International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 7, No. 06 Nov-Dec; 2025 Page. No. 484-496

To cite this article: Yaroslav Ivanov (2025). DEVELOPMENT OF A COMPREHENSIVE BLOCKCHAIN PROJECT EVALUATION MODEL (BLOCKCHAIN PROJECT EVALUATION MODEL), International Journal of Research in Commerce and Management Studies (IJRCMS) 7 (6): 484-496 Article No. 562 Sub Id 994

DEVELOPMENT OF A COMPREHENSIVE BLOCKCHAIN PROJECT EVALUATION MODEL (BLOCKCHAIN PROJECT EVALUATION MODEL)

Yaroslav Ivanov

Chief Visionary Officer at ALTA - Blockchain Labs
Dubai, UAE

DOI: https://doi.org/10.38193/IJRCMS.2025.7639

ABSTRACT

As crypto exchanges and decentralized exchanges have proven untrustworthy, this paper seeks to create a rigorous Blockchain Project Evaluation Model (BPEM) for assessing the trustworthiness of a blockchain project. This BPEM will collate the components of technical audit, on-chain and off-chain analytics, liquidity indicators, and behavioral indicators into a single score of the project. The relevance of this work is driven by widespread instances of trade volume manipulation, opaque tokenomics, and tightening regulatory requirements (including in the context of MiCA). The scientific novelty lies in the creation of a hybrid MCDM architecture with an automated Incongruity Detection System (IDS) module that cross-checks tokenomics, liquidity, on-chain activity, and public statements and introduces a penalty coefficient into the final rating. The results of BPEM validation across case studies of wash trading and hidden centralization demonstrate that the key indicators of project resilience are not nominal volume but market depth, liquidity quality, and the integrity of on-chain data, and that identified inconsistencies act as early markers of scam projects and systemic risks. It is shown that a comprehensive multifactor analysis significantly outperforms the use of isolated metrics and can serve as a backbone for listing and compliance procedures. The article is of practical value for researchers of decentralized finance, risk managers, crypto exchange analysts, and digital asset regulators.

KEYWORDS: blockchain projects, reliability assessment, scoring model, liquidity, on-chain analytics, tokenomics, incongruity detection

1. INTRODUCTION

1.1 Trust crisis in crypto markets

Over the past decade, blockchain technology has transformed from a niche cryptographic experiment into a global financial infrastructure (Alamsyah et al., 2024). However, this rapid evolution has been accompanied by significant structural risks. The decentralized nature of the market, often positioned as an advantage (a trustless environment), has paradoxically created conditions for an unprecedented

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 7, No. 06 Nov-Dec; 2025 Page. No. 484-496

level of information asymmetry. While blockchain transactions are immutable and transparent, the context surrounding these transactions, developers' intentions, the actual distribution of tokens, and sources of liquidity often remain opaque to investors.

The industry faces a systemic problem: the lack of a unified reliability assessment standard. Before the implementation of comprehensive models such as BPEM, data aggregators and exchanges frequently relied on superficial metrics such as reported market capitalization or daily trading volume. These indicators are easily falsified. Research indicates that a substantial share of reported trading volume on centralized exchanges (CEXs) is due to wash trading, a practice in which an asset is bought and sold by the same party to create the illusion of activity (Victor & Weintraud, 2021).

The collapse of giants such as the Terra–Luna ecosystem and the FTX exchange, as well as exploits of protocols such as the Mango Markets attack in October 2022, have underscored the need for deeper analysis (Naifar & Makni, 2025). In the Mango Markets case, the attacker exploited the token's low liquidity to manipulate the price oracle, enabling them to take an undercollateralized loan and drain the protocol's treasury. This incident has become a canonical example of why project evaluation cannot be limited to code review or market price analysis alone, but must also include liquidity stress testing.

1.2 Evolution of evaluation methods and existing gaps

Historically, the evaluation of crypto assets has passed through several stages. During the ICO era (2017–2018), investors primarily relied on the quality of the whitepaper and the team's perceived credibility. However, fraudulent projects rapidly learned to mimic legitimate ones by copying technical documentation and creating fictitious team profiles. Signaling theory, which works well in regulated initial public offering (IPO) markets (where IPOs are subject to specific regulatory audit requirements) seems to have failed in cryptocurrency markets (Hornuf et al., 2021).

