JOURNAL OF CULTURAL ANALYSIS AND SOCIAL CHANGE

Journal of Cultural Analysis and Social Change,
2026, 11(1), 2451-2460
ISSN: 2589-1316

Deconstructing Cryptocurrency Leading Room Fraud: A Multi-stage Crime Script Analysis and Topic Modeling Approach

Seoung Won Choi[1], Julak Lee[2*]

[1] *Department of Public Conflict Intelligence, Chung-Ang University, 84 Heukseok-ro, Dongjak-gu, Seoul, 06974, Republic of Korea, sw9338@cau.ac.kr*
[2] *Department of Industrial Security, Chung-Ang University, 84 Heukseok-ro, Dongjak-gu, Seoul, 06974, Republic of Korea, julaklee71@cau.ac.kr*

*__Corresponding Author:__ julaklee71@cau.ac.kr

Citation: Choi, S. W. & Lee, J. (2026). Deconstructing Cryptocurrency Leading Room Fraud: A Multi-stage Crime Script Analysis and Topic Modeling Approach, *Journal of Cultural Analysis and Social Change*, 11(1), 2451-2460. https://doi.org/10.64753/jcasc.v11i1.4376

Published: January 29, 2026

ABSTRACT

With the rise of cryptocurrency investments, leading room fraud has become a prevalent financial crime in South Korea. As this fraud increasingly exploits victims through sophisticated social engineering tactics, this study employed latent Dirichlet allocation topic modeling and crime script analysis to thoroughly examine the interaction between sociocultural factors and fraud patterns in Korea. The topic modeling revealed three main themes: organized operations and international fraud networks, cryptocurrency investment inducement strategies, and celebrity impersonation and online-based fraud. Crime script analysis revealed that the leading room fraud systematically unfolds through the following stages: foundation establishment, target enticement, trust consolidation & investment escalation, and completion of fund acquisition. Driven by role division, psychological manipulation, and information control, leading room fraud has become especially widespread in Korea, where the combination of a highly digital culture, Confucian social hierarchy, and short-term thinking creates a favorable environment for its growth. These findings provide valuable insights for both comparative research and the development of policy responses to leading room fraud.

Keywords: Cryptocurrency Leading Room Fraud, Cryptocurrency Investment Fraud, Criminal Psychology, Mixed-Methods Analysis, Korean Context

INTRODUCTION

In recent years, changes in the global economic environment have significantly impacted individual investment behavior; the continuous decline in interest rates, expansion of market liquidity, and recurring global economic crises have decisively shifted the focus of asset management from savings to investment (Jun & Joung, 2022). In particular, the election of Donald Trump in 2024 triggered a surge in the cryptocurrency market, and his pro-market policy stance further stimulated investor optimism (Krause, 2024).

While these macroeconomic shifts and the rapid growth of digital financial markets have brought positive changes like diversified investment methods and increased accessibility, they have also facilitated the evolution and spread of financial investment fraud (Park et al., 2011). The characteristics of online-based investment environments—for example, the anonymity of non-face-to-face transactions, a global reach that transcends borders, and the complexity of financial products—have created a crime ecosystem favorable to fraudsters, who are acquiring specialized knowledge of digital technologies to develop increasingly sophisticated scam techniques (Jung, 2024).

The scale of this problem is evident globally—according to a 2024 report by the Global Anti-Scam Alliance, financial fraud losses worldwide totaled USD 1.03 trillion in a single year, which is comparable to the GDP of some countries (Rogers, 2024). In Korea, investment fraud makes up approximately 73% of all cryptocurrency-related crimes, demonstrating that the digital investment system has fundamental weaknesses (Song & Lee, 2023).

Given this context, it becomes essential to investigate cryptocurrency leading room fraud in Korea. The term 'leading room' refers to online spaces where guidance on buying and selling investment assets like cryptocurrencies is provided, along with the sharing of high-value or insider information (Jun & Joung, 2022). The extensive internet connectivity and the confined messaging platforms in Korea create an ideal environment for the systematic spread of such fraudulent activities (Choi et al., 2024). Moreover, cryptocurrency's decentralized system, anonymity, and the ease of moving funds across borders have made it a global crime challenge that no single country can handle alone with its regulations or technology (Kethineni & Cao, 2020). Yet, there is still limited research on how specific fraud schemes are influenced by different legal, cultural, and technological settings. While existing research focuses primarily on fraud classification and general countermeasures, this study fills that gap by analyzing cryptocurrency leading room fraud in the Korean context to provide insights into how these crimes operate and can be prevented.

LITERATURE REVIEW

Leading Room Fraud in Korean Society

While traditional frauds typically focus on face-to-face contact, cryptocurrency leading room frauds use phone calls, texts, and social media via smartphones (Korean National Police Agency, 2025). In particular, KakaoTalk's virtual monopoly in the domestic messenger market (Statista, 2025) allows fraudsters to efficiently build trust with victims, provide information, and use psychological persuasion within a closed messenger platform.

