https://dergipark.org.tr/tr/pub/igdirsosbilder

Iğdır Üniversitesi Sosyal Bilimler Dergisi

E-ISSN: 2147-6152

Yıl 14, Sayı 38, Ocak 2025

[Araştırma Makalesi] **Atıf/Citation**: İli, B. (2025). "Analysis of Complaints Regarding Cryptocurrency Investment Fraud: An Evaluation from the Perspective of New Media Literacy", *Iğdır Üniversitesi Sosyal Bilimler Dergisi*. (38): s. 214-229. **Gönderim Tarihi**: 06.06.2024 **Kabul ve Yayın Tarihi**: 20.12.2024-20.01.2025 **DOI**: 10.54600/igdirsosbilder.1580718

Yazar/Author

Burak İLİ*

Article Name/Makale Adı

Analysis of Complaints Regarding Cryptocurrency Investment Fraud: An Evaluation from the Perspective of New Media Literacy

Kriptopara Yatırım Dolandırıcılığına Yönelik Şikayetlerin İncelenmesi: Yeni Medya Okuryazarlığı Perspektifinden Bir Değerlendirme

ABSTRACT

The aim of this research is to raise awareness regarding cryptocurrency fraud. In this context, the study focuses on cryptocurrency investment frauds and provides an evaluation from the perspective of new media literacy. Throughout the research process, a total of 969 complaints were analyzed under the categories of "Cryptocurrency Investment Fraud" and "Cryptocurrency and Victim Complaints" on the Şikayetvar platform. Adopting an exploratory approach, the complaints were coded under various themes using content and thematic analysis methods. The analysis process was conducted using MAXQDA 24, a qualitative data analysis software. The findings reveal that the theme with the highest frequency among types of fraud is "Fake Coin/Token" (337), illustrating the strategies employed by cryptocurrency fraudsters to deceive investors through fraudulent projects and assets. Additionally, the theme "Withdrawal and Transaction Request Rejection" (159) reflects the difficulties faced by users in conducting transactions and withdrawing their funds on legitimate platforms, showcasing how fraudulent platforms delay their victims. Furthermore, scams conducted through Telegram channels (173) have garnered attention, highlighting the significant role social media platforms play in fraudulent activities. Cryptocurrency frauds underscore the deficiencies in users' new media literacy and emphasize the importance of financial literacy and new media literacy education in an environment where fraud is prevalent.

Keywords: Cryptocurrency, fraud, new media literacy, complaint, fake coin, social media, financial literacy.

ÖZ

Bu araştırmanın amacı kripto dolandırıcılıkları konusunda farkındalığı artırmaktır. Bu doğrultuda, araştırmada kripto para yatırım dolandırıcılıklarına odaklanılarak, yeni medya okuryazarlığı perspektifinden bir değerlendirme sunulmaktadır. Araştırma sürecinde, Şikayetvar platformu üzerindeki "Kripto Para Yatırım Dolandırıcılığı" ve "Kripto ve Mağdur Şikayetleri" başlıkları altında toplamda 969 şikayet incelenmiştir. Keşfedici bir yaklaşım benimseyerek, içerik ve tematik analiz yöntemleri kullanılarak şikayetler, çeşitli temalar altında kodlanmıştır. Analiz süreci, nitel veri analiz yazılımı olan MAXQDA 24 kullanılarak gerçekleştirilmiştir. Elde edilen bulgular, dolandırıcılık türleri arasında en yüksek frekansa sahip olan "Sahte Coin/Token" temasının (337), kripto para dolandırıcılarının sıkça kullandığı sahte projeler ve varlıklar üzerinden yatırımcıları kandırma stratejilerini ortaya koymaktadır. Bunun yanı sıra, "Para Çekme ve İşlem Talep Reddi" (159) teması, kullanıcıların meşru platformlarda işlem yapma ve paralarını çekme konusundaki zorluklarını yansıtarak dolandırıcı platformların mağdurları nasıl oyaladığını göstermektedir. Ayrıca, Telegram kanalları aracılığıyla yapılan dolandırıcılıklar da (173) dikkat çekmekte olup, sosyal medya platformlarının, dolandırıcılık faaliyetlerinde önemli bir rol oynadığı tespit edilmiştir. Kripto para dolandırıcılıkları, kullanıcıların yeni medya okuryazarlığı eksikliklerini gündeme getirmekte ve dolandırıcılıkların yaygın olduğu bir ortamda, finansal okuryazarlık ve yeni medya okuryazarlığı eğitimlerinin önemini ortaya koymaktadır.

Anahtar Kelimeler: Kripto para, dolandırıcılık, yeni medya okuryazarlığı, şikayet, sahte koin, sosyal medya, finansal okuryazarlık.

* Lecturer Dr., Igdir University, Department of Visual and Audio Techniques and Media Production, burak.ili@igdir.edu.tr

Introduction

The digital asset ecosystem is built upon blockchain technology, which is based on the principle of decentralization. This technology has the capacity to offer more agile, accessible, and reliable products and services compared to centralized systems. Cryptocurrencies are defined as innovative digital assets supported by encryption techniques that secure and manage digital currency transactions (Narayanan et al., 2016). They have emerged as a popular asset class in global financial markets, exhibiting rapid growth that encompasses both developed and developing countries. This trend highlights cryptocurrencies as one of the fastest-growing financial markets in the world (Białkowski, 2020). The emergence of this new market and the establishment of investment platforms have made investment opportunities more accessible to ordinary individuals—many of whom lack financial knowledge—under the illusion of high and easy profits. Consequently, there has been a significant increase in the number of non-institutional investors operating with the hope of becoming wealthy in this highly volatile market. While some investors achieve their financial goals during this process, others have lost their entire savings (Almeida and Gonçalves, 2023).

