International Journal of Accounting & Finance in Asia Pasific (IJAFAP)
Vol. 7 No. 3, pp. 461-477, October, 2024
E-ISSN: 2655-6502 P-ISSN: 2684-9763
https://www.ejournal.aibpmjournals.com/index.php/IJAFAP

Cryptocurrency Security Risk: Awareness Among General Public in Malaysia

Azura Abdullah Effendi[1], Boon Keong Teow[2], Kai Guan Teh[3*], Yin Ann Tan[4], Hsue Li Tay[5], Yuxin Tang[6],Simran Chaudhary[7], Daisy Mui Hung Kee[8]
Universiti Sains Malaysia, Pulau Pinang, Malaysia[1,3,4,5,6,8]
IMS Engineering College, Ghaziabad, India[7]
Vitrox College, Pulau Pinang, Malaysia[2]
Corresponding Author: tehkaiguan11@gmail.com[3]

ARTICLE INFORMATION

Publication information

Research article

HOW TO CITE
Abdullah Effendi, A., Teow, B. K., Teh, K. G., Tan, Y. A., Tay, H. L., Tang, Y., Chaudhary, S., & Kee, D. M. H. (2024). Cryptocurrency security risk: Awareness among general public in Malaysia. *International Journal of Accounting & Finance in Asia Pasific*, *7*(3), 461-477.

DOI:
https://doi.org/10.32535/ijafap.v7i3.3619

Received: 16 August 2024
Accepted: 19 September 2024
Published: 20 October 2024

ABSTRACT

In the age of digital payments, cryptocurrencies have gained significant attention as an alternative investment option. However, security risks such as phishing, hacking, and fraudulent exchanges present challenges for investors. This study aims to assess the level of awareness among the general public in Malaysia regarding cryptocurrency security risks. A quantitative research method was employed, using a survey questionnaire distributed to 150 Malaysian citizens via social media platforms. The questionnaire explored respondents' knowledge of cryptocurrencies, awareness of security risks, and protective measures such as security programs, two-factor authentication (2FA), and education. The results of the regression analysis show that the installation of security programs, 2FA, and public education are all significant predictors of increased awareness of cryptocurrency security risks, with a combined R^2 value of 0.523. This suggests that 52.3% of the variance in awareness is explained by these factors. The study concludes that strengthening security measures and providing education can significantly improve public understanding of cryptocurrency risks, leading to safer investment practices. The implications of these findings highlight the need for targeted education and security initiatives to enhance public confidence in cryptocurrency, making digital currency investments more secure.

Keywords: Awareness; Cryptocurrency; General Public; Malaysia; Security Risk

INTRODUCTION

In the contemporary age of advanced technology, our dependency on electronic payment methods like E-wallets, online banking, and DuitNow has grown significantly, eclipsing traditional cash transactions for purchasing goods and services. These digital payment methods have not only gained popularity but have also become an indispensable part of our daily lives (Edeh et al., 2021; Kee et al., 2022a, 2022b). Technological advancements have significantly impacted both the business and stock exchange markets, gradually evolving and offering more advantages to investors and shareholders. Publicly listed companies or those offering shares to the public utilize technology to increase their capital by selling shares. Various investment instruments are available, including corporate bonds, common and preference shares, and treasury bills, among others. While knowledge can help reduce investment risk, it may also lead to lower returns. Additionally, in addition to traditional stock exchanges, investors can now explore over-the-counter markets and even invest in cryptocurrencies, offering further diversification in investment options.

The person or group of programmers known as Satoshi Nakamoto created the first cryptocurrency, Bitcoin, in 2009. A cryptocurrency is a digital currency that serves as a form of payment, created using encryption algorithms (Britannica Money, 2024). Blockchain, an immutable, transparent, and often decentralized digital database, is the underlying technology that makes cryptocurrency possible. This database records transactions so that anyone can see them, but no one can change them (Rahman & Wulandari, 2022). Encryption technology ensures security, enabling cryptocurrency to function as a currency, much like a virtual accounting system (Oswego State University of New York, n.d.). Before using cryptocurrency for payments, users must have a cryptocurrency wallet. The benefits of cryptocurrency include not having to carry physical money like cash or coins, as payments can be made using the value of the cryptocurrency. Examples of cryptocurrencies include Bitcoin, Ethereum, Dogecoin, Litecoin, and USDT.