In this regard, quasi-investment advisory businesses (QIABs), which hold financial business licenses unique to Korea, operate by providing investment information to an unspecified number of people through periodicals or various communication media (Jeong, 2024). Fundamentally distinct from traditional investment advisory services, which provide personalized consultations, QIABs are limited to the unidirectional provision of information to multiple unspecified recipients (Jeong, 2024). Because the Financial Investment Services and Capital Markets Act prohibits QIABs from exclusively providing investment information to multiple unspecified recipients or offering individual consultations with investors, operating leading rooms on social media platforms without proper registration is illegal (Financial Services Commission, 2024).

Information about stocks and cryptocurrencies provided through leading rooms often leads to crimes such as spreading false information, embezzling investments, manipulating market prices, and using non-public information, which undermines trust in the financial ecosystem as a whole (Korean National Police Agency, 2025). In response, the Korean National Police has intensified efforts to combat leading room fraud, leading to 7,232 investigated cases and 3,300 arrests since September 2023 (Korean National Police Agency, 2025). Nevertheless, these efforts remain insufficient due to investors' lack of capacity to identify illegal activities, difficulties in preventing cross-border leading room fraud, and the absence of proactive investor protection measures (Jeong, 2024).

Strategic Manipulation Mechanisms

Cryptocurrency investment-related crimes exploit vulnerabilities in both digital platforms and human psychology, with scammers working to establish their authority and trustworthiness (Siu & Hutchings, 2023). The effectiveness of fraud strategies depends on platform characteristics—the more anonymous and closed a messaging platform, the more conducive it becomes to fraudulent activity (Siu & Hutchings, 2023).

Victims face both technical vulnerabilities and psychological manipulation, including cognitive biases and social pressure (Park & Ryu, 2018; Financial Markets Authority, 2024). Prospect theory explains that people naturally fear losses more than they value equivalent gains (Kahneman & Tversky, 1979). Fraudsters employ Cialdini's (2001) influence principles—authority, social proof, scarcity, and reciprocity—through false expertise, fabricated success stories, artificial scarcity, and initial incentives to manipulate victims. Additionally, social engineering techniques such as overly attractive profit promises and repetitive messages emphasizing the stability of investments make victims believe that their investment decisions are safe (Muzammil et al., 2025).

These psychological tactics operate within group dynamics that amplify investment fraud. Asch's (1956) conformity experiments show that individuals conform to majority opinions despite contradictory facts—a pattern that confederates in leading rooms exploit to undermine victims' rational judgment. Janis (1972) identified groupthink in closed environments, while Bikhchandani et al. (1992) introduced information cascades, demonstrating how individuals follow others rather than rely on independent judgment. In leading rooms, early decisions by confederates trigger information cascades that sequentially influence subsequent investors, amplifying

false signals. When individual psychological vulnerabilities combine with group influence mechanisms, victims internalize fraudulent investment decisions as rational—a combination that explains the persistent power of leading room fraud.

Research Method

Data Collection

This study utilized BIGKinds to collect data on cryptocurrency leading room fraud in Korea. BIGKinds is a news article database operated by the Korea Press Foundation, which has been utilized by many studies for data collection and has the advantage of being highly reliable in terms of data quality (Na & Oh, 2024).

This study searched the site with the keywords "leading room fraud" combined with "cryptocurrency," "virtual currency," "virtual assets," "coin," and "bitcoin" and set the collection period to about three years (January 1, 2022, to December 31, 2024) to obtain 2,071 news articles. Duplicate values or values that were not related to the research topic were then removed from the raw data, and finally, 881 articles were used for latent Dirichlet allocation (LDA) topic modeling. In addition, this study incorporated court rulings and press releases for crime script analysis. Drawing on these additional sources made it possible to better capture the offenders' tactics, the flow of their interactions with victims, and the psychological undercurrents that influenced both sides.

Analytical Methodology

Cryptocurrency leading room fraud is a complex crime involving platform environments, linguistic persuasion, group psychology, and organized operational structures—all of which interact organically (Korean National Police Agency 2025). Moreover, each stage of cryptocurrency fraud is interconnected to form an overall fraud scenario, necessitating combined research methods for in-depth analysis (Jung & Noh, 2024; Madarie et al., 2024). Mixed-methods analysis enhances the overall rigor of research by combining the strengths of both quantitative and qualitative approaches, thereby improving internal consistency, generalizability, and overcoming the limitations of single-method designs (Hussein, 2009).

First, LDA views each document as a blend of topics and applies probabilistic modeling to uncover the hidden semantic structure within the text (Blair et al., 2020; Blei et al., 2003). It works on the assumption that a single document can touch on several topics at once, treating the entire dataset as a probabilistic mix, with each topic represented by a set of closely related keywords (Yu, 2017). Although LDA does not consider the order of documents (Shin, 2019), it can be used to derive consistent topics through hyperparameter tuning without prior domain knowledge (Egger & Yu, 2022), efficiently analyze large document data, and flexibly analyze text data from various sources (Choi & Shim, 2020).

The number of topics must be determined when performing LDA topic modeling (Yu, 2017). This study enabled meaning-based structural analysis beyond simple keyword frequency analysis by determining the optimal number of topics using coherence and perplexity indices. Furthermore, LDA topic modeling was performed on news article data to identify the main characteristics of cryptocurrency leading room fraud in Korea, as well as the components and proportions of each topic.

