**Journal of Information Systems Engineering and Management**
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

# Detecting Digital Investment Scams: The SDQC User-Level Screening Framework for Malaysian Gig Workers

Mohd Fahmy Ishak[1], Wan Mohd Hirwani Wan Hussain[1], Abu Hanifah Ayob[2]
[1]*Graduate School of Business, Universiti Kebangsaan Malaysia,*
[2]*Faculty of Economy and Management, Universiti Kebangsaan Malaysia*

**ARTICLE INFO**

Received: 30 Dec 2024

Revised: 19 Feb 2025

Accepted: 27 Feb 2025

**ABSTRACT**

Digital investment scams targeting gig workers and freelancers in Malaysia have intensified with the expansion of cryptocurrency markets and AI-driven platforms, yet individuals in precarious employment lack access to structured tools for evaluating fraudulent opportunities. This study conceptualises digital scam vulnerability as a user-level decision support problem and develops the Scam Detection Quick-Check (SDQC), a six-dimensional screening framework derived from the synthesis of behavioural, regulatory, and informational scam risk indicators. The study employs a conceptual design supported by targeted literature synthesis and illustrative case analysis of three high-profile Malaysian investment scams: Lavida Coin, Harapan Coin, and JJPTR. The SDQC framework comprises six screening dimensions, namely Source Verification, Credibility Assessment, Offering Clarity, Disclosure and Regulation, External Validation, and Timing Awareness, each mapped to a distinct class of scam vulnerability identified in the literature. Case analysis shows that all three Malaysian cases failed across multiple SDQC dimensions, illustrating the framework's diagnostic relevance in real-world scam contexts. The study makes three scholarly contributions: it reframes individual scam susceptibility as a structured screening problem; it develops the SDQC from literature synthesis and case-based reasoning; and it extends scam prevention research into the digital gig economy context in Malaysia. The SDQC offers a practical user-level screening tool applicable to financial literacy programmes, platform-integrated warning systems, and regulatory guidance in Malaysia and comparable digital labour markets.

**Keywords:** Digital Investment Scams; Gig Economy; Cryptocurrency Fraud; Decision Support; Scam Detection Framework; Malaysia

## 1. INTRODUCTION

Malaysia's digital economy has transformed the way people earn a living, particularly among workers operating outside traditional employment structures. Platforms such as Grab, PandaGo, and GoGet have expanded flexible income opportunities for freelancers and gig workers, but they have also increased exposure to digital financial risks that conventional employment arrangements may partly buffer. Among the most serious of these risks are deceptive digital investment schemes, including fake Initial Coin Offerings (ICOs), cryptocurrency fraud, and AI-simulated trading platforms. Trozze et al. (2022) show that such scams have become globally significant threats, often targeting individuals with limited capacity for independent financial risk assessment.

The structural vulnerability of gig workers is well established. Hamid et al. (2024) confirm that Malaysian gig workers exhibit low financial resilience, with financial literacy identified as a primary determinant of their capacity to withstand adverse financial shocks. Unlike salaried employees who may access employer-sponsored financial guidance, gig workers navigate investment decisions alone. This vulnerability is amplified by social media environments where the Federal Trade Commission (2022) reports that investment scams drove the largest share of social media fraud losses in 2021. The combination of financial precarity, informational isolation, and constant digital exposure creates a uniquely acute risk environment for this population.

Despite the urgency of this problem, a critical gap exists in the literature. Existing research addresses cryptocurrency fraud mechanisms (Bartoletti et al., 2021; Trozze et al., 2022), investor behavioural biases (Ahmad & Lang, 2025;

**Journal of Information Systems Engineering and Management**
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

Zhang et al., 2022), and regulatory frameworks for scam prevention, but does not sufficiently offer a practical, user-level screening framework tailored to the specific conditions faced by gig economy workers in Malaysia. Available detection tools are either technically complex, institutionally oriented, or designed for Western regulatory contexts. No study has yet attempted to synthesise these literatures into a coherent, accessible decision-support instrument calibrated to the behavioural and informational vulnerabilities of Malaysia's digital workforce.

This study addresses that gap by reconceptualising digital scam vulnerability as a user-level decision support problem and developing the Scam Detection Quick-Check (SDQC) framework. The SDQC translates six recurring risk dimensions identified in the scam literature into an actionable screening instrument. These dimensions are: source credibility, team legitimacy, offering transparency, regulatory disclosure, third-party validation, and urgency exploitation.

This study makes three contributions. First, it conceptualises scam screening as a user-level decision support problem. Second, it develops the SDQC framework from literature synthesis and case-based reasoning rather than practitioner intuition. Third, it extends scam prevention research into the underexplored context of Malaysia's digital gig economy. In this sense, the SDQC is positioned not only as a scam awareness framework, but also as a user-facing decision support logic for digital risk evaluation in contemporary platform-based environments.

The remainder of this paper is structured as follows. Section 2 reviews and synthesises the relevant literature, organised by thematic risk dimension. Section 3 presents the methodology underpinning the study's design, literature selection, case selection, and framework development logic. Section 4 introduces and conceptually analyses each SDQC dimension. Section 5 applies the framework to three illustrative Malaysian scam cases. Section 6 discusses implications by stakeholder group. Section 7 addresses limitations and future research directions. Section 8 concludes.

## 2. LITERATURE REVIEW

The following review synthesises empirical and conceptual literature relevant to digital investment scam vulnerability, organised around four thematic clusters: behavioural bias and scam susceptibility; platform trust and social misinformation; regulatory ambiguity and enforcement failure; and decision-support mechanisms in fraud prevention. This thematic structure directly motivates the six dimensions of the SDQC framework developed in Section 4.