In recent years, the popularity of cryptocurrencies has rapidly increased, creating new opportunities for both investors and fraudsters. The high profit potential offered by digital currencies has encouraged individuals to engage in investment activities. Cryptocurrencies have gained broad acceptance in investment and speculation due to their decentralized structure and the ability to facilitate fast and secure transactions. However, the swift proliferation of cryptocurrency markets worldwide has introduced new fraud challenges and risks that are not yet fully understood. This increasing popularity has also contributed to the rise of fraudulent activities. Cryptocurrency fraud manifests in various forms, resulting in significant financial losses for investors. These frauds include scams, phishing attacks, Ponzi schemes, and other criminal activities (Agarwal et al., 2023). Fraudsters manipulate their target audience and create an image of credibility by utilizing social media and online platforms.

New media literacy aims to enhance individuals' skills in accessing, evaluating, and effectively utilizing information in digital environments. In complex and rapidly evolving fields like cryptocurrency fraud, this literacy is of utmost importance. Individuals with insufficient knowledge and experience can easily fall victim to fraudulent investment opportunities and scams. Therefore, new media literacy can help individuals understand the risks they may encounter in cryptocurrency markets, enabling them to make more informed and secure investment decisions. In this context, educational and informational activities play a critical role in making individuals more resilient against fraud.

The primary aim of this research is to reveal the prevalence of cryptocurrency fraud and the experiences of individuals exposed to such frauds. To this end, this study employs a phenomenological design, a qualitative research method. Specifically, it examines 969 complaints shared on Şikayetvar, a platform that offers customer experiences and brand solutions, to analyze the prevalence of fraudulent activities, the strategies employed, and the effects of these situations on users. The financial losses and grievances experienced by victims not only jeopardize individual finances but also threaten the credibility of the cryptocurrency ecosystem. The findings aim to contribute to increasing the knowledge and awareness necessary for cryptocurrency investors to pursue safer investment processes through the lens of new media literacy.

1. Cryptocurrency Fraud

Cryptocurrency is a digital currency that enables transactions to be conducted from anywhere. Due to its entirely digital nature, transactions are stored in online databases. A fundamental characteristic of cryptocurrencies is the verification of transactions through encryption, which ensures security via complex coding. The blockchain technology that underpins cryptocurrencies is a decentralized ledger system, allowing transactions to be executed without reliance on any authority (Velani and Patel, 2023).

Bitcoin (BTC), known as the first cryptocurrency, was introduced in 2008 by an individual or group using the pseudonym Satoshi Nakamoto (Nakamoto, 2008). The timing of this innovation is not coincidental; it parallels the global financial crisis experienced between 2008 and 2010. During the crisis, central banks intervened by significantly increasing the money supply through "money printing," which undermined trust in traditional fiat currencies. The foundation of Bitcoin is based on a peer-to-peer network, public and private key cryptography techniques, and a consensus mechanism known as "Proof of Work." This innovation provides a solution that enables individuals to conduct digital transactions globally, relying on mutual trust without the need for a central authority. Trust in governments or central banks has been replaced by trust in technology (Watorek et al., 2021: 3). Despite being a relatively new concept, cryptocurrencies have rapidly gained acceptance in a broad market and have shown swift development (Farell, 2015). However, cryptocurrencies exist in an online market characterized by significant uncertainty regarding their current and future legal status, positioning them within the realm of gray economic activities (Mackenzie, 2022).

The scientific literature on cryptocurrency fraud has been examined across various disciplines, including computer science (Aziz et al., 2022; Tripathy et al., 2024; Xia et al., 2020), economics (Dutta et al., 2023; Kutera, 2022; Smith, 2018), and law (Reddy & Minnaar, 2018; Sanz-Bas et al., 2021; Trozze et al., 2022). This indicates that the field of cryptocurrency represents an interdisciplinary area of study. The current research contributes to the literature by evaluating cryptocurrency through the lens of new media literacy, specifically by examining the complaints of victimized users.

Cryptocurrency fraud is increasingly diversifying, with various types emerging, including fake smartphone applications, phishing methods that compromise cryptocurrency wallets, initial coin offering scams, and Ponzi schemes (Childs, 2024). Although the literature categorizes types of cryptocurrency fraud based on different criteria (Badawi and Jourdan, 2020; Higbee, 2018), the drawback of existing classifications is their inability to fully capture the multifaceted nature of cryptocurrency fraud. Most scams encompass multiple characteristics, and categorizing them into distinct types often proves inadequate. The boundaries between types of fraud can be ambiguous. For instance, fake mining scams may exhibit similar qualities to Ponzi schemes when they present investment schemes promising higher returns to investors (Bartoletti et al., 2021). The complex structure, diversity, and continuous evolution of these frauds contribute to cryptocurrency fraud becoming an increasingly dangerous issue.

