Linguistic Strategies in Investment Fraud: A Case Study of Language Structuring in Cryptocurrency Investment Website

Wan Farah Wani Wan Fakhruddin[1]*, Wan Nur Asyura Wan Adnan[1], Yasmin Hanafi Zaid[2], Farhana Abu Bakar[2]

[1]Faculty of Social Sciences and Humanities Kuala Lumpur, Universiti Teknologi Malaysia, 54100 Kuala Lumpur, Malaysia

[2]Language Academy, Faculty of Social Sciences and Humanities Kuala Lumpur, Universiti Teknologi Malaysia, 81310, Johor Bahru, Malaysia

DOI: https://doi.org/10.47772/IJRISS.2026.10100079

Received: 30 December 2025; Accepted: 05 January 2026; Published: 22 January 2026

ABSTRACT

In the era of digital finance, cryptocurrency investment fraud has become increasingly prevalent and has significantly affected societal well-being. Although various cybersecurity systems and legal frameworks have been established, there is still a lack of studies examining how language is strategically used to deceive victims. Cryptocurrency investment fraud in Malaysia has grown alongside increasing public interest in digital assets. This phenomenon displays consistent linguistic and semiotic patterns that construct false credibility, normalise risk, and prompt immediate action through the "compression" of space–time–value, as described in the proximisation framework. This study analyses fraudulent landing pages and fake support channels using a multimodal discourse approach to identify strategies used to manipulate victims. In addition to contextualising fraudulent discourse, the study incorporates developments in blockchain-based detection science and social media analytics to develop data-driven educational, policy, and enforcement implications, including dynamic early-warning systems, blockchain-based federated learning, and transparent transaction forensics. The findings are expected to contribute to public literacy, the design of preventive interventions, and more effective legal action against cryptocurrency fraud.

Keywords: cryptocurrency investment, critical discourse analysis, SDG 16, SDG 4, language manipulation

INTRODUCTION

The rise of cryptocurrency as a retail investment has transformed how the public evaluates risk and return. Cryptocurrency value is now frequently shaped by sociotechnical imaginaries disseminated through video platforms and online communities, rendering promotional language and visual cues central drivers of engagement (Keere et al., 2025). Alongside the digitalisation of finance and the diversification of financial products, users are increasingly exposed to high-risk marketing communications. This situation not only expands the scope of user interaction with risky content but also heightens vulnerability to fraud, including exposure to fraudulent investment promotions distributed via email and websites. Notably, studies indicate that higher levels of financial literacy may increase exposure to such content without necessarily reducing the likelihood of victimisation (Rey-Ares et al., 2024).

In the Malaysian context, efforts to strengthen financial institutions through internal regulatory enforcement digital forensics applications, and corporate policy implementation have proven effective in curbing fraud. Nevertheless, the linguistic strategies employed by scammers remain effective where levels of digital discourse literacy among users remain low and behavioural biases are not systematically addressed through education (Mohammed et al., 2023). Consequently, a more comprehensive response is required—one that extends beyond "technical mitigation" towards "discursive deconstruction". This approach is significant because scammers frequently appropriate normative and cognitive legitimacy through the use of institutional logos, expert-style language, and rapid success narratives, thereby exploiting victims' inclination towards immediate gains

(Almahendra et al., 2024).

Cryptocurrencies have garnered widespread attention among Malaysians across age groups, whether as speculative high-risk instruments or as emerging payment infrastructures and digital assets. However, the openness of this ecosystem is also exploited by fraudulent actors who capitalise on relative anonymity, transaction speed, and regulatory ambiguity (Abulaish & Dalal, 2024). Within this landscape, fraudulent cryptocurrency investment websites operate as quasi-organisations, mimicking legitimate institutional forms and language while leveraging "financial expert" narratives, testimonials, and promises of high returns to target novice investors with limited awareness of information legitimacy. This situation poses significant challenges in evaluating and distinguishing genuinely trustworthy sources (Bartoletti et al., 2021; Hadan et al., 2023).