### *2.1 Behavioural Bias and Scam Susceptibility*

A substantial body of evidence demonstrates that cognitive and emotional biases are primary enablers of investment scam victimisation. Ahmad and Lang (2025) establish that bias-induced gullibility fully mediates the relationship between financial literacy and scam victimisation, meaning that even financially knowledgeable individuals remain vulnerable when their judgment is compromised by pre-existing cognitive distortions. Zhang et al. (2022) identify anchoring bias and optimism bias as significant impairments to investment decision quality, particularly under conditions of information asymmetry. These findings are especially consequential for gig workers, who must make financial decisions under conditions of time pressure and income volatility that are known to amplify cognitive biases.

Bartoletti et al. (2024) introduce the concept of crypto-cognitive exploitation, documenting how scammers systematically combine urgency cues, social proof, and authority signals to simultaneously engage multiple bias pathways. This multi-dimensional manipulation is more effective than any single psychological technique alone. Hamid et al. (2024) contextualise these dynamics within the Malaysian gig economy, confirming that income level and financial literacy jointly determine financial resilience, and that those lacking structured financial education face disproportionate exposure. The implication is that scam susceptibility among this group is not a matter of intelligence but of structural disadvantage amplified by cognitive exploitation.

### *2.2 Platform Trust and Social Misinformation*

Social platforms have become the primary vector for investment scam distribution. The Federal Trade Commission (2022) documents that over 95,000 individuals reported social media-initiated investment fraud losses in 2021, with investment scams accounting for the dominant share of losses across all fraud categories. This data establishes social

**Journal of Information Systems Engineering and Management**
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

media not merely as a communication channel but as an active scam infrastructure that amplifies reach while reducing victims' capacity for critical evaluation. Pavone and Rossi (2025) demonstrate that low crypto literacy is associated with fear-based overreaction and uncritical trust in unfamiliar digital investment offers, making platform-active individuals particularly susceptible.

The social embeddedness of trust in digital communities is a critical amplifying mechanism. Sinha et al. (2022) show that users preferentially trust content that appears frequently or is endorsed by peers, creating susceptibility to coordinated disinformation campaigns. In the Malaysian context, Telegram and WhatsApp groups function as informal financial advisory channels, generating echo chambers in which fraudulent claims circulate with apparent community validation. Mackenzie (2022) argues that the grey economy of cryptocurrency trading normalises market abuse as a routine feature of the environment, such that victims may not even recognise fraudulent behaviour as exceptional. This normalisation of deception makes platform-level trust signals an unreliable guide to investment legitimacy.

### *2.3 Regulatory Ambiguity and Enforcement Failure*

Regulatory inadequacy is a structural enabler of cryptocurrency fraud. Trozze et al. (2022) demonstrate through systematic review that regulatory gaps are defining features of the environments in which crypto scams proliferate. These gaps include jurisdictional ambiguity, slow enforcement response, and the absence of mandatory disclosure standards for ICOs. Scam projects routinely exploit regulatory uncertainty to operate without oversight until collapse. Bartoletti et al. (2021) confirm that scam tokens are almost universally characterised by the absence of risk disclosure, verifiable token economics, and regulatory registration, and that these features reliably distinguish fraudulent from legitimate projects.

Wilson et al. (2024) examine the Malaysian regulatory context specifically, noting that law enforcement and regulatory agencies face persistent challenges in responding rapidly to fast-evolving digital scam campaigns. Their qualitative study of Malaysian scam victims and enforcement officers reveals that regulatory responses are typically reactive, with action initiated only after significant public losses, and that awareness of available reporting mechanisms is low among vulnerable populations. This regulatory gap reinforces the case for user-level screening tools that do not depend on institutional intervention to provide protection.

### *2.4 Decision-Support Mechanisms in Fraud Prevention*

While the literature extensively documents scam vulnerabilities, research on user-level decision-support instruments remains limited. Mohd Padil et al. (2022) demonstrate that practical financial literacy education, specifically the development of budgeting discipline and investment scepticism skills, significantly improves scam awareness among Malaysian university students. Kasim et al. (2024) extend this finding to retirees, confirming that structured financial literacy remains the most consistent predictor of scam awareness across age groups. Pavone and Rossi (2025) further argue that demystification of technical investment concepts is a more effective intervention than general fraud awareness messaging, because it addresses the informational asymmetry that scammers exploit.

Chadalapaka et al. (2022) and Ma et al. (2025) demonstrate the potential of automated detection tools, including deep learning models for pump-and-dump identification and psychological technique benchmarks for scam communication analysis. However, these tools remain inaccessible to ordinary users without technical infrastructure. Proofpoint (2024) and Zarifis and Castro (2024) further document the extension of investment fraud into gig economy recruitment contexts and NFT markets, underscoring the need for screening frameworks that are domain-agnostic and adaptable to emerging fraud environments.

Taken together, this literature points to a coherent set of risk dimensions that any effective user-level screening framework must address: source and provenance verification, team identity credibility, investment proposition transparency, adequacy of regulatory disclosure, availability of independent third-party validation, and resistance to urgency-based psychological pressure. These six dimensions form the conceptual foundation of the SDQC framework developed in this study. Rather than treating these issues as separate strands of research, the present study integrates them into a single user-level screening logic, thereby translating dispersed fraud insights into a structured conceptual framework for practical scam evaluation.