Despite proposed regulatory frameworks, there continues to be a global lack of coordinated regulation and transparency within the decentralized finance (DeFi) and cryptocurrency ecosystem. This lack of oversight extends to advertisements for cryptocurrency investments on online platforms. Criminals exploit the popularity of these platforms to promote their investment schemes and defraud investors (Siu and Hutchings, 2023). Fraudsters employ various methods to attract victims, including social media advertisements (on platforms such as

Facebook, YouTube, Twitter, and LinkedIn), Google ads, fake social media accounts, hacked accounts, and direct messages sent through messaging applications (WhatsApp, Facebook Messenger, Telegram, Signal). Victims are often directed to purchase Bitcoin from either legitimate or unreliable cryptocurrency exchanges. Once Bitcoin is acquired, it is transferred to a fraudulent website or used to purchase another cryptocurrency. Scammers persuade victims with promises of quick and substantial returns. If a victim expresses suspicion, they are redirected to a secondary fraudulent website or another cryptocurrency under the pretense of receiving assistance (Chergarova, 2022).

While fraudulent activities in the cryptocurrency sector possess unique technical characteristics and operational methods, they also exhibit many similarities with traditional scams. The digital asset industry has been exposed to various types of fraud, and in this context, nearly all previously recognized fraud tactics have been reimplemented in this area (Perdana and Jiow, 2024). The features of cryptocurrencies, such as anonymity and decentralization, further complicate fraudulent activities, introducing dynamics that differ from traditional methods.

2. New Media Literacy

Media is regarded not only as a tool that shapes culture but also as culture itself (Wu & Chen, 2007). New media technologies have transformed user roles and experiences, revealing the necessity of media literacy in increasingly unregulated environments that are exposed to various dangers. Advances in new media technologies have also contributed to the evolution of the concept of literacy. Considering the transformations occurring in both societal and media contexts, there is a pressing need to reconceptualize media literacy, taking into account the experiences and skill sets that emerge on new media platforms (Ugurhan et al., 2020: 161).

New media literacy is a continuously evolving concept and research area that is still in its infancy, necessitating innovative educational methods to enhance individuals' abilities to access information, evaluate content, and think critically in digital environments (Jocson, 2015). This situation not only equips individuals with better media literacy skills but also promotes democratic participation and critical thinking. The ability to access, analyze, critically evaluate, and create various forms of content, such as text, audio, images, and video in online environments, is referred to as new media literacy (NML) (Park et al., 2014; Zhang et al., 2014). Regardless of demographic characteristics and individual preferences, new media literacy is a skill that individuals can acquire and further develop through media literacy education (Long et al., 2023).

When examining the fundamental components of new media literacy (NML), it encompasses essential skills such as access, analysis, evaluation, criticism, production, and engagement with media content (Lee et al., 2015). As users rapidly adopt new media technologies, they have transitioned from the role of consumers in traditional media to that of producer-consumers (prosumer) (Chen et al., 2018). Users with new media literacy possess awareness of how messages are created, distributed, and commercialized, as well as the purposes behind them (Thoman and Jolls, 2004). Additionally, they can effectively utilize various media tools, evaluate messages from a critical perspective, and actively participate as content creators in new media environments (Kellner and Share, 2007).

New media literacy (NML) represents a fusion of various types of literacy developed in the past, including classical literacy, audiovisual literacy, digital literacy, and information literacy. This contemporary form of literacy is explained within a conceptual framework that encompasses functional and critical consumption as well as functional and critical production literacy.

Functional consumption literacy involves accessing media content and understanding that content. *Critical consumption literacy* enables individuals to analyze media content more deeply and to question the messages, purposes, and effects conveyed by that content. On the other hand, *functional production literacy* encompasses active participation in the process of creating media content, while *critical production literacy* requires consideration of social, cultural, and political contexts in the content production process (Chen et al., 2011).

Factors such as a lack of regulation and the unintentional spread of misinformation have led to disinformation becoming a significant issue today. To effectively combat disinformation, users need to possess the ability to distinguish between fact and fiction (Miller et al., 2024). This necessitates the development of skills such as critical thinking, information verification, and source analysis. By enhancing these skills, individuals can navigate digital environments more consciously and responsibly, thereby improving their ability to protect themselves from misleading information. In the context of cryptocurrency fraud, it has been noted that individuals with low levels of new media literacy struggle to recognize fraudulent projects, leaving them vulnerable to deceptive practices (Martens and Hobbs, 2020).

New media literacy and financial literacy are two essential skills necessary for individuals to make effective and informed decisions in modern society. New media literacy encompasses the ability to access, analyze, and critically evaluate information on digital platforms, while financial literacy aims to enhance individuals' understanding of financial information, management, and investment skills. The integration of these two domains enables individuals to approach the financial content they encounter in online environments with a critical perspective and to manage their personal finances more consciously. Thus, new media and financial literacy contribute to individuals making more sound decisions based on a solid foundation in both the digital world and their economic lives.

3. Methodology

The popularity of cryptocurrencies is rapidly increasing, and the applications of these digital assets are expanding. However, gaps in knowledge and misinformation render investors vulnerable to fraudulent activities. The aim of this research is to examine complaints related to cryptocurrency investment fraud to illustrate how such fraud can be evaluated from the perspective of new media literacy. New media literacy plays a significant role in helping individuals discern information pollution on digital platforms, develop critical thinking skills, and access reliable information. Raising awareness among cryptocurrency investors regarding fraud and emphasizing the role of new media literacy in minimizing such risks underscores the importance of this research. The limitations of the study stem from certain constraints related to the data sources and methodologies used. First, the research is limited to data available on the Şikayetvar platform, which reflects users' experiences with cryptocurrency fraud on that platform. This means potential complaints and victimizations from social media platforms or other complaint sites are excluded. Consequently, the findings may not represent all cryptocurrency investors. Additionally, while the analysis based on 969 complaints provides a substantial dataset, not all complaints may contain the same level of detailed information. This could result in some themes being inadequately represented during the analysis process.