Since the advent of DeFi (2020), TVL (Total Value Locked) has been the standard metric for measuring the success and health of a DeFi product. However, this metric is exploitable as it can be inflated through double-counting, and it relies on short-term incentives (yield farming) that may not be sustainable. Leading international organizations, including the Bank for International Settlements (BIS), have pointed out that the sector is plagued by opacity and the complexity of data analysis (Saggese et al., 2025).

At the time BPEM was initiated, no platform offered a holistic model that would combine technical audit, on-chain analytics, and behavioral factors into a single scoring system. Existing aggregators such as CoinMarketCap and CoinGecko acknowledged data reliability issues and actively sought new

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 7, No. 06 Nov-Dec; 2025 Page. No. 484-496

methodologies for filtering out garbage traffic and projects (Vidal-Tomás, 2022).

The present article describes the theoretical and practical aspects of developing a Comprehensive Blockchain Project Evaluation Model (BPEM).

The main objectives of the study are as follows:

1. To identify a set of quantitative and qualitative parameters that, in aggregate, shape the reliability profile of a decentralized project.
2. To create an algorithmic approach for detecting contradictions between on-chain data and off-chain statements (for example, verifying declared token supply against the actual state of the ledger).
3. To shift from the volume metric to the liquidity metric, based on analysis of order book depth and slippage.
4. To demonstrate the effectiveness of the proposed methodology in risk detection.

The study is based on the hypothesis that integrating heterogeneous data (technical, economic, and social) enables the identification of hidden risks that remain invisible when each component is analyzed in isolation.

2. MATERIALS AND METHODS

2.1 BPEM architecture

The developed BPEM model is a hybrid evaluation system that employs multi-criteria decision-making (MCDM) methods. The model aggregates data from four core domains: technological, market, informational, and economic.

In accordance with restrictions on the disclosure of trade secrets, exact weight coefficients and proprietary algorithms are not disclosed. Instead, a Theoretical Framework is presented that describes the logic and interrelationships of the components.

The generalized formula for the final scoring S_{total} value can be represented as:

$$S_{total} = \left(\sum_{i \in \{A,L,P,C\}} w_i \times M_i \right) \times K_{IDS}$$

where:

M_A - Audit Score;

M_L - Liquidity Score;

M_P - Profile Score;

M_C - Circulating Supply Integrity;

w_i - dynamic weight coefficients depending on the project life cycle stage;

K_{IDS} - a discount (penalty) coefficient calculated by the Incongruity Detection System (IDS). When

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 7, No. 06 Nov-Dec; 2025 Page. No. 484-496

critical anomalies are detected, $K_{IDS} \rightarrow 0$.

2.2 Data collection and processing methodology

Data for the model are collected from heterogeneous sources that can be divided into on-chain (in-network) and off-chain (off-exchange/public) data. Integration of these sources enables cross-validation. Data is retrieved from blockchain nodes (Ethereum, BSC, Solana, etc.), such as wallet balances, past transactions, smart contract or token bytecode, and event logs to track supply, funds flow, and holder activity. Order book depth, latest trades, volume on centralized (CEX) and decentralized exchanges (DEX) are required to compute liquidity and spread metrics. This information is obtained through project websites, GitHub repositories, social networks and news aggregators, and used to measure team activity and sentiment.

2.3 Component 1: Audit and security assessment (M_A)

This module evaluates the technical robustness of a project. In contrast to a binary approach (audit present/no audit), BPEM uses a differentiated scale.

When assessing the quality of smart contract audits, the auditor's reputation is prioritized. Thus, industry practices consider Tier-1 companies like CertiK or Hacken more credible and valuable than smaller companies, given their implied strength and verification standards.

Code coverage is another important metric that measures the percentage of critical smart contracts (such as token, staking, and governance contracts) covered in the audit. Insufficient coverage reduces confidence in audit results. At the same time, the primary focus is placed not merely on the number of discovered vulnerabilities, but on whether they have been remediated. A project in which critical bugs are identified but not fixed must be evaluated at the minimum scale regardless of other factors.
An additional positive indicator is the presence of a bug bounty program. Such reward schemes incentivize white hat hackers to continuously test the system and help detect and eliminate new vulnerabilities promptly.

2.4 Component 2: Liquidity assessment (M_L)

To counteract volume manipulation, BPEM focuses on metrics that are more difficult to falsify. The liquidity calculation algorithm is structured as follows.

