Behavioural Dimensions of Cybersecurity and Cryptocurrency Investment Frequency in Nigeria: An Empirical Investigation

Stephen Alaba John
Department of Finance, Kwara State University, Malete, Nigeria
https://orcid.org/0000-0001-5564-7918

Chigozie Kingsley Ejeofobiri
Department of Computer Science and Digital Technologies, University of East London, London, UK.
https://orcid.org/0009-0008-1495-1858

Oluwadamilola Adeleke
Department of Neuroscience, Rush University Medical Center, USA

Ibukun Koleoso
Business Administration, INSEAD, France
https://orcid.org/0009-0005-7007-3357

ThankGod Lawrence
Department of Finance, American University, USA

Kehinde Oluwasayo Akinola
Department of Computer Science, East Carolina University, USA

ABSTRACT
As cryptocurrency adoption has grown, so too has investor participation, with millions of retail and institutional investors engaging in digital asset trading across exchanges worldwide. However, cryptocurrency market, despite its technological foundation, remains highly vulnerable to cybersecurity threats, hacking incidents, phishing attacks, exchange breaches, and wallet thefts which have led to the loss of billions of dollars globally. This study investigates the effect of cybersecurity-related factors on cryptocurrency investment frequency. Specifically, the study provides a behavioural-finance lens for understanding how cybersecurity perceptions shape investment decisions in the cryptocurrency market. The study adopted a quantitative, cross-sectional survey approach involving 384 active cryptocurrency investors, consisting of Students, Self-employed/Entrepreneur, Public Sector Employees, Private Sector Employee, and Unemployed. Data were analyzed using multiple regression model. The results show that Perceived Cybersecurity ($\beta = 0.284$, $t = 3.94$, $p < 0.05$), Platform Security Features ($\beta = 0.217$, $t = 3.19$, $p < 0.05$) and Trust in platform security ($\beta = 0.298$, $t = 4.03$, $p < 0.05$) have significant positive effects on cryptocurrency investment frequency. This indicates that investors are more willing to trade actively when they perceive strong protective measures and reliable security mechanisms within trading platforms. In contrast, previous exposure to cybersecurity incidents ($\beta = -0.153$, $t = -2.51$, $p < 0.05$) has significant negative effect on cryptocurrency investment frequency, suggesting that negative experiences with cyber breaches or fraud reduce investors' willingness to invest frequently in cryptocurrencies. The study concludes that improving cybersecurity perceptions is pivotal to driving sustained investor engagement in cryptocurrency markets. Practically, the study suggests the need for cryptocurrency platforms to enhance their security infrastructures, promote transparency, and foster trust, while policymakers should develop regulatory frameworks to mitigate cyber risks.

Keywords
Cryptocurrency, Cybersecurity, Perceived Risk Theory, Behavioural Finance, Investment Frequency

1. INTRODUCTION
The global financial landscape has been significantly transformed by the emergence of cryptocurrencies and blockchain-based digital assets (Ciesielska-Maciągowska & Spyra, 2025). Flagship cryptocurrencies like Bitcoin started off with a value of less than a penny and reached its historical high of more than $120,000 (CoinMarketCap, 2025; Angeles, 2024). Bitcoin's success since 2009 has startled the financial sector and led to the development of thousands of other cryptocurrencies referred to as altcoins (McGovern, Thomas, 2022). As of the fourth quarter 2024, over 23,000 cryptocurrencies exist with a combined market capitalization exceeding USD 2 trillion (CoinMarketCap, 2024). Thus, the development of cryptocurrencies has initiated the creation of exchange systems that act as intermediaries in the trading of digital assets and cryptocurrency wallets that allow for the storage of tokens with varying levels of security and the required level of user experience and knowledge (Sharma & Yadav, 2024; Taylor et al., 2022).

As cryptocurrency adoption has grown (Qi et al., 2025), so too has investor participation (Botha et al., 2025), with millions of retail and institutional investors engaging in digital asset trading (Yang et al., 2022) across exchanges like Binance, Coinbase, Kucoin, Gate, Bybit, Uniswap, Pancakeswap, among others have consistently reaffirmed their crucial role in the crypto ecosystem (McDevitt, 2025; Barbon, Ranaldo, 2023). Nevertheless, studies reveal significant user concerns regarding the security and privacy of cryptocurrency market, directly impacting investment decision (Herskind et al., 2020; Tam et al., 2020). Security and privacy are fundamental to sustaining trust and satisfaction in cryptocurrency trading activities (Gan & Lau, 2024; Sentana et al., 2023).

However, this rapid growth has also brought considerable challenges, chief among them, the issue of cybersecurity (Ciesielska-Maciągowska & Spyra, 2025). The cryptocurrency market, despite its technological foundation, remains highly vulnerable to cyber threats. Hacking incidents, phishing attacks, exchange breaches, and wallet thefts have led to the loss of billions of dollars in investor assets globally (Julakanti,

2025; Greubel et al., 2023; Alqahtani & Sheldon, 2022). The inability to trace fund movements complicates the process of identifying criminals by law enforcement. For instance, the Hong Kong-based cryptocurrency exchange platform CoinEx lost $70 million in cryptocurrency due to a cyber-attack in September 2023 (Kovalchuk et al., 2024; Crypto Crime Trends, 2023).

These security breaches not only erode investor wealth but also damage confidence in the entire cryptocurrency ecosystem. According to "The 2023 Crypto Crime Report" by Chainalysis, cryptocurrency-related crime set a record in 2022. The volume of illegal transactions with cryptocurrency reached $20.1 billion compared to $18 billion in 2021. Similarly, Crypto Crime Annual Report (2022), the top 10 countries for cryptocurrency crime in 2022 (fraud by totals) are as follows: North Korea, United States, Russia, China, United Kingdom, Japan, Hong Kong, Canada, British Virgin Islands, and Seychelles (Crypto Crime Trends, 2023; Crypto Crime Trends, 2022; Murphy, 2022).