Cryptocurrencies are not recognized in all countries. In some, government authorities, laws, and regulations prohibit their use and ban any buy-sell transactions involving cryptocurrency. In Malaysia, however, cryptocurrencies are legal and permitted to be traded as securities under the Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019. Although Bank Negara Malaysia (BNM), the Malaysian central bank, does not recognize cryptocurrencies as legal tender or payment instruments, they can be used for securities purposes. The body that regulates cryptocurrency in Malaysia is the Securities Commission Malaysia (SCM) under the same order (Notabene, 2023). Some examples of legally registered cryptocurrency platforms in Malaysia include Hata Digital Sdn Bhd, Luno Malaysia Sdn Bhd, SINEGY DAX Sdn Bhd, Tokenize Technology (M) Sdn Bhd, and Torum International Sdn Bhd (Suruhanjaya Sekuriti, n.d.).

Cryptocurrency is not entirely safe to invest in due to underlying security risks. Unlike traditional currencies, which are backed by governments or central banks, cryptocurrency is not protected in the same way. If security breaches or platform bankruptcies occur, users may face irreversible financial losses (Connecticut's Official State Website, n.d.). Security theft is increasingly common in this era of advanced technology. The general public in Malaysia should be aware of the security risks associated with cryptocurrency. A lack of awareness opens opportunities for hackers and cybercriminals. Security risks may take various forms and can affect cryptocurrency

platforms, including phishing, man-in-the-middle attacks, and fake cryptocurrency exchanges.

Cryptocurrency adoption in Malaysia has gradually grown and expanded, with about RM 21 billion in digital assets traded in 2021 (Madavaram, 2022). It is essential for the general public in Malaysia, especially those participating in cryptocurrency trading, to take necessary precautions to protect their identity, assets, and confidential information. Educating the public on cryptocurrency, its procedures, and the associated risks will increase awareness and enable more informed investment decisions.

This study aims to assess the level of awareness the general public in Malaysia has regarding cryptocurrency security risks. In the context of the growing reliance on digital payment methods and the rise of cryptocurrency as an investment option, this research holds significant relevance. The significance of this study lies in its potential to contribute to a safer cryptocurrency trading environment by identifying the public's current understanding of the risks involved, such as phishing, man-in-the-middle attacks, and fake exchanges. This will provide insights into where further education and preventive measures are needed to ensure that users are better equipped to protect their digital assets.

The novelty of this research stems from its specific focus on the Malaysian context, where cryptocurrency is recognized under legal frameworks yet still poses significant security concerns. This study not only explores the awareness of the public but also integrates key factors like the role of security programs, two-factor authentication, and public education in enhancing security. By addressing these elements, the research fills a gap in the existing literature, which often overlooks how local regulations and public awareness interact in shaping cryptocurrency security practices in emerging markets like Malaysia.

In terms of contribution, this research offers practical recommendations to improve public awareness and protection against security risks associated with cryptocurrencies. By emphasizing the importance of education, secure platforms, and robust authentication processes, the study contributes to the broader understanding of how to safeguard investors in the evolving digital economy. Moreover, the findings can guide policymakers, financial institutions, and educational bodies in developing targeted awareness campaigns, legal protections, and security measures to foster a more secure and informed cryptocurrency ecosystem in Malaysia.

LITERATURE REVIEW

Cryptocurrency Awareness

Cryptocurrency, a virtual asset utilized as a form of digital currency, has transformed global financial systems by enabling the transfer of assets and other forms of financial instruments (Rice, 2019). As of now, over 1,000 virtual currencies are in circulation, with new cryptocurrencies regularly emerging across global markets. This increasing number of cryptocurrencies highlights the growing relevance of this digital asset class. However, awareness remains a crucial element for broader adoption. Awareness is defined as the recognition of the existence and importance of something, and in the case of new technologies like cryptocurrency, it plays a pivotal role in adoption (Roppelt, 2019). Awareness is not merely the initial recognition of cryptocurrency but also encompasses knowledge of the risks and opportunities associated with its use. According to the diffusion of innovation theory, awareness forms the first critical stage of adoption, and without it, subsequent stages of acceptance and usage are hindered.

