From shadows to trust: designing a framework for integrity assessment in digital asset markets

Jenny Jakobs, Benjamin Clapham, Julian Schmidt, Peter Gomber, Jan Muntermann

Angaben zur Veröffentlichung / Publication details:

Jakobs, Jenny, Benjamin Clapham, Julian Schmidt, Peter Gomber, and Jan Muntermann. 2026. "From shadows to trust: designing a framework for integrity assessment in digital asset markets." In *34th European Conference on Information Systems (ECIS 2026) Milan, Italy, June 15-17, 2026, proceedings*, edited by Jan vom Brocke, Wendy Currie, and Ferdinando Pennarola, 1. New York, NY: AIS Electronic Library (AISeL). https://aisel.aisnet.org/ecis2026/blockfintech/blockfintech/1/.

June 2026

From Shadows To Trust: Designing A Framework For Integrity Assessment In Digital Asset Markets

Jenny Jakobs
University of Augsburg, jenny.jakobs@uni-a.de

Benjamin Clapham
Goethe University Frankfurt, clapham@wiwi.uni-frankfurt.de

Julian Schmidt
Goethe University Frankfurt, julian.schmidt@wiwi.uni-frankfurt.de

Peter Gomber
Goethe University Frankfurt, Gomber@wiwi.uni-frankfurt.de

Jan Muntermann
University of Augsburg, jan.muntermann@uni-a.de

FROM SHADOWS TO TRUST: DESIGNING A FRAMEWORK FOR INTEGRITY ASSESSMENT IN DIGITAL ASSET MARKETS

Completed Research Paper

Jenny Jakobs, University of Augsburg, Augsburg, Germany, jenny.jakobs@uni-a.de

Benjamin Clapham, Goethe University Frankfurt, Frankfurt am Main, Germany, clapham@wiwi.uni-frankfurt.de

Julian Schmidt, Goethe University Frankfurt, Frankfurt am Main, Germany, julian.schmidt@wiwi.uni-frankfurt.de

Peter Gomber, Goethe University Frankfurt, Frankfurt am Main, Germany, gomber@wiwi.uni-frankfurt.de

Jan Muntermann, University of Augsburg, Augsburg, Germany, jan.muntermann@uni-a.de

Abstract

Crypto assets are increasingly embedded in the financial system. Digital Asset Markets (DAMs) serve as the core infrastructure for their exchange. However, the rapid evolution of these markets has led to integrity violations, such as hacks, fraud, and market manipulation, that erode trust and hinder further institutional adoption. As there is no holistic conceptual basis for evaluating DAM integrity, this study follows a Design Science Research approach to develop an integrative framework for assessing market integrity in DAMs. Existing research typically examines isolated violations or single aspects of integrity, leaving stakeholders without comprehensive guidance. By synthesizing insights from a systematic literature review and interviews with key stakeholders, we derive, refine, and validate integrity-relevant constructs and their measures. These constructs form the basis of an actionable assessment framework that supports investors, intermediaries, and regulators. We further demonstrate the framework's practical utility through its application to exemplary DAMs.

Keywords: Crypto Assets, Decentralized Finance, Design Science Research, Digital Asset Markets, Market Integrity.

1 Introduction

Digital asset markets (DAMs), such as cryptocurrency exchanges, constitute the core infrastructure for trading crypto assets and thereby play an essential role in the rapidly evolving blockchain and fintech ecosystem. Their growth has been substantial, with monthly trading volumes surpassing USD 2.94 trillion in December 2024 (The Block, 2025). Yet, despite their increasing economic relevance, DAMs remain highly vulnerable to integrity violations, including market manipulation, financial fraud, and large-scale security breaches. Incidents such as the ByBit hack, which caused losses exceeding USD 1 billion (Reuters, 2025), highlight the fragility of current market structures and expose significant governance and risk-management shortcomings. These violations undermine market integrity, understood as the equal access and fair treatment for all participants, transparent price formation, reliable issuer information, and the absence of manipulation, abuse, and fraud (Austin, 2017). In doing so, they hinder the further adoption of crypto-asset trading, particularly by institutional actors. In addition, many major exchanges explicitly limit their responsibility for integrity-related risks. For instance, Binance's user agreements state that customers carry all risks associated with digital asset transactions and may

bear the consequences of unauthorized or irreversible transfers (Binance, 2025b). As a result, the safety of customer assets and a compensation in the event of fraud-related losses are not guaranteed, leaving users exposed to significant residual risks. Reliable and holistic integrity assessment is therefore critical for investors, regulators, and intermediaries, such as banks and fintech firms seeking to integrate crypto-asset trading into their service portfolios. However, such assessment is difficult. Global regulatory regimes remain fragmented, standards for DAM integrity are lacking, and integrity measures from traditional financial markets cannot be transferred one-to-one due to the unique characteristics of blockchain-based assets and decentralized market infrastructures (Hägele, 2024). As a result, stakeholders struggle to determine which DAMs are trustworthy. While prior research provides valuable approaches to detect individual threats, many solutions are not readily deployable (e.g., complex algorithms (Victor & Weintraud, 2021) or machine learning models (Li et al., 2024)), focus on isolated aspects of market integrity (Eigelshoven et al., 2021), or address only single violations such as wash trading (Aloosh & Li, 2024; Fantazzini & Calabrese, 2021; Victor & Weintraud, 2021) or cyberattacks (Hasanova et al., 2019; vom Brocke et al., 2015). A holistic, actionable framework for assessing DAM integrity, which is aligned with the specific risks and structural properties of decentralized financial markets, is still missing.

To address this gap, we adopt a design science research (DSR) approach (Hevner & Chatterjee, 2010; Peffers et al., 2007) to develop an integrity assessment framework tailored to DAMs. Our research is guided by the following questions: **RQ1:** What are the integrity-relevant constructs of DAMs, and how can they be measured? **RQ2**: How can the integrity of DAMs be assessed using these constructs and measures?

Based on a systematic literature review and expert interviews, we first derive integrity-relevant constructs that capture the specific risks and governance challenges of DAMs. These constructs form the foundation of an assessment framework that enables investors, intermediaries, and regulators to evaluate the integrity of DAMs in a structured and comparable manner. While the framework focuses on measuring integrity rather than prescribing specific countermeasures, it provides market operators with guidance for identifying where countermeasures may be required. Beyond its practical utility, the framework also establishes a conceptual basis for future IT artifacts, including design theories, or empirical studies in the context of governance and trustworthiness of decentralized financial infrastructures. The remainder of this paper is structured as follows. Section 2 outlines the background on DAMs and market integrity. Section 3 explains the research design and describes our DSR approach. Section 4 presents the development, demonstration, and evaluation of the artifact. Section 5 concludes the paper by summarizing key implications, outlining limitations, and suggesting avenues for future research.

2 Research Background

The structure of DAMs differs fundamentally from traditional financial markets. This first relates to the nature of the assets and the venue on which they trade and second to the establishment of trust among market participants. Crypto assets are traded on DAMs, which provide liquidity and price discovery for those assets. DAMs can be broadly categorized into two types: centralized and decentralized exchanges (CEXs and DEXs). CEXs are similar to traditional stock exchanges, utilizing centralized order book systems and custody of digital assets. In contrast to CEXs, which hold client assets and intermediate trades, DEXs operate without a central operator and execute swaps directly on-chain through autonomous smart contracts (Hägele, 2024). Trust is key in financial markets, as it leads to systemic resilience, enabling markets to absorb shocks without collapsing (Austin, 2017). It also reduces transaction costs and encourages more frequent participation by investors if they believe in the integrity of the respective market. In DEXs, however, trust is not established by centralized authorities as seen in traditional financial markets. Instead, it is established through decentralization and cryptography (Suga et al., 2020). In the case of CEXs, a single entity concentrates all market functions, including trading, clearing, settlement, and custody, whereas in traditional financial exchanges these functions are typically separated across multiple regulated intermediaries (Hägele, 2024). This leads to a concentration of

power in the absence of equivalent regulatory oversight. These differences give rise to design features with direct implications for market integrity. Unlike traditional assets, crypto assets are not backed by a physical asset, a national economy, or a company. Their value instead depends on confidence in the underlying protocol, in particular the ability of the system to securely record and trace all transactions (Corbet et al., 2019). Because these assets are typically not issued by a central authority and are traded without traditional intermediaries, transaction validity is established collectively through a cryptographic consensus mechanism, and each validated transaction is stored immutably on a distributed ledger (Eigelshoven et al., 2021). Given these structural properties of DAMs, it is necessary to clarify what constitutes market integrity in this context: (i) All participants have non-discriminatory access to trading and are treated fairly. (ii) The market is free from abuse and manipulation, so that no actor benefits from a privileged informational advantage or unauthorized access to investors' assets. (iii) Participants can observe transparent information about prices as well as current supply and demand (Austin, 2017).

