DIGITAL
ASSET
RESEARCH

Digital Asset Vetting Methodology v1.0, Q1 2022

Table of Contents

1. Overview

1.1 Introduction

The Digital Asset Research (DAR) Digital Asset Vetting Methodology is designed to provide market participants with a transparent view of the objective process followed to determine the quality, reliability, and safety of various digital assets whose codebase, monetary policy and network consensus is fully decentralized. This process is intended to provide a comparable view of different decentralized digital assets and encourage best practices among their maintainers by gathering, recording, and comparing a series of quantitative and qualitative data points. While there are centralized digital assets that might follow industry-wide best practices, the scope of this methodology is limited to decentralized digital assets that may be appropriate for a liquid index.

DAR's team of researchers and technical experts works with exchanges, regulators, investors, and digital asset developers 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 digital asset using the vetting criteria described herein to ensure its conclusions remain reflective of the market.

1.2 Process

The Asset Vetting Methodology includes Preliminary Vetting and Comprehensive Vetting components, which are described in subsequent sections.

Assets are vetted on a quarterly basis, with the last weekday of the months ending in February, May, August, and November serving as the data cut-off dates for the vetting process. Asset vetting is completed by 5 p.m. on the Friday following the first full week of the subsequent month.

2. Preliminary Vetting

Preliminary Vetting evaluates the venues where digital assets trade and some additional criteria to determine which assets will go through the Comprehensive Vetting process.

DAR uses a secondary methodology, Exchange Vetting, to evaluate digital asset exchanges via quantitative and qualitative assessments. Exchange Vetting selects venues where real economic activity is reported, and only assets that trade on venues that pass Exchange Vetting are considered for Asset Vetting. To pass Preliminary Vetting, each asset must also:

- Trade on a minimum of two vetted exchanges if the asset passed Comprehensive Vetting in the previous quarter or trade on a minimum of three vetted exchanges if the asset did not pass Comprehensive Vetting in the previous quarter
- Be directly convertible to one of the following fiat or crypto currencies: United States Dollar (USD), South Korean Won (KRW), Chinese Yuan (CNY), Japanese Yen (JPY), Euro (EUR), Pound sterling (GBP), Bitcoin (BTC), Ethereum (ETH), or Tether (USDT)
- Meet one of the following requirements over the past 6 months:
    - Trade volume on vetted exchanges is greater than 10% of the total combined trade volume on vetted and watchlist exchanges
    - The number of trades on vetted exchanges is greater than 10% of the total combined number of trades on vetted and watchlist exchanges
    - The price correlation between vetted and watchlist exchanges is greater than 0.5

Digital assets that pass Preliminary Vetting are added to the Asset Vetting Watchlist, which lists all assets that will go through the Comprehensive Vetting process.

3. Comprehensive Vetting

3.1 Overview

In Comprehensive Vetting, five assessments are used to evaluate each asset on the Asset Vetting Watchlist, as well as the network that supports the asset:

- Codebase Assessment
- Network Security Assessment
- Protocol Security Assessment
- Liquidity Assessment
- Regulatory Assessment

Each assessment is subdivided into factors determined to be essential, which are then individually scored as “Pass”, “Fail”, or “Not Applicable”. Qualitative and quantitative data points are reviewed and considered when evaluating each factor.

The results of these assessments are compiled to form a comprehensive assessment of each evaluated asset. Assessment results are reevaluated quarterly and updated as needed to maintain current and accurate vetting results.

Digital assets that fail Comprehensive Vetting are flagged in the Asset Vetting Review Sheet, which is compiled quarterly.

3.2 Codebase Assessment

3.2.1 Overview and Target Repository Selection

Due to their intrinsic complexity, digital assets require a team of dedicated developers who work to improve the asset's supporting codebase, resolve issues, and add new features. Open source blockchain networks are comprised of multiple pieces of software that live in an open source repository, which is an online folder where the codebase is stored.

The Codebase Assessment selects and evaluates a Target Repository for each digital asset. This is handled differently for Native Digital Assets and Application Tokens, as described below.