The research conducted through a phenomenological design, utilizing qualitative research methods, focuses on the Şikayetvar website (www.sikayetvar.com) as a purposive sampling site. Şikayetvar serves as a solution platform acting as a bridge between customers and brands. In this study, the data collection process involved examining the categories “Cryptocurrency

Investment Fraud" and "Cryptocurrency and Victim Complaints" on the platform, resulting in a total of 969 complaints. An exploratory approach was employed, utilizing content and thematic analysis methods, with the complaints coded under various themes. The analysis considered elements of reliability and validity. To mitigate issues such as bias and participant reactivity that threaten the validity of the research, an external review and peer evaluation were conducted. In qualitative research, reliability typically refers to the consistent coding of data sets by different coders (Creswell and Poth, 2018). Accordingly, the coding process involved comparing paragraphs, sentences, main themes, and sub-themes to achieve consensus among coders. The coding process was carried out using MAXQDA 24, a qualitative data analysis software. The research aims to address the following two fundamental questions:

1. What methods are used in cryptocurrency fraud, and what types of fraud strategies have victims encountered?
2. What role do new media and social media tools play in the victimization associated with cryptocurrency fraud?

4. Findings

Based on the data obtained from the Şikayetvar website, complaints published by cryptocurrency victims have been thoroughly reviewed, and codings have been conducted under specific themes. Explanations regarding the created themes are shared in Table 1.

Table 1. Explanations of the Themes

Themes	Explanations	Frequencies
1. Account Restriction/Blocking	This theme refers to situations where cryptocurrency users face restrictions or complete denial of access to their accounts.	*65*
2. Deepfake	Deepfake technology involves creating fake images and videos that impersonate individuals. In cryptocurrency scams, this method is often employed to deceive victims by impersonating celebrities, investment experts, or trusted figures.	*2*
3. Phishing	Phishing is a fraud method aimed at stealing personal information	

	through fake emails, messages, or websites. In the cryptocurrency world, scammers use phishing techniques to obtain users' wallet information or private keys.	*11*
4. Fake Websites/Platforms	Fraudsters create fake websites that resemble official cryptocurrency exchanges or financial platforms. Users are encouraged to invest through these sites, leading them to lose their money to the scammers.	*23*
5. Fake Calls	In cryptocurrency scams, fraudsters may call victims, presenting themselves as experts or authorities. These calls aim to lead victims into conducting fake transactions or to obtain their personal information.	*8*
6. Fake Coin/Token	Fake cryptocurrencies and tokens are digital assets that are often presented as legitimate projects but have no real value. Scammers entice investors to purchase these fake crypto assets by promising significant returns in the future. When victims buy such tokens, they eventually realize that their assets hold no value.	*337*

7. Withdrawal and Transaction Request Denial	This theme relates to victims' inability to withdraw their money from cryptocurrency exchanges or platforms, or the rejection of their withdrawal requests. When victims attempt to withdraw their funds, the platforms may continuously reject the transactions to delay the process or completely deny the request.	*159*
8. Instagram	In cryptocurrency fraud, victims are deceived by crypto investors through advertisements and accounts on Instagram.	*25*
9. WhatsApp	Fraudsters attempt to deceive victims through messages and calls via WhatsApp.	*8*
10. Telegram	It involves fraudulent activities conducted through Telegram channels.	*173*
11. Excessive Payment/Commission Request	Another common method of cryptocurrency fraud is the demand for additional money or commission fees from users in order to carry out transactions or withdraw their earnings. Scammers direct victims to pay these extra fees, collecting more money, but even if the victims comply with these	*68*

	requests, the transactions do not take place.	
12. Unauthorized Transaction/Transfer	Unauthorized transactions or transfers made from users' accounts without their knowledge fall within the scope of this theme. These transactions, conducted through cryptocurrency exchanges or wallets, are typically carried out by scammers who have obtained the victims' information. This situation results in the rapid transfer of assets from the victims' accounts to other accounts.	*90*
TOTAL		*969*

A total of 969 complaints from cryptocurrency victims have been coded in accordance with the themes established in Table 1. Among these, the *Fake Coin/Token* theme is the type of fraud represented with the highest frequency (337). This indicates that cryptocurrency scammers frequently employ strategies to deceive investors through fake projects and assets. The allure of investment opportunities in cryptocurrency markets facilitates the presentation of fraudulent assets, particularly during the marketing of new projects. Investors' tendencies to gravitate towards such assets in hopes of achieving significant future gains create an environment ripe for exploitation by scammers. Several complaints from victims of Fake Coin/Token schemes are shared below:

- “I bought a coin called Puf for $350, but I can't sell it because I'm getting a compatibility issue with v3. I saw it in a Telegram group. Kripto, and it turns out they are scammers. I hope someone can help. I'm a student, and I've lost all my money.”
- “Hello, I was directed to buy a fake cryptocurrency by someone on Telegram, and since I'm new, I didn't realize the situation. The cryptocurrency shows up in my account, but the money is not visible at all, and I can't withdraw it. I bought it from my Bidget wallet; I wish I hadn't. I've lost all my savings.”
- "I bought a cryptocurrency called 'Giggle' from Pancakeswap, and now I can't sell it. “he coin is listed as suspicious and was sold to us as if it were legitimate. I demand that my victimization be addressed.”

These complaints clearly illustrate the prevalence and potential risks associated with cryptocurrency fraud. Scammers target new and inexperienced investors by utilizing social media platforms such as Telegram, capitalizing on their lack of knowledge.