Due to the differences in governance, design, and trading technology, there also exist integrity violations that are absent in traditional financial markets (Clapham et al., 2023). CEX design offers advantages such as lower transaction costs, higher trading speed and greater convenience. However, their centralized nature introduces risks, e.g., potential single points of failure (Hägele, 2024). A common violation in CEXs is the hack of hot wallets, a cyberattack where criminals compromise the exchange-managed wallets that are connected to the internet (Suga et al., 2020). CEXs are subject to the oversight of financial regulators and must comply with applicable laws. However, these regulations often focus on traditional financial instruments and do not take into account the unique characteristics of crypto assets (Hägele, 2024). Differences in jurisdictional regulations can also lead to regulatory arbitrage, where exchanges relocate to crypto-friendly jurisdictions to avoid stricter regulatory requirements (Johnson, 2021). While DEXs eliminate the need for intermediaries, they also introduce unique vulnerabilities. For example, DEXs are particularly susceptible to manipulation techniques such as sandwich attacks, akin to front-running practices already observed in traditional financial markets (Park, 2023). Operating without a central authority, DEXs rely on smart contracts and blockchain-based algorithms to facilitate transactions. Many use automated market makers (AMMs) to ensure continuous liquidity and promote decentralization (Park, 2023). However, the absence of intermediaries and custodial oversight also means that DEXs often lack clear accountability and typically operate beyond the reach of any single jurisdiction. Their anonymous and globally accessible nature enables trading without adherence to Know Your Customer (KYC) or Anti-Money Laundering (AML) regulations, making them particularly vulnerable to illicit financial activities (Johnson, 2021). The existing literature discusses a variety of different types of integrity violations in DAMs (e.g., Eigelshoven et al. (2021), Clapham et al. (2023)). While Clapham et al. (2023) provide a taxonomy of such violations and Jakobs et al. (2024) address risk-related aspects of crypto assets more broadly, none of the existing studies provides a solution to measure and compare the integrity of DAMs. Instead, studies at most propose approaches to detect specific types of integrity violations such as wash trading (e.g.,Aloosh & Li, 2024). First approaches to this problem take the form of practitioner-developed dashboards that rank marketplaces. However, these rankings commonly incorporate additional criteria beyond market integrity, such as liquidity and trading volume (Kaiko, 2025). Moreover, such dashboards lack a theoretical foundation, and the justification of the scoring methods is often not transparent. Accordingly, there is a need for a framework specifically designed to measure integrity of DAMs and support real-world integrity assessments.

3 Research Design

3.1 Literature Analysis

The research design of this study is based on the DSR paradigm, which strives to create artifacts to address real-world problems. Such artifacts include constructs, models, methods, instantiations, and design theory (Hevner & Chatterjee, 2010). To guide our DSR approach, we follow the well-established

process model of Peffers et al. (2007) shown in Figure 1. We devise a strategy to develop the artifact from two data sources. To build upon the existing knowledge base, we first conduct a systematic literature review (SLR) to develop a set of relevant constructs based on integrity measures identified in the literature corpus and to develop a first version of our integrity assessment framework. In a second phase, we iteratively evaluate and improve the framework based on expert interviews until saturation is reached, i.e., when additional expert interviews no longer resulted in changes or new insights. We adapted the original process suggested by Peffers et al. (2007) for this iterative process, in line with Hevner et al. (2004) and their idea of build-test cycles. Finally, we demonstrate the applicability of the framework.

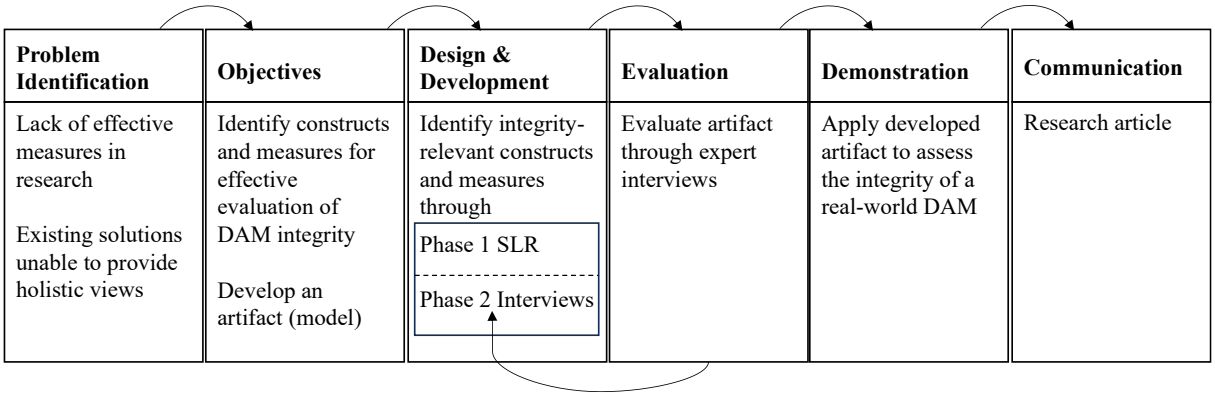

Figure 1. DSR process adapted from Peffers et al. (2007).

In a first phase of Design & Development, relevant literature is reviewed by following the approach of Webster and Watson (2002), as detailed in Figure 2. This search aims to conceptualize the object under consideration, i.e., integrity measurement in DAMs. We searched Web of Science, EBSCOhost, and the AIS eLibrary. The query *(cryptocurr* OR Bitcoin OR Ethereum OR token OR "digital asset") AND (manipulation* OR fraud OR governance OR hack OR violation OR incident OR security OR integrity)* was applied to the title and abstract fields (the topic field in Web of Science). The search string was specifically designed to find articles on integrity violations in DAMs, which allowed us to derive suitable integrity measures.

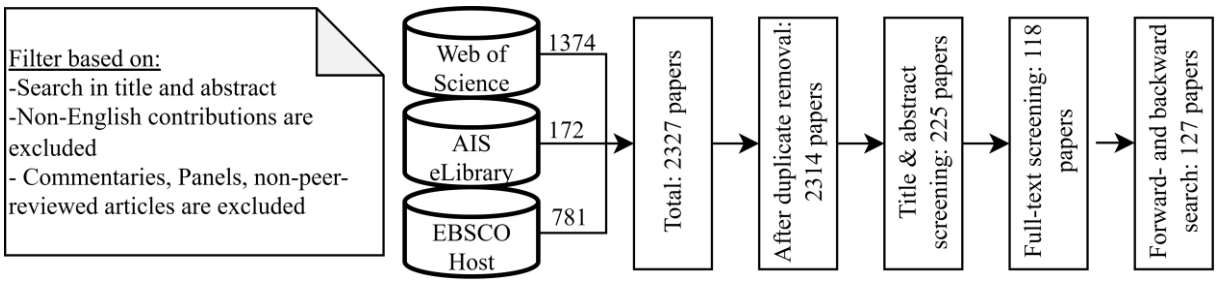

Figure 2. Literature research process.

We specified additional criteria to the search: non-English articles, commentaries and panels as well as non-peer-reviewed sources were excluded. The search returned 2314 records without duplicates. We screened each abstract and excluded papers that did not address measures or whose measures were limited to blockchain- or coin-specific contexts rather than marketplaces, as well as articles that purely focus on technical aspects without applying them to DAMs (i.e., the mechanics of consensus mechanisms), leaving 118 articles. We then conducted backward and forward citation searches using the same criteria, identifying nine additional studies. All included articles underwent full-text screening, and relevant passages were coded to extract integrity measures; the full coding procedure is reported in Section 3.4.