Unlike traditional financial markets, which benefit from regulatory safeguards, deposit insurance, and institutional protection, many crypto platforms operate under loose or non-existent regulatory oversight, further heightening perceived risks among investors (Lynn, 2024). In the volatile and risk-laden environment which makes cryptocurrency investment risky for investors with lower tolerance for financial uncertainty (Ahmmed et al., 2025), cybersecurity and the absence of robust investor protections have become defining factors influencing investor behaviour and investment frequency (Hayashi & Routh, 2024).

Cryptocurrency investment is shaped not only by rational assessments of risk and return but also by psychological, perceptual, and behavioural factors (Zhafira & Pramono, 2025). Ramashar et al. (2022) argue that psychological factors may play a significant role in investment decision-making. Firdaus et al. (2022) opine that investment decisions are often based on others' actions or market rumors rather than objective information or fundamental factors of digital assets. Rahayu et al. (2020) add that investment decisions are frequently influenced by irrational factors, such as incomplete information, limited analytical skills, and the urgency to act quickly to avoid missing opportunities.

In the cryptocurrency space, where market fluctuations are extreme and regulation is limited (Raza et al., 2023; Al-Shboul et al., 2023), investing in cryptocurrency is particularly sensitive to external cues such as news of cyber breaches or the presence of strong security protocols on investment platforms (Qi et al., 2025; Sukumaran et al., 2023). Thus, cyber-related behavioural factors such as perceived cybersecurity, trust in platform security, previous exposure to cyber incidents, and the presence of robust platform security features may explain how frequently and confidently individuals invest in cryptocurrencies. Some investors may respond to strong cybersecurity assurance with increased investment activity, while others, especially those who have experienced cyber breaches at one point or the other, may become risk-averse, investing less frequently or exiting the market altogether.

Existing studies such as Zhafira and Pramono (2025), Botha et al. (2025), Laki-laki et al. (2025), on cryptocurrency adoption have often focused on herding behaviour, price volatility, regulatory uncertainty, or financial literacy. However, limited empirical studies has examined how digital asset security and investor trust influence investment frequency, particularly from a behavioural perspective. The concept of perceived risk, drawn from Perceived Risk Theory, suggests that investors weigh potential threats heavily in their decision-making, often avoiding participation when risks are high or unknown. Similarly, the Technology Acceptance Model (TAM) highlights the importance of perceived ease of use and security in the adoption of new technologies, such as crypto trading platforms. Finally, Behavioural Finance Theory offers insights into how psychological factors such as fear, confidence, and past experience shape investment patterns in high-risk environments.

Given the increasing frequency of cyber incidents (Gürsoy, 2025; Julakanti, 2025; Sharma & Yadav, 2024) in the crypto space and the growing participation of individual investors, it is crucial to understand how security-related factors influence investment frequency. This study, therefore, aims to investigate the behavioural impact of cybersecurity on cryptocurrency investment frequency. This study addresses a critical gap in cryptocurrency literature by exploring the intersection of behavioural dimensions of cybersecurity and cryptocurrency investment frequency, offering practical insights for platform developers, regulators, and investors seeking to navigate the complex and rapidly evolving world of digital assets. As such, this study contributes to both academic discourse and policy discussions around investor protection, platform design, and cybersecurity regulation in the digital finance ecosystem.

2. LITERATURE REVIEW

According to Shaik et al. (2022), an investment refers to a financial asset purchased to generate income or to be traded at a higher value in the future. Investment frequency refers to the regularity with which an investor engages in buying or selling financial assets over a specific period (Chen et al., 2021). It reflects how often investors participate in trades, which is a direct measure of their behavioural engagement. Investment frequency is influenced not only by economic factors such as price volatility and expected returns but also by psychological and technological factors such as trust, perceived risks, and platform security (Ahmad & Shah, 2020; Rahayu et al., 2020; Corbet, Lucey & Yarovaya, 2019). Thus, it serves as a practical proxy for investor behaviour in volatile and high-risk digital asset markets.

The security of digital assets remains a critical concern for investors, particularly given the history of high-profile cyberattacks targeting cryptocurrency exchanges and wallets. Perceived cybersecurity risk influences investment decisions, as outlined in Perceived Risk Theory. Even when objective security measures exist, the subjective perception of risk can deter investment or reduce trading frequency. Studies have shown that investors who perceive higher cybersecurity risks tend to adopt more conservative strategies or refrain from investing altogether (Gupta et al., 2020).

Perceived cybersecurity refers to an investor’s subjective evaluation of the safety and resilience of cryptocurrency platforms against cyber threats such as hacking, phishing, and malware. While objective security measures may exist, perceptions often drive decision-making more strongly than actual risk. Investors who perceive higher cybersecurity risks tend to reduce their trading activity or adopt conservative strategies, highlighting the importance of perception as a determinant of behaviour in cryptocurrency investment (Gupta et al., 2020).

Platform security features represent the visible and functional safeguards integrated into cryptocurrency exchanges and wallets, including two-factor authentication, encryption, cold storage, and regulatory compliance mechanisms. These

features signal trustworthiness and reliability, which in turn influence investor confidence and engagement. Studies show that strong and well-communicated platform security features enhance adoption and retention, whereas weak or opaque measures discourage trading activity (Li et al., 2020).

Previous exposure to cybersecurity incidents refers to an investor's direct or indirect experience with security breaches, hacks, or fraud involving digital assets. Such experiences shape behavioural responses through fear, caution, and loss aversion, as explained by Behavioural Finance Theory. Research shows that victims of cyberattacks or those aware of major hacks often reduce their trading frequency, withdraw from platforms, or switch to alternatives perceived as more secure. This variable captures the long-term psychological and behavioural impact of security breaches on investors.

Trust in platform security is defined as an investor's belief in the reliability, competence, and integrity of cryptocurrency platforms to protect their assets and personal data. Trust is critical in technology adoption, particularly in high-risk environments like cryptocurrency markets. Studies show that higher trust reduces perceived risk and increases investment frequency, while low trust, often caused by past breaches or weak communication of security measures, discourages engagement (Wang et al., 2019).

