Potestas Solutions
LEADING CHANGE

April 24, 2025

A Crypto Asset Risk Classification Methodology: CARR (Crypto Asset Risk Rating)

Absence of a Universal Framework

Denise Mejia
Potestas Solutions LLC
Support@potestassolutions.com

Abstract: The rapid expansion of crypto assets and decentralized finance (DeFi) ecosystems has introduced a broad spectrum of new risks. However, there is no universally accepted methodology for classifying and assessing individual crypto assets risks. This absence creates notable challenges for investors, regulators, custodians, and technology providers, who must navigate inconsistent standards and incomplete risk profiles. The lack of a unified risk classification methodology leads to fragmented decision-making and increased risk exposure across the cryptocurrency value chain.

This whitepaper offers a solution to the critical need for a unified Crypto Asset Risk Classification Methodology that can bridge regulatory expectations, institutional requirements, and evolving blockchain technologies. It examines risk factors unique to digital assets and is a method for applying weighted values and calculations to the underlying conditions that increase risks, resulting in a risk classification. By establishing a clear, adaptable classification methodology, stakeholders can better assess, mitigate, and communicate crypto-asset risks in a scalable way.

1. Introduction

CoinGecko utilizes an informal framework that focuses on investment risk rather than security or regulatory risk that applies implicit risk classification. Basel Committee on Banking Supervision (BCBS) Crypto Exposure Guidelines groups crypto assets into risk classifications based on predefined criteria, supporting capital adequacy and systematic risk of financial institutions. Swiss regulator FINMA classifies crypto assets into Payment Tokens, Utility Tokens, and Asset Tokens, focusing on AML (Anti-Money Laundering).

The World Economic Forum (WEF) Token Taxonomy Framework focuses on technical and functional risk classification, examining governance structures, token behavior, economic rights, and regulatory implications. Many institutions use NIST SP 800-30 Rev. 1 and SP 800-37 to develop custom risk models for crypto assets, focusing on threat actors, vulnerabilities, and impact areas. Currently, NIST does not provide a dedicated risk-scoring methodology for crypto assets (e.g., Bitcoin, stablecoins, NFTs, etc.). However, NIST offers risk assessment frameworks and methods that can be used to assess the risk of crypto assets as part of a broader digital ecosystem.

Chainalysis developed a tool for blockchain Analytics that classifies wallets and assets' illicit activity response, geolocation of counterparties, and transaction behavior. While all these frameworks and tools serve a purpose, no comprehensive investor-friendly risk-scoring methodology is available today.

Out of scope: For this whitepaper will not be analyzing risk vectors since they can be tied to each of the risk categories above. For example, poorly written code falls under Technology Risk.

2. Known Risk Factors of Crypto Assets

Understanding and classifying types of crypto asset risks is essential for effectively managing and anticipating potential threats in the cryptocurrency ecosystem. Today, there is no consistent methodology that easily assesses the risk of individual cryptocurrency assets, considering all the crypto risk categories, such as market risk, security risk, technology risk, adaptation risk, and regulatory risk. Investors should carefully analyze these risk factors before investing in cryptocurrency assets. If there was a systematic way to conduct the analysis, the market could gain more credibility. Risk classification of crypto assess is a developing area, several methodologies to evaluate risk type, severity and regulatory impact are evolving.

In cryptocurrency, risk factors can be defined as the underlying conditions that increase risk or make it more likely to happen:

Market risk is the possibility of financial loss that investors face due to fluctuations in cryptocurrency market prices or conditions. This risk affects assets that are traded or valued, including cryptocurrencies.
Technology risk is a specific condition within a technology system that increases the likelihood or impact of failure, breach, or disruption.
Adaption risk refers to the risk that users, systems, or stakeholders will not successfully adapt to the new change, technology, process, or environment.
Regulatory risk is the likelihood that a change in laws, regulations, or performance will negatively impact a project or a crypto asset directly or indirectly.
Security Risk is the likelihood that someone could break into your system and steal data, causing damage or disrupting operations.

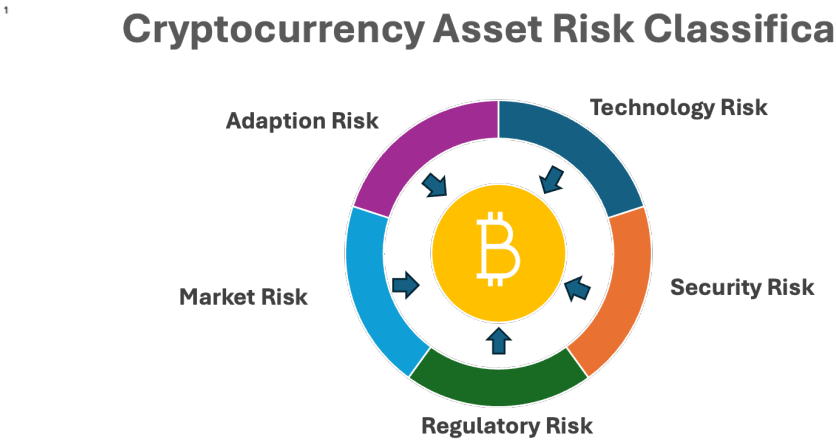
Suppose we want to identify the risk rating for crypto Asset A. Below is a recommended method for assigning risk to a crypto asset.