3.2 Interview Analysis

To iteratively evaluate and improve the framework in the second phase, we conducted online or in-person qualitative interviews with domain experts. All interviews were audio-recorded and transcribed. Participants included experts from both industry and academia. A semi-structured interview approach was employed (Myers & Newman, 2007), using open-ended questions to further develop the proposed integrity assessment framework and its associated measures. This approach combined a structured framework with the flexibility to adapt to the evolving dynamics of each interview. The semi-structured interview guide began with questions on participants' professional background and the relevance of (violations in) DAMs in their daily work. Participants were then introduced to the design objectives derived and the current state of the integrity measurement framework and asked to evaluate the relevance and completeness (Mayring, 2015). Next, the participants were presented with the integrity measures. They assessed the proposed measures, discussing their applicability, potential challenges in implementation (e.g., data availability, interpretability), and possible alternative metrics. The interview concluded with an open-ended prompt for any additional feedback. Interviews lasted 45 minutes on average. To ensure a diverse perspective on DAMs, we employed a quota sampling strategy (Robinson, 2014), selecting high-level domain experts from research, practice, and regulatory contexts, all with several years of both personal and professional experience in the field of crypto assets. Between January and April 2025, we conducted interviews with five expert practitioners, two researchers focused on DAMs, and two professionals from supervisory authorities. See Table 1 for more information on their demographics, such as experience in crypto assets. Based on the insights gained from each interview, we revised the integrity measurement framework. As the interviews progressed, it became evident that the additional insights gained diminished significantly. This suggests that the framework represents a satisfying problem solution in its final form and that data saturation has been reached (Corbin & Strauss, 2015). Consequently, the recruitment of further participants was discontinued. Finally, all interviews were transcribed and iteratively coded using an inductive approach (Braun & Clarke, 2006). The nine interviews, conducted in German, were transcribed in the original language and subsequently translated into English. Initial coding was performed by one author and then independently reviewed by a second author; discrepancies were discussed until consensus was reached to incorporate multiple perspectives. We open-coded the material to extract codes related to integrity measures and to the integrity measurement framework, as further described in Section 3.4.

ID	Professional Role	Experience (in years)	Category
1	Project Manager for the crypto asset business at a major bank	3	Practitioner
2	Researcher conducting empirical studies on crypto assets	3	Researcher
3	Managing Director at a crypto trading and custody service provider	8	Practitioner
4	DLT expert in supervisory authority	6	Regulator
5	Infrastructure expert in supervisory authority	7	Regulator
6	CEO at a crypto trading and custody service provider	7	Practitioner
7	Fintech advisor and blockchain and tokenization expert	5	Practitioner
8	Executive assistant at a DAM infrastructure provider	6	Practitioner
9	Researcher conducting mostly empirical studies on crypto assets and DLT	4	Researcher

Table 1. Interview participants.

3.3 Problem Identification and Objectives

As described in the research background, the unique design of DAMs has led to novel types of integrity violations coupled with a lack of effective measures to detect them. Thus, new measures are needed to identify these violations and assess DAM integrity. We call this problem class "integrity violations in DAMs". Since we are dealing with a novel problem observed in an emerging phenomenon, we first create constructs, since no existing ones are available. These constructs will then form the foundation

for developing an artifact in the form of a framework to effectively address these challenges (Hevner et al., 2004). The development of our artifact is guided by three design objectives (DOs), derived from our research background and validated through expert interviews. DO1 requires that measures are clearly defined, interpretable, and measurable to ensure their applicability. Measures relying on machine learning models are excluded, as they cannot be interpreted or acted upon by most stakeholders (Hägele, 2024). DO2 requires that the framework is usable across different stakeholder groups, such as intermediaries, regulators or investors, since market integrity assessment must serve all participants fairly and equally (Austin, 2017). DO3 requires that the framework should be applicable across all market types, including both CEXs and DEXs, given their fundamentally different governance structures and vulnerability profiles (Hägele, 2024). These objectives guided both the extraction and filtering of measures from the literature and their subsequent evaluation and refinement during the interview phase.

3.4 Design and Development

The design and development phase proceeded in two iterations: a first iteration derived and filtered candidate measures from the systematic literature review, and a second iteration refined the resulting framework through expert interviews.

The 127 full-text articles were coded using three categories: (1) Measure (name of the measure, or "NA" if no measure was reported), (2) Applicability to DAMs, and (3) Interpretability, i.e., whether the measure was clearly defined, measurable, and interpretable following DO1. Coding was conducted by one author and independently reviewed by a second author, with any discrepancies resolved through discussion. Table 2 presents the coding scheme along with representative examples.

Source	Example Statement	Measure	Applicability	Interpretability
La Morgia et al. (2023)	"[..] stopping transactions on a cryptocurrency when it gains or loses more than some threshold [..]."	Circuit breaker	Yes	Yes
Wang et al. (2025)	"PSPL, a compressed sensing oversampling-based Peephole LSTM approach [..]."	Detect Ponzi Schemes using LSTM	Yes	No, too technical (DO1)
Sofi et al. (2025)	"The consensus algorithm selection depends on various factors [..]"	Consensus Upgrade	No, asset not DAM-specific	Yes

Table 2. Coding Examples from the Literature Analysis.

We derived 67 measures applicable to DAMs. These integrity measures were evaluated against DO1, which addresses the measure level, while DO2 and DO3 relate to the framework level. With respect to DO1, we excluded 35 measures deemed not interpretable or not measurable without training a machine learning model, leaving 32 integrity measures at this point. For instance, "detect Ethereum Ponzi schemes using machine learning models", which was mentioned in 24 articles, was excluded as it lacks interpretability, and "delist crypto assets with shallow trading volume" for lacking a consistent definition (La Morgia et al., 2023). Among the 32 literature-derived measures, five measures are mentioned by three or more sources (measures 1.4, 1.9, 3.1, 3.7, and 3.9), five measures are derived from exactly two sources (measures 1.7, 2.7, 3.2, 3.3, and 3.4), and 22 measures rely on a single source.

The interviews from the second iteration were coded with respect to the applicability of the identified measures, potential implementation challenges, and alternative or missing measures, as illustrated in Table 3 through representative examples. Overall, this interview phase resulted in several adjustments: eleven measures were added, four were refined, and three were removed. The eleven additional measures reflect practitioner and regulatory insights not captured in the literature, such as wallet forensics screening against sanctions lists (1.5) and Directors and Officers liability insurance (2.10). The three removals were primarily driven by concerns regarding applicability. The measure "Number of scam tokens listed on a DAM" (Dupuis et al., 2023) was excluded because defining a "scam" token is

inherently difficult, as some projects fail for legitimate reasons (ID2), and comprehensive historical listings are rarely available. Similarly, "Previous pumps conducted in the marketplace are listed" (Dhawan & Putniņš, 2023) was removed due to the absence of a standard definition for pump-and-dump events and the substantial historical market data required to identify them, making the measure impractical for most stakeholders, particularly retail investors (ID2). The measure "No severe security breach" (Lee & Milunovich, 2023) was also discarded, as experts noted that breach incidence tends to increase over time regardless of cybersecurity quality (ID3), and that transparent disclosure is more relevant than the mere occurrence of breaches (ID4).

ID	Example Statement	Measure	Insight	Action
ID8	"Whether you are a crypto exchange or [..], if you have not taken out, for example, D&O insurance to protect your management and the board, that would appear questionable to me and would be a risk concern."	D&O insurance	New yet missing measure	Add measure
ID2	"[..] some projects fail for reasons that are completely legitimate [..] and complete historical listings are rarely available"	Number of scam tokens listed	Difficulty in applicability	Remove measure
ID3	"Exact thresholds should be applied with flexibility, as overly rigid criteria risk creating barriers to entry that could hinder competition and limit innovation in the market."	Established Market	Measure valid, threshold context-depended	Add critical discussion
ID4	"The mere existence of the entity is not, in itself, a reliable indicator that nothing is amiss, because another requirement is that the legal entity is adequately staffed, that genuine work is being carried out there, and that it is not a shell company."	Legal entity	Measure needs refinement	Add "no empty shell"

Table 3. Coding Examples from the Expert Interviews.

Several measures, such as Established Market (2.3), incorporate numerical thresholds discussed during the expert interviews. While some interviewees highlighted that these thresholds are context-dependent (ID2; ID7), others emphasized their importance for non-technical stakeholders who require concrete decision criteria (ID3; ID5; ID8). Accordingly, the reported values should be understood as empirically grounded defaults that users are expected to adapt to their specific context.

Starting with the 40 identified measures, we applied a generalization process to identify three theoretical constructs that served as the basis for the integrity measurement framework. The process began with three authors independently labeling the measures. These labels were then discussed collaboratively until consensus was reached. In the next step, we considered appropriate names, ultimately resulting in three final constructs: Market Abuse, Governance, and Cybersecurity. Building on these constructs and measures, we developed the proposed three-step integrity measurement framework. The framework, along with its constructs and measures, is illustrated in Figure 3. This figure represents both the central outcome of our design and development process and a practical guide for applying the framework in a DAM assessment. To enable a comprehensive understanding of how the framework works in practice, the following section provides a detailed description of each step in the framework and especially its associated measures. Such an in-depth description of the framework is essential for transparency, replicability, and practical applicability.