To evaluate liquidity quality, several sequential steps are used. First, the system regularly collects order book snapshots for all trading pairs involving the analyzed asset. This enables recording the state of the order book over time and tracking market depth, the distribution of orders across price levels, and structural changes in liquidity.

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 7, No. 06 Nov-Dec; 2025 Page. No. 484-496

Next, slippage is calculated. For this purpose, the execution of market orders of various sizes, for example, USD 1,000, 10,000, and 100,000, is simulated. For each scenario, the expected trade price is compared with the actual execution price. Slippage in percentage terms is determined by the formula

$$Slippage(\%) = \frac{|P_{expected} - P_{executed}|}{P_{expected}} \times 100$$

where $P_{expected}$ is the best quote in the order book at the time the order is submitted, and $P_{executed}$ is the volume-weighted average execution price across the entire order book depth.

In parallel, the spread between the best bid and best ask prices is evaluated. The relative spread is calculated, and on this basis, a conclusion is drawn about liquidity quality: a narrow spread combined with low slippage indicates deep, resilient liquidity for the asset.

At the final stage, anomaly filtering is performed. Heuristics are applied to exclude trading pairs with suspicious or artificially generated activity, for example, pairs exhibiting high trading volume with an effectively empty order book. This helps avoid distortions in liquidity assessments and focuses the analysis on genuinely traded, structurally sound markets.

2.5 Component 3: Profile assessment and supply verification (M_P, M_C)

This block would verify key economic and transparency conditions.

To calculate the market cap of the asset, the Circulating Supply (CS) must be validated. BPEM does not exclusively depend on the values returned by the project in response to API calls, but independently computes the following:

$$CS = Total\ Supply - (LockedWallets + TeamReserves + BurdenTokens)$$

The model identifies wallets belonging to the team, funds, or vesting smart contracts and excludes them from the calculation, preventing artificial inflation of the rating.

For project profile analysis, the project's technical documentation is reviewed, and the project's whitepaper is analyzed using natural language processing (NLP) for originality, clarity, and technical content. This can sometimes reveal whether the material is superficial or carefully considered, as well as describe the asset's architecture, tokenomics, and protocol.

Developer activity is additionally considered. Project repositories on GitHub are analyzed for commit frequency, update dynamics, and evidence of ongoing work on the codebase. Suppose a repository has no commits for six months. In that case, the project receives a penalty for elevated abandonment

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 7, No. 06 Nov-Dec; 2025 Page. No. 484-496

risk, as prolonged inactivity may indicate discontinued development, declining team interest, or winding down of the initiative.

2.6 Innovation: Incongruity Detection System (IDS)

A key element of the BPEM methodology is the use of the Incongruity Detection concept, i.e. the automated search for logical and factual contradictions in project data. The system cross-checks core parameters of tokenomics, liquidity, on-chain activity, and team statements, identifying discrepancies between declared information and the actual state of affairs.

One typical type of incongruity is Tokenomics Mismatch. For example, a whitepaper may state that the team holds 10% of the total token supply, whereas on-chain analysis shows that wallets linked to the smart contract deployer control 40%. Such divergence indicates hidden token concentration and elevated manipulation risk.

Another type of incongruity is Volume/Liquidity Divergence. In this case, a project reports a high daily trading volume, for instance, USD 50 million, but a simulation of a USD 10,000 market order reveals slippage above 5%. This situation frequently signals wash trading, where volumes are artificially inflated without real market depth.

A third example is Roadmap/Code Lag: public statements may claim a mainnet launch, yet the public repository lacks any core network code, indicating a gap between the declared progress and the actual development status.

When such incongruities are detected, the coefficient K_{IDS} assumes a penalty value, for example 0.5 or 0. This leads to an abrupt reduction in the project's final rating within the model and automatically marks its status as Unverified or Risky on aggregator platforms. Thus, the Incongruity Detection mechanism acts as a filter, protecting users from projects with distorted or unreliable information.

3. RESULTS AND DISCUSSION

The implementation of BPEM has enabled a more objective view of the market by distinguishing genuine projects from those driven solely by marketing and manipulative practices. The system architecture and its application are analyzed below.

3.1 Evaluation system architecture

Figure 1 presents a high-level scheme of data flows within BPEM. It shows how raw data are transformed into a final trust rating.