Theoretical Framework

Perceived Risk Theory

Perceived Risk Theory, introduced by Bauer (1960), emphasizes that individuals make decisions based not only on objective risk but also on how they subjectively perceive those risks. Risk perception spans multiple dimensions, including financial, performance, social, psychological, and security risks. In the context of cryptocurrency, security risk is especially critical due to the digital and decentralized nature of assets, where vulnerabilities such as hacking, phishing, and wallet theft are common. For investors, perceived cybersecurity directly influences their investment frequency, as fear of potential losses or breaches may reduce trading activity or prevent participation altogether. Similarly, the visibility of platform security features such as two-factor authentication, encryption, and cold storage mitigates perceived risk, increasing investor confidence and participation. Hence, this theory underpins the relationship between perceived cybersecurity, platform security features, and investment frequency. Lower perceived risks, often achieved through transparent and guaranteed cybersecurity practices, encourage more frequent investment activity (Gupta et al., 2020).

Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM), developed by Davis in 1989, explains the determinants of technology adoption and usage. The model identifies two key constructs: Perceived Usefulness (PU), the extent to which technology improves user performance, and Perceived Ease of Use (PEOU), the degree to which technology is user-friendly and requires minimal effort. In subsequent extensions of TAM, trust and security perceptions have been incorporated as critical determinants of adoption in online financial platforms (Julakanti, 2025; Juma'h et al., 2025).

TAM suggests that investors' adoption and continued use of trading platforms depend not only on functional ease but also on trust in platform security. Robust security features, such as insurance against breaches, regulatory compliance, and authentication protocols, enhance both perceived ease of use and usefulness by creating a secure, reliable trading environment. Thus, the trust in platform security acts as a mediating factor that encourages higher investment frequency. Conversely, poorly designed or insecure platforms create friction, reducing both adoption and trading activity. In this study, TAM provides a framework for examining how security-enhancing features drive investor confidence and participation in cryptocurrency markets (Julakanti, 2025; Juma'h et al., 2025).

Behavioural Finance Theory

While Perceived Risk Theory and TAM emphasize rational and cognitive aspects of decision-making, Behavioural Finance Theory (BFT) highlights the psychological and emotional dimensions that shape investor behaviour. Traditional finance assumes rational investors who maximize returns while minimizing risk, but behavioural finance demonstrates that decisions are often influenced by cognitive biases, heuristics, and emotional reactions (Zhafira & Pramono, 2025; Ahmmed et al., 2025).

In cryptocurrency markets, these biases become especially pronounced due to high volatility, weak regulation, and frequent cybersecurity threats. Previous exposure to cybersecurity incidents (personal or indirect) can trigger loss aversion, where investors become overly cautious or withdraw entirely from the market (Laki-laki et al., 2025). Similarly, widespread reports of breaches may induce herd behaviour, where investors collectively engage in panic selling, regardless of individual exposure. On the other hand, overconfidence bias may lead some investors to underestimate risks if they perceive platforms as highly secure, resulting in excessive trading or speculative investments (Laki-laki et al., 2025; Zhafira & Pramono, 2025).

Together, these three theories provide a comprehensive framework for understanding how guaranteed cybersecurity influences cryptocurrency investment behaviour. Perceived Risk Theory explains how subjective risk perception shapes investment activity. TAM highlights the role of platform design, ease of use, and trust in shaping technology adoption and trading behaviour. BFT adds depth by accounting for emotional and psychological biases, particularly the impact of previous exposure to cyber incidents. Integrating these perspectives allows this study to investigate how cybersecurity concerns, through perceptions, platform features, and behavioural responses, determine investment frequency in the cryptocurrency market.

Review of Related Literature

The growth of cryptocurrency markets has attracted increasing attention from both scholars and practitioners, particularly regarding how cybersecurity, digital asset security, and behavioural dynamics shape investor participation. Several strands of literature inform the present study, including research on the role of cybersecurity, investor attitudes and behavioural tendencies.

Sharma and Yadav (2024) explored the attitudes and behaviours of retail investors in India toward cryptocurrency by surveying 200 equity market participants. Their findings revealed that while awareness of cryptocurrency is relatively high, actual participation remains limited due to concerns about risk and security. They highlighted that perceived ease of use and perceived benefits significantly influence investor attitudes and behavioural intentions. Interestingly, vulnerability did not shape attitudes but did affect behavioural intentions, suggesting that risk perceptions, particularly security-related risks, are critical in driving actual investment behavior.

Gürsoy (2025) examined the impact of cyber incidents on

Metaverse coin prices and trading volumes using event study and impulse response analysis. Results demonstrated that cybersecurity events such as the Coincheck hack and Ronin breach led to significant short-term declines in both price and trading volume, highlighting the material consequences of breaches for investor confidence. Similarly, Botha, Singh, and Leenen (2025), through a case study of the fraudulent Elite-Bit trading platform, revealed the devastating consequences of weak security and scams, underscoring the urgent need for robust regulation and investor protection.

The intersection between regulation and economic implications has also been examined. Laki-laki et al. (2025) conducted a systematic review on cryptocurrency in Indonesia and identified tensions between regulatory bodies: Bank Indonesia's stability-oriented approach contrasted with the Ministry of Trade's growth perspective. These conflicting stances not only heightened uncertainty but also amplified concerns over volatility and cybersecurity risks. Their findings underscore the importance of regulatory clarity in fostering investor confidence.

From a technological standpoint, Julakanti (2025) emphasized the transformative role of artificial intelligence in digital asset security. By leveraging machine learning and neural networks, AI-driven systems can detect fraud, analyze vulnerabilities, and respond to threats more effectively than traditional approaches. Such innovations promise stronger protection of digital assets and greater resilience against cyberattacks, thereby potentially enhancing investor trust in cryptocurrency platforms. Complementing this, Juma'h, Alnsour, and Kartal (2025) analyzed over 64,000 user reviews of cryptocurrency mobile applications and found that perceived security and privacy strongly influenced user satisfaction and app ratings, with robust security features boosting adoption.