**Journal of Information Systems Engineering and Management**
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

## 3. METHODOLOGY

### *3.1 Study Design*

This study adopts a conceptual design supported by targeted literature synthesis and illustrative Malaysian case analysis. Conceptual papers that develop theoretical frameworks from literature and case evidence are a well-established mode of scholarly contribution in information systems and financial crime research, particularly where the phenomenon of interest is too recent or context-specific for large-scale empirical data collection. The SDQC framework is positioned as a conceptual model requiring subsequent empirical validation, and its development follows a structured process of four stages: thematic literature synthesis, risk dimension identification, framework construction, and illustrative case application. This design is appropriate because the study aims to develop a conceptually grounded screening framework for an emerging problem area where user-level decision tools remain underdeveloped and context-specific empirical models are still limited.

### *3.2 Literature Selection*

Literature was identified through systematic searching of databases including Scopus, Web of Science, Google Scholar, and SSRN, using search terms spanning scam psychology, cryptocurrency fraud, investor behaviour, platform trust, regulatory ambiguity, and financial literacy. Priority was given to peer-reviewed sources published between 2019 and 2025 to ensure contemporary relevance, with foundational earlier works included where they remained analytically indispensable. Sources were screened for relevance to the gig economy context, the Malaysian regulatory environment, and the specific risk dimensions of interest. Grey literature from authoritative institutional sources such as the Federal Trade Commission and Proofpoint was included where it provided empirical evidence unavailable in the academic literature. A targeted body of recent and relevant sources meeting these criteria was incorporated into the analysis.

### *3.3 Case Selection*

Three Malaysian investment scam cases were selected for illustrative framework application: Lavida Coin (2018), Harapan Coin (2018), and JJPTR (2017). Cases were selected on four criteria: Malaysian provenance, ensuring contextual alignment with the study's geographic focus; public visibility, allowing verification of case details through regulatory records and media reporting; variation in primary manipulation strategy, enabling demonstration that the SDQC addresses diverse scam architectures; and analytical usefulness, with each case exhibiting failures across multiple distinct SDQC dimensions. Together, the three cases represent authority-based manipulation in Lavida Coin, symbolic-political trust exploitation in Harapan Coin, and return-driven financial manipulation in JJPTR, providing a representative spread of scam typologies documented in the literature.

### *3.4 Framework Development*

The SDQC framework was developed through a process of iterative mapping between literature-identified risk themes and operational scam indicators. The four thematic clusters identified in the literature review, namely behavioural bias, platform trust, regulatory ambiguity, and decision-support, were decomposed into discrete risk signals that a non-expert user could feasibly evaluate without technical infrastructure. Each of the six SDQC dimensions emerged from this decomposition. Source Verification addresses provenance opacity. Credibility Assessment addresses identity fabrication. Offering Clarity addresses informational opacity. Disclosure and Regulation addresses regulatory evasion. External Validation addresses self-referential legitimacy claims. Timing Awareness addresses urgency-based psychological pressure. This mapping ensures that the framework is theoretically grounded rather than practitioner-intuitive, and that each dimension can be traced to a specific class of scam vulnerability documented in the empirical literature.

## 4. THE SDQC FRAMEWORK

The Scam Detection Quick-Check (SDQC) is a user-level screening model for evaluating the legitimacy of digital investment opportunities, derived from the synthesis of behavioural, regulatory, and informational scam risk indicators identified in the literature. It is not a compliance checklist or regulatory instrument; rather, it is a structured cognitive aid that enables non-expert users to systematically evaluate the observable signals of investment

**Journal of Information Systems Engineering and Management**
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

legitimacy across six dimensions. Each dimension addresses a distinct class of vulnerability and draws its conceptual basis from the empirical literature reviewed in Section 2. The six dimensions are presented below with their theoretical foundations.