Next, crime script analysis is useful for understanding criminal activities as sequential and structured processes and investigating the strategic, psychological, and technical mechanisms involved in each stage (Cornish, 1994). By distilling complex data into structured frameworks, this approach allows researchers to better understand how each strategic move made by offenders influences the steps that follow (Brayley et al., 2011). In addition, continuous collection and analysis of the latest data enables updates to crime scripts, laying the foundation for future expansion and deepening of related research areas (Beauregard et al., 2010). This study used this approach to identify the step-by-step procedures and division of roles involved in the execution of crimes and to understand the strategies used by fraudsters to persuade and control their victims. Following the conventional three-stage crime script framework of pre-crime, crime occurrence, and post-crime phases (Beauregard & Leclerc, 2007; Hutchings & Holt, 2015), this study encompassed all these phases while providing a more detailed analysis by subdividing the process into four distinct stages.

RESULTS

LDA Topic Modeling

As shown in Figure 1, the coherence score peaks when the number of topics is set to three, while the perplexity score decreases steadily up to three topics, temporarily increases at four topics, and then decreases again. Taking both metrics into account, the number of topics for LDA topic modeling was set to three. The results are presented in Table 1.

Topic 1 (40.4%), *Organized Operations and International Fraud Networks*, is dominated by keywords such as "fraud," "investment," "organization," "leading room," "mastermind," and "overseas," which appear with high co-occurrence frequency. These results suggest that cryptocurrency leading room fraud operates through organized structures and transnational networks rather than as isolated acts by individuals. Criminal groups are typically divided into specialized units—a mastermind and operations and consultation teams—with overseas actors often tasked with laundering illicit funds.

Topic 2 (30.9%), *Cryptocurrency Investment Inducement Strategies*, shows that terms tied to digital asset trading—"coin," "listing," "exchange," "item," and "market price" —frequently co-occur with persuasive language like "recommendation" and "suggestion." These patterns reveal how scammers combine trading terminology with psychological manipulation, using unverifiable or false information to entice investors. For instance, fraudsters use phrases such as "guaranteed high returns" and "privileged information on upcoming listings" to compromise rational judgment.

Topic 3 (28.7%), *Celebrity Impersonation and Online-based Fraud*, reveals that fraudsters engage in "celebrity" "impersonation" by fabricating endorsements and using celebrity images on "online," "platforms" like YouTube and Facebook. By distributing targeted advertisements and utilizing phishing or spam techniques, they expand their reach and create a convincing, yet deceptive, sense of credibility.

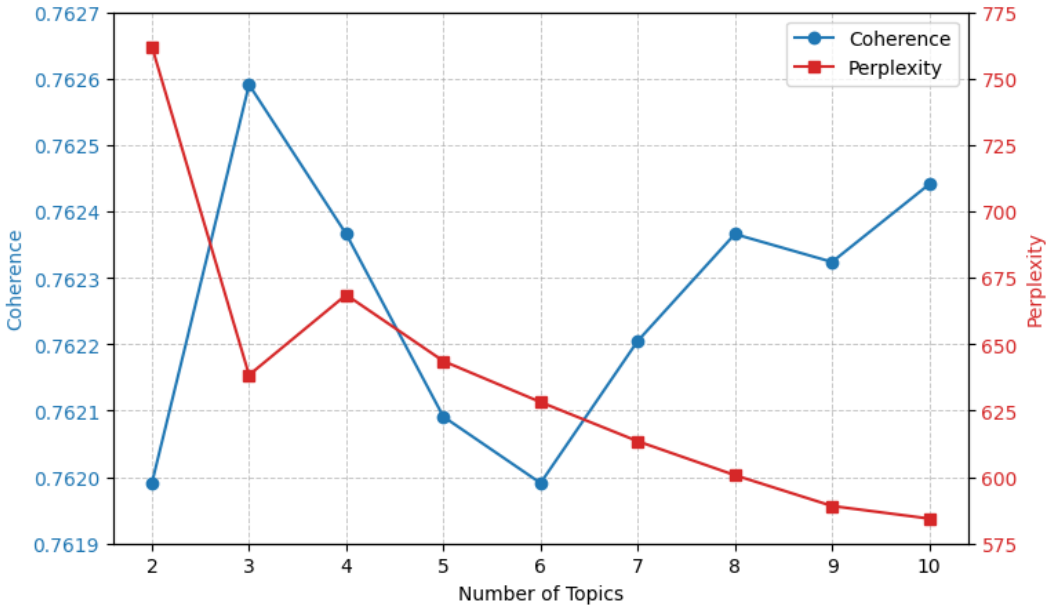

Figure 1. Topic model evaluation metrics

Table 1. LDA topic modeling results

Topic	Document Ratio	Relevant Terms
1	40.4%	fraud, investment, organization, leading room, profit, crime, operation, site, mastermind, member, overseas, gang, gambling, method, company, account, SNS (social network service), consultation, money laundering, cash
2	30.9%	investment, leading room, coin, fraud, asset, listing, exchange, finance, item, company, information, profit, case, recommendation, purchase, method, strategy, price, market price, suggestion
3	28.7%	fraud, impersonation, advertisement, investment, leading room, celebrity, online, platform, information, account, finance, message, phishing, SNS, entertainer, spam, Facebook, photo, YouTube, messenger

Crime Script Analysis

This study used crime script analysis to examine how cryptocurrency leading room fraud occurs in Korea. The results show that this type of scam follows a pyramid-shaped structure with four main stages: "foundation establishment," "target enticement," "trust consolidation & investment escalation," and "completion of fund acquisition" (Figure 2). The main characteristics and strategies for each phase are detailed below.