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 7, No. 06 Nov-Dec; 2025 Page. No. 484-496

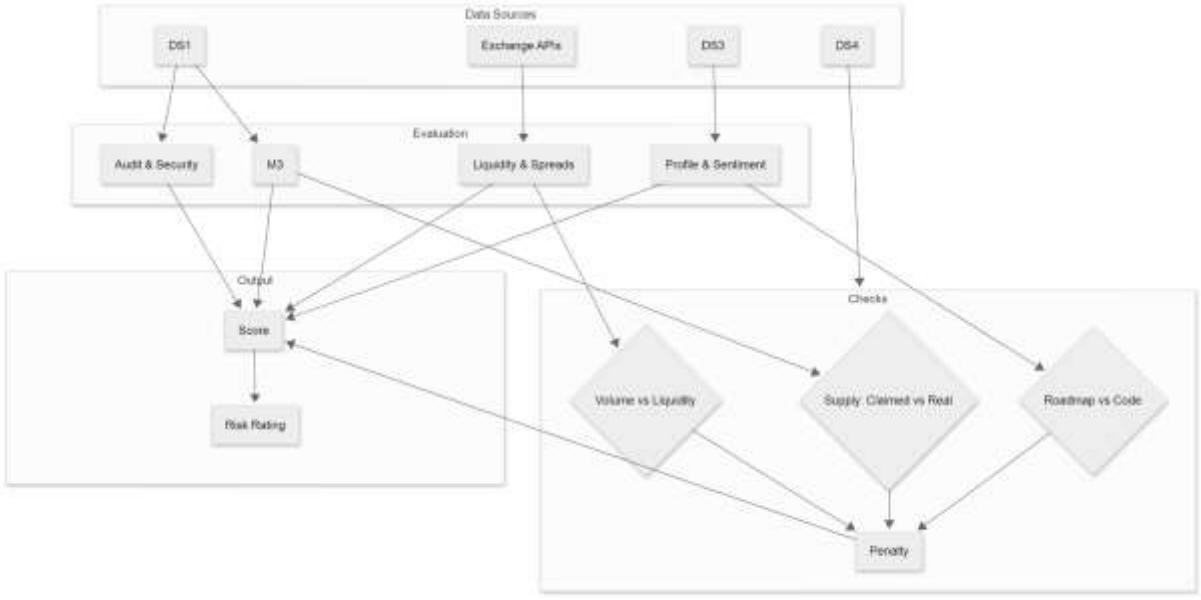

Figure 1. BPEM model architecture and data flows

The diagram illustrates the integration of heterogeneous data and the IDS's central role in adjusting the final assessment.

3.2 Case study analysis

3.2.1 Case Study A: Detection of Wash Trading (Liquidity Problem)

In the case of project Alpha, the token was then listed on multiple second-tier exchanges, with a reported daily trading volume of USD 20 million. This ensures that Alpha remained high in volume rankings, and created the impression that the token is widely traded and possesses high liquidity to end users and data aggregators.

When analyzed using the BPEM methodology, the liquidity module triggered first. It applied a slippage test by simulating the execution of a market sell order of USD 50,000 in tokens. The simulation revealed that at this order size, the token's market price would decline by approximately 12%. For a genuinely liquid market with a reported daily volume of USD 20 million, such a significant price impact is anomalous: expected slippage in this situation should be below 0.1%, i.e., practically negligible.

Subsequently, an IDS Check was performed, during which the system compared the reported trading volume with the actual market depth reflected in the order book. A critical imbalance was detected in the Volume/Depth Ratio: high nominal trading volume was not supported by sufficient order book

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 7, No. 06 Nov-Dec; 2025 Page. No. 484-496

density. This inconsistency indicates that a substantial portion of the volume may be the result of artificial activity such as wash trading or other forms of metric manipulation.

As a result, project Alpha received a very low integrated Liquidity Score of 23 out of 1000 and was automatically flagged as Possible Volume Manipulation. Aggregators using the BPEM methodology excluded the project's reported volume from calculations of average market price and other aggregate metrics. This reduced the risk for users who might otherwise purchase the asset at an artificially inflated rate, relying on misleading trading volume figures. Figure 2 presents a diagram describing the liquidity verification logic.