Beyond security concerns, several studies highlight behavioural and psychological factors in cryptocurrency investment. Qi, Zhang, and Ouyang (2025) examined advisory information sources in the U.S. and revealed that reliance on financial advisors decreased crypto investment, while dependence on media and social networks significantly boosted both current investments and future intentions. This reflects the powerful influence of trust and confidence in external information sources. Similarly, Zhafira and Pramono (2025) found a strong positive relationship between herding behaviour and cryptocurrency investment decisions in Indonesia, demonstrating that many investors follow market trends rather than making independent evaluations. Behavioural biases also surface in more specific investment contexts: Ahmmed, Boadi, and Guillemette (2025) showed that investors engaging in margin trading were significantly more likely to invest in cryptocurrency, consistent with behavioural finance theory that associates higher risk-taking with cognitive biases.

3. METHODOLOGY

This study adopts a quantitative research design using a cross-sectional survey approach to examine the influence of cybersecurity factors on investment frequency among cryptocurrency investors. The quantitative method allows for the systematic measurement of variables and testing of hypothesized relationships between perceived cybersecurity, platform security features, previous exposure to cybersecurity incidents, trust in platform security, and investment frequency.

The population for this study comprises individual cryptocurrency investors who have actively traded in cryptocurrencies within the past 12 months. The population is geographically limited to Nigeria to provide contextual relevance. A purposive sampling technique was employed to select respondents who meet the inclusion criteria. This non-probability sampling approach is appropriate due to the specialized nature of the population and the difficulty in accessing a comprehensive sampling frame. Data were collected through online cryptocurrency communities and social media groups (Telegram, WhatsApp, X/Twitter, and Reddit). The sample size was determined using the Cochran formula for sample size calculation.

Table 1: Inclusion and Exclusion Criteria

S/N	Inclusion Criteria	Exclusion Criteria
1.	Are Nigerian residents aged 18 years and above	Represent institutional investors (e.g., banks, hedge funds, corporate investment firms)
2.	Have actively traded cryptocurrencies within the past 12 months	Have not engaged in any cryptocurrency trading or investment activity in the last 12 months
3.	Provided informed consent to voluntarily participate in the study	Declined to provide informed consent or withdrew during the data collection process.

Source: Authors

Sample Size Determination

To determine the minimum sample size required for proportion-based estimates when the population size is large or unknown, this study applies Cochran's (1977) formula:

$$n_0 = \frac{Z^2 p(1-p)}{e^2}$$

where; n_0 = required sample size for an effectively infinite population, Z = z-score corresponding to the desired confidence level (e.g., 1.96 for 95% confidence), p = estimated proportion of the attribute present in the population, 1 – p = complement of p, and e = desired margin of error (precision), expressed as a proportion.

Given the absence of a reliable prior estimate of the true proportion among Nigerian individual crypto investors, we adopt the conservative p = 0.50 (maximizes variance and hence yields the largest required n_0). With a 95% confidence level (Z=1.96) and a 5% margin of error (e=0.05):

$$n_0 = \frac{(1.96^2)\ x\ 0.5(0.5)}{0.05^2}$$

$$n_0 = \frac{3.8416\ x\ 0.25}{0.0025}$$

$$n_0 = \frac{30.9604}{0.0025} = 384$$

Thus, the minimum recommended sample is 384 respondents.

Data were collected using a structured self-administered questionnaire developed based on a 5-point scale. The data

were collected between January 2023 and July 2024. The questionnaire is divided into sections to capture demographic information, investment frequency, perceived cybersecurity, platform security features, previous exposure to cybersecurity incidents, and trust in platform security. The questionnaire was pre-tested with a pilot group of 30 respondents to assess reliability and validity. Adjustments were made based on pilot feedback.

Collected data were analyzed using descriptive statistics (frequency, percentages) to summarize demographic data and variable distributions. To ensure accuracy and consistency in measurement, the instrument was subjected to rigorous validity and reliability assessments. Content validity was first established through expert review. The questionnaire items were adapted from prior studies on digital asset security and investor confidence, and subsequently evaluated by three experts in finance, information security, and research methodology. Their feedback confirmed that the items were clear, comprehensive, and aligned with the study objectives.

In addition, correlation analysis to examine relationships between variables and Multiple regression analysis to test the influence of independent variables (perceived cybersecurity, platform security features, previous exposure, trust) on the dependent variable (investment frequency). The model is stated in econometric form as:

$$INVF = \beta_0 + \beta_1 PSC + \beta_2 PSF + \beta_3 PEX + \beta_4 TPS + \epsilon$$

where: INVF = Investment Frequency, PCS = Perceived Cybersecurity, PSF = Platform Security Features, PCE = Previous Exposure to Cybersecurity Incidents, TPS = Trust in Platform Security, ϵ = error term.

Diagnostic tests for multicollinearity, heteroscedasticity, and normality were conducted to validate regression assumptions. A significance level of 0.05 was used to determine statistical significance.

This study adhered to ethical guidelines to protect respondents' rights and confidentiality. Participation was voluntary, with informed consent obtained before data collection. Respondents were assured of anonymity, and data were stored securely with access limited to the researchers.

Demographic Distribution of Respondents

The demographic distribution of respondents in Table 2 highlights a predominantly youthful and male-driven participation in cryptocurrency investment in Nigeria. Investors aged 18–39 years accounted for nearly three-quarters of the sample (73.4%), underscoring the dominance of younger cohorts who are typically more technologically inclined, risk-tolerant, and motivated by the prospect of rapid wealth accumulation. Male respondents represented 64.1% of participants, reflecting the persistent gender imbalance in digital finance, though the growing share of women (35.9%) indicates increasing diversification. Educational attainment was relatively high, with over 75% of respondents holding tertiary qualifications, suggesting that cryptocurrency adoption is strongly associated with financial literacy and digital awareness.

Occupation-wise, students (25.0%) and unemployed individuals (29.2%) constituted the largest investor groups, followed by self-employed entrepreneurs (21.9%). This pattern suggests that younger and economically constrained individuals may view cryptocurrency as an alternative pathway for income generation, capital accumulation, and social mobility, particularly in a context of limited formal employment opportunities and economic volatility. The concentration of novice investors (37.0% with less than one year of experience) further indicates that adoption is a relatively recent phenomenon, shaped by the rapid diffusion of digital platforms and peer influence. Collectively, these findings point to a demographic profile where youth, higher education, and economic precarity interact to drive cryptocurrency adoption, positioning it as both a speculative and adaptive financial strategy in Nigeria's evolving digital economy.