4 The Integrity Measurement Framework

1. Market Type

First, the user must decide whether to evaluate a CEX or a DEX, as each market type is subject to different kinds of integrity violations and requires different measurement approaches as described in the literature section above. The majority of trading activity occurs via CEXs, which operate similarly to traditional stock exchanges, typically using off-chain open limit order books (The Block, 2025; Hägele, 2024). In contrast, DEXs usually offer on-chain trading and settlement, eliminating the need for

intermediaries in the transfer and custody of assets (Hägele, 2024), leading to unique integrity assessment measures.

2. Integrity-relevant constructs

After selecting the market type, a user of the framework has to select the constructs to be measured in the second node, which are Market Abuse, Governance and Cybersecurity. Market abuse encompasses all forms of market manipulation and unfair practices, where an individual exploits privileged information, causing harm to other market participants (Austin, 2017). We understand the Governance construct as equivalent to platform governance, since a DAM operates as a platform. It includes governance by the platform, through its design choices, algorithms, and policies, and governance of the platform, through regulation and oversight by external actors such as governments and regulators (Gorwa, 2019). The Cybersecurity construct consists of measures related to cybersecurity to prevent hacks and theft of investor assets. When applying this framework, users can determine whether to weight all measures equally or to concentrate on one specific area.

3. Integrity measures

The measure-level findings of each interview are documented inline throughout Section 4, identified by interviewee ID; what follows summarizes the construct- and framework-level feedback.

Market Abuse. **Access to historical market data (1.1)** is essential for detecting market abuse and other violations in DAMs (Khodabandehlou & Golpayegani, 2022). However, it was perceived ambiguously in the context of emerging marketplaces, as such data is often unavailable (ID7, ID 8). While we keep the measure, it may not be applicable in the evaluation of newly established markets. The **public disclosure of trading rules and matching or allocation algorithms (1.2)** outlines the entire matching and price discovery process to ensure an orderly functioning of the marketplace and traceability of all trading outcomes (ID1, ID3). When a **DAM stops transactions in an asset when it gains or loses more than some threshold (1.3)** (akin circuit breaker) it can help combat pump-and-dump schemes as well as prevent irrational decision-making during periods of extreme volatility, allowing the market to stabilize (La Morgia et al., 2023). **Customer identity verification processes (1.4)** can be implemented to enhance transparency. Additionally, KYC/AML protocols enable DAMs to trace and recover coins in the event of theft (Suga et al. 2020). The next measure assesses whether the DAM conducts **wallet forensics (1.5)** to identify wallets linked to illicit activities during onboarding or ongoing monitoring (**ID6, ID8**). This process includes screening for wallets associated with illicit transaction histories, such as those involving fake transactions, cryptocurrency mixers, or addresses listed on sanctions lists (e.g., OFAC list (OFAC, 2025)). **Market surveillance (1.6)** is essential to detect and prevent suspicious trading activities (Dhawan & Putniņš, 2023). **Monitoring of social media pump-and-dump groups (1.7)** can be done to avoid such manipulation from continuing (Dhawan & Putniņš, 2023), as pump-and-dump activities in crypto markets are often openly promoted in social media groups by fraudsters. **Self-trade functionality to prevent wash trading (1.8)** can be implemented, meaning an account cannot fulfill its own buy or sell orders, in order to prevent wash trading (Victor & Weintraud, 2021). **Deviations of trade sizes from Benford's law (1.9)** can be measured to detect wash trading. Benford's law states that the first digits of trade sizes on DAMs should follow a logarithmic distribution, with the percentage of trades starting with digit i (where $i \in \{1, 2,\ldots,9\}$) given by $\log10(i + 1) - \log10(i)$. Deviations from this expected distribution, measured using a $\chi 2$ statistic, can help identify unusual trading patterns such as wash trading (Aloosh & Li, 2024). **Clustering of trading volumes (1.10)** can be performed to detect wash trading. Trade size clustering occurs because human trades often concentrate around round numbers. To quantify this, the frequency of trades at rounded sizes is compared to nearby unrounded sizes, calculated as a ratio of trades at specific sizes to total trades in a range (Aloosh & Li, 2024). The **deviation of number or volume of trades from lognormal distribution (1.11)** can be measured to detect wash trading. Specifically, the mean and standard deviation of log-transformed trading volumes and number of trades are calculated over 10-minute intervals monthly. The cumulative distribution function of the empirical distribution is then compared to a normal distribution with the same mean and variance using the Kolmogorov–Smirnov statistic, which measures the maximum difference between the two (Aloosh & Li, 2024). When the **number of**

trade partners per trader account is below a certain threshold (1.12), it can be used to detect accounts that perform wash trading by identifying how many trades per trade partner a trader account has. However, if there is only a limited amount of traders in a specific token market, limiting the number of trades which can be performed with a trade partner can disrupt legitimate trades (Victor & Weintraud, 2021) (ID5).

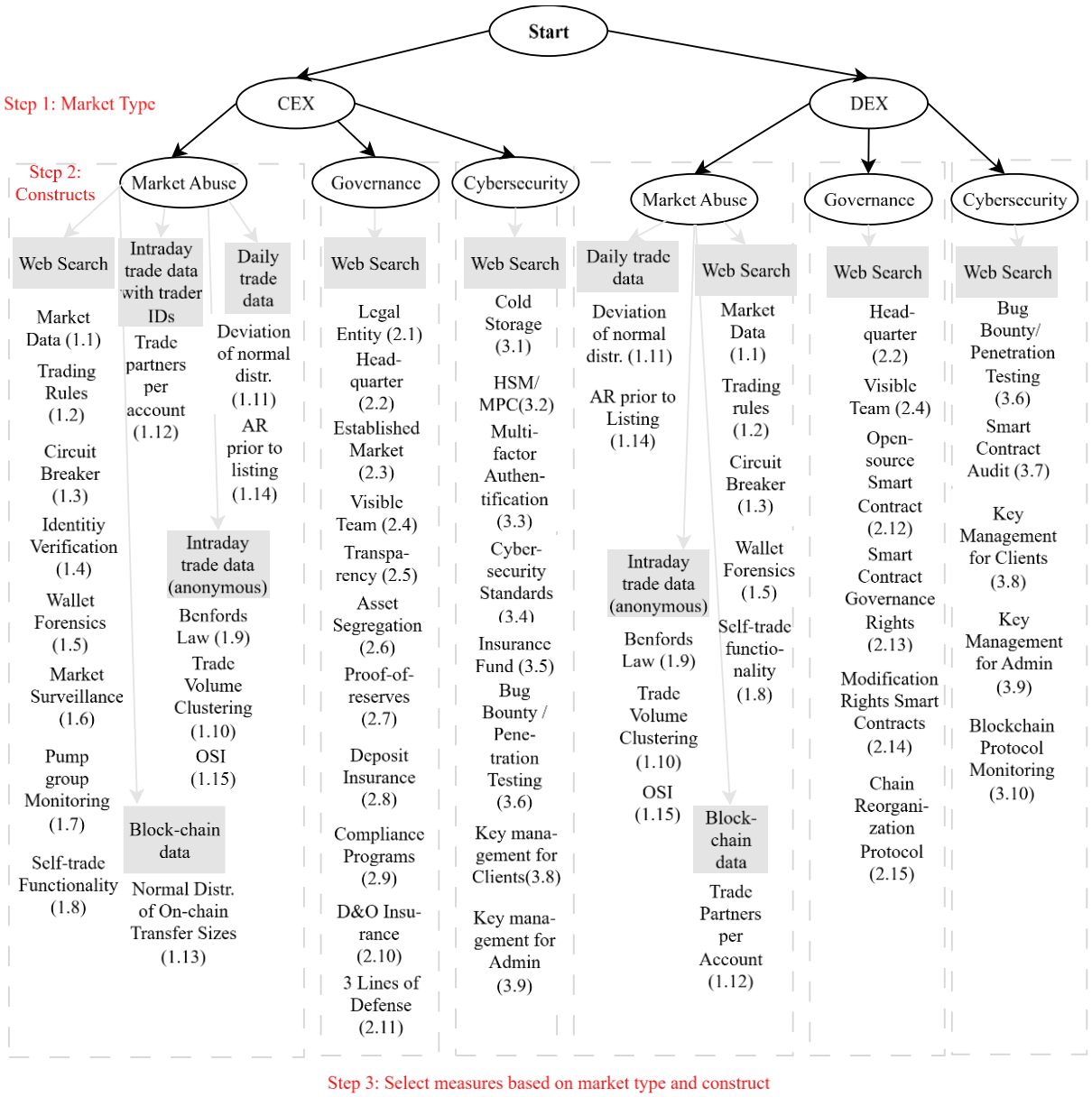

Figure 3. Integrity Measurement Framework.