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 7, No. 06 Nov-Dec; 2025 Page. No. 484-496

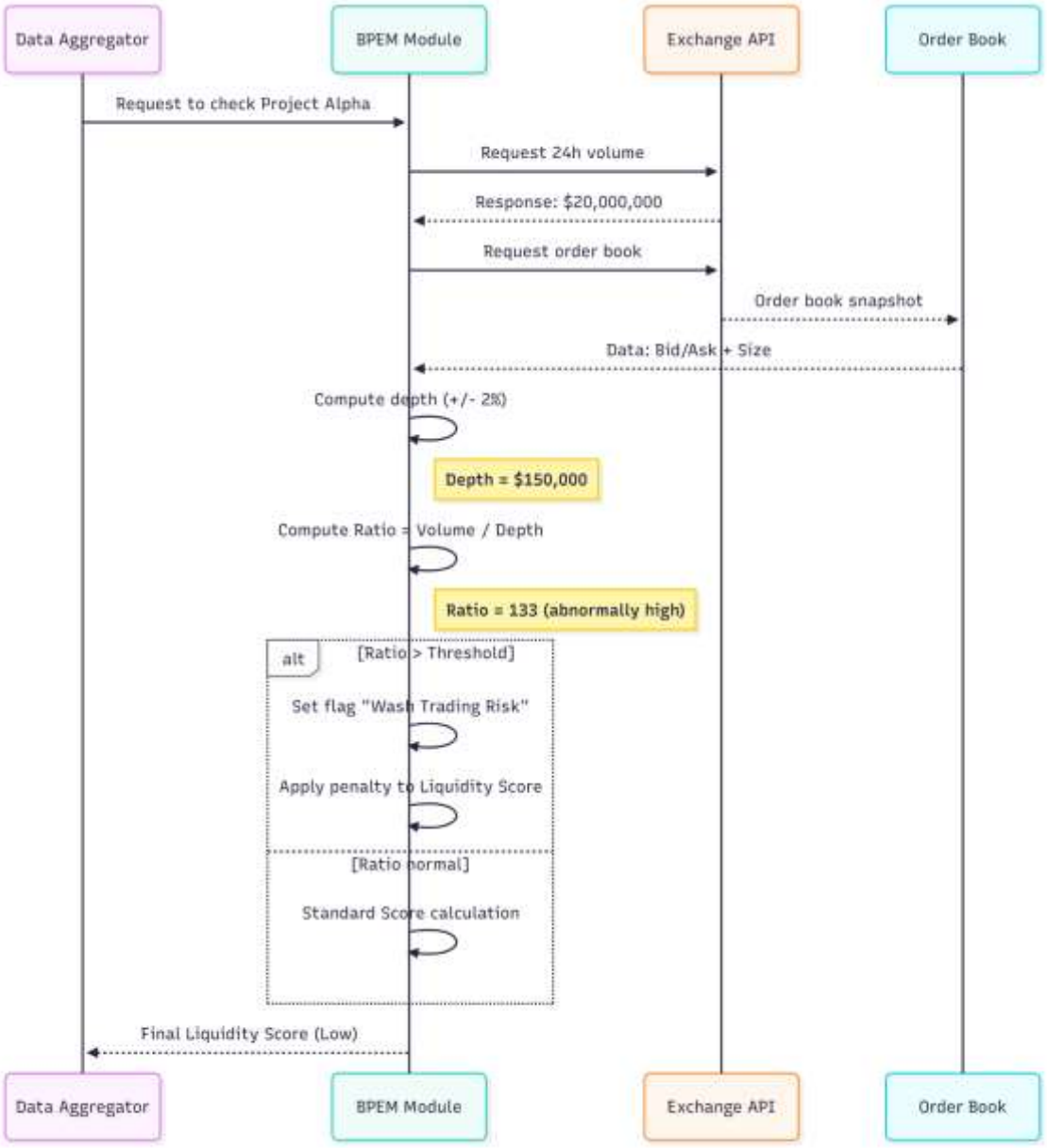

Figure 2. Liquidity verification and wash trading detection logic

3.2.2 Case Study B: Hidden Centralization (Tokenomics Problem)

In this case, project Beta positioned itself as a decentralized autonomous organization with full community governance and claimed that the token was 100% community-owned. Such positioning implies broad distribution of tokens among many independent holders and the absence of control concentration in the hands of a narrow group of addresses.

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 7, No. 06 Nov-Dec; 2025 Page. No. 484-496

During analysis under the BPEM methodology, the Supply Module performed a wallet clustering analysis. The goal was to determine the token ownership structure and identify potential centers of concentration. At the IDS Check stage, it was discovered that 60% of the total token supply was held in five wallets that were not identified as smart contracts or exchange addresses. Additional analysis of transaction histories showed that all these wallets had previously been funded by the same deployer address, which indirectly points to their affiliation and to de facto control by a single party or a small group of actors.