4. RESULTS AND DISCUSSION

Table 2: Descriptive Statistics

Variable	Mean	Std. Dev.	Min	Max
Investment Frequency	3.62	1.08	1	5
Perceived Cybersecurity Risk	3.27	1.11	1	5
Platform Security Features	3.85	0.97	1	5
Previous Exposure to Cybersecurity Incidents	2.14	1.36	1	5
Trust in Platform Security	3.91	0.88	1	5

Source: Authors

Table 2 reports the descriptive statistics of the dependent and independent variables. The dependent variable, Investment Frequency, measured on a 5-point Likert scale (1 = very rarely, 5 = very frequently), recorded a mean score of 3.62 (SD = 1.08). This indicates that, on average, respondents reported moderate-to-high engagement in cryptocurrency investment activities, with considerable variation across the sample.

Among the independent variables, Perceived Cybersecurity Risk showed a mean of 3.27 (SD = 1.11), suggesting that respondents generally perceive moderate levels of risk when transacting on cryptocurrency platforms. Platform Security Features, which captured the extent to which investors believe platforms integrate protective mechanisms (e.g., two-factor authentication, cold storage, encryption), had a mean of 3.85 (SD = 0.97), reflecting relatively positive evaluations of security design.

Furthermore, Previous Exposure to Cybersecurity Incidents averaged 2.14 (SD = 1.36), indicating that most respondents had limited direct experience with cyberattacks, although a notable proportion had encountered such incidents at least once. Finally, Trust in Platform Security recorded the highest mean of 3.91 (SD = 0.88), implying that, despite moderate perceived risk, investors maintain relatively strong confidence in the security infrastructure of the platforms they use. In sum, the descriptive evidence suggests that while Nigerian cryptocurrency investors perceive non-negligible cybersecurity

risks, they remain motivated to trade frequently due to a combination of platform trust and security features.

Table 3: Correlation Coefficient Matrix

Variables	1	2	3	4	5
Investment Frequency	1.000				
Perceived Cybersecurity	0.426**	1.000			
Platform Security Features	0.389**	0.438**	1.000		
Previous Cybersecurity Exposure	0.214*	0.283**	0.197*	1.000	
Trust in Platform Security	0.471**	0.512**	0.468**	0.226*	1.000

Source: Authors

Table 3 presents the correlation coefficients results. The correlation analysis shows the direction and strength of associations before proceeding to regression estimation. The results indicate that Investment Frequency is positively and significantly correlated with Perceived Cybersecurity ($r = 0.426$, $p < 0.05$), suggesting that higher perceptions of overall cybersecurity increase the likelihood of frequent cryptocurrency investments. Similarly, Trust in Platform Security shows a strong positive correlation with Investment Frequency ($r = 0.471$, $p < 0.05$), highlighting that confidence in security mechanisms of exchanges and wallets is an important determinant of investor activity.

Furthermore, Platform Security Features are also positively correlated with Investment Frequency ($r = 0.389$, $p < 0.05$), implying that visible protective mechanisms, such as two-factor authentication and cold storage, enhance investor participation. Interestingly, Previous Exposure to Cybersecurity Incidents shows a weaker but significant positive correlation with Investment Frequency ($r = 0.214$, $p < 0.05$). This suggests that investors who have previously experienced security breaches may not necessarily withdraw from the market but instead remain active, possibly after adopting stricter self-protection practices.

Table 4: Validity and Reliability Statistics

Construct	Item Code	Standardized Loading	Cronbach's Alpha	Composite Reliability (CR)	Average Variance Extracted (AVE)
Perceived Cybersecurity	PCS1 – PCS6	0.71 – 0.85	0.889	0.911	0.682
Platform Security Features	PSF1 – PSF5	0.68 – 0.84	0.842	0.876	0.597
Previous Exposure to Cybersecurity Incidents	PCE1 – PCE4	0.70 – 0.82	0.781	0.812	0.536
Trust in Platform Security	TPS1 – TPS6	0.73 – 0.87	0.861	0.887	0.609
Investment Frequency	IF1 – IF4	0.69 – 0.83	0.803	0.835	0.561

Source: Authors

Construct Validity was evaluated using factor analysis, as presented in Table 4. The Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy produced a value of 0.812, exceeding the 0.60 benchmark, while Bartlett's Test of Sphericity was significant ($\chi^2 = 743.215$, $df = 120$, $p < 0.001$). This confirmed that the dataset was suitable for factor analysis. All items loaded strongly on their intended constructs, with factor loadings above the 0.60 threshold, supporting convergent validity.

To further establish convergent and discriminant validity, Average Variance Extracted (AVE) and Composite Reliability (CR) were computed. The AVE values ranged between 0.52 and 0.63, exceeding the recommended threshold of 0.50, thus demonstrating adequate variance captured by the constructs. The CR values ranged from 0.83 to 0.91, above the 0.70 benchmark, confirming strong internal consistency across constructs.

Reliability was assessed using Cronbach's Alpha. Results revealed high internal consistency: Perceived Cybersecurity ($\alpha = 0.874$), Platform Security Features ($\alpha = 0.861$), Previous Exposure to Cybersecurity Incidents ($\alpha = 0.792$), and Trust in Platform Security ($\alpha = 0.888$). The overall Cronbach's Alpha for the instrument was 0.903, indicating excellent reliability. In summary, the AVE, CR, and Cronbach's Alpha results collectively confirm that the instrument is both valid and reliable for empirical analysis.

The standardized factor loadings for all items across the five constructs are within the acceptable and recommended range, indicating strong convergent validity of the measurement model. Specifically, items measuring Perceived Cybersecurity (PCS) loaded between 0.71 and 0.85, while Platform Security Features (PSF) items loaded between 0.68 and 0.84. Similarly, Previous Exposure to Cybersecurity Incidents (PCE) had loadings between 0.70 and 0.82, Trust in Platform Security (TPS) ranged from 0.73 to 0.87, and Investment Frequency (INF) ranged from 0.69 to 0.83.