The log-normal distribution of on-chain transfer sizes from user wallets to exchange wallets (1.13) can be measured to detect wash trading. Specifically, on-chain deposit patterns can be analyzed to detect anomalous wallet behavior indicative of market abuse before trade execution (ID4). Unlike measures that focus on executed trades, this measure analyzes inbound on-chain flows to exchanges, identifying unusual user behavior before trade execution by examining whether the distribution of deposit transfers deviates significantly from log-normal expectations. **Measuring significant abnormal returns or volumes prior to official exchange listing announcements or similar information events (1.14)** can be used to detect insider trading. Specifically, the measure follows the event study methodology proposed by Félez-Viñas et al. (2022). Significant abnormal returns are identified by analyzing

cumulative abnormal returns (CAR) around listing announcements on a DAM, linking pre-announcement price surges to insider trading through blockchain transaction data. Calculating the **buy-sell order size imbalance indicator (OSI) (1.15)** can be used to detect insider trading. The imbalance is calculated as: $\mathrm{OSI}_{q,t} = 100 \times (\mathrm{B}_{q,t} - \mathrm{S}_{q,t})/(\mathrm{B}_{q,t} + \mathrm{S}_{q,t})$, where $\mathrm{OSI}_{q,t}$ represents the order size imbalance for the q-quantile on day t. $\mathrm{B}_{q,t}$ is the size of buy-initiated orders within the q-quantile on day t. $\mathrm{S}_{q,t}$ is the size of the sell-initiated orders within the q-quantile on day t (Feng et al., 2018).

Governance. The measure **DAM is associated with a legal entity (no empty shell) (2.1)** and has a relevant headcount (Milunovich & Lee, 2022) is the first measure under the governance construct. The refinement "no empty shell" was proposed frequently during the expert interviews (ID 4,5,7). It can be operationalized by verifying that the legal entity maintains a sufficient headcount and is not a letterbox company. DAM-specific regulations mitigate risks associated with illicit activities. The **existence of a headquarter of the DAM (in jurisdiction with relevant regulation) (2.2**) is the next measure. Regulatory oversight plays a central role for DAM integrity but can only be applied where an official headquarter exists (Milunovich & Lee, 2022). Since regulatory frameworks vary considerably across jurisdictions, the jurisdictional qualifier was added based on expert input (ID1, ID2, ID3, ID4, ID5). In the European Union, some governance measures may therefore be redundant due to existing regulation (ID2; ID3; ID4; ID5), while remaining highly relevant in less strictly regulated jurisdictions. An **established market (2.3)** is more likely to survive. It is defined to be "established" if it is either active for more than 3.5 years or has a daily trading volume of more than $300 million (Milunovich & Lee, 2022). While several experts (ID2, ID3) agreed on the relevance of this measure, they noted that thresholds should evolve as the market matures, and strict enforcement could discourage new entrants (ID3). When the **management or development team of the DAM is visible (2.4)**, research indicates that DAMs are perceived as more trustworthy and have higher survival rates (Lee & Milunovich, 2023). When a **DAM is transparent with disclosure of financial figures, security breaches, etc. (2.5)**, it fosters trust and accountability. Breaches become more likely over time, regardless of cybersecurity quality (ID3), and transparency in disclosing such incidents is more important than their mere occurrence (ID4). **Segregation of operator and customer assets (2.6)** refers to the practice of managing customer assets separately from the DAM's own holdings. This minimizes the risk of customer losses in case of mismanagement or insolvency of the exchange. If all customer assets are managed using a single cryptographic key pair, the entire fund could be compromised due to a breach (Suga et al., 2020). **Proof-of-reserves protocols (in legitimate digital assets) (2.7)** enable DAMs to demonstrate their solvency to customers by verifying that they hold sufficient reserves to cover all liabilities. They ensure transparency by preventing DAMs from hiding losses due to cyberattacks and deter them from selling assets they do not own (Dutta & Vijayakumaran, 2019). The refinement "in legitimate digital assets" reflects the view that proof-of-reserves held in credible assets is more reliable and trustworthy than reserves held in less credible or highly volatile assets (ID4). *"The existence of reserves is one thing; the composition of the reserves is another, I would say. If they hold everything in USDT or the like, that is of course different from holding it in Trump-Coin. – ID4".* **Deposit insurance systems against insolvency (2.8)** are designed to protect customers by covering losses incurred due to internal failures or the insolvency of a cryptocurrency exchange (Oosthoek & Doerr, 2021). **Compliance programs (2.9)** ensure adherence to AML and combating the financing of terrorism (CFT) regulations. By implementing robust compliance measures, DAMs can enhance their credibility and reduce vulnerabilities (Kaal, 2020). **Directors and Officers (D&O) liability insurance (2.10)** signals strong governance by protecting executives from personal financial losses arising from legal claims related to their decisions, while its absence may indicate poor transparency or oversight (ID8). The **three-lines of defense risk-management model (business, risk & control, audit) (2.11)** ensures clear risk management roles (ID4, ID5). This widely recognized model (Arndorfer & Minto, 2015) clarifies risk management responsibilities and is mandated by regulators for financial institutions as a governance best practice. **Smart contracts that are transparent (2.12)**, i.e., open-source and adequately described, enhance accountability and reliability (ID4, ID5). When **governance rights in smart contracts are divided legitimately between investors and third parties (2.13)**, it ensures that investors retain access

to their funds and are protected from unauthorized interventions (ID5). When the **modification rights in smart contracts are governed (2.14)**, it ensures transparency and safeguards against unilateral or unauthorized modifications. If the logic or parameters of a smart contract can be altered post-deployment, the authority to make such changes must be clearly defined and appropriately governed (ID6). The existence of **chain reorganization protocol (2.15)** is specific to DEXs regarding transaction finality. Unlike CEXs, which may implement off-chain mistrade rules, DEXs rely entirely on the underlying protocol. Thus, understanding when a transaction becomes final, whether it can be reversed, and what procedures exist in the event of a chain reorganization is crucial (ID8).

Cybersecurity. **Cold wallets (with legitimate access management) (3.1)** function by keeping digital assets and private keys entirely offline to prevent unauthorized access. They should be used to store the majority of a DAM's assets securely (Suga et al., 2020). The refinement "with legitimate access management" was added to include access control, ensuring cold wallet access is governed by legitimate management procedures to prevent centralized risk (ID6). Although hot wallets are less secure than cold wallets, they provide the advantage of convenience by allowing quick transactions through internet connectivity. To enhance their security, DAMs can use **hardware security modules (HSM) or multi-party computation (MPC) to safeguard hot wallets (3.2)** (Suga et al., 2020) (ID6). MPC offers an alternative to HSMs by distributing private key control across multiple parties, reducing the risk of a single point of failure (Du & Atallah, 2001). The **existence of multifactor authentication (3.3)** enhances security by requiring different independent forms of verification for user authentication and therefore protects individual accounts from unauthorized access (Moore et al., 2018).
Cybersecurity standards (3.4), such as ISO 27001/27002, are useful in assessing the security level of an implementation. They monitor things such as security of private key management or continuous threat analysis by the DAM (Suga et al., 2020). E.g., ISO 27001 is a standard to ensure effective information security management systems (Fantazzini & Calabrese, 2021). **Insurance funds or reimbursement policies after a breach (3.5)** in DAMs serve as a critical safety measure, ensuring that users are compensated in the event of a breach or loss of funds (Moore et al., 2018). The existence of a **bug bounty program or penetration testing (3.6)** enhances security in DAMs. Penetration tests simulate potential attacks to uncover weaknesses that fraudsters could exploit, while bug bounty programs incentivize ethical hackers and cybersecurity specialists to detect and report software bugs in exchange for rewards (Fantazzini & Calabrese, 2021). A **security audit of smart contracts (3.7)** in DAMs conducted by independent and accredited providers or reliable verification mechanisms involves systematically reviewing systems and processes to identify vulnerabilities and ensure compliance with security standards (He et al., 2020) (ID8). The selection of a reliable source for the audit is especially important, as the quality of such audits can vary significantly depending on the provider.
The next measure involves the existence of **key management policies for clients (3.8)**. Signature keys enable the transfer of digital assets. Leaked or stolen signature keys cannot be revoked, nor can transactions be rolled back. Backups of signature keys or key management policies for customers that lost keys can be recovered, preventing permanent loss of access to assets (Suga et al., 2020). The measure **"existence of multi-signature key management for operator/ admin" (3.9)** enhances DAM security by distributing signing privileges among multiple stakeholders, ensuring that transactions require multiple approvals for validation. This prevents asset loss if a single key is compromised while protecting against malicious transactions (Suga et al., 2020). The continued relevance of signature backups (3.8) and multi-signature key management (3.9) was emphasized during the expert interviews. While these are standard among established CEXs, they play a critical role in operational security (ID2).
The measure **"monitoring of key functionalities of the underlying blockchain protocol" (3.10)** assesses protocol-level monitoring to ensure key functions, like fund transfers, remain operational in DEXs (ID5, ID8). Specifically, it addresses the extent to which the underlying blockchain protocol is actively monitored to ensure the availability of critical functionalities, such as the ability of investors to transfer and withdraw funds from the protocol. Given the absence of a centralized operator in most DEXs, such monitoring typically occurs through protocol-level mechanisms, including automated alerts or decentralized governance structures. This is particularly important as blockchain protocols differ significantly in terms of architecture and reliability.