Native Digital Assets are a network's main medium-of-exchange and the currency used to pay network transaction fees, such as Ether (ETH) on the Ethereum Network. When evaluating Native Digital Assets, the Codebase Assessment focuses on the digital asset network's Client, which is its most important piece of software. Network participants use the Client to send, receive, relay, and validate digital asset transactions. The Client also enforces rules that define key properties of the Native Digital Asset, such as its inflation, divisibility, and transferability. When evaluating Native Digital Assets, the Target Repository is the repository where the most used network Client lives.

Application Tokens exist within a digital asset network and are solely used within an application, such as the 0x (ZRX) token that is supported by the Ethereum Network. When evaluating Application Tokens, the Target Repository is the core repository of the application itself. The software in Application Token repositories is often in the form of smart contracts, which are contracts written in a language that can be processed by the application's parent network. For example, the Target Repository for ZRX is the smart contract codebase that supports its Decentralized Exchange protocol, which is 0x's main application.

Once a digital asset's Target Repository is determined, the Codebase Assessment evaluates a set of Mandatory Qualitative Factors that review the licensing, maintenance, and operational procedures that support the asset's repositories and codebases. An asset that passes the Mandatory Qualitative Factors evaluations then undergoes a series of Quantitative Tests that measures the activity in its developer ecosystem and the effectiveness of its developers.

3.2.2 Mandatory Qualitative Factors

As part of the Codebase Assessment, a digital asset must pass the requirements of the following Mandatory Qualitative Factors, which are detailed in subsequent sections:

- Open Source Requirement

- Compatible Open Source License
- Distributed Version-Control System
- Full Attribution and Plagiarism Identification
- Secure Software Release
- Base Layer Stability
- Client Accessibility
- Formalized Vulnerability Reporting Workflows

A digital asset that does not meet the requirements of all Mandatory Qualitative Factors will fail Asset Vetting.

3.2.2.1 Open Source Requirement

To enable a review of the entirety of a digital asset's codebase and determine its Target Repository, the entirety of a project's source code must be made publicly available in an open and free-to-access repository.

3.2.2.2 Compatible Open Source Licenses

A digital asset must use a standardized open source license to govern the software's external use. Specifically, Target Repositories must use an open source license recognized by the Open Source Initiative (OSI), an organization that maintains and standardizes open source licenses. As of 1Q20, the list of acceptable open source licenses is as follows:

Popular and widely-used or with strong communities

- Apache License 2.0 (Apache-2.0)
- 3-clause BSD license (BSD-3-Clause)
- 2-clause BSD license (BSD-2-Clause)
- GNU General Public License (GPL)
- GNU Lesser General Public License (LGPL)
- MIT license (MIT)
- Mozilla Public License 2.0 (MPL-2.0)
- Common Development and Distribution License 1.0 (CDDL-1.0)
- Eclipse Public License 2.0 (EPL-2.0)

International licenses

- CeCILL License 2.1 (CECILL-2.1)
- European Union Public License (EUPL-1.2)
- Licence Libre du Québec – Permissive (LiLiQ-P) version 1.1 (LiLiQ-P-1.1)
- Licence Libre du Québec – Réciprocité (LiLiQ-R) version 1.1 (LiLiQ-R-1.1)
- Licence Libre du Québec – Réciprocité forte (LiLiQ-R+) version 1.1 (LiLiQ-Rplus-1.1)

Special purpose licenses

- BSD+Patent (BSD-2-Clause-Patent)
- Educational Community License, Version 2.0 (ECL-2.0)
- IPA Font License (IPA)
- Lawrence Berkeley National Labs BSD Variant License (BSD-3-Clause-LBNL)
- NASA Open Source Agreement 1.3 (NASA-1.3)
- OSET Public License version 2.1 (OSET-PL-2.1)
- SIL Open Font License 1.1 (OFL-1.1)
- Upstream Compatibility License v1.0

