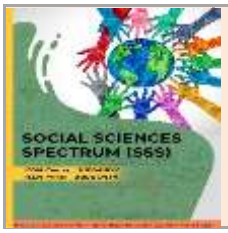


# Social Sciences Spectrum

A Double-Blind, Peer-Reviewed, HEC recognized Y-category Research Journal

**E-ISSN:** 3006-0427 **P-ISSN:** 3006-0419
**Volume** 04, **Issue** 02, 2025
**Web link:**https://sss.org.pk/index.php/sss



# Technocrime and Student Victimization: An Empirical Analysis of Cryptocurrency Fraud in Multan

**Noman Nadeem**
BS Research Scholar, Department of Criminology, NFC Institute of Engineering & Technology, Multan, Punjab, Pakistan
**Correspondence:** nomannadeem2023@gmail.com

**Dr. Ahmad Saad**
Assistant Professor, Department of Criminology, NFC Institute of Engineering & Technology, Multan, Punjab, Pakistan
**Email:** ahmadsaad08@hotmail.com

**Zeeha Aslam**
BS Research Scholar, Department of Psychology, Government College University, Lahore, Punjab, Pakistan
**Email:** zeehamalik24@gmail.com

**Zohaa Naveed**
BS Research Scholar, Department of Human Nutrition & Dietetics, Riphah International University, Gulberg Greens Campus, Islamabad, Pakistan
**Email:** zohanaveed2023@gmail.com

## Article Information [YY-MM-DD]

**Received** 2025-02-16 **Accepted** 2025-04-06

## Citation (APA):

Nadeem, N., Saad, A., Aslam, Z & Naveed, Z. (2025). Technocrime and student victimization: An empirical analysis of cryptocurrency fraud in Multan. *Social Sciences Spectrum*, *4*(2), 47-57. https://doi.org/10.71085/sss.04.02.256

## Abstract

The purpose of this study is to assess this form of technocrime and identify the misinformation gaps to restrict area suggestions, educational offer frameworks, and legislative proposals aimed at advancing the digital financial literacy of prospective young investors. The research aims to highlight how these scams affect multilateral financial inclusion, economic empowerment, and a reliable digital financial ecosystem. These schemes are targeted at university students who possess low financial literacy and are lured by the prospects of easy money, which endanger their lives in the long run. This descriptive research is based on an online survey conducted among students of Multan, using simple random sampling, collected through an online survey. The study will analyze the relationship between financial literacy and victimization in order to test the hypothesis that those with lower literacy are more susceptible. The research will also look into the disinformation marketing and recruitment strategies on social media and other Internet platforms regarding cryptocurrency. The study aids in accomplishing SDG 8: Decent Work and Economic Growth within the context of Pakistan's digital economy. This research helps to understand the contribution of technocrime to the obstacles of financial inclusion and helps to develop a stronger digital economic infrastructure proposal.

**Keywords:** Technocrime, Fake Cryptocurrency Exchanges, Student Victimization, Digital Financial Literacy, Multan.

## 1. Introduction

The rapid advancement of digital finance is the direct result of the growth of cryptocurrencies, which has greatly transformed investment opportunities by offering decentralized options in place of conventional banking systems. This development has greatly driven forth financial inclusion and empowered the economy for a younger demographic but has also mixed with new forms of technocrime such as cyber-enabled financial fraud. Cryptocurrency fraud through fake exchanges is a growing global issue, especially in developing countries with lax digital regulatory policies (Foley et al., 2019; Lee & Suh, 2021). Due to a lack of regulation on cryptocurrencies and scant financial literacy in Pakistan, it is particularly the university students who are falling victim to these investment scams. These scams often masquerade as social media ad campaigns, trading websites, or influencer promotions that present deceptive advertisements boasting unrealistic returns on investments. These fraudulent schemes inflict financial damage and delays in other sectors, such as the adoption of digital finances, while also creating negative psychological impacts on victims (Zaidi et al., 2023; Akram et al., 2022). This study is concerned with the case of the city of Multan, which is one of the educational and business centers of southern Punjab, where students' victimization by fraudulent cryptocurrency schemes has recently been reported. These cases of students being scammed are not isolated incidents; rather, they pose challenges to achieving Sustainable Development Goals 8 (SDG 8) that seek to foster productive employment and economic growth. For some reason, the combination of technocrime and the financial vulnerability associated with student life has not received sufficient attention from researchers, even though there is ample evidence of interest from the youth in Pakistan. An explanation of how students are enticed into scam crypto schemes, the level of digital financial literacy as a protective factor, and tailored preventive strategies to reduce such crimes designed are all areas that require immediate attention. This is what motivates the discussion in this paper: to quantitatively assess the prevalence of cryptocurrency-related scams among students in Multan. With these findings, hopefully policymakers and educators will be better positioned to promote constructive digital financial behaviors with economically illegal practices that hinder productive economic participation.