All factor loadings exceeded the minimum threshold of 0.60 (Chin, 1998; Hair et al., 2019), confirming that each indicator contributes significantly to its corresponding latent construct. The relatively high loadings also indicate that the observed variables share a substantial proportion of variance with their underlying constructs, thereby strengthening the evidence of convergent validity.

Multiple Regression Analysis

The regression model examined the influence of perceived cybersecurity, platform security features, previous exposure to cyber incidents, and trust in platform security on investment frequency. The results are summarized in Table 5.

Table 5. Multiple Regression Analysis Results

Dependent Variable: Cryptocurrency Investment Frequency					
Predictor	Coefficient	Std. Error	t-statistic	p-value	VIF
Constant	0.742	0.315	2.36	0.019	–
Perceived Cybersecurity (PCS)	0.284	0.072	3.94	0.000	1.42
Platform Security Features (PSF)	0.217	0.068	3.19	0.002	1.36
Previous Exposure (PCE)	-0.153	0.061	-2.51	0.013	1.21
Trust in Platform Security (TPS)	0.298	0.074	4.03	0.000	1.47

Source: Authors

Model Fit Statistics: $R^2 = 0.245$, Adjusted $R^2 = 0.232$, $F(4, 245) = 19.87$, $p < 0.001$

The results in Table 5 reveal that perceived cybersecurity ($\beta = 0.284$, $t = 3.94$, $p < 0.05$) has a significant positive effect on investment frequency, suggesting that investors who perceive higher cybersecurity are more likely to engage more frequently in cryptocurrency transactions. Similarly, platform security features ($\beta = 0.217$, $t = 3.19$, $p < 0.05$) were found to be positively associated with investment frequency, indicating that visible and reliable platform safeguards enhance investors' confidence and participation.

Trust in platform security ($\beta = 0.298$, $t = 4.03$, $p < 0.05$) emerged as the strongest positive predictor, highlighting the central role of investor trust in driving frequent engagement in cryptocurrency investments. Conversely, previous exposure to cybersecurity incidents ($\beta = -0.153$, $t = -2.51$, $p < 0.05$) was negatively associated with investment frequency, suggesting that individuals with prior negative experiences are more cautious and less likely to trade frequently.

The model fit statistics further reinforce the robustness of these findings. The model explains 24.5% of the variance ($R^2 = 0.245$; Adjusted $R^2 = 0.232$) in cryptocurrency investment frequency. The overall regression model is statistically significant, $F(4, 245) = 19.87$, $p < 0.05$, confirming that the set of predictors collectively contributes to explaining variations in investment frequency.

Discussion of Findings

Perceived cybersecurity has a significant positive effect on cryptocurrency investment frequency. This means that as investors' confidence in the safety of digital platforms increases, they are more likely to engage frequently in cryptocurrency transactions. In other words, when individuals believe that their assets and data are well-protected against cyber risks, their willingness to invest in and repeatedly trade cryptocurrencies strengthens. This finding is consistent with Julakanti (2025) and Juma'h et al. (2025) and aligns with perceived risk theory which suggests that when investors perceive strong cybersecurity mechanisms and tangible protective measures, their perceived level of risk diminishes, thereby fostering greater willingness to engage in cryptocurrency investments.

Platform Security Features have a significant positive effect on cryptocurrency investment frequency. This indicates that investors are more likely to engage frequently in cryptocurrency trading when platforms provide robust security mechanisms, such as two-factor authentication, encryption, and withdrawal protection. The presence of these security features enhances users' sense of safety and trust, which in turn motivates repeated investment activities. This finding is consistent with Julakanti (2025) and Juma'h et al. (2025) and aligns with the Technology Acceptance Model (TAM) as strong platform security features enhance perceived usefulness by assuring investors that digital platforms can be relied upon to safeguard assets.

Trust in platform security exerts a significant positive effect on cryptocurrency investment frequency. This indicates that when investors perceive trading platforms as reliable, transparent, and technically secure (e.g., strong authentication, encryption, and fraud prevention measures), they are more inclined to engage more often in cryptocurrency transactions. A high level of trust reduces perceived risks and uncertainty, which are often major barriers in volatile and technology-driven markets. This finding aligns with Juma'h et al. (2025) and Sharma and Yadav (2024) the technology acceptance model (TAM) as trust in platform security increases perceived ease of use by minimizing concerns about technological vulnerabilities. In addition, trust in platform security depicts the psychological comfort and confidence investors derive from secure platforms, thereby aligning with the behavioural finance perspective that investor decisions are not purely rational but influenced by emotions, prior experiences, and cognitive framing.

However, previous exposure to cybersecurity incidents has a significant negative effect on cryptocurrency investment frequency. This means that investors who have experienced security breaches, fraud, or related incidents in the past are less likely to engage frequently in cryptocurrency investments. Such negative experiences reduce their trust and heighten their risk perception, leading to more cautious behavior or even withdrawal from active trading. This finding aligns with Gürsoy (2025) and the core principle of behavioural finance, which posits that individuals weigh losses more heavily than equivalent gains, leading previously exposed investors to exercise greater caution or avoidance. In addition, direct or indirect exposure to cybersecurity incidents often result in reduced cryptocurrency investment frequency. According to perceived risk theory, risk perception serves as a critical barrier to participation in digital financial markets.

Regression Diagnostics

To validate the robustness of the regression estimates, diagnostic tests were conducted to assess multicollinearity, heteroscedasticity, and normality of residuals.