Other/Miscellaneous licenses

- Adaptive Public License (APL-1.0)
- Artistic license 2.0 (Artistic-2.0)
- Open Software License (OSL-3.0)
- Q Public License (QPL-1.0)
- Universal Permissive License (UPL)
- Zero-Clause BSD/Free Public License 1.0.0 (0BSD)
- zlib/libpng license (Zlib)

Licenses that are redundant with more popular licenses

- Academic Free License 3,0 (AFL-3.0)
- Attribution Assurance License (AAL)
- Eiffel Forum License V2.0 (EFL-2.0)
- Historical Permission Notice and Disclaimer (HPND)
- Lucent Public License Version 1.02 (LPL-1.02)
- The PostgreSQL License (PostgreSQL)
- University of Illinois/NCSA Open Source License (NCSA)
- X.Net License (Xnet)

Non-reusable licenses

- Apple Public Source License (APSL-2.0)
- Computer Associates Trusted Open Source License 1.1 (CATOSL-1.1)
- eCos License version 2.0
- EU DataGrid Software License (EUDatagrid)
- Entessa Public License (Entessa)
- Frameworx License (Frameworx-1.0)
- IBM Public License 1.0 (IPL-1.0)
- LaTeX Project Public License 1.3c (LPPL-1.3c)
- Motosoto License (Motosoto)
- Multics License (Multics)
- Naumen Public License (Naumen)
- Nethack General Public License (NGPL)
- Nokia Open Source License (Nokia)

- OCLC Research Public License 2.0 (OCLC-2.0)
- PHP License 3.0 (PHP-3.0)
- Python License (Python-2.0)
- CNRI Python license (CNRI-Python) (CNRI portion of Python License)
- RealNetworks Public Source License V1.0 (RPSL-1.0)
- Ricoh Source Code Public License (RSCPL)
- Sleepycat License (Sleepycat)
- Sun Public License 1.0 (SPL-1.0)
- Sybase Open Watcom Public License 1.0 (Watcom-1.0)
- Vovida Software License v. 1.0 (VSL-1.0)
- W3C License (W3C)
- wxWindows Library License (WXwindows)
- Zope Public License 2.o (ZPL-2.0)

Superseded licenses

- Apache Software License 1.1 (Apache-1.1)
- Artistic license 1.0 (Artistic-1.0)
- Common Public License 1.0 (CPL-1.0)
- Eclipse Public License 1.0 (EPL-1.0)
- Educational Community License, Version 1.0 (ECL-1.0)
- Eiffel Forum License V1.0 (EFL-1.0)
- Lucent Public License ("Plan9"), version 1.0 (LPL-1.0)
- Mozilla Public License 1.0 (MPL-1.0)
- Mozilla Public License 1.1 (MPL-1.1)
- Open Software License 1.0 (OSL-1.0)
- Open Software License 2.1 (OSL-2.1)
- Reciprocal Public License, version 1.1 (RPL-1.1)

3.2.2.3 Distributed Version-Control System

A digital asset project must use an open source, distributed version-control protocol, such as Git, to track, authenticate, and validate all codebase changes. Projects must also maintain a web-based interface, such as GitHub or GitLab, that allows for programmatic measurement of Target Repository activity via an API.

3.2.2.4 Full Attribution and Plagiarism Identification

Digital asset projects may use software developed by other projects when structuring core functionality, but this software must be properly attributed to its creators.

3.2.2.5 Secure Software Release

To prevent the download of compromised software, users must be able to assess the validity of all software releases from a digital asset project's core development team.

A digital asset project must have the lead maintainers of its Target Repository sign its releases and make their public PGP keys easily accessible so users can verify the software's validity. Alternatively, a digital asset project can employ hash matching or checksum techniques, whereby common hash functions are used to verify the integrity of the software release.

3.2.2.6 Base Layer Stability

The underlying data structure used to keep track of digital asset ownership changes must be a blockchain, whereby transactions are grouped into blocks in pre-specified epochs. Acyclic graphs can be used within the Client implementation instead of a blockchain only if there is global consensus on a single, widely distributed ledger.

Privacy-focused digital assets will be evaluated only if they offer View Keys, which enable third parties trading these assets to comply with required regulations.