3. Four Steps to Calculate Risk Rating for a Crypto Asset

Step 1:
Identify the applicable Risk Factors (RF) impacting the "Asset A."

Crypto Asset A Risk Factors					
Factors (RF)	Market Risk	Adaption Risk	Security Risk	Technology Risk	Regulatory Risk

The illustration below shows the risk components (risk factors) affecting an individual cryptocurrency asset. This methodology is designed to incorporate additional risk factors as the ecosystem evolves and new areas of risk are identified.



Step 2

Define the **Risk Rating Values (RRV)** as Low (L), Moderate (M), High (H), and Very High (VH) risks.

Risk Rating Values (RRV)	
L =	1
M =	2
H =	3
VH =	4

Step 3

Assign a **Risk Factor Weight Value (RFWV)** to each Risk Factor (RF) (pick a number from 1 to 4) to qualify their relative importance to the overall risks of Asset A. Assign a value to each Risk Factor impacting crypto asset A.

Risk Factors Weight Values (RFWV)	
Low Significance =	1
Moderate Significance =	2
Significant =	3
Very Significant =	4

Risk Factors Weight Values (RFWV)						Total
Risk Factors (RF)	Market Risk	Adaption Risk	Security Risk	Technology Risk	Regulatory Risk	
Asset A Weight (WV)	3	2	3	2	4	14

In this scenario for crypto asset A, the sum of Risk Factors Weighted Values (RFWV) is 14

Step 4

Determine the **Crypto Asset Risk Rating (CARR)** by dividing the sum of Total Risk Factors Weighted Values by 5 (number of risk factors) based on the previously defined risk factor values in step 2. The CARR is calculated as the average of all Risk Factor Weighted Values (RFWVs). In the example provided, a total score of 14 across five risk factors yields a CARR of 2.8, which falls within the **Moderate Risk** range.

Formula:

$$\text{CARR} = \frac{\sum_{i=1}^{n} \text{RFWV}_i}{\text{n}} = \frac{14}{5} \quad 2.8$$

Where:

CARR = Crypto Asset Risk Rating

RFWVi = Weighted Value of each risk factor

n = Total number of risk factors

In the given example: 14/ 5= 2.8514 → **Moderate Risk**

4. Conclusion

We have proposed a scalable universal method for calculating the risk rating of individual cryptocurrency assets that consists of four steps and can be systematically applied to the risk rating calculation of crypto assets using oracles to fetch currently available information about specific risk factors. The model allows for flexibility as the risk score values can be modified by the organization adopting the framework. The methodology can be consistently adapted so that risk ratings can systematically change based on risk factor data available to crypto companies. Existing methodologies and tools can be integrated into risk-scoring calculations based on the risk categories defined in Step 1. The framework is flexible to adjust to additional risk factors as blockchain technology evolves and new types of crypto assets are introduced. Artificial intelligence (AI) models should be used to detect new risk factors for risk rating computations based on data available on existing risk vectors.

References

[1] Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments* (NIST Special Publication 800-30 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

[2] International Organization for Standardization. (2022). *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Information security risk management*. ISO. https://www.iso.org/standard/80585.html

[3] Bashir, I. (2023). *Mastering blockchain: Unlocking the power of cryptocurrencies, smart contracts, and decentralized applications* (4th ed.) Packt Publishing.

[4] Chainalysis. (2020, August 20). Cryptocurrency typologies guide: Who's who on the blockchains? Chainalysis, APA (7th Edition). https://www.chainalysis.com/blog/cryptocurrency-typologies-guide-2020

[5] CoinGecko. (2024). *How to evaluate and invest in cryptocurrencies*. CoinGecko. https://www.coingecko.com/en/methodology

[6] Basel Committee on Banking Supervision. (2022). *Prudential treatment of cryptoasset exposures* (Final standard, December 2022). Bank for International Settlements. https://www.bis.org/bcbs/publ/d545.pdf

[7] Swiss Financial Market Supervisory Authority (FINMA). (2019). *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*. FINMA. https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung

[8] World Economic Forum. (2021). *Digital Assets, Distributed Ledger Technology, and the Future of Capital Markets: Token Taxonomy and Classification Framework*. WEF. https://www3.weforum.org/docs/WEF_Token_Taxonomy_Framework_2021.pdf