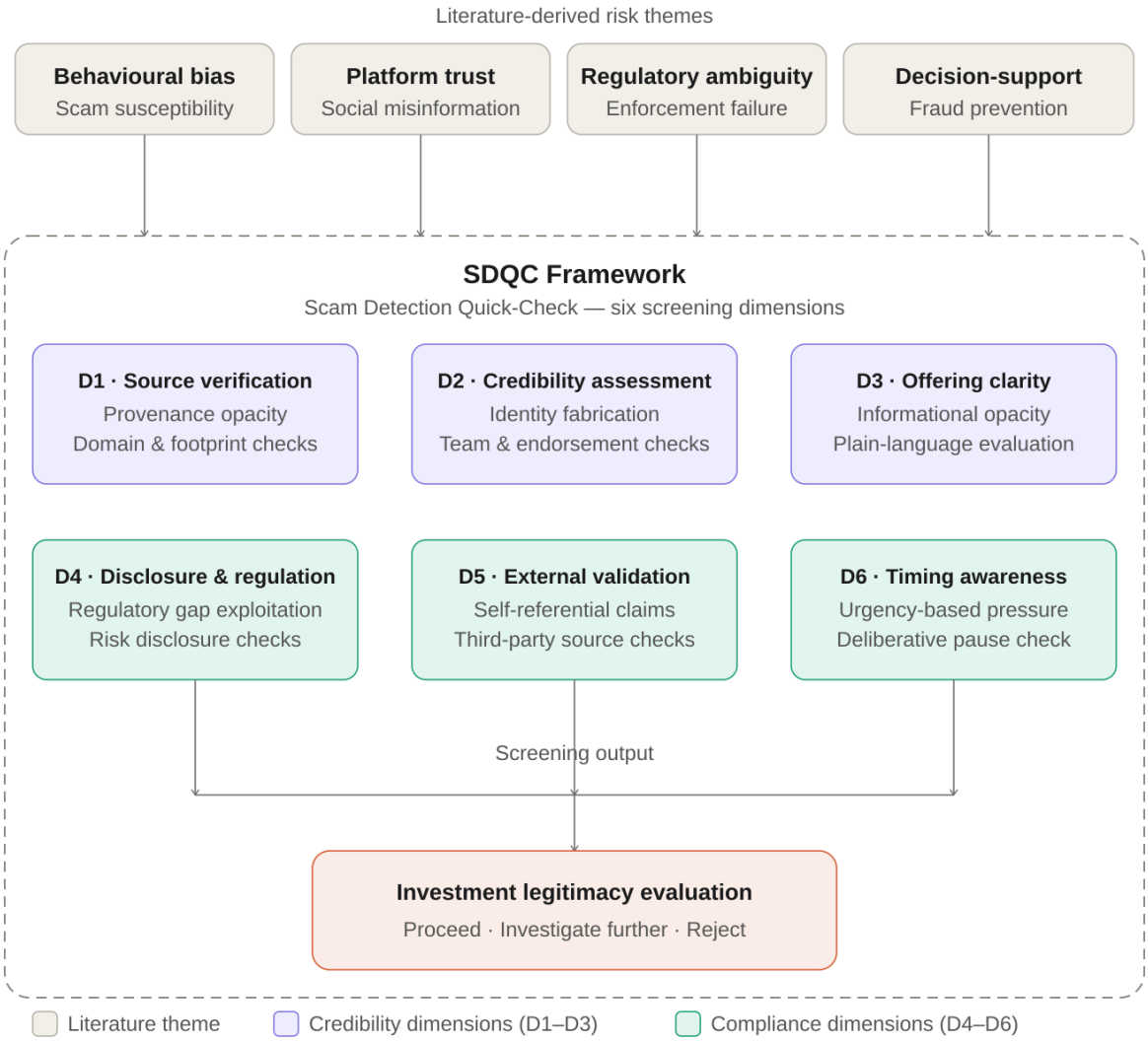


*Figure 1.* ***The Scam Detection Quick-Check (SDQC) Framework: From Literature Themes to Screening Dimensions***

### *4.1 Source Verification*

Source Verification addresses the vulnerability arising from provenance opacity, which refers to the deliberate concealment or fabrication of an investment opportunity's origin. Scammers routinely establish fraudulent digital identities through quickly registered lookalike domains, cloned whitepapers, and fake project websites that mimic legitimate infrastructure. Trozze et al. (2022) document that scam ICOs characteristically operate from domains registered within days of the scheme's launch, with no verifiable institutional or regulatory history. Chadalapaka et al. (2022) demonstrate that metadata-level signals such as domain age, registration patterns, and keyword clustering are effective early fraud indicators. This dimension operationalises those findings by prompting users to verify the provenance, registration age, and consistency of the opportunity's digital footprint before engaging further.

### *4.2 Credibility Assessment*

Credibility Assessment addresses the vulnerability arising from identity fabrication, which includes the creation of synthetic founder profiles, misappropriated credentials, and misleading endorsement claims. Bartoletti et al. (2024)

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

demonstrate that scammers systematically construct false authority by combining fabricated professional identities with genuine celebrity or institutional names, exploiting authority bias to suppress scepticism. Pavone and Rossi (2025) confirm that users with low crypto literacy are particularly susceptible to these manufactured legitimacy signals. Wilson et al. (2024) further document that political and celebrity endorsements in Malaysian scam cases created false security without any corresponding legal or regulatory foundation. This dimension addresses that vulnerability by directing evaluation toward independently verifiable evidence of team identity, professional history, and institutional affiliation.

### *4.3 Offering Clarity*

Offering Clarity addresses the vulnerability arising from deliberate informational opacity, which involves the use of technical jargon, vague roadmaps, and conceptually obscure investment propositions to prevent critical evaluation. Ahmad and Lang (2025) establish that bias-induced gullibility is particularly pronounced when individuals encounter persuasive messaging they cannot independently evaluate, creating a cognitive pathway through which opacity becomes a direct fraud enabler. Mackenzie (2022) identifies opacity as a defining feature of crypto grey economy scams, arguing that legitimate projects distinguish themselves through transparency of purpose, mechanism, and risk. This dimension operationalises that distinction by asking whether the investment proposition can be articulated in plain terms, whether the revenue model is coherent, and whether technical claims are verifiable.

### *4.4 Disclosure and Regulation*

Disclosure and Regulation addresses the structural vulnerability arising from regulatory gap exploitation, characterised by the deliberate absence of risk disclosures, token economics, and legal registration to operate without accountability. Trozze et al. (2022) establish that regulatory ambiguity is a primary enabler of ICO fraud, with scam projects routinely avoiding jurisdictions with disclosure requirements. Bartoletti et al. (2021) confirm that the absence of risk sections, disclaimers, and verifiable legal entity information is an overwhelmingly reliable marker of fraudulent intent among cryptocurrency projects. This dimension does not require users to conduct legal analysis; rather, it prompts evaluation of whether the basic disclosure infrastructure of a legitimate investment offering is present and internally consistent. This includes risk warnings, token economics, and an identifiable legal entity.