3.2.2.7 Client Accessibility

The Client software used to join a digital asset's network must be accessible to a wide range of users. The reference Client must be available for installation on a stable distribution of at least two of the following operating systems:

- GNU/Linux
- macOS
- Windows

3.2.2.8 Formalized Vulnerability Reporting Workflows

Due to their complexity, digital asset networks rely on their community of users for issue identification and reporting. A digital asset project must provide a formalized method to report bugs and security vulnerabilities. Users must be able to open issues, discuss bugs, and suggest potential remediation strategies on a platform such as GitHub. Digital asset networks must also provide instructions for reporting sensitive vulnerabilities, such as inflation bugs, which require secrecy.

3.2.3 Quantitative Factors

The Codebase Assessment uses a set of four quantitative tests to evaluate and identify digital asset project developer activity and effectiveness in the Target Repository. Developer activity data is collected on a rolling basis via the GitHub and GitLab APIs and the quantitative tests are applied to a data set that begins 6 months prior to the cut-off date. Note that while Watchlist Assets are evaluated on a quarterly basis, a rolling 6-month data sample is used in testing because it provides a more complete look at cyclical activity in the Target Repository and long-term events, such as the onboarding of new developers.

Each quantitative test carries equal weight and results are recorded as “Pass” or “Fail”. To pass the quantitative portion of the Codebase Assessment, a digital asset project must not fail more than 4 tests over the course of 2 vetting cycles. For example, if a project fails 2 of 4 quantitative tests in a vetting cycle, it must not fail more than 2 tests in the following cycle to pass the Codebase Assessment. Projects that fail the Codebase Assessment are sent to the Review Committee.

3.2.3.1 Commit-to-Contributor Threshold Requirement

The Commit-to-Contributor Threshold Requirement is a measure of developer activity. Contributors are accounts that represent individual developers or development shops that have implemented changes to the Target Repository in the past 6 months. After Contributors are identified, the total number changes to the codebase, known as Commits, made by Contributors is counted. To pass the Commit-to-Contributor Threshold Requirement, a digital asset project must have at least 5 Contributors implement at least 5 total Commits in the 6 months prior to the cut-off date.

3.2.3.2 Open-to-Close-Issue (OCI) Ratio Requirement

The Open-to-Close Issue (OCI) Ratio is a direct measure of developer effectiveness over the 6-month period prior to the cut-off date. It is calculated by dividing the total number of Open Issues (codebase issues not fixed by the development team) by the total number of Closed Issues (codebase issues fixed by the development team). To pass the OCI Ratio Requirement, the resulting ratio must be lower than 0.5.

3.2.3.3 Minimum Proposed Pull Request (PPR) Requirement

The Minimum Proposed Pull Request (PPR) Requirement is a measure of developer activity. It is calculated by adding the total number of Pull Requests (requests to change the codebase) from a digital asset project’s internal developers, external developers, and users. To pass the Minimum PPR Requirement, a digital asset project must have at least 5 Pull Requests proposed to its Target Repository in the 6-month period prior to the cut-off date.

3.2.3.4 Minimum Merged Pull Request (MPR) Requirement

The Minimum Merged Pull Request (MPR) Requirement is a measure of developer activity. It is calculated by adding the total number of Pull Requests implemented by a digital asset project’s internal or external developers. To pass the Minimum MPR requirement, a digital asset project must have at least 2 Pull Requests merged to its Target Repository in the 6-month period prior to the cut-off date.

3.3 Network Security Assessment

The Network Security Assessment is designed to measure a network's susceptibility to a hostile takeover, which occurs when a malicious entity gains control of the process that validates new transactions in the ledger.

This assessment is applicable to the network that supports a digital asset. Assets that are supported by the same network will have the same Network Security Assessment results. For example, Ether and all ERC-20 Standard Application Tokens are supported by the Ethereum Network and thus have the same Network Security Assessment results.