Accordingly, this study examines how linguistic manipulation and visual symbolism are deployed synergistically to construct false credibility and prompt immediate decision-making among victims, as articulated in strategies identified by Ye and Chen (2022). The primary objectives are to identify dominant linguistic and semiotic strategies, assess their effects on target perceptions and actions, and propose educational and enforcement recommendations that account for advances in dynamic detection methods and blockchain forensics (Wu et al., 2024; Xu et al., 2024).

LITERATURE REVIEW

Previous studies indicate that fraudulent discourse is typically structured to mimic legitimate institutional features and to fabricate communities of interest. Within the proximisation framework, spatial proximisation is used to "bring closer" target identities to authoritative symbols, temporal proximisation creates urgency, and value proximisation borrows moral legitimacy. Together, these dimensions synergistically increase individuals' propensity to accept risk without critical scrutiny (Ye & Chen, 2022). From a psychological perspective, time pressure has been shown to heighten susceptibility to fraud, particularly when narratives are framed in terms of loss avoidance rather than gain seeking, underscoring the importance of mitigating temporal effects in educational interventions (Lyu et al., 2025).

Cryptocurrency-based fraud also exploits social momentum and influencer effects, with platforms such as X and Telegram facilitating pump-and-dump phenomena. These strategies reinforce false social proof in real time and trigger significant price reactions, sustaining an illusion of legitimacy among targets (Mirtaheri et al., 2019; Cary, 2021). From a systemic perspective, cryptocurrency fraud is increasingly conceptualised as a form of "network scam" operating across multiple channels and platforms, necessitating prevention efforts that trace overlapping reputation networks, communities, and promotional infrastructures (Swartz, 2022).

METHODOLOGY

This study adopts a qualitative case study design focusing on a fraudulent cryptocurrency investment website written in Malay and targeting Malaysian users. The analysed data comprise the homepage, "About Us" section, investment package offers, written testimonials, and captions embedded within visual elements such as logos and certificates. All materials were archived and transcribed to ensure that textual content embedded in images was incorporated into the analytical corpus.

Data were collected through systematic observation of fraudulent cryptocurrency investment landing pages and fake support channels operating in Malaysia between 2023 and 2025. Sources included screenshots, archived web pages, and interaction transcripts, analysed to capture synchronisation between promotional channels and "customer service" channels that are typically combined to reinforce fraudulent narratives (Swartz, 2022).

Multimodal discourse analysis was employed to examine the interaction between linguistic and semiotic dimensions shaping psychological effects on targets. Linguistic dimensions included urgency lexicon, authority claims, social-proof narratives, and risk–reward framing, while semiotic dimensions encompassed corporate typography, colour palettes, security icons, and return visualisations (Ye & Chen, 2022). The proximisation framework was subsequently applied to trace compression across three aspects: space (achieved through institutional mimicry and community construction), time (manifested through opportunity windows,

countdowns, and guarantees of rapid returns), and value (expressed through alignment with financial aspirations and cultural norms). Collectively, these elements form pathways of compliance without critical scrutiny, highlighting how discourse and visual symbols jointly influence decision-making processes (Ye & Chen, 2022; Lyu et al., 2025).

From a technical perspective, mapping these discursive features to indicators within cryptocurrency transaction networks was considered as support for dynamic early-warning system design. This educational linkage aligns with advances in temporal graph modelling and disentangled learning that enable clearer differentiation between fraudulent patterns and legitimate transactions (Kang & Buu, 2024; Xu et al., 2024; Nam et al., 2025).

RESULTS

The study identifies five principal strategies consistently employed across fraudulent cryptocurrency investment websites. Table 1 summarises these strategies, their functions, and implementation examples. Collectively, these strategies operate synergistically to construct false credibility, exert decision pressure, and influence target actions.