Data Requirements: Users need to evaluate the feasibility of implementing a particular measure, given data requirements. Some require only a web search, e.g., whether a DAM has a bug bounty program (3.6). Others rely on historical price and trading volume data, e.g., for calculating daily returns (1.14) or the distance of trading volumes from a lognormal distribution (1.11). Additionally, the buy-sell order size imbalance indicator (OSI) to detect insider trading (1.15) requires access to intraday market data. Measures applicable at daily frequencies (e.g., 1.9, 1.10, 1.11) can also be computed using more granular data, such as the records of individual trades, when intraday data are available. One measure requires information about intraday trading activity, including trader IDs, to compute trade partner diversity (1.12) and one requires information on blockchain data for wallet analysis. Measures requiring more specific data are often more costly or challenging to obtain and process.

4.1 Evaluation

The primary objective of the evaluation was to assess whether the developed framework constitutes an acceptable problem solution, as reflected by the design objectives, derived constructs and measures, as well as to examine its applicability across diverse stakeholder groups. To achieve this, the integrity assessment framework for DAMs was evaluated through the iterative series of expert interviews. Interviewees confirmed the appropriateness of the design objectives (ID2; ID3; ID6; ID7) and supported the three constructs as a suitable categorization of DAM integrity risks (ID3; ID5; ID6), with one describing Market Abuse and Cybersecurity as "the appropriate integrity-relevant constructs for DAMs" (ID3). While the Governance construct was noted as the least immediately intuitive of the three (ID3), its scope is precisely defined as platform governance, encompassing both governance by the platform through its design choices and governance of the platform through regulatory oversight (Gorwa, 2019). The distinction between CEX and DEX was generally supported as participants highlighted substantial differences between the two, particularly in terms of trading mechanisms and asset custody. Only one expert (ID9) noted that the differences between CEXs and DEXs might diminish in the future without affecting the validity of the measures, since DAMs evolve to meet diverse user needs by integrating the most effective features of both centralized and decentralized systems, which are also discussed as hybrid exchanges (HEXs) in the literature (Hägele, 2024). One expert specifically noted that governance plays a more critical role in ensuring the integrity of CEXs (ID1). Regarding the final output of the framework for a concrete assessment of the integrity of a specific DAM, one expert (ID1) suggested aggregating measures into a single score. Another expert (ID2) argued for minimum standards for measures to classify markets as having sufficient or high integrity, rather than a single score, citing the diverse nature of integrity constructs and measures. Other experts stressed that the measures vary in importance and should not be treated as equivalent (ID7, ID8). Achieving universally applicable standards is challenging because requirements vary widely among stakeholders. For instance, banks demand higher integrity standards than retail investors, making it difficult to create universal criteria. Since the final interview (ID9) did not yield any new measures or revisions to existing ones, saturation has been reached.

4.2 Demonstration of Goal Attainment

The next stage in the process is to apply the developed artifact to real-world DAMs (Peffers et al., 2007). To this end, we assess it through three hypothetical stakeholders with differing objectives. The first stakeholder is a *tech-savvy retail investor* considering trading crypto assets via Uniswap, the largest DEX by volume. We assume that this investor is aware of the importance of cybersecurity for DEX integrity and therefore evaluates Uniswap based on the *Cybersecurity* construct, systematically considering all measures in this construct applicable to DEXs: A web search reveals that Uniswap maintains an active bug bounty program (3.6) offering up to $15.5 million for critical vulnerabilities and subjects each major protocol upgrade to multi-layered audits by independent blockchain security firms (3.7). Uniswap requires users to use a non-custodial wallet and states it has no custody or ability to recover keys or reverse transactions (3.8). Administrative controls rely on multi-signature key management (3.9); for example, the Uniswap Accountability Committee uses two multi-signature wallets to oversee incentive distributions and fund custody. Uniswap also monitors underlying blockchain infrastructure (3.10) and maintains a committee that evaluates bridge providers to ensure

secure cross-chain operations (Uniswap, 2025). Overall, Uniswap meets most Cybersecurity-related integrity requirements.

The second hypothetical stakeholder is a *bank* that is considering the introduction of crypto services for its clients and seeks to evaluate the CEX Binance as a potential marketplace for customer order execution and business cooperation, thereby evaluating all measures under the Cybersecurity and Governance constructs. The analysis shows that Binance operates through multiple global entities with more than 5,000 employees (2.1) but lacks a clearly defined global headquarters (2.2). Founded in 2017, Binance is the largest CEX and an established market participant (2.3). The company has visible leadership (CEOs Richard Teng and Yi He) (2.4) and discloses information on financial performance and security incidents but, as a private firm, does not publish full financial statements (2.5). It segregates customer and operational funds (2.6), employs a proof-of-reserves mechanism diversified across over 30 crypto assets (2.7), and maintains the Secure Asset Fund for Users (SAFU) as an emergency insurance pool for customer losses (2.8). However, no information regarding the existence of compliance programs (2.9) is disclosed on the company's website. With respect to internal governance, they follow a three-lines-of-defense risk model integrating business operations, risk control, and internal audit (2.11), though Binance has not confirmed whether it holds D&O insurance for management (2.10). Regarding Cybersecurity, Binance uses cold storage for client assets (3.1), multi-party computation for hot-wallet security (3.2), and mandatory two-factor authentication (3.3). It adheres to ISO 27001 standards (3.4), maintains a bug bounty program (3.6), and conducts regular penetration testing (3.6). Binance has previously compensated users for breaches via SAFU (3.5) and provides extensive user guidance on private-key protection (3.8) and multi-signature management (3.9) (Binance, 2025a). Overall, Binance fulfills most integrity criteria in Governance and Cybersecurity.

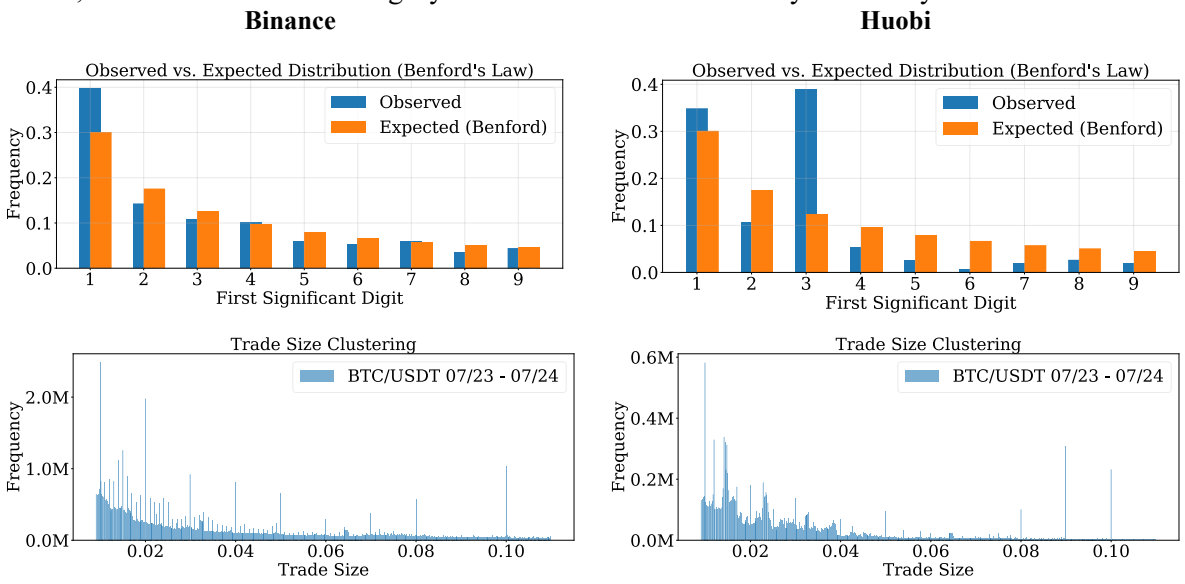

Figure 4. Wash trading detection on Binance and Huobi.