The rapid development of cryptocurrency has not only disrupted traditional financial systems but also introduced new risks, including financial crime and cybercrime. This phenomenon has prompted a demand for heightened awareness and education among potential cryptocurrency users to better understand the process and implications of engaging in cryptocurrency transactions (Eigbe, 2018). Effective awareness campaigns can bridge the knowledge gap for users and provide the necessary tools to navigate the complexities of the cryptocurrency ecosystem.

Cryptocurrency Security Risks

With the rise in cryptocurrency usage, the potential for criminal activities facilitated by its inherent anonymity has become evident. Cryptocurrencies, particularly those utilizing Blockchain technology, allow for decentralized transactions while providing anonymity through distributed ledgers and cryptographic techniques (Al-Amri et al., 2019). This anonymity, while enhancing privacy, also makes cryptocurrencies appealing to individuals involved in illicit activities. Criminal behavior tracking has thus become a significant challenge, necessitating stronger risk management strategies. Risk management theory is central to identifying, assessing, and managing risks associated with cryptocurrency, especially as these emerging markets introduce novel forms of threats (Ajupov et al., 2019).

In the context of the cryptocurrency ecosystem, several security risks have emerged. Phishing attacks, where fraudsters attempt to deceive users by prompting them to click on malicious links or access fake websites, are among the most common. This method allows cybercriminals to steal personal information, especially from users who are unaware of such tactics (Fu et al., 2022). Another prevalent issue is the man-in-the-middle attack, where hackers intercept and alter communication between two parties during cryptocurrency transactions, redirecting funds to their own wallets (Shaik, 2021). Additionally, fake cryptocurrency exchanges are used to scam users by deceiving them into depositing funds, which ultimately leads to financial losses without legitimate trading (Luchkin et al., 2020).

Installation of Security Programs

The installation of security programs has emerged as a vital response to the security risks associated with cryptocurrency trading. Security programs enhance the protection of users during transactions by implementing various security features such as email verification and phone verification (Mirčevski et al., 2023). According to Protection Motivation Theory, individuals are motivated to adopt protective measures when they perceive potential threats. This theory applies to the adoption of security programs, as users believe that such installations reduce the likelihood of cyber threats (Boerman et al., 2021).

Keeping security programs updated is critical in protecting against known vulnerabilities. New features and software improvements provide more robust defense mechanisms against emerging security risks (Pacheco, 2024). Programs like Bitdefender, Norton, and Kaspersky offer comprehensive protection, detecting potential threats such as suspicious emails and malicious URL links, which are common vectors of attacks in cryptocurrency trading. Ensuring a secure browsing experience during the exchange process is essential to maintaining the integrity of the transactions and the safety of users' assets.

Two-Factor Authentication

Two-factor authentication (2FA) has become a popular security measure in cryptocurrency trading due to its ability to provide an additional layer of protection. By requiring a combination of password security and personal identity verification, 2FA helps prevent cyber attackers from easily accessing users' accounts (Liu et al., 2023). The Technology Acceptance Model (TAM) suggests that users' awareness and understanding of new technologies significantly influence their willingness to adopt security measures like 2FA (Zaineldeen et al., 2020).

2FA plays a crucial role during transactions, particularly when large sums of money or key recovery requests are involved. By triggering additional verification steps in such scenarios, it ensures that only the rightful owner can access and transfer assets. However, careful consideration is needed, as security questions used in 2FA systems can sometimes be exploited by attackers through social engineering or guesswork (Breuer et al., 2021). Thus, while 2FA is a powerful tool, its implementation must be carefully managed to prevent any vulnerabilities that might arise from weak authentication methods.