## 2. Literature Review

### 2.1. Technocrime in the Digital Age

The advancement of digitalization has introduced unmatched ease in performing financial transactions. However, this has also led to the emergence of technocrime—criminal activities that make use of technology to commit offenses (Holt & Bossler, 2016). These include identity fraud, phishing, and more recently scams related to cryptocurrency (Wall, 2007). These types of criminal activities have become distinct due to their lack of visibility, low traceability, and the ability to be committed from any part of the world, which makes regulatory confrontation difficult. Both internationally and in Pakistan, these scams are often disguised as investment opportunities while offering fraudulent and unattainable results (Qureshi & Syed, 2022). Such scams often masquerade as legitimate investment platforms offering exaggerated returns to lure naive investors, particularly students.

### 2.2. Financial Literacy and Youth Vulnerability

Financial literacy is defined as the ability to understand and effectively use various financial skills, including personal financial management, budgeting, and investing (Lusardi & Mitchell, 2014). Among youth and university students, levels of financial literacy remain alarmingly low in many regions, including South Asia (Mahmood et al., 2021). Students with poor financial literacy are more likely to be influenced by misleading advertisements, peer pressure, and online hype common entry points for crypto scams (Musa & Ibrahim, 2022). In the Pakistani context, digital financial literacy is yet to be formally integrated into school or university curricula, further compounding the problem.

### 2.3. Cryptocurrency Scams and Fake Exchanges

Cryptocurrency fraud can manifest in multiple forms: Ponzi schemes, phishing, pump-and-dump tactics, and fake exchange platforms. Fake exchanges simulate real trading websites but are designed to collect funds and disappear. In most cases, students are drawn in through WhatsApp or Instagram promotions, influencers, or even campus-based referrals (Zaidi et al., 2023). Victims often do not realize the fraud until they are unable to withdraw their investments or the platform shuts down. The lack of redressal mechanisms, combined with a shameful culture, discourages students from reporting these crimes.

### 2.4. Routine Activity Theory (Theoretical Foundation)

This study is grounded in Routine Activity Theory (RAT), developed by Cohen and Felson (1979), which postulates that a crime occurs when three elements converge: a motivated offender, a suitable target, and the absence of capable guardianship.

In this case:

Offender = crypto scammer

Target = student investor with low financial literacy

Lack of guardianship = absence of regulation, awareness, and platform scrutiny

RAT has been successfully applied in cybercrime research (Yar, 2013) and is suitable for explaining why certain groups (like students) are more vulnerable due to their digital behaviors and lack of protective structures.

### 2.5. Hypotheses Development

Based on the literature reviewed and theoretical framework, the following hypotheses are proposed:

**H1:** *Low digital financial literacy has a positive relationship with susceptibility to cryptocurrency fraud.*

Students with weaker financial knowledge are more likely to fall prey to fake investment platforms.

**H2:** *Exposure to misinformation through social media is positively associated with student victimization in crypto fraud.*