Measure/ Marketplace	**Benford's Law**		**Logn. Distribution**		**Trade Size Clustering**	**OSI** *(Buy imbalance increases with trade size quintiles)*
	χ^2/N	Econ. relevant	K-S	Econ. relevant		
Binance	0.01***	No	0.06***	No	No anomalies	No
Gate.io	0.03***	No	0.03***	No	Yes	No
Huobi	0.76***	Yes	0.07***	No	Yes	No
KuCoin	0.03***	No	0.08***	No	Yes	No
OKX	0.01***	No	0.03***	No	No anomalies	No

Table 4. Wash trading detection on the analyzed DAMs.

The third stakeholder, a *regulatory authority*, seeks to evaluate potential market abuse across five DAMs (Binance, Gate.io, Huobi, KuCoin, and OKX), with a focus on wash trading and insider trading, and thus tests all related measures. Using historical order-book and trade data from Crypto Lake for BTC/USDT between July 2023 and July 2024, the regulator applies four quantitative indicators: Benford's law (1.9), trade-size clustering (1.10), deviation from lognormal distribution (1.11), and the buy-sell order size imbalance (OSI) (1.15). Deviations from expected norms signal potential manipulation. The results are summarized in Table 4, which reports all measures across the five DAMs, and in Figure 4, which visualizes two selected measures, Benford's law and trade-size clustering, for Binance and Huobi. For Benford's law, trade-size leading digits should follow a logarithmic distribution. Binance shows no deviation, indicating no manipulative behavior; Huobi shows notable deviations, suggesting irregularities. Distance from lognormal distribution, measured by the Kolmogorov–Smirnov (K-S) statistic, is significant across all DAMs due to sample size but economically negligible relative to prior thresholds (e.g., 0.225 for wash trading, 0.035 for non-wash trading; Aloosh & Li, 2024). Trade-size clustering examines whether trades cluster around round numbers. Binance's trades cluster at 0.001 and 0.01 BTC/USDT and multiples, consistent with normal trading, whereas Huobi exhibits additional clustering around odd-lot sizes, hinting at potential manipulation. Overall, there is no evidence of wash trading on Binance and OKX, mixed signals for Gate.io and KuCoin, and potential irregularities on Huobi. The OSI indicator finds no significant insider trading across the five DAMs. Based on these results, the regulator may initiate a detailed investigation of Huobi.

5 Discussion and Conclusion

This paper addresses the challenge of integrity measurement in DAMs by answering the research questions: **RQ1:** What are integrity-relevant constructs of DAMs and how can they be measured? and **RQ2:** How can the integrity of DAMs be assessed using these constructs and measures? Following a DSR approach, we conducted a systematic literature review and a series of expert interviews to identify and evaluate integrity measures for DAMs. This process resulted in the development of 40 measures, categorized into three constructs - Market Abuse, Governance, and Cybersecurity - which together form the basis of the developed integrity assessment framework. It provides stakeholders with a structured framework to evaluate DAM integrity and can support market operators in implementing effective countermeasures, thereby creating a more secure and trustworthy trading environment. If widely adopted and used by regulators, these measures could encourage DAMs to take stronger precautions, ultimately reducing the risk of integrity violations. In cases where a DAM exhibits deficiencies across several integrity measures, investors and financial institutions may opt to refrain from trading on or engaging with that platform and instead choose alternatives that meet the integrity criteria, while regulators may prioritize closer supervision and monitoring of DAMs that perform poorly along specific integrity dimensions. However, the framework functions as a probabilistic risk-screening tool rather than a definitive integrity evaluation; practitioners should weight measures according to their specific use case and stakeholder perspective, as reflected in Section 4.1.

As scientific contribution, we propose a novel, theoretically grounded framework for assessing the integrity of DAMs. We demonstrated the practical applicability on real-world DAMs and verified its efficacy in an evaluation with experts. The inductively derived constructs provide a coherent systematization of integrity measures. In contrast to prior research that has largely focused on isolated aspects, such as pump-and-dump detection (Dhawan & Putniņš, 2023) or identifying the types of violations in DAMs (Eigelshoven et al., 2021), this work offers a holistic approach to assessing market integrity. It is developed through a DSR approach, combining a systematic literature review and expert interviews, ensuring both theoretical rigor and practical relevance. In doing so, we offer the first transparent, stakeholder-oriented tool for evaluating integrity in both CEXs and DEXs. Such survey-oriented DSR contributions constitute a valuable contribution in their own right when grounded in rigorous methodology and practical relevance (Ågerfalk, 2014). We validated the content of our constructs and the developed integrity assessment framework through an evaluation with expert

interviews and an application by three hypothetical stakeholders. We did not, however, validate the individual constructs in terms of testing their relationship with each other. This can be studied in future research, e.g., by conducting a confirmatory factor analysis to check whether items designed to measure the same construct exhibit strong correlations. One form of market abuse not captured by a dedicated measure in the framework is maximal extractable value (MEV), defined as profit extracted through control over transaction ordering. MEV is structurally inherent to AMM-based DEXs, whereas CEXs, which operate through off-chain order books, are insulated from this phenomenon. As a result, MEV is not included as an integrity measure, since it is specific to a subset of market architectures rather than a general feature of digital asset markets. Instead, it is a design-specific externality of DEX infrastructure that falls outside the scope of the governance, cybersecurity, and market abuse related integrity measures defined in this framework. Addressing MEV explicitly is therefore left as an important avenue for future research, particularly in light of emerging MEV-resistant AMM and transaction sequencing designs (Gramlich et al., 2024). Another limitation is the scope of our search string. Some measures mentioned in interviews, such as the existence of D&O liability insurance, are discussed in the literature (Xia et al., 2024) but were not retrieved by the SLR. However, a subsequent design cycle could identify the interview-derived measures in the literature as well, thereby validating them. Despite an extensive literature analysis and evaluation, we may not have included all possible measures. Nevertheless, the framework is designed to be expandable, and can incorporate new constructs and measures as integrity risks evolve in the DAM landscape, for example extending to HEX if their relevance increases (ID9). There are also limitations regarding the applicability of our construct for certain stakeholders. Specifically, some measures require access to extensive intraday data covering all transactions executed on a DAM. Such data are often (1) difficult to obtain due to high costs or technical effort required to retrieve them directly through blockchain node queries or decentralized indexing services (e.g., The Graph), and (2) challenging to analyze because they demand advanced data science expertise. Consequently, for stakeholders, such as retail investors or small institutions, the practical application of these measures is limited. Nevertheless, a wide range of alternative measures for each construct can be applied through a simple web search, but comprehensive searches across many DAMs are time-consuming. Finally, a limitation of this study is that the final framework was not re-evaluated by the domain experts due to time constraints. However, our iterative approach inherently enables continuous improvement, as each interviewer can build on the insights of the previous one. This offers a promising methodological pathway for future research involving feedback from time-limited high-quality experts. Future work could embed the integrity framework in an automated decision-support system. Key aspects include enabling users to select relevant metrics, providing customizable weighting with predefined user group-specific recommendations, and defining must-have criteria. Results could be shown as a personalized, peer-benchmarked ranking of DAMs on relative scales. Additionally, the system could display results through a personalized ranking of DAMs, using relative scales benchmarked against peers for clearer interpretation. Such a system could support more informed decisions about integrity when trading, collaborating, or supervising DAMs. Future research could also explore the integration of the framework with existing security standards and regulatory frameworks, such as DORA or MiCA, to further strengthen its real-world applicability.

References

Ågerfalk, P. J. (2014). Insufficient theoretical contribution: a conclusive rationale for rejection? *European Journal of Information Systems*, *23*(6), 593–599.

Aloosh, A., & Li, J. (2024). Direct Evidence of Bitcoin Wash Trading. *Management Science*, *70*(12), 8875–8921.

Arndorfer, I., & Minto, A. (2015). The "four lines of defence model" for financial institutions: Taking the three-lines-of-defence model further to reflect specific governance features of regulated financial institutions. *Financial Stability Institute Working Paper-BIS*(11), 1–29.