Thus, an apparent contradiction emerged between the declared 100% community-owned model and the actual concentration of ownership. The project received a penalty under the Trust Score category, which reflects the level of trust and transparency. Instead of the reported market capitalization calculated based on 100% of the emission, capitalization was recalculated using the actual free float, representing only 40% of the total token supply. This led to a significant downward adjustment in the project's ranking, by approximately 200 places, and enabled investors and aggregators to more accurately assess its risk profile and degree of centralization.

3.3 Industry impact and applications

The development of BPEM has a systemic impact on the entire crypto industry as the proposed system is in line with volume reporting standards of crypto's market leaders. Metrics like Liquidity Score and Confidence Indicator are focusing less on volume and more on real liquidity. Although it remains possible to inflate volume using bots, volume-increasing becomes ineffective due to the order book depth required for a high score.

When applied to internal listing (due diligence) processes, BPEM principles can be used to protect against early-stage scam projects, reputational harm, and client asset loss. The principles of disclosure and verification are aligned with emerging regulatory frameworks, such as the EU Markets in Crypto-Assets (MiCA) regulation (ESMA, 2025). The MiCA whitepaper registry uses similar disclosure content requirements.

Figure 3 shows the incongruity processing workflow which has become the de facto approach used for screening projects prior to listing.

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 7, No. 06 Nov-Dec; 2025 Page. No. 484-496

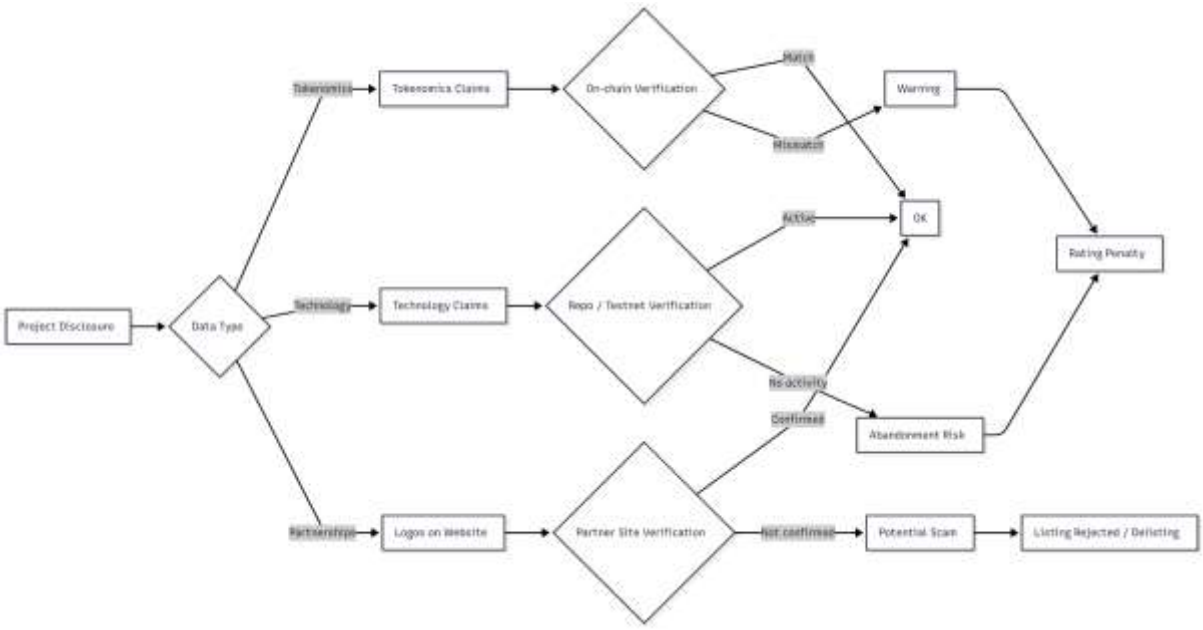

Figure 3. Non-conformity Detection System (IDS) workflow

3.4 Limitations of the study

Despite its overall effectiveness, the BPEM model has a few important limitations when interpreting its results that should be noted. One of these limitations is the model's blind spot for off-chain events, e.g. over-the-counter (OTC) sales or private contracts between founders and investors that are not publicly recorded on the blockchain or captured in smart contract interactions. Consequently, some risks related to ownership concentration or covert control may remain invisible to the system.