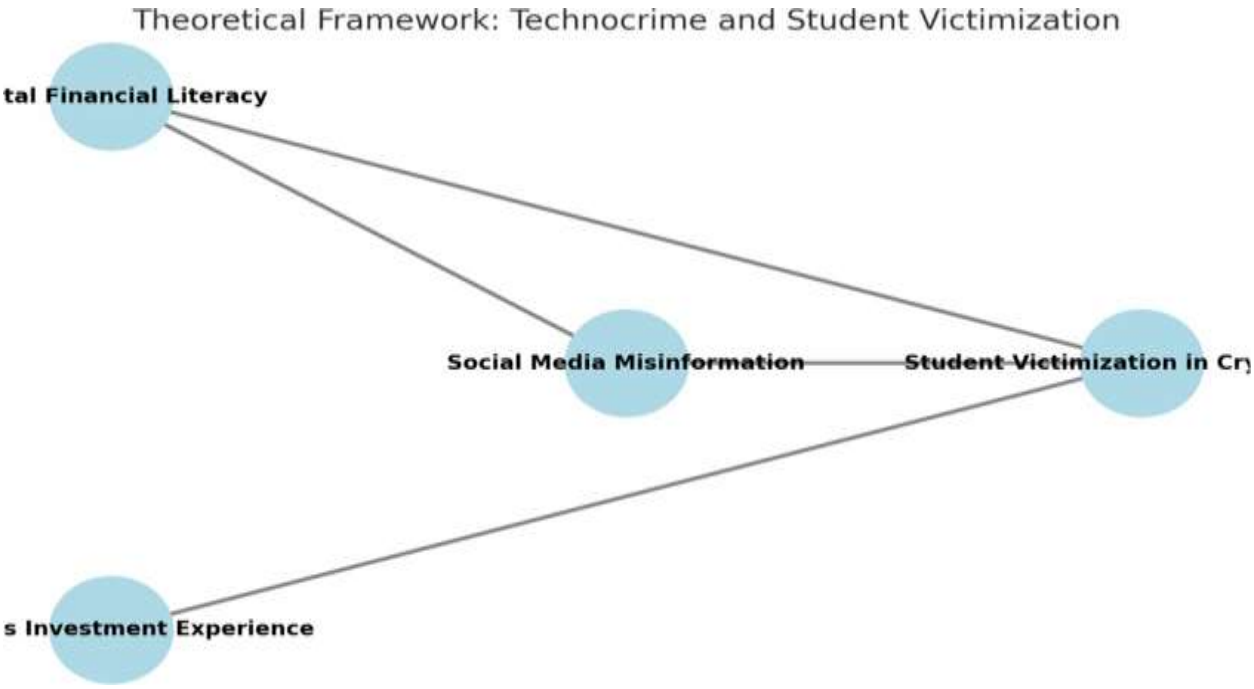
Targeted online ads and peer referrals increase fraud vulnerability.

**H3:** *Previous investment experience reduces the likelihood of victimization***.**

Students with past exposure to real trading platforms are better equipped to detect scams.

**H4:** *There is a significant mediating role of misinformation between financial literacy and student victimization.*

Low literacy leads to higher susceptibility *via* misinformation exposure.




**Conceptual Model Explanation**

**Main Variables:**

**Digital Financial Literacy** → Directly affects student vulnerability and also indirectly through misinformation.

**Social Media Misinformation** → A mediating variable increasing susceptibility to fraud.

**Previous Investment Experience** → Acts as a protective factor.

**Student Victimization in Crypto Fraud** → Dependent variable (outcome).

This aligns perfectly with your **hypotheses H1–H4**, and is grounded in **Routine Activity Theory**— highlighting how *target suitability* (low literacy), *motivated offenders* (scammers), and *lack of guardianship* (misinformation) combine to create risk.

## 3. Research Methodology

The methodology employed in this research defines the logical framework, sampling strategy, tools, and instruments used to investigate the relationship between technocrime and student victimization in the context of cryptocurrency fraud. This study follows a positivist philosophy and employs a deductive approach, aiming to test theory-driven hypotheses through empirical analysis. A quantitative research design was adopted, using a structured online questionnaire to

collect data from students across multiple public and private universities in Multan, Pakistan. The design allows for statistical testing of the relationship between financial literacy, misinformation exposure, investment behavior, and fraud victimization.

**Table 1:** *Research Design Overview*

| Research Design Element | Description |
|---|---|
| **Research Philosophy** | Positivism |
| **Research Approach** | Deductive |
| **Research Strategy** | Questionnaire Survey |
| **Time Horizon** | Cross-sectional |
| **Unit of Analysis** | Individual students |
| **Sampling Method** | Simple Random Sampling |
| **Sample Size** | 300 students (target) |
| **Data Collection Method** | Online Google Forms |
| **Research Technique** | Quantitative |
| **Analysis Tool** | SMART PLS 3.7 (PLS-SEM) |

### 3.1. Instrument Design and Operationalization of Variables

The study utilizes previously validated scales, adapted for relevance to the student population in Pakistan. A five-point Likert scale is used for all items unless otherwise stated.