3.3.1 Byzantine Fault-Tolerant Consensus

Byzantine fault tolerance is a feature that allows a distributed network to resist against arbitrary or erratic information produced by a fraction of its participants. Digital asset networks require participants to coordinate and continuously reach consensus on the validity of network transactions. When a minority of coalition participants begins to contradict global consensus by producing erroneous transactions, a Byzantine Fault-Tolerant (BFT) network is still able to function adequately, making this a critical feature. Byzantine faults are not necessarily malicious, as they can result from faulty software or a configuration error, but consensus failures are extremely disruptive to digital asset networks and can enable fraudulent activity. To prevent Byzantine faults and network attacks, a digital asset network must use Proof-of-Stake, Proof-of-Work, or a hybrid consensus solution.

For this assessment, a digital asset project's whitepaper is reviewed to determine how its consensus algorithm and miners, or block producers, handle Byzantine fault tolerance. To pass the Byzantine Fault-Tolerant Consensus requirement, a network must be able to sustain consensus when at least 33% of its participants are Byzantine actors. A network's consensus algorithm and the specifications of its Sybil protection mechanism, such as Proof-of-Work or Proof-of-Stake, are reviewed to determine if the network meets this requirement.

3.3.2 Open and Permissionless Access

In order to guarantee censorship-resistance and optimize data availability, a digital asset project must not require network participants to sign a contractual agreement to join its network and validate the most recent height of its blockchain. This includes but is not limited to non-disclosure agreements (NDAs), access fees, or any form of legal agreement.

The Open and Permissionless Access requirement is evaluated by reviewing a digital asset project's Target Repository and the documentation for its most popular Client implementation. If necessary, DAR may run the Client and document the process to perform an Initial Blockchain Download (IBD) during its evaluation.

3.3.3 Diverse Validation Quorum

Blockchains are designed to be appended each time a specific set of consensus rules are satisfied. Network participants are financially incentivized to attempt to append the ledger and to relay information on new blocks to other participants so the entire network shares the same ledger. A diverse set of participants must be engaged in this process to prevent a malicious party from taking over the network and enacting new consensus rules, censoring transactions, or dictating higher network fees.

To meet the Diverse Validation Quorum requirement, a digital asset network must have at least 5 publicly identifiable validators actively producing blocks on a randomly sampled day. Validators are identified using an official block explorer, a hashrate distribution dashboard, or a Coinbase transaction record. Large block producers, like mining pools, are identified by reviewing the metadata attached to a block's header.

3.4 Protocol Security Assessment

Public-key cryptography provides a way for users to prove ownership of balances and securely transfer assets within digital asset networks. As part of the Protocol Security Assessment, the security of the cryptographic tools used by a digital asset project is examined. Specifically, the digital asset's custody standards in the context of private key generation and its accompanying transfer protocols are reviewed, as well as the digital signature algorithm used to produce signatures and authorize transfers.

3.4.1 Compatibility with Hierarchical Deterministic Wallets (BIP32/BIP44)

A digital asset must be compatible with the Hierarchical Deterministic (HD) wallet protocol, as implemented in Bitcoin Improvement Proposal (BIP) numbers 32 and 44. The standards described in BIP32 and BIP44 allow multiple public and private key pairs to be derived from a single starting point, known as a seed. Using a seed for key derivation simplifies digital custody workflows and increases security. Additionally, the use of BIP32, BIP44, or a close variant, enables compatibility with Hardware Security Modules (HSMs) for non-networked storage of private keys.

To pass the Protocol Security Assessment, a digital asset must use a protocol that is standardized and replicates the functions described in BIP32 or BIP44.

3.4.2 Compatibility with Mnemonic Passphrase Backups (BIP39)

Digital assets must allow for the creation of HD wallets via mnemonic keys, which use a group of pseudo-random words to derive a private key. This seed derivation protocol simplifies the

custody of digital assets, increases the security of private key backups, and makes digital assets more user friendly.

To pass the Protocol Security Assessment, a digital asset must use mnemonic standards that are based on BIP39.