### *4.5 External Validation*

External Validation addresses the vulnerability arising from self-referential legitimacy claims, which refers to the reliance on internally generated testimonials, unverifiable endorsements, and platform-specific community activity as evidence of legitimacy. Bartoletti et al. (2021) demonstrate that scam tokens are almost universally absent from independent verification platforms such as CoinMarketCap and reputable blockchain audit services. Sinha et al. (2022) show that users' tendency to trust frequently encountered or peer-endorsed content creates susceptibility to coordinated disinformation campaigns that simulate external validation. This dimension addresses that vulnerability by directing evaluation toward neutral, third-party sources beyond the project's own communication channels, and by prompting scrutiny of review patterns for signs of bot-generated or coordinated content.

### *4.6 Timing Awareness*

Timing Awareness addresses the vulnerability arising from urgency-based psychological pressure, which involves the deliberate use of countdown mechanisms, scarcity messaging, and social pressure to suppress deliberative evaluation. Ma et al. (2025) identify these urgency techniques as among the most consistently deployed psychological tools in real-world scam communications, noting that their primary function is to activate FOMO-driven decision-making before rational evaluation can occur. Ahmad and Lang (2025) confirm that urgency exploitation is particularly effective when combined with existing financial pressure, as is characteristic of the gig worker context. This dimension operationalises the protective value of deliberate pausing: if an opportunity penalises careful evaluation by threatening loss of access or returns, that urgency signal itself constitutes evidence of fraudulent intent warranting heightened scepticism.

The framework's value lies not in functioning as a technical detection instrument, but in providing a structured cognitive scaffold through which complex, multi-dimensional fraud research can be translated into an accessible

**Journal of Information Systems Engineering and Management**
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

user-level screening process. By sequentially applying the six dimensions, users introduce deliberative structure at precisely the moment when scam tactics are designed to suppress it.

## 5. CASE STUDIES: ILLUSTRATIVE FRAMEWORK APPLICATION

This section applies the SDQC framework to three high-profile Malaysian investment scams: Lavida Coin, Harapan Coin, and JJPTR. The purpose is not to provide exhaustive historical reconstruction, but to illustrate how the SDQC functions as a diagnostic tool in real scam environments. Each case represents a distinct primary manipulation strategy, thereby showing how different legitimacy failures can be identified through the framework's six screening dimensions.

### *5.1 Lavida Coin: Authority Bias and Personality-Driven Trust*

Lavida Coin was launched in 2018 under the promotion of entrepreneur and public figure Dato' Seri Vida, with claims of high returns linked to the acquisition of a television broadcast station. The case exemplifies the authority bias exploitation pattern identified by Bartoletti et al. (2024): celebrity endorsement was used as the primary legitimacy signal, effectively bypassing users' evaluative processes. The coin possessed no verifiable whitepaper, no credentialled project team, and no regulatory filing. This concern is reinforced by the Securities Commission Malaysia, which issued a notice directing the promoters of Lavidacoin to cease all promotional activities and placed related promoters on its Investor Alert List, thereby underscoring the absence of credible regulatory standing behind the project (Securities Commission Malaysia, 2018). Bartoletti et al. (2021) confirm that the absence of verifiable documentation is a reliable scam indicator. Applied against the SDQC, Lavida Coin fails Source Verification (no verifiable domain history or institutional identity), Offering Clarity (no coherent token utility or revenue model), and Credibility Assessment (team identity reducible to a single celebrity without verifiable project credentials). This case suggests that personality-driven trust functions as a fragile legitimacy signal because it does not depend on verifiable project infrastructure and may be borrowed, exaggerated, or misinterpreted without substantive institutional grounding.

### *5.2 Harapan Coin: Symbolic Trust and Regulatory Absence*

Harapan Coin, also launched in 2018, claimed to be Malaysia's first political fundraising cryptocurrency, capitalising on the national political climate surrounding the then-opposition coalition. This case illustrates symbolic trust exploitation: the appropriation of politically charged national sentiment to create a sense of legitimacy and shared purpose that bypasses rational evaluation. Wilson et al. (2024) document that political branding reduced critical scrutiny among Malaysian investors by aligning the opportunity with nationalistic identity. Yet the project lacked token economics, regulatory approval from the Securities Commission of Malaysia, and any independent third-party audit or listing. Contemporary Malaysian reporting also indicated that the legal and regulatory status of Harapan Coin remained under official consideration, further highlighting the project's uncertain governance and disclosure position (Bernama, 2019). Applied against the SDQC, Harapan Coin fails Regulatory Disclosure (no regulatory registration or risk disclosure), Credibility Assessment (political association misrepresented as institutional endorsement), and External Validation (absent from all independent verification platforms). This case highlights that symbolic legitimacy, constructed through political or ideological alignment, is structurally distinct from regulatory and informational legitimacy and cannot serve as a substitute for either.