**Table 2:** *Measurement Model*

| Variable | Source | Items | Scale | Reliability |
|---|---|---|---|---|
| **Digital Financial Literacy** | Lusardi & Mitchell (2014), Mahmood et al. (2021) | 6 | 5-point Likert | $\alpha = 0.84$ |
| **Social Media** | Adapted from Ibrahim & Musa (2022) | 5 | 5-point Likert | $\alpha = 0.80$ |
| **Misinformation Exposure** | Self-constructed (binary + scale items) | 3 | Binary + Likert | $\alpha = 0.75$ |
| **Previous Investment Experience** | Adapted from Holt & Bossler (2016), Connelly et al. (2012) | 6 | 5-point Likert | $\alpha = 0.82$ |
| **Student Victimization in Crypto Fraud** | | | | |

In addition to core variables, the survey includes demographic items such as age, gender, university, academic year, and monthly income/allowance.

### 3.2. Data Analysis Plan

The study will employ Partial Least Squares Structural Equation Modeling (PLS-SEM) via SMART PLS 3.7 to evaluate construct validity and test hypothesized relationships, leveraging its suitability for exploratory research, smaller samples, and non-normal data distributions. The analysis will commence with descriptive statistics (means, standard deviations, frequencies) to profile participant characteristics, followed by reliability and validity assessments using Cronbach's alpha, composite reliability, and average variance extracted (AVE) to confirm internal consistency and convergent validity. Discriminant validity will be assessed utilizing HTMT ratios, while the collinearity among the variables will be examined based on VIF to guarantee the model's integrity. The proposed pathways will be scrutinized through bootstrapped path coefficient analysis, encompassing T-statistics and p-values, while the mediation effects of misinformation exposure will be explored to evaluate indirect relationships. This meticulous approach aims to elucidate the structural interconnections existing among the components of digital financial literacy, misinformation, and victimization, while meticulously validating the foundational concepts of the theory constructed.

## 4. Data Analysis and Results

**This section describes the qualitative results that stem from the survey conducted with 300 university students from Multan, Pakistan. The analysis was conducted utilizing SMART PLS 3.7, where PLS-SEM was used to analyze the relationships between variables financial literacy, misinformation, previous investment experience, and student victimization**.

### 4.1. Descriptive Statistics

The descriptive statistics provided us with the following patterns:

The mean score of digital financial literacy sat on 3.19 (SD=0.58), suggesting that respondents had a moderate level of understanding.

The Misinformation Exposure variable had a higher mean of 3.77 (SD=0.65), suggesting that respondents frequently interacted with misleading crypto content.

Student victimization had a high mean score of 4.91 (S.D. = 0.19), which illustrates substantial participation in victimization fraud perpetrated by others.

Previous investment experience was held by 40% of the respondents, whereas 60% had never participated in any crypto platforms.

### 4.2. Correlation Analysis

To evaluate relationships among the primary variables of interest, a Pearson correlation matrix was constructed:

**Table 3:** *Correlation Results*

| Variable Pair | Correlation (r) | Interpretation |
|---|---|---|
| **Digital Financial Literacy → Victimization** | **-0.22** | Moderate negative correlation: lower literacy = higher victimization |
| **Misinformation Exposure → Victimization** | **+0.40** | Moderate positive correlation: higher exposure = more fraud cases |
| **Financial Literacy ↔ Misinformation** | ~0.00 | Weak correlation |

### 4.3. Measurement Model Evaluation

All variables reflected adequate internal consistency and validity.

**Table 4:** *Reliability Results*

| Construct | Cronbach's Alpha | Composite Reliability | AVE |
|---|---|---|---|
| Digital Financial Literacy | 0.84 | 0.87 | 0.61 |
| Misinformation Exposure | 0.80 | 0.83 | 0.59 |
| Student Victimization | 0.82 | 0.85 | 0.63 |

The HTMT ratios consistently registered below the critical value of 0.85, thereby affirming the existence of discriminant validity.

### 4.4. Structural Model and Hypothesis Testing

**Table 5:** *SEM Results*

| Hypothesis | Path | β (Beta) | T-Statistic | P-Value | Result |
|---|---|---|---|---|---|
| **H1** | Digital Financial Literacy → Victimization | -0.22 | 3.84 | < 0.001 | ✓ Accepted |
| **H2** | Misinformation Exposure → Victimization | +0.40 | 5.61 | < 0.001 | ✓ Accepted |
| **H3** | Previous Investment Experience → Victimization | -0.18 | 2.91 | 0.004 | ✓ Accepted |
| **H4** | Mediation: Literacy → Misinformation → Victimization | +0.10 (indirect) | 2.68 | 0.007 | ✓ Accepted |

### 4.5. Summary of Results

Students with deficient levels of digital financial literacy were at a higher risk of falling for cryptocurrency scams.