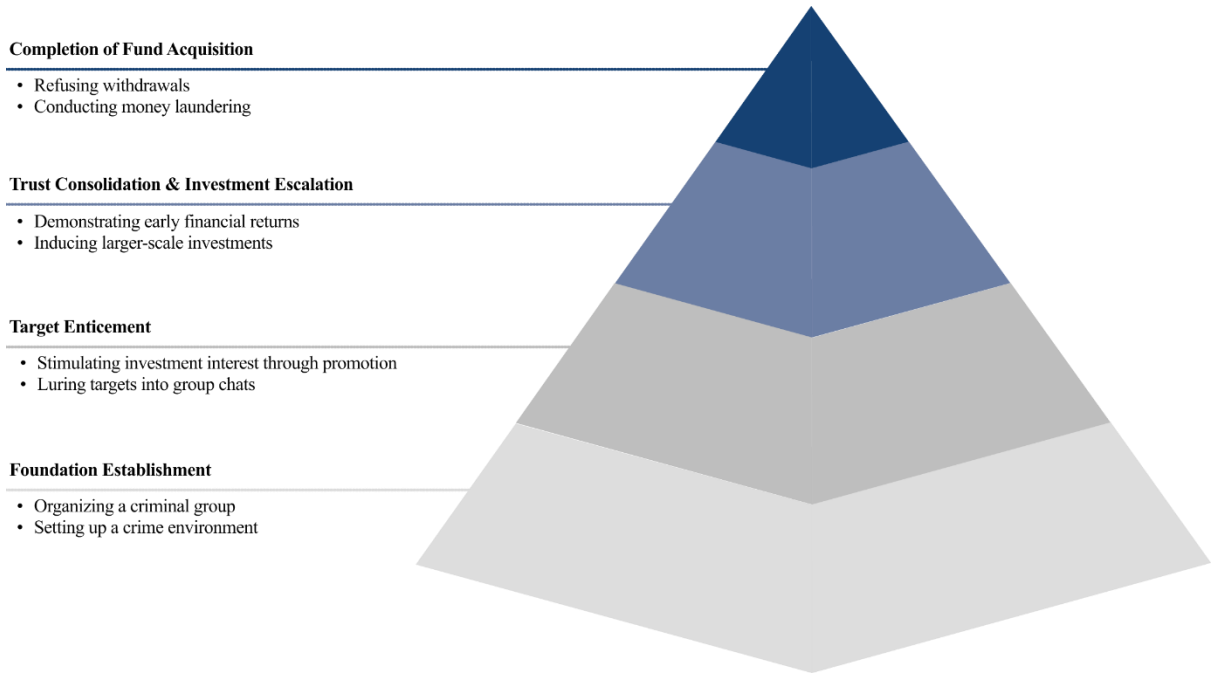

Figure 2. Cryptocurrency leading room fraud pyramid

Foundation Establishment

Cryptocurrency leading room fraud organizations meticulously design their strategic foundations before executing their plans. The organization is structured with an overseas-based chief overseeing strategic decisions and profit distribution, while promotional, operational, and financial teams each perform their respective roles beneath them. Cryptocurrency issuance and price manipulation teams are added as needed. This transnational structure is designed to make tracking difficult for investigative authorities.

The PR team disseminates provocative messages like “guaranteed daily high returns” or “VIP information provided” on YouTube and social media. Simultaneously, they build public trust through fake likes and comments. The operations team consists of leaders and followers. Leaders pose as investment experts or celebrities to establish authority, while followers emphasize stable returns and investment certainty according to pre-written scripts. They create intense peer pressure within the group, weakening victims' critical thinking and driving aggressive investment decisions.

The funds team obstructs investigative tracking by establishing multiple accounts and complex transaction routes. They subsequently deliver the liquidated funds to the mastermind. The cryptocurrency issuance team develops fake digital coins and creates white papers through shell companies to grant superficial legitimacy. They proceed through brokers to list on overseas exchanges. The market manipulation team artificially fluctuates prices overseas to stimulate victims' investment psychology.

Criminal organizations leverage cutting-edge technology to build an environment optimized for deceiving people. They produce impersonation videos of celebrities using deepfake or voice cloning technology. In Korean society, image theft of celebrities or securities experts is prevalent, and they strategically exploit the social culture that trusts experts. A multi-layered fraud infrastructure composed of fake social media accounts, forged documents, and fraudulent exchange platforms underpins the survivability and longevity of these crimes.

These organizations are designed with a modular structure, so each member handles only a part of the criminal activity. Even if one person is arrested, the impact on overall operations is minimal. The upper-level decision-making structure remains intact, and personnel are replaced as needed to continue operations. This structural resilience acts as a key factor reinforcing the complexity and persistence of modern cyber financial crime.

Target Enticement

Fraudsters place provocative advertisements on popular platforms such as SNS, YouTube, and Facebook while simultaneously sending bait messages via phone calls, texts, or SNS promising free investment information. These ads include links to group chat rooms and contact details, prompting potential targets to act immediately. They also inflate engagement with fake likes and comments to create an artificial sense of popularity, drawing in unsuspecting victims.