The Withdrawal and Transaction Request Denial theme (159) is also noteworthy. Complaints in this area reflect users' issues with being unable to execute transactions or withdraw their funds on cryptocurrency platforms. Scammer platforms delay victims by denying transaction requests, effectively preventing them from accessing their assets entirely. Some examples of victim complaints regarding this issue are as follows:

- "I earned 12,693.8 on Binance TR 1.5 months ago and wanted to withdraw it. Customer service asked me to pay a 10% tax (1,269 dollars) in order to withdraw the money. I requested that this amount be deducted from my earnings, but it was not accepted. I was told that the payment would be processed if I deposited the money."
- "I have been waiting for about a month and a half to withdraw my cryptocurrencies. I cannot reach customer service; the automatic call ends after an hour. I cannot find anyone to speak to. I submitted a withdrawal request, and now I know that it won't come through either. I will file a complaint with the prosecutor's office starting Monday."
- "I downloaded the Erospro program from the Google Play Store and suffered a financial loss of $55,000 through cryptocurrency exchanges. I couldn't withdraw my money, and they presented themselves as a US company. I have been victimized, and all my savings are gone; they closed the site. I want my victimization to be addressed."

An examination of victim complaints within this theme reveals the difficulties users encounter on cryptocurrency exchanges and their concerns regarding the reliability of these processes. Users experience victimization due to both financial losses and a lack of communication, which undermines trust in the cryptocurrency ecosystem.

Frauds conducted via *Telegram* also exhibit a high frequency (173). Given that Telegram is a widely used platform, particularly among cryptocurrency communities, scammers exploit these channels to deceive victims with fake projects or transactions. Similarly, the frauds occurring on *Instagram* (25) and *WhatsApp* (8) underscore the significant role social media platforms play in fraudulent activities. Some user complaints related to victimization through social media platforms are as follows:

- "Through the Telegram application, a person using the username e*** deceived people with a fake account. As soon as I found out, they blocked and deleted me. They are promising people profits from Bitcoin through a page that shares real-time updates about the war in Palestine and taking their money."
- "A Binance Turkey l40 platform has been opened through WhatsApp, and they are presenting themselves as authorized crypto experts from Binance. They appear completely like official Binance representatives and are conducting fraudulent transactions."
- "The account named H**A*, which is advertising on Instagram, is deceiving people by getting them to buy a cryptocurrency called 'b****', which they created and is not available for sale, through the Binance Web3 wallet on Telegram."

The relationship of these complaints with social media highlights how fraudulent activities proliferate on these platforms and how users fall victim to such schemes. Social media has become both a marketing tool for scammers and an accessible means of reaching their target audience.

Furthermore, complaints categorized under themes such as *Account Restriction/Block* (65), *Unauthorized Transaction/Transfer* (90), *and Excessive Payment/Commission Request* (68) indicate that victims experience significant issues regarding account security, unauthorized transactions, and additional payment requests. These methods employed by scammers are among the strategies that exacerbate victims' financial losses and complicate recovery efforts. Additionally, despite having lower frequencies, themes like *Phishing* (11), *Fake Calls* (8), and *Deepfake* (2) reveal that scammers resort to methods for collecting personal information and establishing trust. Notably, the emergence of deepfake technology in cryptocurrency fraud serves as an example of how scammers exploit technological advancements for malicious purposes.

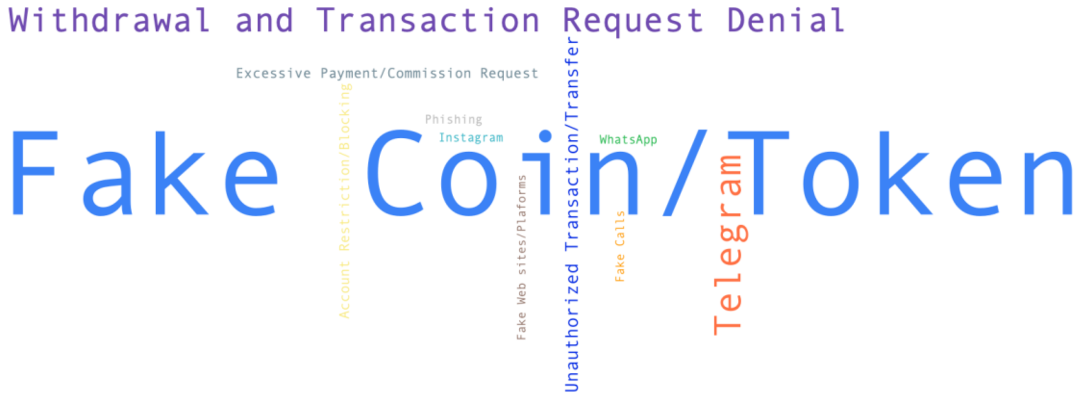

Figure 1. Code Cloud (Frequencies of Codes)

This code cloud visually represents the importance and frequencies of themes derived from victim complaints related to cryptocurrency fraud. Terms that appear in larger and more prominent font sizes indicate issues that are more frequently encountered in the complaints, while smaller terms represent topics with lower frequencies. Accordingly, Fake coins/tokens, frauds conducted through Telegram, and Withdrawal and Transaction Request Denial emerge as the most prominent and dangerous issues.