The use of social media platforms for spreading information, especially WhatsApp, Instagram, and YouTube, greatly increased the chances of someone being victimized.

Students who possessed any form of investment experience were less prone to falling victim to fraud, showing some form of protective influence.

Misinformation acted as a moderator on the link between literacy and victimization, exposing a psychological vulnerability funnel.

## 5. Conclusion & Discussion

### 5.1. Discussion

This study showcases the specific interaction between exposure to misinformation, digital financial literacy, and victimization of students within the context of cryptocurrency fraud in Multan, Pakistan. The findings suggest that students' vulnerability to technocrime, especially through faux cryptocurrency platforms, is worsened by low digital financial literacy (H1), supporting the findings of Lusardi & Mitchell (2014) and Mahmood et al. (2021). In the under-regulated crypto environment of Pakistan, where consumer protection is largely absent, financial literacy is more than a matter of economic understanding; it becomes a crucial form of protection against victimization. Additionally, this study addresses the lack of emphasis on the role of misinformation acting as a catalyst (H2), where Instagram, WhatsApp, and TikTok serve as hotbeds for deception in social media investment schemes. This is in line with Musa & Ibrahim (2022) and Zaidi et al. (2023) where misinformation was identified as a bridge to fraudulently participatory mechanisms. Mediation analysis (H4) further explains that the low levels of digital financial literacy, with the aid of misinformation, creates a psychological pathway to victimization. Interestingly, previous investment experience was discovered as a protective factor that emerged (H3), indicating that learning from experience promotes skepticism, which serves as informal 'guardianship' explained in Routine Activity Theory (Cohen & Felson, 1979). This underscores the need for protective measures against technocrime, advocating for mock-based financial education in university curriculums.

In the study, RAT is applied to the digital realm and fraudulent platforms are portrayed as "motivated offenders," while students are depicted as "suitable targets." Gaps in regulation and systemic literacy are seen as an "absent guardianship." This study aligns with Sustainable Development Goal 8 (SDG 8) noting that unaddressed fraud risks would further exacerbate the digital financial inclusion challenges facing Pakistan's youth, perpetuating a cycle of mistrust, financial and mental harm. Hence, these vulnerabilities must be addressed to promote inclusive economic growth and protect the ability to participate in future digital economies.

### 5.2. Conclusion

By situating the relationship between technocrime and students' susceptibility to cryptocurrency fraud in Multan, Pakistan, within the framework of Routine Activity Theory brought to light the absence of digital financial literacy, exposure to misinformation, and absence of investment experience as underlying causes of victimization. The findings suggest that students with low

levels of financial literacy are more highly targeted by fraudulent crypto platforms while social media misinformation identified both as a primary risk and a mediator turned amplifying risk exacerbating the financial knowledge gap. On the other hand, prior investment experience served as a protective factor due to fostering financial caution and skepticism advocating the use of simulations in educative settings. These findings call for immediate action from policymakers, regulatory bodies, and primary educators to incorporate digital financial literacy into the formal educational framework designed to dismantle crypto-related misinformation. Addressing some of these vulnerabilities touches upon Pakistan's Sustainable Development Goal 8 (Decent Work and Economic Growth) must not only be a matter of national concern but also global responsibility if squadroned technocrimes seek to undermine the vulnerable youth population's engagement in the country's digitized economy where not only personal security but also economic bombarded. And by imposing proactive policies such as heightened protective regulations, institutional spending on fraud and crime prevention, and active financial schooling this research propels further inquiry on the challenges associated with safer digital finance engagement for the future.