To deepen initial interest and weaken potential victims’ defenses, scammers deploy sophisticated social engineering tactics. They bolster trust by impersonating famous investors, celebrities, or influencers through deepfake videos or voice cloning to recommend investments. Alternatively, they form romantic attachments via

dating apps or one-on-one chat platforms, then propose "investing together" at a specific moment to break down the victim's defenses. By designing systems to let emotional trust override economic logic or rational judgment, scammers prompt targets to voluntarily enter the group chat (e.g., KakaoTalk Open Chats or Naver Band) guided by the scammer, believing it to be a genuine investment community.

Internally, roles and scenarios are meticulously organized, with a small number of administrators using multi-login programs or bot systems to simulate far more participants than actually exist. This organized interaction generates intense peer pressure and psychological anxiety about non-participation leading to financial loss, causing victims to ultimately decide to transfer funds or make additional investments within a false sense of certainty.

Trust Consolidation & Investment Escalation

Having placed targets in a state of expert dependency in the previous stage, criminal organizations now reinforce trust through fabricated profits. By directly controlling the exchanges and manipulating transaction records, they make profits appear on the victim's screen as if they have been generated. Though entirely false, these fabricated gains look like genuine money growth to the victim. This false success instills deep trust and convinces the victim of the investment system's legitimacy, acting as powerful psychological validation that incentivizes further investment.

Fraudsters gradually intensify psychological pressure to pull victims into the investment phase. They further strengthen emotional bonds by creating a sense of VIP privilege, telling targets, "You've been specially selected for our VIP investment group" or "We will share our proven internal strategies exclusively with you." This manufactured exclusivity makes victims feel they possess insider information unavailable to ordinary investors. Simultaneously, fraudsters showcase fabricated testimonials from alleged successful investors within the group, reinforcing the perception that others are profiting while the target risks missing out on lucrative opportunities. This combination of exclusive access, insider status, and fear of missing out overwhelms rational resistance and drives increasingly aggressive investment decisions.

To make larger investments appear attractive, they introduce a tiered reward system. Specifically, they urge victims to incrementally increase their investment amounts by stating, "Investments above a certain amount yield a 200% return." Additionally, they manufacture urgency by emphasizing the scarcity of the opportunity. Phrases like "exclusive to institutional investors" or "short-term intensive project" imply limited time. This artificial time pressure, combined with emotional bonding and promises of exceptionally high returns, pushes victims beyond rational judgment. As a result, victims proceed with large, impulsive investments.

Completion of Fund Acquisition

Fund acquisition is completed through withdrawal refusals and money laundering. At this stage, the victim's assets are confiscated and evidence is destroyed. Criminal organizations initially allow small withdrawals to build trust. However, once large investments are secured, they restrict access. They refuse withdrawals using various excuses like tax payments, withdrawal fees, or identity verification procedures. Paradoxically, withdrawal refusals encourage additional deposits. Scammers repeatedly convey false hope to victims, telling them, "Just deposit a little more, and you can recover everything."

Some criminal organizations exploit the lending features of virtual asset exchanges. They persuade victims to take out loans using existing assets as collateral. They weaken psychological resistance by justifying it as "temporary liquidity acquisition" or "full repayment after guaranteed profits." This method also has the effect of obscuring legal liability, as it creates the appearance that the victim voluntarily moved the funds.

Acquired funds are rapidly dispersed through laundering processes utilizing overseas networks. Criminal organizations first distribute stolen funds across multiple personal wallets. They then send these funds to mixer and tumbler services. These services mix funds with numerous other wallets and transaction pools while simultaneously pooling, dispersing, and redistributing cryptocurrency from multiple users. Consequently, it becomes difficult to identify the original source, trace the flow of funds, and directly link specific wallets to crimes.

Criminal organizations also employ chain-hopping techniques. They exchange assets from public blockchains like Bitcoin or Ethereum for privacy coins. Alternatively, they sequentially move funds across multiple blockchain networks using stable coins and low-fee chains. This fragments the flow of funds. This pattern of consecutive chain hops and multi-token utilization is a classic laundering tactic. It fragments the transaction path, making tracking via blockchain analysis significantly harder.

In the final stage, funds are converted into other cryptocurrencies using decentralized exchanges (DEXs) or exchanged for fiat-linked financial products via overseas virtual asset service providers (VASPs) with weak regulation and over-the-counter (OTC) brokers. By converting illicit digital proceeds into real estate, luxury goods, and corporate accounts—packaged as legitimate assets—criminal organizations complete their criminal lifecycle while ensuring both the concealment of the crime and the long-term enjoyment of the proceeds.

DISCUSSION AND CONCLUSION

This paper investigates how cryptocurrency leading room fraud takes shape and why it has become especially common in Korea. Korea's digital culture, Confucian hierarchical culture, and short-termism create conditions that make these schemes more likely to succeed.

Korea's distinctive patterns of internet use and monopolistic messaging ecosystem provide an ideal platform for the efficient spread of leading room fraud. Korea has near-complete internet coverage and a mobile-based digital finance system. In the past five years, internet use among people over 70 has increased 1.7-fold, and a growing number of older adults are actively using digital services. Over half of those in their 80s also now use online video services. These trends increase the likelihood that adults seeking investment opportunities will be exposed to leading room fraud promotions.