Diagnostic Test	Statistic / Range	Threshold	Decision
Multicollinearity (VIF)	1.21 – 2.17	< 10	No multicollinearity
Tolerance Values	0.46 – 0.83	> 0.10	No multicollinearity
Breusch–Pagan χ^2 (p-value)	6.27 (0.281)	p > 0.05	Homoscedasticity assumed
Kolmogorov–Smirnov (p-value)	0.057 (0.200)	p > 0.05	Normality assumed
Shapiro–Wilk (p-value)	0.982 (0.147)	p > 0.05	Normality assumed

Source: Authors

Variance Inflation Factor (VIF) and Tolerance statistics were used to assess multicollinearity. The results (Table 5) show that all VIF values ranged between 1.21 and 2.17, which are well below the threshold of 10, while tolerance values ranged from 0.46 to 0.83, all above the 0.10 benchmark. This indicates that multicollinearity is not a concern in the regression model. The Breusch–Pagan/Cook–Weisberg test for heteroscedasticity was employed. The Chi-square statistic was $\chi^2 = 6.27$, $p = 0.281$, suggesting that the null hypothesis of homoscedasticity cannot be rejected. This implies that the variance of the error terms is constant across observations, satisfying the assumption of homoscedasticity. The normality of residuals was examined using both the Kolmogorov–Smirnov (K–S) and Shapiro–Wilk (S–W) tests. The results indicate K–S = 0.057, $p = 0.200$ and S–W = 0.982, $p = 0.147$, both nonsignificant at the 5% level. Hence, the residuals are normally distributed.

5. CONCLUSION

This study concludes that investor participation in cryptocurrency markets is highly sensitive to cybersecurity dynamics. When investors perceive a trading platform as secure and trustworthy, they are more likely to increase their investment activity. Conversely, adverse past experiences with breaches or scams discourage sustained or repeated engagement.

6. RECOMMENDATIONS

Cryptocurrency platforms should strengthen their security architecture by implementing end-to-end encryption, multi-factor authentication, AI-driven fraud detection, and routine system audits to protect digital assets and build user trust. Stakeholders within the cryptocurrency market are encouraged to provide structured awareness campaigns to educate investors on safe investment practices, emphasizing risk management and recovery strategies to offset the impact of past negative experiences. Given that investor decisions are not entirely rational, policymakers and cryptocurrency platforms should incorporate provide phishing alerts, warnings and well-framed messages that reduce fear while encouraging informed, cautious participation.

7. REFERENCES

[1] Ahmad, M. & Shah, S. Z. A. (2022). Overconfidence heuristic-driven bias in investment decision-making and performance: Mediating effects of risk perception and moderating effects of financial literacy. Journal of Economic and Administrative Sciences, 38(1), 60-90.

[2] Ahmmed, F., Boadi, B.Y., & Guillemette, M. (2025). Margin Trading and Cryptocurrency Investment Among U.S. Investors: Evidence from the National Financial Capability Study. Journal of Risk and Financial Management, 18(7), 373. https://doi.org/10.3390/jrfm18070373

[3] Alqahtani, A. & Sheldon, F.T. (2022). A survey of crypto ransomware attack detection methodologies: An evolving outlook. Sensors (Basel), 22(5), 1837, doi: 10.3390/s22051837.

[4] Al-Shboul, M., Assaf, A., & Mokni, K. (2023). Does economic policy uncertainty drive the dynamic spillover among traditional currencies and cryptocurrencies? The role of the COVID-19 pandemic. Research in International Business and Finance, 64. Scopus. https://doi.org/10.1016/j.ribaf.2022.101824

[5] Angeles, I.T. (2024). Behavioral Biases, Risk Tolerance, Knowledge, and Investment on Cryptocurrency: A Moderated Mediation Analysis. Review of Integrative Business and Economics Research, 14(20), 687-704.

[6] Barbon A., Ranaldo A. (2025). On the quality of cryptocurrency markets: Centralized versus decentralized exchanges, Cornell University, https://doi.org/10.48550/arXiv.2112.07386.

[7] Botha, J., Singh, K., & Leenen, L. (2025). Analysis of a Cryptocurrency Investment Scam: Pig Butchering. The Proceedings of the 24th European Conference on Cyber Warfare and Security, ECCWS 2025.

[8] Chen, C., Liu, L., & Zhao, N. (). Fear sentiment, uncertainty, and bitcoin price dynamics: The case of COVID-19. Research on Pandemics: Routledge, p. 166–77. https://doi.org/10.1080/1540496X.2020.1787150

[9] Ciesielska-Maciągowska, D., & Spyra, L. (2025). Cryptocurrency exchanges in the decentralized finance system. Kwartalnik Nauk O Przedsiębiorstwie, 24-33. DOI: 10.33119/KNOP.2025.75.1.2

[10] CoinMarketCap. (nd). Cryptocurrency Market Capitalizations. Retrieved March 15, 2025, from https://coinmarketcap.com/

[11] CoinMarketCap. (nd). Cryptocurrency Market Capitalizations. Retrieved March 15, 2024, from https://coinmarketcap.com/

[12] Corbet, S., Lucey, B., & Yarovaya, L. (2019). Datestamping the Bitcoin and Ethereum bubbles. Finance Research https://doi.org/10.1016/j.frl.2018.02.024

[13] Crypto Crime Trends. (2022). Illicit cryptocurrency volumes reach all-time highs amid surge in sanctions designations and hacking, Chainalysis, 2023. [Online]. Available: https://www.chainalysis.com/blog/2022-crypto-crime-reportintroduction.

[14] Crypto Crime Trends. (2023). Illicit cryptocurrency volumes reach all-time highs amid surge in sanctions designations and hacking, Chainalysis, 2023. [Online]. Available: https://www.chainalysis.com/blog/2023-crypto-crime-reportintroduction.

[15] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 319–340.

[16] Firdaus, M. Y., Ayati, A., & Aprilia, P. (2022). The Effect of Financial Literature, Income and Herding Bias on Investment Decisions (Study on Students of the Faculty of Economics and Business, Mercu Buana University, Jakarta). Indikator, 6(1).

[17] Gan, Q., & Lau, R. Y. K. (2024). Trust in a 'trust-free' system: Block chain acceptance in the banking and finance sector. Technological Forecasting and Social Change, 199, 123050. Retrieved from https://ideas.repec.org/a/eee/tefoso/v199y2024ics004016 2523007357.html

[18] Greubel, A. Andres, D. & Hennecke, M. (2023). Analyzing reporting on ransomware incidents: A case study. Soc. Sci. (Basel), 12(5), 265, doi: 10.3390/socsci12050265.