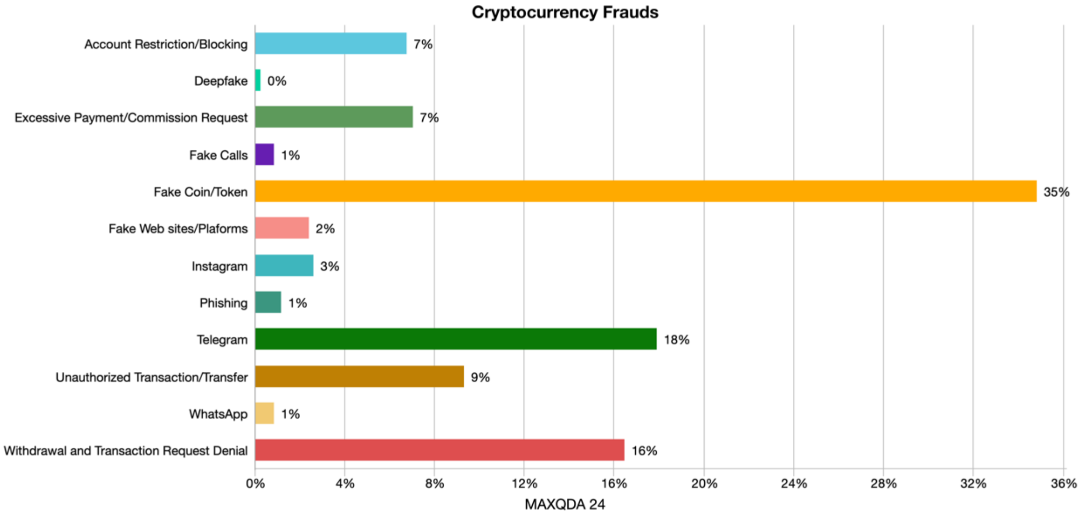

Figure 2. Percentage Chart of the Themes

The percentage graph of the themes presented in Figure 2 illustrates the proportions of various types of cryptocurrency fraud. The most prevalent type of fraud is "Fake Coin/Token," accounting for 35%. This figure is significantly higher than all other types of fraud, indicating that the most common risk faced by investors in the cryptocurrency space involves fake token or coin projects. The second highest proportion is attributed to frauds conducted via "Telegram," at 18%, highlighting the use of popular messaging applications by cryptocurrency scammers. Similarly, "Withdrawal and Transaction Request Denial" fraud, at 16%, is noteworthy; this type of fraud arises from the obstruction of users' attempts to withdraw their investments or the denial of their transactions. Additionally, "Unauthorized Transaction/Transfer" has been reported at 9%, resulting in victimization due to transactions conducted without the account holder's knowledge. Fraud occurring on "Instagram" is observed at 3%, demonstrating that social media platforms provide a venue for scammers to advertise and market their schemes. Other types of fraud have been reported at varying rates between 1% and 7%. These findings highlight the types of fraud that cryptocurrency users are most commonly exposed to, emphasizing the areas where users should exercise caution.

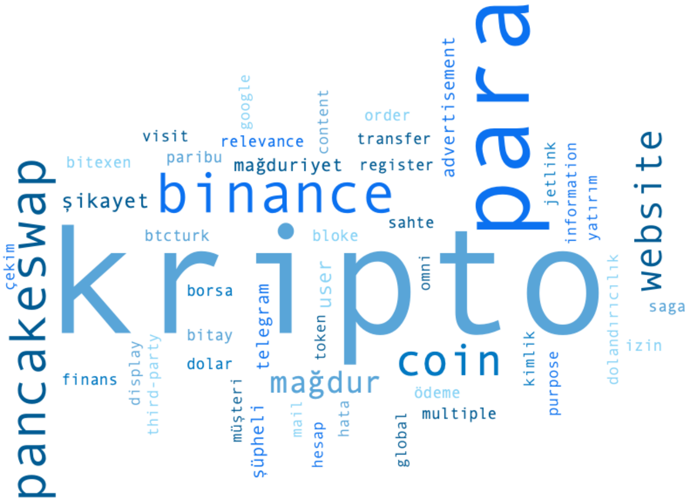

Figure 3. Word Cloud (Frequencies of Words)

The word cloud depicted in Figure 3 visually represents the data derived from complaints by cryptocurrency victims, highlighting the key issues encountered within the examined complaints. The size of the words indicates how frequently the corresponding concepts are repeated and their level of importance. Accordingly, the two largest words, "crypto" and "money," constitute the general subject of the complaints, demonstrating that the victims' grievances are directly related to cryptocurrencies. Problems encountered during the investment and usage processes are central to this theme. Prominent cryptocurrency exchanges such as Binance and Pancakeswap frequently appear in the complaints, indicating that a significant portion of victimization stems from users being defrauded or experiencing technical issues on these platforms. Users seem to take on greater risks, especially in transactions conducted on decentralized exchanges like Pancakeswap. The terms "victim" and "complaint" directly express the impact of cryptocurrency fraud on users. It is evident that users commonly report their victimization through complaint platforms, highlighting the prevalence of this situation. The words "coin" and "token" represent fraudulent crypto assets, illustrating that victims have invested in fake projects and have been subjected to scams involving such assets. In particular, fake coins and tokens are among the most frequently employed methods by scammers. The words "Telegram" and "website" indicate the communication channels and methods used by fraudsters. Telegram emerges as a social media platform that scammers frequently utilize to reach victims, while fake websites serve as another significant medium for fraudulent activities. In summary, this word cloud reveals that victimization in the cryptocurrency world, particularly through scams involving fake projects and platforms, is widespread. It is clear that social media platforms like Telegram and fake websites are critical tools for scammers in this process. Moreover, even on popular exchanges, issues such as technical problems and the denial of withdrawal requests constitute significant concerns among users. To protect themselves from these risks and engage in safer investment processes, cryptocurrency users must address their deficiencies in financial literacy and new media literacy.