Regarding the messaging ecosystem, KakaoTalk plays such a central role in everyday communication for Koreans that the government has described it as "national infrastructure" (Lee, 2023). In Korea, it holds approximately 79% of the messaging market share (Statista, 2025), unlike in the U.S., where platforms like Facebook Messenger, Instagram, iMessage, and WhatsApp have relatively even shares (Statista, 2024). This dominant status, combined with open chat features that offer anonymity and exclusivity, creates a digital space that is easily exploited by criminals (Choi & Kim, 2020).

Moreover, Korea's collectivist decision-making conventions and Confucian hierarchical structure function as cultural mechanisms reinforcing authority dependence and collective conformity phenomena within leading rooms. In Korea and other East Asian countries, culturally collectivist thinking (group mentality) and social hierarchical structures operate closely (Boyle et al., 2025; Prabowo, 2024). In turn, this cultural foundation is distinctly reflected in investment behaviors, such as the pronounced tendency to make investment decisions based on group conformity pressure and trust in authority figures. Within leading room environments, consensus-building and mutual conformity reinforce decision-making processes that rely on group-derived consensus rather than individual autonomous judgment.

Korea's hierarchical social order, influenced by long-standing Confucian values, is characterized by an internalized respect and obedience for elders, experts, and the upper classes (Im et al., 2013; Shim, 2001). It creates an environment in which statements from self-proclaimed "expert leaders" within leading rooms are seen as highly credible. In particular, modern Korea's examination-centered education system and competition-based social structure have increased the tendency to use authoritative information sources or leader advice as bases for rapid decision-making (Chi, 2004; Yeo, 2008). This cultural foundation encourages investors to follow leaders' recommendations. In addition, the rise of K-pop, dramas, and other Korean media has increased the influence of celebrities and influencers, giving scammers more chances to exploit their image through deepfake impersonation (Kim, 2023; Han & Na 2022).

Furthermore, the short-termism derived from Korea's experience of rapid and intensive economic growth reinforces the persuasiveness of such scams and promotes individuals' vulnerability to high-risk, high-return investment incentives. As Korean society emphasizes quick results, Koreans have come to focus on rapid outcomes not only in employment and education but also in asset-related returns (Lee & Kim, 2024; Yoo & Kim, 2015). Moreover, socioeconomic conditions such as employment instability, asset polarization, and the rapid increase in real estate prices have reinforced skepticism and distrust toward traditional asset accumulation methods (Kim & Park, 2024; Lee, 2023). Against this backdrop, investment messages emphasizing high short-term returns appear to be a rational choice for individuals, ultimately hindering their critical thinking (Ahn, 2024). In turn, investors' psychological pathways become oriented toward accepting high-risk investments amid structural inequality and future instability, which can be viewed as a manifestation of crime vulnerability combining social deprivation and uncertainty rather than mere greed. Scammers exploit behavioral economic biases, including confirmation bias, overconfidence, and loss aversion (Bhat & Kolhe, 2024; Tversky & Kahneman, 1991). Repeated interactions with imposters lead victims to trust their own judgment and gradually fall into cognitive self-deception. Ultimately, even though they recognize the possibility of fraud, they internalize unrealistic profit expectations and voluntarily accept high-risk investments. In short, this psychological structure stems from the complex interaction of Korea's short-term performance-oriented thinking and unstable opportunity consciousness, which make individuals more vulnerable to fraud crimes.

In summary, these characteristics of Korean society create a setting where leading room fraud can spread quickly and operate with sophistication. While similar elements may exist in other countries, the way they come together and reinforce one another in Korea is unusually complex and relatively rare. Thus, the present analysis goes beyond simple financial crime research that examines the interactions between Korean society's cultural and structural characteristics and cybercrime; it also illuminates how similar crimes can take root and spread in other East Asian cultural spheres and digitally advanced societies. Against this backdrop, this research is of considerable academic value because it provides not only a reference point for comparative research on countries belonging to

digital cultural spheres similar to Korea's but also a more in-depth understanding of the structural and diffusion mechanisms of criminal phenomena, emphasizing the establishment of prevention and response strategies appropriate to each society's unique context.

Funding

This paper was supported by Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (RS-2024-00415520, HRD Program for Industrial Innovation)

REFERENCES

Ahn, Y. (2024). A phenomenological analysis of the adverse experiences of stock addicts in advisory rooms. Korean Association of Addiction Crime Review, 14(4), 115-134. http://doi.org/10.26606/kaac.2024.14.4.5

Asch, S. E. (1956). Studies of independence and conformity: I. A minority of one against a unanimous majority. Psychological monographs: General and applied, 70(9), 1-70. https://doi.org/10.1037/h0093718

Beauregard, E., & Leclerc, B. (2007). An application of the rational choice approach to the offending process of sex offenders: A closer look at the decision-making. Sexual Abuse: A Journal of Research and Treatment, 19, 115-133. http://doi.org/10.1007/s11194-007-9043-6