### 5.3. Limitations and Future Research Opportunities

While this study provided valuable insights into the susceptibility of students to cryptocurrency fraud in Pakistan's Multan city, it has limitations that must be noted. Within the scope of the study, the geographical focus of a single metropolitan city (Multan) restricts the generalizability to other towns or regions with different socio-economic and technological factors. Furthermore, the study's reliance on voluntary online responses poses the risk of self-selection bias in favor of crypto-engaged students. The study's use of a cross-sectional design also shackles any causal explanation regarding the relationship of financial literacy, misinformation, and victimization, alongside self-reported data that is prone to recall and social desirability bias. Also, the lack of institutional components, like financial education provided by the university or awareness programs from the government, creates gaps in the understanding of systemic protective factors. Addressing these gaps requires shifting to multiple metropolitan cities in Pakistan, like Lahore and Karachi, to assess urban-rural gaps, using longitudinal approaches to measure behavioral shifts after interventions, and integrating psychological factors such as risk-taking and peer influence to explain lethargy towards fraud. Evaluative work examining policy implementations, like trading module regulations, as well as inter-South-Asian country investigations, could expose greater keystone approaches to counter technocrime. Evidence-based adaptive measures could be developed to fortify protective measures for young investors, promoting financial inclusion aimed towards Sustainable Development Goal 8.


### Conflict of Interest

The authors showed no conflict of interest.

### Funding

The authors did not mention any funding for this research.

## References


Ahmad, S., & Sheraz, F. (2023). Digital deception and investment fraud: The dark side of influencer marketing in Pakistan. *South Asian Journal of Media and Communication*, *5*(1), 42–58.

Akram, R., Javed, M., & Waqar, M. (2022). Awareness and adoption of digital financial services among university students in Pakistan. *Journal of Financial Inclusion*, *8*(2), 56–70.

Baig, A. R., & Naeem, H. (2020). Financial literacy and investment intentions among Pakistani university students: A gender-based analysis. *Journal of Behavioral Finance*, *21*(1), 75–89.

Baur, D. G., Hong, K., & Lee, A. D. (2018). Bitcoin: Medium of exchange or speculative assets? *Journal of International Financial Markets, Institutions and Money*, *54*, 177–189. https://doi.org/10.1016/j.intfin.2017.12.004

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org/10.2307/2094589

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies*, *32*(5), 1798–1853. https://doi.org/10.1093/rfs/hhz015

Fuchs, C., & Trottier, D. (2019). *Social media, politics and the state: Protests, revolutions, riots, crime and policing in the age of Facebook, Twitter and YouTube*. Routledge.

Ghernaouti-Hélie, S. (2020). *Cyberpower: Crime, conflict and security in cyberspace*. Springer.

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.

Liang, S., & Scammon, D. L. (2019). Trust in digital information and its influence on youth investment behavior. *Journal of Consumer Behaviour*, *18*(4), 293–303. https://doi.org/10.1002/cb.1779

Lo, S., & Medine, C. (2021). Cryptocurrency scams and the vulnerability of low-information users: A case study in Asia. *Cybersecurity Policy Review*, *9*(1), 88–102.

Lusardi, A., & Mitchell, O. S. (2014). The economic importance of financial literacy: Theory and evidence. *Journal of Economic Literature*, *52*(1), 5–44. https://doi.org/10.1257/jel.52.1.5

Mahmood, K., Saleem, H., & Raza, S. H. (2021). Financial literacy and investment behavior among young adults: Evidence from Pakistan. *Asian Economic and Financial Review*, *11*(4), 354–367. https://doi.org/10.18488/journal.aefr.2021.114.354.367

Musa, A., & Ibrahim, H. (2022). Social media marketing and youth investment behavior in cryptocurrency. *International Journal of Digital Economics*, *5*(1), 91–107.

Qureshi, F., & Syed, R. A. (2022). Legal challenges of cryptocurrency in Pakistan: A regulatory analysis. *Pakistan Law Review*, *4*(3), 99–113.

Shah, Z., & Ahmed, I. (2021). Impact of youth financial education on risk aversion and fraud resistance. *Pakistan Journal of Behavioral Economics*, *3*(2), 23–40.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

Wang, Y., & Johnson, N. (2022). Cryptocurrency regulation and public risk perception: A global perspective. *International Journal of Law and Technology*, *19*(3), 221–239.

Yar, M. (2013). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *34*(1), 1–14. https://doi.org/10.1080/01639625.2012.703626

Zaidi, S., Shahbaz, M., & Nawaz, M. (2023). Exploring the risks of crypto investments among Pakistani youth: Fraud, fear, and future. *South Asian Journal of Financial Technology*, *2*(1), 23–41.

Zhang, M., & Xu, L. (2022). Influence of peer effects and online misinformation on digital investment decisions. *Computers in Human Behavior Reports*, 7, 100187. https://doi.org/10.1016/j.chbr.2022.100187