### *5.3 JJPTR: Return-Driven Manipulation and Disclosure Failure*

JJ Poor to Rich (JJPTR), which collapsed in 2017 with losses exceeding RM1 billion, operated as a Ponzi scheme under the guise of a financial education platform, promising monthly returns of up to 20 per cent. This case represents return-driven manipulation: the exploitation of unrealistic return promises to engage investors' reward-seeking bias while systematically concealing the absence of a legitimate underlying business model. Bartoletti et al. (2021) note that Ponzi scheme structures continuously evolve their narrative framing to remain ahead of regulatory detection; Mackenzie (2022) similarly documents how familiar criminal scripts are repackaged in novel legitimacy frames. JJPTR's promise of financial empowerment through education is a clear example of this form of narrative reframing. This interpretation is further supported by the Malaysian regulatory context, as Bank Negara Malaysia listed JJPTR in its consumer alert materials, reinforcing concerns about the scheme's lack of legitimate regulatory standing (Bank Negara Malaysia, n.d.). Applied against the SDQC, JJPTR fails Timing Awareness (urgency and social

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

pressure to recruit referrals), Disclosure and Regulation (no risk sections, no transparent fee structure, no regulatory registration), and Credibility Assessment (founder credentials unverifiable beyond self-promotional claims). This case indicates that educational framing can function as a legitimacy veneer that reduces scepticism while subtly shifting responsibility for failure onto the investor's perceived lack of understanding.

### *5.4 Cross-Case Analytical Synthesis*

Across all three cases, several recurring patterns emerge that reinforce the SDQC's theoretical foundation. First, each scam deployed at least one high-salience legitimacy signal designed to dominate users' evaluative attention and suppress scrutiny of underlying structural deficiencies. These signals took the form of celebrity endorsement in Lavida Coin, political association in Harapan Coin, and an educational mission in JJPTR. This aligns with Bartoletti et al.'s (2024) model of crypto-cognitive exploitation, wherein multi-dimensional manipulation creates conditions where no single evaluative question is sufficient to detect fraud. Second, all three cases exhibited complete regulatory disclosure failure: none possessed regulatory registration, risk warnings, or verifiable legal entity information, consistent with Trozze et al.'s (2022) documentation of regulatory evasion as a structural scam feature. Third, social media amplification was a core distribution mechanism in all three cases. Lavida Coin spread through Instagram and Facebook, Harapan Coin through political networks, and JJPTR through referral-based recruitment. This confirms the Federal Trade Commission's (2022) finding that social platforms are the primary vector for investment scam reach. The SDQC's External Validation and Source Verification dimensions are specifically designed to interrupt these amplification pathways by directing evaluation to neutral, platform-independent information sources. Taken together, these recurring patterns support the usefulness of the SDQC as a structured screening framework capable of identifying multiple, interacting legitimacy failures before investment commitment occurs.

Table 1. **Scam Case Summary, SDQC Checkpoint Analysis, and Primary Manipulation Tactic**

| No. | Case | Year | Main Claims | Red Flags (Per SDQC) | SDQC Dimensions Failed | Primary Manipulation Tactic |
|---|---|---|---|---|---|---|
| 1 | Lavida Coin | 2018 | High returns linked to TV station acquisition; promoted by celebrity Dato' Seri Vida | No whitepaper; unverifiable team; no regulatory filing | Source Verification, Offering Clarity, Credibility Assessment | Authority bias exploitation via celebrity endorsement |
| 2 | Harapan Coin | 2018 | Malaysia's first political fundraising coin tied to opposition coalition | No token economics; no regulatory approval; absent from independent platforms | Regulatory Disclosure, Credibility Assessment, External Validation | Symbolic trust via political identity alignment |
| 3 | JJPTR | 2017 | 20% monthly returns via financial education platform; operated as Ponzi scheme | Unrealistic returns; no transparency; no risk disclosures; referral pressure | Timing Awareness, Disclosure and Regulation, Credibility Assessment | Return-driven manipulation with educational legitimacy veneer |

**Journal of Information Systems Engineering and Management**
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

## 6. DISCUSSION AND IMPLICATIONS

The findings of this study carry differentiated implications for four stakeholder groups: individual gig workers and investors, digital platforms, regulatory bodies, and the research community. The following subsections address each in turn, with recommendations linked to the SDQC framework and supporting literature.

### *6.1 Implications for Gig Workers and Individual Investors*

For individual digital workers, the SDQC provides a structured cognitive aid that can be applied at the point of investment evaluation without requiring technical expertise or institutional support. Mohd Padil et al. (2022) demonstrate that practical, habit-based financial literacy significantly improves scam awareness among Malaysian students; the SDQC operationalises this finding by providing a specific behavioural routine of six sequential evaluative questions that can be applied consistently across diverse investment contexts. Kasim et al. (2024) further confirm that among retirees, financial literacy is the most reliable predictor of scam awareness, reinforcing the value of structured learning tools. The SDQC is most effective when users treat Timing Awareness as a metacognitive trigger: the experience of urgency itself should prompt activation of the remaining five dimensions rather than accelerated decision-making.

Ahmad and Lang (2025) establish that even financially literate individuals are vulnerable when bias-induced gullibility is activated, suggesting that periodic self-evaluation of one's cognitive state is as important as evaluating the investment itself. This is particularly true in high-pressure or emotionally charged investment contexts. The SDQC is best understood not as a pass-or-fail checklist, but as a structured pause mechanism that introduces deliberative distance between emotional response and financial commitment.

### *6.2 Implications for Digital Platforms*

For platforms hosting gig workers and financial content, including social media platforms, freelancing marketplaces, and messaging applications, the SDQC dimensions offer a framework for developing embedded scam warning systems. The Federal Trade Commission (2022) documents that investment scams are the dominant category of social media fraud by financial value, establishing a clear case for platform-level intervention. Wilson et al. (2024) argue that reporting tools must be integrated directly into the platforms where scams occur, rather than requiring victims to navigate external reporting channels. Platforms may incorporate SDQC-derived warning prompts within investment discussion spaces, promotional content, and payment confirmation flows in order to encourage source verification, credibility assessment, and disclosure scrutiny before user engagement. Chadalapaka et al. (2022) and Ma et al. (2025) demonstrate that AI-based detection tools can flag pump-and-dump activity and psychological manipulation techniques in real time, suggesting that platform-level SDQC integration could be automated for high-risk content categories.