Beauregard, E., Rebocho, M. F., & Rossmo, D. K. (2010). Target selection patterns in rape. Journal of Investigative Psychology and Offender Profiling, 7(2), 137-152. https://doi.org/10.1002/jip.117

Bhat, A. H., & Kolhe, D. (2024). Crime and fraud at the community level: Social networking understanding into economic crimes and psychology motivations. Journal of Social Sciences and Economics, 3(2), 109-128. http://doi.org/10.61363/g0kb2s44

Bikhchandani, S., Hirshleifer, D., & Welch, I. (1992). A theory of fads, fashion, custom, and cultural change as informational cascades. Journal of political Economy, 100(5), 992-1026. http://doi.org/10.1086/261849

Blair, S. J., Bi, Y., & Mulvenna, M. D. (2020). Aggregated topic models for increasing social media topic coherence. Applied intelligence, 50, 138-156. http://doi.org/10.1007/s10489-019-01438-z

Blei, D. M., Ng, A. Y., & Jordan, M. I. (2003). Latent Dirichlet Allocation. Journal of Machine Learning Research, 3, 993-1022.

Boyle, P., Li, D., Peng, Z., & Yang, Y. (2025). The oversea Chinese fund: A complex affinity-based Ponzi scheme. Journal of Economic Criminology, 8, 100142. https://doi.org/10.1016/j.jeconc.2025.100142

Chi, E. (2004). Examining the perception of students, parents, teachers, and experts about the excessive competition for university admission in Korea. Journal of Educational Evaluation, 17(2), 147-164.

Choi, H., & Shim, D. (2020). Analysis of Korean ICT convergence trend using text mining methodology. Innovation Studies, 15(3), 257-281. http://doi.org/10.46251/INNOS.2020.08.15.3.257

Choi, J. H., & Kim, Y. H. (2020). The effect of information characteristics of open chatting on perceived usefulness of information and visit intention. Culinary Science and Hospitality Research, 26(3), 122-132. http://doi.org/10.20878/cshr.2020.26.3.012

Choi, S. W., Lee, J., & Lee, S. H. (2024). Cryptocurrency Ponzi schemes and their modus operandi in South Korea. Security Journal, 37(4), 1285-1300. http://doi.org/10.1057/s41284-024-00417-5

Cialdini, R. B. (2001). Influence: Science and practice (4th ed.). Pearson Education.

Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. Crime prevention studies, 3(1), 151-196.

Egger, R. & Yu, J. (2022). A topic modeling comparison between lda, nmf, top2vec, and bertopic to demystify twitter posts. Frontiers in Sociology, 7, 886498. http://doi.org/10.3389/fsoc.2022.886498

Financial Markets Authority. (2024, May 13). Fake celebrity investment scam – Multiple trading platforms. https://www.fma.govt.nz/library/warnings-and-alerts/fake-celebrity-investment-scam/

Financial Services Commission. (2024, January 26). [Press Release] Strengthening Investor Protection by Regulating Unfair Business Practices Such as Illegal Operation of Unlicensed Investment Advisory "Leading Rooms" – Amendment to the Capital Markets Act Passed by the National Assembly –. https://www.fsc.go.kr/no010101/81575?srchCtgry=&curPage=2&srchKey=&srchText=&srchBeginDt=&srchEndDt=

Han, M., & Na, E. (2022). Generational fandom culture shift in K-Pop idol fandom and social media use. The Journal of the Korea Contents Association, 22(2), 605-616. http://doi.org/10.5392/JKCA.2022.22.02.605

Hussein, A. (2009). The use of triangulation in social sciences research: can qualitative and quantitative methods be combined? Journal of comparative social work, 4(1), 106-117. http://doi.org/10.31265/jcsw.v4i1.48

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. British Journal of Criminology, 55(3), 596-614. http://doi.org/10.1093/bjc/azu106

Im, T., Campbell, J. W., & Cha, S. (2013). Revisiting Confucian bureaucracy: Roots of the Korean government's culture and competitiveness. Public Administration and Development, 33(4), 286-296. http://doi.org/10.1002/pad.1656

Janis, I. L. (1972). Victims of groupthink: A psychological study of foreign-policy decisions and fiascoes. Houghton Mifflin.

Jeong, D. H. (2024). Quasi investment advisors and the" leading rooms" problems-The analysis and suggestions for improvements of such a unique institution. Journal of Korean Law, 23(2), 413-450. http://doi.org/10.23110/jkl.2024.23.2.007

Jun, J., & Joung, S. (2022). Analysis of factors affecting consumer damage experience in new investment fraud 'leading room'. Journal of Consumption Culture, 25(3), 57-78. http://doi.org/10.17053/jcc.2022.25.3.004

Jung, D. (2024, February 1). Digital finance as a double-edged sword: "We need to strengthen systems to counter financial crimes." Edaily. https://www.edaily.co.kr/News/Read?newsId=03834326638786256&mediaCodeNo=257

Jung, J. Y., & Noh, K. Y. (2024). A study on the current state of crime and countermeasures related to the sexual exploitation of children and adolescents online: Focusing on the Darknet. Korean Journal of Industry Security, 14(3), 299-325. https://doi.org/10.33388/kais.2024.14.3.299

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. Econometrica, 47(2), 263-292. https://doi.org/10.2307/1914185