Conclusion and Discussion

This study addresses complaints related to cryptocurrency investment fraud, highlighting the strategies employed by scammers and the primary issues faced by victims. According to the results of content and thematic analyses, cryptocurrency fraud is predominantly conducted through fake projects, technical issues, and social media platforms. In particular, fake coins and tokens rank among the most commonly used methods by scammers, with investors often drawn to these assets by promises of high returns. The data-driven word cloud analysis visualizes the key concepts of victimization, indicating that victims predominantly experience problems related to cryptocurrency exchanges. Users who have been defrauded or encountered technical issues on popular exchanges like Binance and Pancakeswap have lodged complaints regarding these platforms. Furthermore, it has been observed that higher risks are taken in transactions conducted on decentralized exchanges such as Pancakeswap.

In this context, cryptocurrency investors and users must enhance their skills in both financial literacy and new media literacy to become more resilient against fraud. New media literacy equips individuals to approach information on social media and digital platforms with a critical eye and to discern misinformation. Increased awareness of fraud cases encountered on social media platforms will help protect investors from such dangers. Furthermore, awareness of fake coin and token projects should be heightened, and investors must be educated about conducting transactions only on reliable and verified platforms. In line with these recommendations, financial literacy training should be made accessible to a broader audience, and awareness campaigns regarding new media literacy should be organized. Educational programs can enable users to acquire essential knowledge about digital assets and better manage potential risks on digital platforms. Additionally, governments and regulators should implement stricter oversight and regulations to prevent cryptocurrency fraud. Specifically, regulations targeting fake projects and decentralized exchanges will enhance the protection of investors against such scams.

This research posits that new media literacy serves as a crucial defense mechanism against cryptocurrency investment fraud and suggests that future researchers can make significant contributions to the field by conducting in-depth studies on the relationship between cryptocurrency investment fraud and new media literacy. In this regard, researchers could explore the extent to which individuals with varying levels of new media literacy are exposed to fraud risks as cryptocurrency investors. Furthermore, cryptocurrency fraud methods are continuously evolving in parallel with technological advancements. Investigating how new tactics employed by scammers, particularly in relation to developments in deepfake technology, artificial intelligence, and decentralized finance (DeFi), affect fraud strategies could enhance our understanding of the risks present in cryptocurrency markets. Finally, a deeper examination of how social media platforms such as Telegram, Instagram, and Twitter are utilized in cryptocurrency fraud would be valuable for understanding how the algorithmic structures of these platforms create an environment conducive to scams. Researchers can analyze how fraud spreads across these platforms and investigate the roles of moderation, security measures, and algorithmic recommendation systems in either mitigating or facilitating fraudulent activities. In particular, the role these platforms play in the virality of fake projects and fraudulent content, as well as how users interact with such content, warrants comprehensive investigation. Additionally, studying the effectiveness and shortcomings of existing policies on social media platforms aimed at preventing fraud could contribute to the development of more effective strategies for addressing this issue.

References

Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. (2024). Blockchain and crypto forensics: Investigating crypto frauds. *International Journal of Network Management*, *34*(2), e2255. https://doi.org/10.1002/nem.2255

Almeida, J., & Gonçalves, T. C. (2023). A decade of cryptocurrency investment literature: A cluster-based systematic analysis. *International Journal of Financial Studies*, *11*(2), 71. https://doi.org/10.3390/ijfs11020071

Aziz, R. M., Baluch, M. F., Patel, S., & Ganie, A. H. (2022). LGBM: a machine learning approach for Ethereum fraud detection. *International Journal of Information Technology, 14(*7), 3321-3331. https://doi.org/10.1007/s41870-022-00864-6

Badawi, E., & Jourdan, G. V. (2020). Cryptocurrencies emerging threats and defensive mechanisms: A systematic literature review. *IEEE Access, 8*, 200021-200037. https://doi.org/10.1109/ACCESS.2020.3034816

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., & Serusi, S. (2021). Cryptocurrency scams: analysis and perspectives. *IEEE Access, 9*, 148353-14837.

Białkowski, J. (2020). Cryptocurrencies in institutional investors' portfolios: Evidence from industry stop-loss rules. *Economics Letters, 191*, 108834. https://doi.org/10.1016/j.econlet.2019.108834

Chen, D.T., Wu, J., & Wang, Y. (2011). Unpacking new media literacy. *Journal of Systemics Cybernetics and Informatics, 9*(2), 84–88.

Chen, D. T., Lin, T. B., Li, J. Y., & Lee, L. (2018). Establishing the norm of new media literacy of Singaporean students: Implications to policy and pedagogy. *Computers & Education, 124*, 1-13. https://doi.org/10.1016/j.compedu.2018.04.010

Chergarova, V., Arcanjo, V., Tomeo, M., Bezerra, J., Vera, L. M., & Uloa, A. (2022). Cryptocurrency fraud: A study on the characteristics of criminals who are using fake profiles on a social media platform to persuade individuals to invest into cryptocurrency. *Issues in Information Systems, 23*(3), 242-252. https://doi.org/10.48009/3_iis_2022_120

Childs, A. (2024). 'I guess that's the price of decentralisation… ': Understanding scam victimisation experiences in an online cryptocurrency community. *International Review of Victimology, 30*(3), 539-555. https://doi.org/10.1177/02697580231215840

Creswell, J. W., & Poth, C. N. (2016). Qualitative inquiry and research design: Choosing among five approaches. Sage Publications.