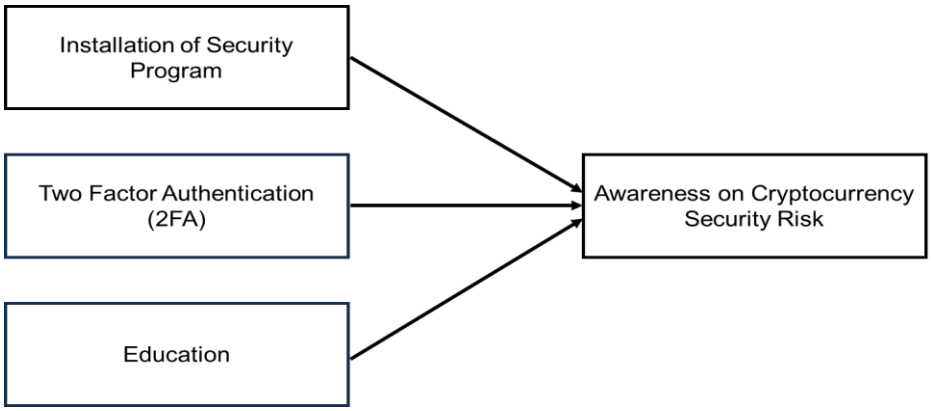
Education

Public education is essential to increasing awareness and understanding of the security risks associated with cryptocurrency trading. Educational campaigns, conferences, and other platforms provide opportunities for the public to build confidence and develop a deeper understanding of cryptocurrency technology and its associated risks (Shahzad et al., 2024). Connectivism theory, which emphasizes the importance of learning through digital networks, is highly relevant in the context of cryptocurrency, as individuals often rely on digital platforms to stay informed about the rapidly changing landscape of digital assets (Peter & Ogunlade, 2024).

Educational efforts, such as blogs, podcasts, and online courses, provide an accessible way for younger audiences and new users to grasp the basics of cryptocurrency. According to Zubir et al. (2020), education plays a pivotal role in shaping users' behavior in financial markets. Users with limited knowledge are more vulnerable to unexpected market fluctuations or regulatory changes, as they are less equipped to manage such risks (Camp, 2024). As more people become educated about cryptocurrency, broader acceptance and integration into mainstream financial systems will likely follow. Educated users are also better equipped to make informed decisions, thus reducing their vulnerability to cyber threats and enhancing the overall safety of cryptocurrency ecosystems (Camp, 2024).

Figure 1 below represents the theoretical framework of this research.

Figure 1. Theoretical Framework



H1: The installation of security programs creates awareness among the general public about cryptocurrency security risks.
H2: 2FA creates awareness among the general public about cryptocurrency security risks.
H3: Education creates awareness among the general public about cryptocurrency security risks.

These hypotheses form the basis of the theoretical framework, investigating the relationship between awareness of cryptocurrency security risks, the installation of security programs, 2FA, and education in cryptocurrency.

RESEARCH METHOD

The survey questionnaire for this study was developed to explore the topic of Cryptocurrency Security Risk: Awareness among the General Public in Malaysia. A quantitative research design was employed, using an online Google Form to collect data from 150 respondents, all Malaysian citizens. The survey was distributed via popular social media platforms such as WhatsApp, WeChat, Instagram, and Facebook to ensure a broad reach. The sampling technique used was voluntary sampling, where participants self-selected to be involved in the study. This method allowed individuals with an interest or knowledge of cryptocurrency to participate, ensuring a more engaged respondent pool. Participants were assured that their personal information would remain confidential, thus ensuring ethical data handling and privacy during the collection process.

The questionnaire itself was divided into four sections. Section A focused on gathering demographic data, such as gender, age, ethnicity, education level, occupation, and annual income, to provide a detailed background of the participants. This demographic information was essential for understanding the diversity of the respondent pool and its potential impact on cryptocurrency awareness. Section B assessed respondents' knowledge of cryptocurrency, examining their familiarity with key concepts like Blockchain technology, how cryptocurrencies work, and the associated risks. Section C explored specific cryptocurrency security risks, such as phishing attacks, hacking, and the use of fraudulent cryptocurrency exchanges. The aim here was to gauge how aware participants were of these threats and whether they had encountered any of them. Section D focused on protective measures, including the use of security programs, 2FA, and the role of education in enhancing security awareness. This section helped determine what steps respondents were taking to protect themselves in the cryptocurrency space.

For all sections, a 5-point Likert scale was used to measure respondents' agreement with various statements, ranging from 1 ("Strongly Disagree") to 5 ("Strongly Agree"). This provided a structured approach to quantifying opinions and attitudes. The collected data was then analyzed using Pearson SPSS version 27. The analysis began with a demographic summary to understand the respondent profile, followed by descriptive statistics to summarize the levels of awareness, knowledge, and concerns about cryptocurrency security risks. Correlation analysis was conducted to identify potential relationships between demographic factors (such as education level or occupation) and cryptocurrency security awareness. It also explored whether knowledge of cryptocurrency correlated with the adoption of protective measures, such as 2FA or security program installations. This comprehensive approach to data analysis provided valuable insights into the state of cryptocurrency security awareness among the general public in Malaysia.