### *6.3 Implications for Regulators*

For regulatory bodies including Malaysia's Securities Commission, Bank Negara Malaysia, and the National Scam Response Centre (NSRC), this study's findings reinforce the case for proactive public education campaigns tied to specific, evaluable risk dimensions rather than general fraud awareness messaging. Trozze et al. (2022) establish that regulatory gaps are structural enablers of ICO fraud, and that jurisdictional coordination is essential for effective enforcement. Wilson et al. (2024) document low awareness of existing reporting channels among Malaysian gig workers, suggesting that the SDQC's Disclosure and Regulation dimension could be anchored to specific regulatory reference points such as the Securities Commission's Investor Alert List, making regulatory resources directly actionable within the screening process. Regulators may also consider incorporating SDQC-informed guidance into financial literacy provisions associated with registered freelancing platforms, thereby extending scam prevention outreach beyond conventional awareness campaigns.

### *6.4 Implications for Researchers*

For the research community, this study contributes to a nascent literature on user-level decision support for fraud prevention in digital labour markets. The SDQC framework is positioned as a conceptual model requiring empirical validation, and its development identifies several productive research directions. Future studies could test the SDQC's

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

discriminant validity by examining whether investments that pass more SDQC dimensions exhibit lower rates of fraud, and whether SDQC training reduces victimisation rates in controlled or quasi-experimental settings. Zarifis and Castro (2024) and Proofpoint (2024) document the extension of investment fraud into NFT markets and gig economy recruitment contexts, suggesting that future iterations of the SDQC may require domain-specific calibration. Comparative studies across Malaysia, Indonesia, the Philippines, and other Southeast Asian digital labour markets would establish whether the framework's risk dimensions generalise across regulatory and cultural contexts.

## 7. LIMITATIONS AND FUTURE RESEARCH

### *7.1 Limitations*

This study has several limitations that constrain the scope of its claims and underscore the need for future empirical work. First, the SDQC framework is conceptual in nature: it is derived from literature synthesis and illustrated through case analysis rather than validated through empirical data on user behaviour or investment outcomes. The framework's effectiveness in reducing scam victimisation among gig workers has not been tested, and it is possible that real-world application introduces usability barriers or cognitive biases not anticipated in the conceptual development process. Second, the case selection is illustrative rather than exhaustive. The three Malaysian cases of Lavida Coin, Harapan Coin, and JJPTR were selected to represent variation in manipulation strategy, but they do not constitute a representative sample of Malaysian investment scams, and the analytical insights drawn from them may not generalise to all scam typologies. Third, the study's findings are contextualised within Malaysia's specific regulatory, cultural, and digital economy environment. The applicability of the SDQC framework to other national contexts, particularly those with different regulatory frameworks, digital literacy profiles, or gig economy structures, requires separate investigation. Fourth, the literature synthesis reflects the state of available published evidence through 2025 and may not capture more recent developments in scam tactics, regulatory responses, or detection technologies.

### *7.2 Future Research Directions*

Several productive directions for future research emerge from this study. The most immediate priority is empirical validation of the SDQC framework: experimental or quasi-experimental studies testing whether SDQC training reduces scam engagement rates among gig workers would provide direct evidence of its protective efficacy and identify dimensions requiring refinement. Survey-based research could additionally examine which SDQC dimensions are most salient across different demographic profiles, including age, education level, and digital literacy, enabling framework calibration for specific population subgroups. Future research could extend the SDQC to emerging fraud environments: Zarifis and Castro (2024) document the replication of investment scam dynamics in NFT markets, while Proofpoint (2024) identifies DeFi recruitment scams as a growing threat in gig economy contexts. Domain-specific SDQC extensions may be required to address the distinctive legitimacy signals and vulnerability patterns in these emerging spaces. Comparative cross-national studies examining SDQC applicability across Southeast Asian digital labour markets, particularly Indonesia, the Philippines, Thailand, and Vietnam, would establish the framework's generalisability and identify context-specific adaptations. Finally, platform-level implementation studies examining how embedding SDQC-derived warning prompts within social media or freelancing platforms affects user behaviour would provide evidence on the most scalable deployment pathway for the framework.

## 8. CONCLUSION

This study addresses a significant gap in the scam prevention literature by reconceptualising digital investment scam vulnerability as a user-level decision support problem and by developing the Scam Detection Quick-Check (SDQC) as a structured screening framework for Malaysian gig workers. It makes three contributions. First, it reframes scam susceptibility as a structured evaluative challenge rather than merely a financial literacy deficit. Second, it develops the SDQC from a theoretically grounded synthesis of behavioural, regulatory, and informational risk dimensions. Third, it extends scam prevention research into the underexplored intersection of gig economy labour, financial literacy, and digital fraud in the Malaysian context. Through three illustrative Malaysian cases, the study shows how the framework can identify multiple legitimacy failures across different scam architectures.

The SDQC framework responds to a structural mismatch between the complexity of contemporary digital investment scams and the limited decision-making resources available to many gig economy workers at the point of financial choice. Regulatory enforcement, platform safeguards, and technical detection systems remain important, but they often operate at scales or timelines that do not directly protect individuals during the moment of evaluation. The SDQC is intended to address that gap by offering a theory-informed, portable screening framework that helps users ask structured legitimacy questions before financial commitment occurs. Future research should test the framework empirically across different user groups and emerging fraud contexts, including DeFi, NFT, and recruitment-linked investment scams.