Table 1. Dominant Strategies Used in Cryptocurrency Investment Fraud

Strategy	**Function**	**Example of Implementation**
Urgency language	Reduces deliberation time and increases susceptibility	Phrases such as "*register now*", "*limited offer*"
Authority claims	Creates immediate credibility through references to false experts or entities	"*Financial experts*", celebrity endorsements, institutional rhetoric
Social proof	Reinforces trust through testimonials and community interaction	"*Active users*" counters, chat groups, social media reinforcement
Professional visual semiotics	Constructs institutional atmosphere and signals technical stability	Corporate logos, security badges, return graphs
Temporal compression	Forces rapid action before due diligence	Promises such as "*20% daily*", "*double your capital in a week*"

As shown in Table 1, the integration of discursive and semiotic strategies creates a cohesive persuasion chain, in which time pressure, visual and authoritative credibility, and social proof interact synergistically to trigger impulsive action. Consistent use across multiple channels, including landing pages, social media, and messaging applications, reinforces the "network scam" structure and normalises false credibility through repeated exposure.

Urgency language functions as a cognitive lever that systematically reduces critical thinking time, particularly when offers are framed as loss avoidance rather than immediate gain (Lyu et al., 2025). Authority is established through references to "financial experts", celebrities, or fictitious compliance entities, imitating the rhetoric and appearance of formal organisations to generate immediate trust and shorten verification processes (Ye & Chen, 2022). Social proof is maintained through testimonials, "active user" counters, and chat communities reinforced via social media, exploiting herding and real-time hype phenomena (Mirtaheri et al., 2019; Cary, 2021). Professional visual semiotics, such as corporate logos, security badges, audit statements, and return visualisations, create an institutional atmosphere that reduces scepticism (Bartoletti et al., 2021). Finally, temporal compression strategies lock in investor decisions before due diligence can occur, aligning with temporal proximisation mechanisms (Ye & Chen, 2022).

DISCUSSIONS

The effectiveness of linguistic and semiotic strategies in cryptocurrency investment fraud largely stems from the

interaction between discursive proximisation and cognitive biases among novice investors. Urgency-based language and temporal compression exploit situational pressure to reduce deliberation time, while authority claims and professional visual semiotics generate false credibility that accelerates uncritical information acceptance. Social proof strategies capitalise on herding and real-time hype, reinforcing legitimacy perceptions and creating psychological pressure to act (Hadan et al., 2023; Lyu et al., 2025).

Within the cryptocurrency ecosystem, fraudulent discourse establishes feedback loops whereby victim actions indirectly signal legitimacy. This pattern is particularly evident in pump-and-dump dynamics and influencer-driven responses, illustrating how linguistic and symbolic manipulation operates not only at the individual level but also stabilises collective market illusions (Mirtaheri et al., 2019; Cary, 2021).

From an enforcement and educational perspective, gaps in taxonomy, inconsistent reporting, and the absence of mandatory disclosure hinder effective systemic monitoring, despite blockchain transparency theoretically enabling robust asset flow forensics (Bartoletti et al., 2021; Cole, 2023; Wu et al., 2024). Integrating discourse analysis with dynamic early-warning systems, disentangled learning, and temporal mapping holds potential to strengthen early identification of high-risk entities and bridge the gap between discourse literacy and technical protection (Kang & Buu, 2024; Xu et al., 2024; Yang et al., 2024; Zhang et al., 2024; Ghosh et al., 2025; Nam et al., 2025).

CONCLUSION

This study examined dominant linguistic and semiotic strategies in cryptocurrency investment fraud, assessed their implications for target perceptions and actions, and proposed educational and enforcement recommendations informed by advances in dynamic detection and blockchain forensics. The findings confirm five core strategies; urgency language, authority claims, social proof, professional visual semiotics, and temporal compression which are used synergistically to accelerate action, constrain critical deliberation, and construct false credibility through spatial, temporal, and value proximisation (Ye & Chen, 2022; Lyu et al., 2025).

This study highlights that discursive strategies affect individuals and shape “network scam” structures operating across multiple channels, normalising impulsive behaviour through repeated exposure. Recommendations include strengthening public discourse literacy education, enhancing dynamic early-warning detection infrastructures, and developing standardised taxonomies, mandatory reporting, and cross-institutional data-sharing mechanisms. Together, coordinated literacy education, detection technologies, and enforcement policies provide a holistic response to cryptocurrency fraud, aligned with the complex, cross-channel nature of network scams (Cong et al., 2025).