Dutta, A., Voumik, L. C., Ramamoorthy, A., Ray, S., & Raihan, A. (2023). Predicting cryptocurrency fraud using ChaosNet: The ethereum manifestation. *Journal of Risk and Financial Management, 16*(4), 216. https://doi.org/10.3390/jrfm16040216

Farell, R. (2015). An analysis of the cryptocurrency industry. *Wharton Research Scholars, 130*, 1-23.

Higbee, A. (2018). The role of crypto-currency in cybercrime. *Computer Fraud & Security, 2018*(7), 13-15. https://doi.org/10.1016/S1361-3723(18)30064-2

Jocson, K.M. (2015) New media literacies as social action: The centrality of pedagogy in the politics of knowledge production, *Curriculum Inquiry, 45*(1), 30-51. https://doi.org/10.1080/03626784.2014.982490

Kellner, D., & Share, J. (2007). Critical media literacy, democracy, and the reconstruction of education. In D. Macedo & S. R. Steinberg (Eds.), Media literacy: A reader (pp. 3–23). Peter Lang Publishing.

Kutera, M. (2022). Cryptocurrencies as a subject of financial fraud. *Journal of Entrepreneurship, Management and Innovation, 18*(4), 45-77.

Lee, L., Chen, D. T., Li, J. Y., & Lin, T. B. (2015). Understanding new media literacy: The development of a measuring instrument. *Computers & Education, 85*, 84-93.

Liu, Y., Tsyvinski, A., & Wu, X. (2022). Common risk factors in cryptocurrency. *The Journal of Finance, 77*(2), 1133-1177. https://doi.org/10.1111/jofi.13119

Long, S., Zhu, T., & Chen, X. (2023). With high new media literacy, can we prevent problematic internet use?--A case study of Chinese college students. *Digital Education Review, 44*, 33-44.

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

Martens, H., & Hobbs, R. (2015). How media literacy supports civic engagement in a digital age. *Atlantic Journal of Communication, 23*(2), 120-137. http://dx.doi.org/10.1080/15456870.2014.961636

Miller, S., Menard, P., & Bourrie, D. (2024). I'm not fluent: How linguistic fluency, new media literacy, and personality traits influence fake news engagement behavior on social media. *Information & Management, 61*(2), 103912. https://doi.org/10.1016/j.im.2023.103912

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Goldfeder, S. (2016), Bitcoin and cryptocurrency technologies: A comprehensive introduction, Princeton University Press

Park, S., Kim, E. M., & Na, E. Y. (2014). Online activities, digital media literacy and networked individualism of Korean youth. *Youth & Society*, *47*(6), 1–20. https://doi.org/10.1177/0044118X14561008

Perdana, A., & Jiow, H. J. (2024). Crypto-Cognitive Exploitation: Integrating Cognitive, Social, and Technological perspectives on cryptocurrency fraud. *Telematics and Informatics*, 102191. https://doi.org/10.1016/j.tele.2024.102191

Reddy, E., & Minnaar, A. (2018). Cryptocurrency: A tool and target for cybercrime. *Acta Criminologica: African Journal of Criminology & Victimology, 31*(3), 71-92.

Sanz-Bas, D., del Rosal, C., Náñez Alonso, S. L., & Echarte Fernández, M. Á. (2021). Cryptocurrencies and fraudulent transactions: Risks, practices, and legislation for their prevention in Europe and Spain. *Laws, 10*(3), 57. https://doi.org/10.3390/laws10030057

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).

Smith, S. S. (2018). How Cryptocurrencies Are Changing What CPAs Need to Know about Fraud Prevention. *Theoretical Economics Letters, 8*(14), 3252-3266. https://doi.org/10.4236/tel.2018.814201

Thoman, E., & Jolls, T. (2004). Media literacy: A national priority for a changing world. *American Behavioral Scientist, 48*(1), 18–29.

Tripathy, N., Balabantaray, S. K., Parida, S., & Nayak, S. K. (2024). Cryptocurrency fraud detection through classification techniques. *International Journal of Electrical and Computer Engineering (IJECE), 14(*3), 2918-2926. https://doi.org/10.11591/ijece.v14i3.pp2918-2926

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*, 1-35. https://doi.org/10.1186/s40163-021-00163-8

Xia, P., Wang, H., Zhang, B., Ji, R., Gao, B., Wu, L., ... & Xu, G. (2020). Characterizing cryptocurrency exchange scams. *Computers & Security, 98*, 101993. https://doi.org/10.1016/j.cose.2020.101993

Wątorek, M., Drożdż, S., Kwapień, J., Minati, L., Oświęcimka, P., & Stanuszek, M. (2021). Multiscale characteristics of the emerging global cryptocurrency market. *Physics Reports, 901*, 1-82. https://doi.org/10.1016/j.physrep.2020.10.005

Wu, S., & Chen, S. (2007). Media literacy education. Taipei, Taiwan: Chiuliu

Velani, J., & Patel, D. S. (2023). A review: Fraud prospects in cryptocurrency investment. *International Journal of Innovative Science and Modern Engineering, 11*(6), 1-4. https://doi.org/10.35940/ijisme.e4167.0611623

Zhang, H., Zhu, C., & Sang, G. (2014). Teachers' stages of concern for media literacy education and the integration of MLE in Chinese primary schools. *Asia Pacific Education Review, 15*(3), 459–471.

Financial disclosures

The author declared that this study did not receive any financial support.

Acknowledgements

The author have nothing to acknowledge of any persons, grants, funds, institutions.