3.4.3 Standardized Signature Algorithm

The cryptographic protocol that a digital asset uses to secure user assets must be a standardized and widely accepted scheme. This minimizes the possibility of unknown security vulnerabilities, which are frequently found in recently developed cryptographic algorithms.

To pass the Protocol Security Assessment, the signature algorithm that a digital asset uses to sign network transactions must be approved by the National Institute of Standards and Technology (NIST).

3.5 Liquidity Assessment

The Liquidity Assessment is designed to measure the relationship between the price a digital asset can be sold for and its speed of sale. In a liquid market, there is a mild trade-off between these factors; selling quickly will not reduce an asset's price. In a relatively illiquid market, selling a digital asset quickly will require cutting its price by some amount. The Liquidity Assessment evaluates free float and market capitalization because they offer insight into a digital asset's volatility.

3.5.1 Free Float Above 10%

Free float, also referred to as circulating supply, represents the number of tokens issued through a digital asset protocol that are currently available for trading. For digital assets that employ Proof-of-Work, free float determinations can be made algorithmically by tracking the issuance of assets via block rewards. For assets that performed a public sale through an ICO, STO, or IEO, further analysis may be required to determine free float.

To pass the Liquidity Assessment, a digital asset's free float must be 10% or more of the total supply.

3.5.2 Market Capitalization Above $50M

Market capitalization is used to compare the sizes of different digital asset markets. A digital asset's market capitalization is calculated by multiplying the number of outstanding assets by its price as of the cut-off date.

To pass the Liquidity Assessment and assure a level of market maturity, a digital asset's market capitalization must be above $50M USD as of the cut-off date.

3.6 Regulatory Assessment

The Regulatory Assessment evaluates whether a digital asset has violated a regulation that exists as of the cut-off date.

3.6.1 Regulatory Enforcement

Digital assets cut across jurisdictional boundaries and can fall into gaps between regulatory authorities. Additionally, determinations of whether an asset fits the definition of a security in a specific jurisdiction are outside of the scope of this methodology. However, all regulatory developments related to an asset as of the cut-off date are reviewed to determine if the asset will pass the Regulatory Assessment.

4. Conclusion

DAR's Digital Asset Vetting Methodology is designed to encourage best practices among decentralized projects, promote transparency, and address the concerns of participants entering the digital asset market. This methodology is continuously reviewed to ensure it meets the needs of the maturing digital asset market.

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

Appendix 1: Changelog

Changes to the Digital Asset Vetting Methodology are tracked in the table below.

Version	Date	Changes
0.8	October 2021	• Clarified Preliminary Vetting criteria with regards to where an asset must trade
0.4	October 2020	• A new requirement regarding trade volume, the number of trades, or price correlation was added to the Preliminary Vetting criteria
0.3	May 2020	• Added Table of Contents • Changed section numbering throughout based on content reorganization • Minor changes to wording throughout for additional clarity • Clarified Asset Vetting timing in Process subsection • Moved Preliminary Vetting content to a top-level section • Renamed Assessments section to Comprehensive Vetting and moved comprehensive vetting overview to this section • Categorized list of acceptable open source licenses • Moved Changelog to Appendix • Added Version to Changelog
0.2	Feb. 2020	• Added standalone sections on preliminary vetting and the exchange vetting methodology • Refined process overview • Defined Watch List Assets, Exchange Vetting, Asset Vetting Review Sheet • Clarified difference between network assessment vs asset assessment • Added list of NIST-standardized approved signatures • Added note on Privacy assets and view keys • Added distinctions between Token vs. Network • Narrowed scope of the codebase assessment on the Client (for standalone networks) and the Application (for application tokens) • Added OSI list of acceptable open source licenses • Added new “Base Layer Stability” factor • Added 4 quantitative codebase assessments and passing criterion for each • Clarified the process for removal from the index • Increase the minimum capitalization requirement to $50M • Changed criteria to “Pass”, “Fail” and “Not Applicable” • Added five trading pairs to preliminary testing (CNY, KWR, GBP, EUR, USDT)
1.0	April 2022	• *Process* section updated to reflect change in timeline for Asset Vetting