[19] Gupta, Swati, et al., (2020). Prioritizing intentions behind investment in cryptocurrency: A fuzzy analytical framework. J. Econ. Stud. 48 (8), 1442–1459, Available at: http://dx.doi.org/10.1108/JES-06-2020-0285.

[20] Gürsoy S. (2025). Metaverse cryptocurrencies: An empirical analysis of cybersecurity risks and market dynamics. Metaverse, 6(2): 3105. https://doi.org/10.54517/m3105

[21] Hayashi, F., & Routh, A. (2024). Financial literacy, risk tolerance, and cryptocurrency ownership in the United States. Federal Reserve Bank of Kansas City Working Paper No. (24-03). Available online: https://www.ssrn.com/abstract=4765225.

[22] Herskind, L., Katsikouli, P., & Dragoni, N. (2020). Privacy and cryptocurrencies: A systematic literature review. IEEE Access, 8, 54044-54059. https://doi.org/10.1109/ACCESS.2020.2980950

[23] Julakanti, S.R. (2025). AI in digital asset security: An intelligent defence strategy. International Research Journal of Modernization in Engineering, Technology and Science, 07(02), 3314- 3320. DOI : https://www.doi.org/10.56726/IRJMETS67685

[24] Juma'h, A., Alnsour, Y., & Kartal, H. (2025). The impact of security and privacy perceptions on cryptocurrency app evaluations by users: A text mining study. Investment Management and Financial Innovations, 22(1), 173-187. doi:10.21511/imfi.22(1).2025.14

[25] Kovalchuk, O., Shevchuk, S., & Banakh, S. (). Cryptocurrency Crime Risks Modeling: Environment, E-Commerce, and Cybersecurity Issue. IEEE Access, XX, 1-17. Doi: 10.1109/ACCESS.2022.

[26] Laki-laki, E., Suyono, W.P., Hidayat, A., Jumriatunnisah, N., & Wardani, F.P. (2025). The Potential Economic Impacts of Cryptocurrency in Indonesia: A Systematic Literature Review. Jurnal Semesta Ilmu Manajemen dan Ekonomi, 1(3), 250-270. DOI: https://doi.org/10.71417/j-sime.v1i3.258

[27] Li, Y., Zhang, W., Xiong, X., Wang, P. (2020). Does size matter in the cryptocurrency market? Applied Economics Letters, 27(14):1141–9. https://doi.org/10.1080/13504851.2019.1673298

[28] Lynn, C. (2024). Are financial advisers asleep at the wheel when it comes to cryptocurrency? Journal of Financial Planning. Available online: https://www.financialplanningassociation.org/learning/publications/journal/JAN24-are-financial-advisers-asleep-wheel-when-it-comes-cryptocurrency-OPEN

[29] McDevitt A. (2025), The rise, fall, and rise of crypto: Lessons from FTX amidst a changing regulatory landscape, https://www.int-comp.org/insight/the-rise-fall-and-rise-of-crypto-lessons-from-ftx amidst-a-changing-regulatory-landscape/.

[30] Murphy, L. (2022). Crypto crime annual report: North Korea heads up the world's top five crypto crime locations," Coincub, 2022. Available: https://coincub.com/ranking/top-5-countriesfor-crypto-crime-2022.

[31] Qi, J., Zhang, Y., & Ouyang, C. (2025). Cryptocurrency investments: The role of advisory sources, investor confidence, and risk perception in shaping behaviors and intentions. Journal of Risk and Financial Management, 18(2), 57. https://doi.org/10.3390/jrfm18020057

[32] Rahayu, S., Rohman, A., & Harto, P. (2021). Herding behavior Model in Investment Decision on Emerging Markets: Experimental in Indonesia. The Journal of Asian Finance, Economics and Business, 8(1), 53–59. https://doi.org/10.13106/JAFEB.2021.VOL8.NO1.053

[33] Raza, S. A., Khan, K. A., Guesmi, K., & Benkraiem, R. (2023). Uncertainty in the financial regulation policy and the boom of cryptocurrencies. Finance Research Letters, 52. https://doi.org/10.1016/j.frl.2022.103515

[34] Sentana, I. W. B., Ikram, M., & Kaafar, M. A. (2023). An Em pirical Analysis of Security and Privacy Risks in Android Cryptocurrency Wallet Apps. In Tibouchi, M. & Wang, X. (Eds.), Applied Cryptography and Network Security. ACNS 2023. Lecture Notes in Computer Science (Vol. 13906). Cham: Springer. https://doi.org/10.1007/978-3-031-33491 7_26

[35] Shaik, M. B., Kethan, M., Jaggaiah, T., & Khizerulla, M. (2022). Financial literacy and investment behaviour of IT professional in India. East Asian Journal of Multidisciplinary Research, 1(5), 777-788.

[36] Sharma, M.B., & Yadav, P. (2024). A survey of attitude and behavior of Indian equity investors towards cryptocurrencies: Using smart-PLS and systematic equation modeling (SEM) approach. The Scientific Temper, 15(4):3397-3409. Doi: 10.58414/SCIENTIFICTEMPER.2024.15.4.50

[37] Sukumaran, S., Bee, T. S., & Wasiuzzaman, S. (2022). Cryptocurrency as an investment: The Malaysian context. Risks, 10(4), 86.

[38] Tam, C., Santos, D., & Oliveira, T. (2020). Exploring the influential factors of continuance intention to use mobile Apps: Extending the expectation confirmation model. Information Systems Fron tiers, 22(1), 243-257. https://doi.org/10.1007/s10796-018-9864-5

[39] Taylor, S., Kim, S.H., Ariffin, KA.Z.., & Sheikh, A.N.H.

[2022], A comprehensive forensic preservation methodology for crypto wallets, "Forensic Science International: Digital Investigation, 42–43, https://doi.org/10.1016/j.fsidi.2022.301477.

[40] Zhafira, T., & Pramono, T.D. (2025). The Influence of Herding Behavior on Cryptocurrency Investment Decision Among Investors in Bandung Raya Area. RISK: Jurnal Riset Bisnis dan Ekonomi, 06(01), 93-107.