RESULTS

Table 1. Respondent's Demography Summary (N=150)

Responses	Frequency	Percentage (%)
Gender		
Female	80	53.3
Male	70	46.7
Age		
18 and below	17	11.3
19-22	98	65.3
23-26	24	16
27-30	4	2.7
31-34	3	2
35 and above	4	2.7
Ethnicity		
Chinese	91	60.7
Indian	24	16
Malay	35	23.3
Educational Level		
Bachelor's Degree	102	68
Diploma	1	0.7
Master	11	7.3
PhD	2	1.3
Pre-university	28	17.4
Secondary School	6	5.3
Occupation		
Government	2	1.3
Housewife	1	0.7
Private enterprises	11	7.3
Self-employed	2	1.3
Student	126	84
Unemployed	8	5.3
Annual Income		
118,001 and above	1	0.7
98,001 - 118,000	0	0
78,001 - 98,000	1	0.7
58,001 - 78,000	0	0
38,001 – 58,000	2	1.3
18,001 – 38,000	16	10.7
18,000 and below	60	40
No income	70	46.7

Demographics refer to the statistical characteristics of populations. Based on Table 1, the majority gender in the sample is female, comprising 80 respondents or 53.3%. The age distribution is divided into six groups, with the largest group being those aged 19-22, representing 98 people or 65.3%. In terms of ethnicity, the majority of respondents are Chinese, making up 91 people or 60.7%. Regarding educational level, the majority hold a bachelor's degree, accounting for 102 people or 68% of the sample. In terms of occupation, students dominate, with 126 people or 84% of the respondents identifying as such. Finally, for annual income, the majority of respondents have no income, as 70 people, or 46.7%, are students participating in the survey.

Table 2. Descriptive Statistics, Cronbach's Coefficients Alpha, and Zero-order Correlations for All Study Variables

	Variables	1	2	3	4
1.	Awareness among general public on cryptocurrency security risk	0.931			
2.	Installation of security program	0.658**	0.879		
3.	Two factor authentication (2FA)	0.662**	0.750**	0.910	
4.	Educate the public before investing cryptocurrency	0.657**	0.733**	0.751**	0.847
Number of items		4	4	3	3
Mean		4.031	4.145	4.040	4.076
Standard deviation		0.1	0.055	0.0447	0.1414

Note: N = 150; *p < 0.05, **p < 0.01, ***p < 0.001. The diagonal entries represent Cronbach's coefficients alpha.

In Table 2, the Cronbach's Coefficient Alpha for awareness among the general public regarding cryptocurrency security risks associated with the installation of security programs is 0.658, which is statistically significant at $p < 0.01$. This indicates a moderate internal consistency within the dataset, signifying that the variables used to measure this aspect of awareness are sufficiently reliable. The positive correlation demonstrates that as awareness of cryptocurrency security risks increases, the likelihood of installing security programs also rises among the general public. This suggests that individuals who understand the potential dangers of engaging with cryptocurrency—such as phishing, man-in-the-middle attacks, and malware—are more inclined to take proactive measures to secure their digital assets by installing protective software. It also aligns with existing literature, which highlights the essential role of security programs in mitigating cybersecurity risks (Mirčevski et al., 2023).

Similarly, the correlation between risk-related awareness and the use of 2FA is 0.662, also significant at $p < 0.01$. This suggests that heightened awareness of cryptocurrency risks positively influences the adoption of 2FA, reinforcing the idea that users who are more knowledgeable about potential threats are more likely to use this added layer of protection to safeguard their accounts. 2FA, by requiring a secondary authentication method, provides a critical barrier against unauthorized access to cryptocurrency wallets, reducing the risk of cyberattacks like hacking or account compromise. This correlation suggests that educating the public on cryptocurrency security should emphasize the importance of 2FA as an integral aspect of account protection, a sentiment echoed by Reese et al. (2019).

The Cronbach's Coefficient Alpha for the relationship between the installation of security programs and the use of 2FA is 0.750, which is statistically significant at $p < 0.01$. This high correlation indicates that individuals who install security programs are also more likely to adopt 2FA, showing a strong relationship between the two security measures. This finding reflects a broader trend where individuals who are committed to enhancing the security of their cryptocurrency transactions are likely to adopt multiple layers of protection. This synergy between security programs and 2FA highlights the effectiveness of using a combination of defensive strategies to create a more robust security framework against various cyber threats.