Additional complexity arises from the dynamic nature of smart contracts. Even projects which obtain a passing audit and a high security rating can change the way their logic is implemented through the use of the proxy pattern, and be subject to malicious code or insecure practices after an audit is complete, therefore an audit can never be conclusive evidence of a safe project. Reducing this would mean always verifying that the on-chain contract implementation matches the verified one at every step, which is both expensive and requires extensive analysis.

Another limitation is linked to the difficulty of deanonymizing network participants. The use of mixer services, such as Tornado Cash, significantly complicates tracing wallet linkages when analyzing token distribution and identifying affiliated addresses. Under these conditions, the system is forced to rely on heuristic clustering methods and indirect indicators that only partially compensate for the loss of transparency. This reduces, but does not eliminate, the scope for covert manipulation.

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 7, No. 06 Nov-Dec; 2025 Page. No. 484-496

4. CONCLUSION

This work presents a Comprehensive Blockchain Project Evaluation Model (BPEM) that offers a scientifically grounded approach to addressing the trust problem in decentralized finance. The transition from intuitive or easily manipulated metrics (such as trading volume) to verifiable indicators (liquidity, audit quality, on-chain supply verification) has enabled the creation of a robust tool for investors, analysts, and exchanges.

The analysis shows that the key determinant of asset resilience is not the reported trading volume, but the quality of its liquidity. Genuine market reliability and stability are defined by order book depth, the distribution of orders across price levels, and bid–ask spreads. Nominal volume, especially on less transparent venues, can be substantially overstated and often fails to reflect actual trading activity.

Logical and factual incongruities between on-chain data and public project statements constitute a distinct risk dimension. Use of a variation of the IDS method has high risk detection rates; based on statistics, projects are much more likely to be fraudulent or to fail if their tokenomics, liquidity, or codebase differ from their marketing. Such discrepancies may be used as an indicator of problems and lead to timely risk reassessment.

At the same time, the comprehensiveness of the approach is critically important. No single parameter, not even the presence of an audit by a reputable firm, can be treated as a sufficient guarantee of safety. An audit may be outdated, incomplete, or fail to account for subsequent changes to code and the ownership structure. Only the combined analysis of technical protocol characteristics, economic parameters (liquidity, token distribution, model resilience), and social factors (team transparency, community activity, industry reputation) can yield a relevant and sustainable project assessment.

The proposed methodology has already become part of an emerging industry standard. Future development of the model will focus on integrating machine learning (ML) methods for automatic detection of complex manipulation patterns and semantic analysis of smart contracts to identify hidden intents. In a context of tightening global regulation (MiCA, SEC), BPEM represents a ready-made framework for compliance procedures and investor protection in the digital era.

REFERENCES

Alamsyah, A., Kusuma, G. N. W., & Ramadhani, D. P. (2024). A Review of Decentralized Finance Ecosystems. *Future Internet*, *16*(3), 76. https://doi.org/10.3390/fi16030076

ESMA. (2025). *Markets in Crypto-Assets Regulation (MiCA)*. ESMA. https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica

Hornuf, L., Kück, T., & Schwienbacher, A. (2021). Initial coin offerings, information disclosure, and fraud. *Small Business Economics*, *58*, 1741–1759. https://doi.org/10.1007/s11187-021-00471-y

Naifar, N., & Makni, M. S. (2025). Dynamics of Cryptocurrencies, DeFi Tokens, and Tech Stocks: Lessons from the FTX Collapse. *International Journal of Financial Studies*, *13*(3), 169. https://doi.org/10.3390/ijfs13030169

Saggese, P., Fröwis, M., Kitzler, S., Haslhofer, B., & Auer, R. (2025). *BIS Working Papers No 1268*. BIS. https://www.bis.org/publ/work1268.pdf

Victor, F., & Weintraud, A. M. (2021). Detecting and Quantifying Wash Trading on Decentralized Cryptocurrency Exchanges. *WWW '21: Proceedings of the Web Conference 2021*, 23–32. https://doi.org/10.1145/3442381.3449824

Vidal-Tomás, D. (2022). Which cryptocurrency data sources should scholars use? *International Review of Financial Analysis*, *81*(2), 102061. https://doi.org/10.1016/j.irfa.2022.102061