Kethineni, S., & Cao, Y. (2020). The rise in popularity of cryptocurrency and associated criminal activity. International Criminal Justice Review, 30(3), 325-344. https://doi.org/10.1177/1057567719827051

Kim, J. M. (2023). The impact of idol human brand characteristics on idol worship, fan engagement, and purchase intention -Focusing on 1st generation K-POP idols-. Journal of the Korean Society of Design Culture, 29(3), 81-91. http://doi.org/10.18208/ksdc.2023.29.3.81

Kim, J. S., & Park, M. C. (2024). The relationship between employment transition status and mental health among young adults: A focus on employment instability. Korean Journal of Social Welfare Studies, 55(4), 321-359. http://doi.org/10.16999/kasws.2024.55.4.321

Korean National Police Agency. (2025, February 27). Special enforcement status and preventive measures for investment leading rooms. https://police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1002&q_bbscttSn=20250226134123437

Krause, D. (2024). Deregulation, Bitcoin, and the Trump era: A new chapter for cryptocurrency governance. Available at SSRN 5023943.

Lee, K. (2023, November 20). The Republic of real estate and asset inequality. Weekly Kyunghyang. https://weekly.khan.co.kr/khnm.html?mode=view&art_id=202311160700011&dept=114

Lee, K., & Kim, D. K. (2024). Compressed development, decompression, and diverging convergence in South Korea: which varieties of capitalism in contemporary Korea?. Review of Evolutionary Political Economy, 5(1), 173-200. http://doi.org/10.1007/s43253-024-00117-1

Madarie, R., Weulen Kranenbarg, M., & de Poot, C. (2024). Introducing object-oriented modelling to cybercrime scripting: visualisation for improved analysis. Crime Science, 13(1), 27. http://doi.org/10.1186/s40163-024-00227-5

Ministry of Science and ICT. (2024, May 13). 2023 Internet usage survey final report. https://www.msit.go.kr/bbs/view.do?sCode=user&mId=99&mPid=74&bbsSeqNo=79&nttSeqNo=3173621

Muzammil, M., Pitumpe, A., Li, X., Rahmati, A., & Nikiforakis, N. (2025, April). The poorest man in Babylon: A longitudinal study of cryptocurrency investment scams. In Proceedings of the ACM on Web Conference 2025 (pp. 1034-1045).

Na, G., & Oh, S. Y. (2024). Analysis on 'short-form' trends using BIG KINDS. Korean Journal of Leisure, Recreation & Park, 48(2), 113-125. https://doi.org/10.26446/kjlrp.2024.6.48.2.113

Park, C. S., Hwang, J. T., & Yang, S. D. (2011). An empirical study on the types of the investment fraud. Korean Criminpological Review, 22(4), 287-314.

Park, J. P., & Ryu, J. K. (2018). Social engineering evaluation of electronic financial fraud: Analysis of actual victims through FGI. Journal of Digital Convergence, 16(7), 9-17. http://doi.org/10.14400/JDC.2018.16.7.009

Prabowo, H. Y. (2024). When gullibility becomes us: exploring the cultural roots of Indonesians' susceptibility to investment fraud. Journal of Financial Crime, 31(1), 14-32. https://doi.org/10.1108/JFC-11-2022-0271

Rogers, S. (2024, November 7). International scammers steal over $1 trillion in 12 months in Global State of Scams Report 2024. Global Anti-Scam Alliance. https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai

Shim, Y. H. (2001). Feminism and the discourse of sexuality in Korea: Continuities and changes. Human Studies, 24(1), 133-148. http://doi.org/10.1023/A:1010775332420

Shin, A. (2019). Keyword and topic analysis on free semester policy using big data (Doctoral dissertation, Seoul National University).

Siu, G. A., & Hutchings, A. (2023, July). "Get a higher return on your savings!": Comparing adverts for cryptocurrency investment scams across platforms. In 2023 IEEE European symposium on security and privacy workshops (EuroS&PW) (pp. 158-169).

Song, J., & Lee, M. (2023, May 21). 5 trillion won in damages from illegal crypto activities over 5 years—73% related to investment fraud. Yonhap News. https://www.yna.co.kr/view/AKR20230520030200004

Statista. (2024, May). Penetration of leading messenger platforms in the United States as of March 2024. https://www.statista.com/statistics/294439/messenger-app-share-us-users/

Statista. (2025, January). Most used messenger by brand in South Korea as of December 2024. https://www.statista.com/forecasts/1371497/most-used-messenger-by-brand-in-south-korea

Tversky, A., & Kahneman, D. (1991). Loss aversion in riskless choice: A reference-dependent model. The quarterly journal of economics, 106(4), 1039-1061. https://doi.org/10.2307/2937956

Yeo, E. (2008). A study of the influence of education on social mobility. Health and Social Welfare Review, 28(2), 53-80. http://doi.org/10.15709/hswr.2008.28.2.53

Yoo, S., & Kim, J. (2015). The dynamic relationship between growth and profitability under long-term recession: The case of Korean construction companies. Sustainability, 7(12), 15982-15998. https://doi.org/10.3390/su71215796

Yu, Y. (2017). Analysis of media coverage on 2015 revised curriculum policy using big data analysis (Doctoral dissertation, Seoul National University).