Austin, J. (2017). What Exactly Is Market Integrity: An Analysis of One of the Core Objectives of Securities Regulation. *William and Mary Business Law Review*, *8*, 215–240.

Binance. (2025a). *Binance*. https://binance.com

Binance. (2025b). *Terms of Use*. https://www.binance.com/en/terms

The Block. (2025). *Cryptocurrency Monthly Exchange Volume*. https://www.theblock.co/data/crypto-markets/spot/cryptocurrency-exchange-volume-monthly

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Clapham, B., Jakobs, J., Schmidt, J., Gomber, P., & Muntermann, J. (2023). A taxonomy of violations in digital asset markets. *ICIS 2023 Proceedings*.

Corbet, S., Lucey, B., Urquhart, A., & Yarovaya, L. (2019). Cryptocurrencies as a financial asset: A systematic analysis. *International Review of Financial Analysis*, *62*, 182–199.

Corbin, J., & Strauss, A. (2015). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (4th ed.). Sage Publications.

Dhawan, A., & Putniņš, T. J. (2023). A New Wolf in Town? Pump-and-Dump Manipulation in Cryptocurrency Markets. *Review of Finance*, *27*(3), 935–975.

Du, W., & Atallah, M. J. (2001). Secure multi-party computation problems and their applications. In V. Raskin, S. J. Greenwald, B. Timmerman, & D. Kienzle (Eds.), *Proceedings of the 2001 workshop on New security paradigms* (pp. 13–22). ACM.

Dupuis, D., Smith, D., & Gleason, K. (2023). Old Frauds with a New Sauce: Digital Assets and Space Transition. *Journal of Financial Crime*, *30*(1), 205–220.

Dutta, A., & Vijayakumaran, S. (2019). MProve: A Proof of Reserves Protocol for Monero Exchanges. In *2019 IEEE European Symposium on Security and Privacy Workshops* (pp. 330–339). IEEE.

Eigelshoven, F., Ullrich, A., & Parry, D. (2021). Cryptocurrency Market Manipulation-A Systematic Literature Review. *ICIS 2021 Proceedings 2021*.

Fantazzini, D., & Calabrese, R. (2021). Crypto Exchanges and Credit Risk: Modeling and Forecasting the Probability of Closure. *Journal of Risk and Financial Management*, *14*(11), 516.

Félez-Viñas, E., Johnson, L., & Putnins, T. J. (2022). Insider Trading in Cryptocurrency Markets. *SSRN Electronic Journal*.

Feng, W., Wang, Y., & Zhang, Z. (2018). Informed Trading in the Bitcoin Market. *Finance Research Letters*, *26*, 63–70.

Gorwa, R. (2019). What is platform governance? *Information, Communication & Society*, *22*(6), 854–871.

Gramlich, V., Jelito, D., & Sedlmeir, J. (2024). Maximal extractable value: Current understanding, categorization, and open research questions. *Electronic Markets*, *34*(49).

Hägele, S. (2024). Centralized Exchanges vs. Decentralized Exchanges in Cryptocurrency Markets: A Systematic Literature Review. *Electronic Markets*, *34*(33).

Hasanova, H., Baek, U., Shin, M., Cho, K., & Kim, M.-S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management*, *29*(2), Article e2060.

He, D., Deng, Z., Zhang, Y., Chan, S., Cheng, Y., & Guizani, N. (2020). Smart Contract Vulnerability Analysis and Security Audit. *IEEE Network*, *34*(5), 276–282.

Hevner, A. R., & Chatterjee, S. (2010). *Design Research in Information Systems: Theory and Practice* (Vol. 22). Springer.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105.

Jakobs, J., Muntermann, J., & Nickerson, R. (2024). Navigating Risks in the Crypto Landscape–A Taxonomy of Risk-Related Aspects of Crypto Assets. In M. Mandviwalla, M. Söllner, & T. Tuunanen (Eds.), *Lecture Notes in Computer Science. Design Science Research for a Resilient Future* (Vol. 14621, pp. 370–383). Springer.

Johnson, K. N. (2021). Decentralized Finance: Regulating Cryptocurrency Exchanges. *William and Mary Law Review*, *62*(6), 1911–2001.

Kaal, W. A. (2020). Digital Asset Market Evolution. *Journal of Corporation Law*, *46*, 909–964.

Kaiko. (2025). *Kaiko Spot Exchange Ranking*. https://www.kaiko.com/indices/exchange-ranking

Khodabandehlou, S., & Golpayegani, S. A. H. (2022). Market Manipulation Detection: A Systematic Literature Review. *Expert Systems with Applications*, *210*, 118330.

La Morgia, M., Mei, A., Sassi, F., & Stefa, J. (2023). The Doge of Wall Street: Analysis and Detection of Pump and Dump Cryptocurrency Manipulations. *ACM Transactions on Internet Technology*, *23*(1), 1–28.

Lee, S. A., & Milunovich, G. (2023). Digital Exchange Attributes and the Risk of Closure. *Blockchain: Research and Applications*, *4*(2), 100131.

Li, D., Han, D., Zheng, Z., Weng, T.-H., Li, K.-C., Li, M., & Cai, S. (2024). Does Short-and-Distort Scheme Really Exist? A Bitcoin Futures Audit Scheme through BIRCH & BPNN Approach. *Computational Economics*, *63*(4), 1649–1671.

Mayring, P. (2015). Qualitative Content Analysis: Theoretical Background and Procedures. In A. Bikner-Ahsbahs, C. Knipping, & N. Presmeg (Eds.), *Advances in Mathematics Education. Approaches to Qualitative Research in Mathematics Education* (pp. 365–380). Springer.

Milunovich, G., & Lee, S. A. (2022). Cryptocurrency Exchanges: Predicting which Markets will Remain Active. *Journal of Forecasting*, *41*(5), 945–955.

Moore, T., Christin, N., & Szurdi, J. (2018). Revisiting the Risks of Bitcoin Currency Exchange Closure. *ACM Transactions on Internet Technology*, *18*(4), 1–18.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*(1), 2–26.

OFAC. (2025). *Sanctions List Search*. https://sanctionssearch.ofac.treas.gov/

Oosthoek, K., & Doerr, C. (2021). Cyber Security Threats to Bitcoin Exchanges: Adversary Exploitation and Laundering Techniques. *IEEE Transactions on Network and Service Management*, *18*(2), 1616–1628.

Park, A. (2023). The Conceptual Flaws of Decentralized Automated Market Making. *Management Science*, *69*(11), 6731–6751.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77.

Reuters. (2025). *Bybit says $1.5 billion worth of crypto stolen in ether wallet hack*. https://www.reuters.com/technology/crypto-exchange-bybit-says-ether-wallet-hacked-2025-02-21/

Robinson, O. C. (2014). Sampling in Interview-Based Qualitative Research: A Theoretical and Practical Guide. *Qualitative Research in Psychology*, *11*(1), 25–41.

Sofi, A. A., Mir, A. H., & Jabeen, Z. (2025). Bitcoin attacks: A comprehensive study. *Journal of Network and Computer Applications*, *243*, 104297.

Suga, Y., Shimaoka, M., Sato, M., & Nakajima, H. (2020). Securing Cryptocurrency Exchange: Building up Standard from Huge Failures. In M. Bernhard, A. Bracciali, L. J. Camp, S. Matsuo, A. Maurushat, P. B. Rønne, & M. Sala (Eds.), *Lecture Notes in Computer Science. Financial Cryptography and Data Security* (Vol. 12063, pp. 254–270). Springer.

Uniswap. (2025). *Uniswap Blog*. https://blog.uniswap.org/

Victor, F., & Weintraud, A. M. (2021). Detecting and Quantifying Wash Trading on Decentralized Cryptocurrency Exchanges. In J. Leskovec, M. Grobelnik, M. Najork, J. Tang, & L. Zia (Eds.), *Proceedings of the Web Conference 2021* (pp. 23–32). ACM.

vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., & Cleven, A. (2015). Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research. *Communications of the Association for Information Systems*, *37*, 205-224.

Wang, L., Cheng, H., Sun, Z., Tian, A., & Yang, Z. (2025). PSPL: A Ponzi scheme smart contracts detection approach via compressed sensing oversampling-based peephole LSTM. *Future Generation Computer Systems*, *166*, 107655.

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), xiii–xxiii.

Xia, H., Ling, S., Liu, Z., & Treepongkaruna, S. (2024). Corporate governance and corporate social responsibility: Evidence from directors' and officers' liability insurance. *Corporate Social Responsibility and Environmental Management*, *31*(4), 3006–3030.