## REFRENCES

[1] Ahmad, Z., & Lang, J. (2025). Investment scams: The effect of bias-induced gullibility on victimization propensity. Crime, Law and Social Change, 83, Article 17. https://doi.org/10.1007/s10611-024-10187-1
[2] Bartoletti, M., Carta, S., Pompianu, L., & Serra, M. (2024). Crypto-cognitive exploitation: Integrating cognitive, social, and responsibility issues on cryptocurrency scams. Journal of Behavioral and Experimental Finance, 35, 100762. https://doi.org/10.1016/j.jbef.2024.100762
[3] Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., & Serusi, S. (2021). Cryptocurrency scams: Analysis and perspectives. IEEE Access, 9, 148353-148373. https://doi.org/10.1109/ACCESS.2021.3123894
[4] Chadalapaka, V., Chang, K., Mahajan, G., & Vasil, A. (2022). Crypto pump and dump detection via deep learning techniques. arXiv. https://arxiv.org/abs/2205.04646
[5] Federal Trade Commission. (2022). Social media: A gold mine for scammers in 2021. FTC Consumer Protection Data Spotlight. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/01/social-media-gold-mine-scammers-2021
[6] Hamid, R. A., Musa, R., Majid, M., & Salleh, M. N. M. (2024). Adapting to the gig economy: Determinants of financial resilience among Giggers. Journal of Retailing and Consumer Services, 77, 103671. https://doi.org/10.1016/j.jretconser.2024.103671
[7] Kasim, E. S., Awalludin, N. R., Zainal, N., Ismail, A., & Ahmad Shukri, N. H. (2024). The effect of financial literacy, financial behaviour and financial stress on awareness of investment scams among retirees. Journal of Financial Crime, 31(3), 652-666. https://doi.org/10.1108/JFC-04-2023-0080
[8] Ma, S., Ma, T., Liu, J., Song, W., Liang, Z., Xiao, X., & Ye, Y. (2025). PsyScam: A benchmark for psychological techniques in real-world scams. arXiv. https://arxiv.org/abs/2505.15017
[9] Mackenzie, S. (2022). Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial. The British Journal of Criminology, 62(6), 1537-1552. https://doi.org/10.1093/bjc/azab118
[10] Mohd Padil, H., Kasim, E. S., Muda, S., Ismail, N., & Md Zin, N. (2022). Financial literacy and awareness of investment scams among university students. Journal of Financial Crime, 29(1), 355-367. https://doi.org/10.1108/JFC-01-2021-0012
[11] Pavone, F., & Rossi, G. (2025). Afraid of the unknown: Crypto literacy and fear of online fraud. Finance Research Letters, 49, 103981. https://doi.org/10.1016/j.frl.2024.103981
[12] Proofpoint Threat Insight Team. (2024, October). Pig butchers join the gig economy: Cryptocurrency scammers target job-seekers. Proofpoint Threat Insight. https://www.proofpoint.com/us/blog/threat-insight/pig-butchers-join-gig-economy-cryptocurrency-scammers-target-job-seekers
[13] Sinha, A. R., Goyal, N., Dhamnani, S., Asija, T., Dubey, R. K., & Theocharous, G. (2022). Personalized detection of cognitive biases in user actions. arXiv. https://arxiv.org/abs/2206.15129
[14] Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. Crime Science, 11(1), 1. https://doi.org/10.1186/s40163-021-00163-8
[15] Wilson, S., Hassan, N. A., Khor, K. K., Sinnappan, S., Abu Bakar, A. R., & Tan, S. A. (2024). A holistic qualitative exploration on the perception of scams, scam techniques and effectiveness of anti-scam campaigns in Malaysia. Journal of Financial Crime, 31(5), 1140-1155. https://doi.org/10.1108/JFC-06-2023-0151
[16] Wired Staff. (2022, June). Pig butchering scams are now a $3 billion threat. Wired. https://www.wired.com/story/pig-butchering-fbi-ic3-2022-report

[17] Zarifis, A., & Castro, M. (2024). The dark side of non-fungible tokens: Understanding risks in the NFT market. Journal of Financial Innovation, 10, Article 684. https://doi.org/10.1186/s40854-024-00684-6
[18] Zhang, M., Nazir, M. S., Farooqi, R., & Ishfaq, M. (2022). Moderating role of information asymmetry between cognitive biases and investment decisions: A mediating effect of risk perception. Frontiers in Psychology, 13, 828956. https://doi.org/10.3389/fpsyg.2022.828956
[19] Bank Negara Malaysia. (n.d.). JJ Poor To Rich (JJPTR) - Consumer Alert. Financial Consumer Alert List, Bank Negara Malaysia. https://www.bnm.gov.my/financial-consumer-alert?p_p_id=fca_WAR_fcaportlet&p_p_lifecycle=0&_fca_WAR_fcaportlet_name=JJPTR
[20] Bernama. (2019, January 12). Legality of cryptocurrency still under consideration - Khalid Samad. Bernama. https://www.bernama.com/en/general/news.php?id=1693347
[21] Securities Commission Malaysia. (2018, September 5). SC issues notice to cease all activities promoting Lavidacoin. Securities Commission Malaysia. https://www.sc.com.my/resources/media/media-release/sc-issues-notice-to-cease-all-activities-promoting-lavidacoin