suspicious market behavior. Some exchanges use third-party market surveillance software, while others use internal solutions such as a dedicated surveillance team or software that was developed in-house.

Under the Market Surveillance Software factor, DAR gathers information on an exchange’s market surveillance practices by reviewing publicly available information and communicating directly with the exchange.

3.2.2 Surveillance Sharing Agreements

Regulators often encourage intermarket communication as it helps to deter market manipulation and identify suspicious behavior. As part of the Surveillance Sharing Agreement factor, an exchange is asked about any information sharing agreements it has with other market participants.

3.2.3 Insurance

An exchange should hold an insurance policy that will cover losses that may be incurred as a result of a cyberattack. In the absence of a third-party insurer, an exchange should self-insure through a dedicated insurance fund. The Insurance factor asks an exchange about its insurance strategy.

3.2.4 Audit

It is best practice for an exchange to undergo a transparent and thorough audit completed by a known and reputable third party. An audit can help assure regulators and an exchange's investors that client funds are properly held. The Audit factor gathers information regarding an exchange's audit process or plans for an audit process.

4. Technical Assessment

The Technical Assessment reviews factors such as an exchange's data availability via an API, downtime history, security practices, and more. This assessment also considers any deficiencies identified in an exchange's operational security procedures.

4.1 Mandatory Factors

4.1.1 Centralized, Spot Exchanges (Preliminary Criteria)

An exchange must operate as a centralized organization which facilitates spot delivery transactions of underlying assets. If an exchange operates a futures market in addition to a spot market, the trading domains and asset pairs in these markets must be entirely separated. An exchange that meets these conditions will be given a designation of "Met" for this factor, while a decentralized or non-spot exchange will receive a "Not Met" designation.

4.1.2 Required Data (Preliminary Criteria)

An exchange must make data fields that show the asset pair, price, volume, and an accurate timestamp for each trade available via an API, Websocket, or other real time transfer protocol. An exchange that fails to provide any of the listed data will be given a designation of "Not Met" for this factor.

4.1.3 No Meaningful Security Lapses

In the 12 months immediately preceding the review, an exchange must not have suffered a security breach that resulted in a loss of client or exchange funds that exceeded 1% of total

holdings. Breaches are typically widely reported publicly. If a breach is suspected but unconfirmed, DAR may launch its own investigation by aggregating exchange addresses and performing blockchain analysis.

An exchange with no meaningful security lapses in the 12 months preceding the review will be given a designation of “Met” for this assessment. An exchange that is found to have suffered a meaningful security breach will be given a designation of “Not Met”; this designation can only be overcome after 12 continuous months without an additional security breach.

4.1.4 No Known Deficiencies in Operational Security

An exchange can have no known operational security deficiencies. Ideally, an exchange will have passed an independent security audit to show it has mitigated potential attack vectors and operational risks. In the absence of a public audit or an audit that is shared privately, an exchange will only receive a designation of “Not Met” if there is evidence from third-party sources or DAR’s analysis that the exchange is negligent with regards to its security practices; security deficiencies covered by other criteria in the Exchange Vetting Methodology, such as security breaches, exchange downtime, and criminal misconduct, are not considered when evaluating this factor.

When making a determination on this factor, DAR reviews public security policy disclosures, confers with the exchange about questionable or unclear security procedures, and reviews security procedures through the confidential diligence process. Absent confirmed audits or deficiencies, determinations of “Not Met” under this criterion require committee review.

4.1.5 No More Than 48 Hours of Downtime in a 30-day Period

An exchange must remain accessible and active to eligible users, and must not experience more than 48 hours of downtime in a given 30-day period, excluding expected and pre-announced maintenance downtime. For an exchange to be considered active, eligible users must be able to make trades, deposit funds, and withdraw funds.

To track downtime, DAR continuously pings the exchange and records periods of inaccessibility when data is not flowing and trades are not executed and recorded. Specifically, the trade history endpoint for an exchange’s highest traded Bitcoin (BTC) pair is pinged and the time between responses that do not return trades is recorded.

An exchange that is seen to have an aggregate of 48 hours of inaccessibility in one or more 30-day periods prior to the assessment will be given a designation of “Not Met”. An exchange may overcome a previous assessment of “Not Met” only after completing 6 continuous months with less than 48 hours of total downtime per month.

4.2 Auxiliary Factors

4.2.1 Confirmed Use of SegWit

Segregated Witness, or SegWit, is technology that increases the security and efficiency of Bitcoin transactions. SegWit mitigates against transaction malleability attacks, which occur when an attacker tricks an exchange's API into believing a withdrawal request failed to process when, in reality, the withdrawal was sent to the attacker's address. Successful attackers replay withdrawal requests and could potentially drain an exchange's entire hot wallet.