ACKNOWLEDGEMENT

This study was funded by Universiti Teknologi Malaysia under the New Researcher Grant (Potential Academic Staff – PAS) (Q.K130000.2753.03K70).

REFERENCES

1. Acharya, B., Saad, M., Cinà, A. E., Schönherr, L., Nguyen, H. D., Oest, A., Vadrevu, P., & Holz, T. (2024). Conning the Crypto Conman: End-to-End Analysis of Cryptocurrency-based Technical Support Scams. 2024 IEEE Symposium on Security and Privacy SP, 17-35. https://doi.org/10.1109/SP54263.2024.00156
2. Almahendra, R., Viyani, A. O., & Nabawi, M. (2024). Is crypto legitimate? Study on the relationship between legitimacy and public engagement on crypto market in Indonesia. Intangible Capital. https://doi.org/10.3926/ic.2425
3. Barnett, M., Vleet, S. V., Griffin, R., Fontanese, M., Mallender, W., Boynton, H., & Coldiron, A. (2024). Vesta: a groundbreaking tool for enhancing financial literacy and scam resilience among older adults. Innovation in Aging, 8, 1108-1108. https://doi.org/10.1093/geroni/igae098.3559
4. 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

5. Cong, L. W., Harvey, C. R., Rabetti, D., & Wu, Z. (2025). An Anatomy of Crypto-Enabled Cybercrimes. Management Science, 71, 3622-3633. https://doi.org/10.1287/mnsc.2023.03691
6. Keere, K. D., Trans, M., & Milan, S. (2025). The value of crypto? Sociotechnical imaginaries on cryptocurrency in YouTube content. Socio-Economic Review, 23(2), 759-785. https://doi.org/10.1093/ser/mwae081
7. Li, X., Yepuri, A., & Nikiforakis, N. (2023). Double and Nothing: Understanding and Detecting Cryptocurrency Giveaway Scams. Proceedings of 2023 Network and Distributed System Security Symposium. https://doi.org/10.14722/ndss.2023.24584
8. Mohammed, D., Asokan, K., & Arunasalam, K. (2023). Anti-fraud measures and corporate policies to combat financial fraud in the financial institutes of Malaysia. E3s Web of Conferences. https://doi.org/10.1051/e3sconf/202338909028
9. Mohammed, D., Asokan, K., & Arunasalam, K. (2023). Anti-fraud measures and corporate policies to combat financial fraud in the financial institutes of Malaysia. E3s Web of Conferences. https://doi.org/10.1051/e3sconf/202338909028
10. Phillips, R. C., & Wilder, H. (2020). Tracing Cryptocurrency Scams: Clustering Replicated Advance-Fee and Phishing Websites. 2020 IEEE International Conference on Blockchain and Cryptocurrency ICBC, 1-8. https://doi.org/10.1109/ICBC48266.2020.9169433
11. Rey-Ares, L., Fernández-López, S., & Álvarez-Espiño, M. (2024). The role of financial literacy in consumer financial fraud exposure (via email) and victimisation: evidence from Spain. International Journal of Bank Marketing. https://doi.org/10.1108/ijbm-03-2023-0169
12. Ridho, W. F. (2023). Unmasking online fake job group financial scams: a thematic examination of victim exploitation from perspective of financial behavior. Journal of Financial Crime. https://doi.org/10.1108/jfc-05-2023-0124
13. Wang, D., & Zou, T. (2024). Financial literacy, Cognitive bias, And personal investment decisions: A new perspective in behavioral finance. Environment and Social Psychology. https://doi.org/10.59429/esp.v9i11.3050
14. Ye, H., & Chen, K. (2022). A study on the discourse strategy of telecommunication fraud based on proximization theory. Discourse and Communication, 17, 155-173. https://doi.org/10.1177/17504813221129517