Transactions that use SegWit technology use an easily identifiable addressing system relative to legacy Bitcoin addresses. DAR analyzes an exchange's deposit addresses to determine whether the exchange has mitigated potential malleability attacks by implementing SegWit.

4.2.2 Cold Wallet Storage Custody Policy

Cold wallet storage is a custody technique that substantially decreases the potential for digital asset theft. It involves storing the keys that authorize ownership changes for the majority of assets held on an exchange in a completely closed, non-networked environment.

When reviewing an exchange's cold wallet storage custody policy, DAR evaluates publicly available information and communicates directly with the exchange to gain an understanding of its custody workflows. When deemed necessary, DAR can perform blockchain analysis to make a determination about an exchange's security procedures.

4.2.3 Business Continuity Plan

An exchange should have a written business continuity plan that creates sufficient redundancies and other systems for recovery from security breaches and catastrophic events. At a minimum, the business continuity plan should include:

- A list of critical tasks for continued operation
- Information on data and exchange website backups
- Instructions for key employees
- Details on user expectations

5. Data Science Assessment

The Data Science assessment confirms an exchange is accurately reporting trading volume between real users and that an exchange is not engaging in, or allowing users to engage in,

wash or other non-economic trading. To evaluate whether an exchange meets these requirements, DAR runs numerous tests on public trading and order book data sourced from the exchange to confirm:

- Trading patterns do not widely diverge from the wider market (preliminary criteria)
- Trading occurs at natural and expected lot levels (preliminary criteria)
- Price data follows natural patterns that track the market
- Trading volume data follows natural patterns that track the market
- Price data does not widely diverge from the wider market
- Trading volume data aligns with user engagement

For additional details on the tests run during the Data Science Assessment, please contact info@digitalassetresearch.com.

6. Conclusion

DAR's Exchange Vetting Methodology is designed to apply independent and objective rigor to the cryptocurrency marketplace. It intends to provide a clean price, encourage best practices, promote transparency, and address the concerns of participants entering the space. The methodology is continually reviewed to ensure it meets the needs of the maturing market.

Upon request, eligible clients can access the results of the Exchange Vetting process and utilize its findings in their own application.

Appendix 1: Changelog

Substantive changes to the Exchange Vetting Methodology are tracked in the table below.

Date	Change	Description
9/2019	Addition of Section 1.3, “Committee Review”	Committee Review, Enhanced Review Status, and penalty imposed for previously failing either preliminary data science test.
9/2019	Change in value to variable F_c	“Minimum frequency difference” variable for the Buy-Sell Permutation test changed from 8% to 5%.
3/2020	Removal of Section 2.1.3	Auxiliary factor: “Licensed with Appropriate Regulatory Bodies Based on the Location of Users”
3/2020	Removal of an auxiliary factor	Sound Banking Relationships
3/2020	Removal of an auxiliary factor	Uniformly Applied Egress/Withdrawal Protocols
3/2020	Removal of an auxiliary factor	Uniformly Applied Corporate Action Policies
3/2020	Updated correlation scores	With the larger influx of exchanges this quarter, the correlation critical values were updated to reflect this
6/2020	Removal of Data Science test details	Data Science assessment test details were removed and are available by request
6/2020	Content updated	Minor changes were made to wording throughout document for additional clarity
6/2020	Section numbering updated	Section numbering was changed throughout the document
11/2020	Sanctions List factor added	The Sanctions List item was added as a mandatory factor under the Governance and Institutional Assessment.

Disclaimer

All information is provided for information purposes only and provided "as is" without warranty of any kind. Neither Digital Asset Research (“DAR”) nor its respective directors, officers, employees, partners or licensors make any claim, prediction, warranty or representation whatsoever, express or implied, as to the accuracy, timeliness, completeness, merchantability or the fitness or suitability for any particular purpose of any information contained herein or any information or results to be obtained from the use of DAR products. Neither DAR, nor its respective directors, officers, employees, partners or licensors, provide investment advice and nothing contained in this document constitutes financial or investment advice. No responsibility or liability can be accepted by DAR nor their respective directors, officers, employees, partners or licensors for (a) any loss or damage in whole or in part caused by, resulting from, or relating to any error (negligent or otherwise) or other circumstance involved in procuring, collecting, compiling, interpreting, analyzing, editing, transcribing, transmitting, communicating or delivering any such information or data or from use of this document or links to this document or (b) any direct, indirect, special, consequential or incidental damages whatsoever resulting from the use of, or inability to use, such information. No part of this information may be reproduced, stored in a retrieval system or transmitted in any form or by any means without prior written permission of DAR. Use and distribution of any data or product provided by DAR requires a license from DAR and/or their respective licensors.