Furthermore, Cronbach's Coefficient Alpha for educating the public about cryptocurrency before investing is 0.657 for awareness of security risks, 0.733 for the installation of security programs, and 0.751 for 2FA, all statistically significant at $p < 0.01$. These correlations demonstrate that individuals who prioritize educating themselves before investing in cryptocurrency are not only more aware of potential security risks but also more likely to take actionable steps to mitigate those risks through the installation of security programs and the use of 2FA. The role of education as a critical factor in promoting comprehensive security measures among cryptocurrency users cannot be understated. By equipping users with the necessary knowledge about the vulnerabilities in the cryptocurrency landscape, education empowers them to take informed actions that protect their investments. This finding supports previous research, such as Camp (2024), which emphasizes the importance of public education in navigating the complex and often risky world of digital currencies.

Overall, the results indicate that education significantly influences a user's approach to securing their cryptocurrency transactions. Educated users are not only more cognizant of the security risks but are also more likely to engage in protective behaviors like installing security programs and using 2FA, thereby reducing their susceptibility to cyberattacks. This strong link between education and security practices underscores the importance of implementing educational initiatives aimed at improving public understanding of cryptocurrency risks and the measures available to mitigate them. Consequently, governments, financial institutions, and educational organizations should collaborate to launch comprehensive awareness campaigns and training programs that target both novice and experienced cryptocurrency users to foster a safer digital investment environment.

Table 3. Summary of Regression Analysis

Variables		Awareness Among the General Public of Cryptocurrency Security Risk
1.	Installation of security program	0.267***
2.	Two-factor authentication (2FA)	0.264***
3.	Educate the public before investing in cryptocurrency	0.263***
R^2		0.523
F Value		53.44
Durbin-Watson Statistic		1.715

Note: N=150, *p < 0.05, **p < 0.01, ***p < 0.001

Based on Table 3, the results align well with the proposed hypotheses and confirm the positive relationship between the independent variables—installation of security programs, two-factor authentication (2FA), and education—and the dependent variable, awareness of cryptocurrency security risks among the general public in Malaysia.

H1, which posits that the installation of security programs creates awareness of cryptocurrency security risks, is supported by the regression analysis. The significant p-value (***p < 0.001) and the positive coefficient of 0.267 indicate that installing security programs significantly increases awareness. This shows that the presence of such programs plays a critical role in educating the public about potential risks.

H2, which suggests that 2FA creates awareness of cryptocurrency security risks, is also substantiated by the results. With a coefficient of 0.264 and a highly significant p-value (***p < 0.001), the use of 2FA clearly enhances public awareness. This supports the

hypothesis that implementing additional layers of security leads to better risk comprehension and protection of digital assets.

H3, which asserts that education creates awareness of cryptocurrency security risks, is confirmed as well. The regression coefficient of 0.263 and a significant p-value (***p < 0.001) show that educating the public about cryptocurrency increases awareness. This emphasizes the value of knowledge in mitigating risks and guiding investment decisions.

In conclusion, the results support all three hypotheses, demonstrating that the installation of security programs, the use of 2FA, and education are all critical in raising awareness about cryptocurrency security risks, with these factors explaining 52.3% of the variance in public awareness.

DISCUSSION

The results of this study underscore the significant role that security measures such as the installation of security programs, the implementation of two-factor authentication (2FA), and public education play in raising awareness about cryptocurrency security risks among the general public in Malaysia. The findings showed that these three factors were positively correlated with increased awareness, supporting the hypotheses that the installation of security programs (H1), the use of 2FA (H2), and public education (H3) all contribute to mitigating risks in the cryptocurrency space.

As cryptocurrency continues to gain traction, its attractiveness stems from its potential use not only as a medium of exchange but also as a speculative asset and mining opportunity (Hayes, 2017). Cryptocurrencies such as Bitcoin have even been found to act as a hedge against market volatility (Bouri et al., 2021). However, as highlighted by Extance (2015), the value of cryptocurrencies is market-driven, not network-driven, underscoring the critical need for security awareness. The findings that public awareness about phishing, one of the most common cryptocurrency risks, is high, align with Fu et al. (2022), who emphasized phishing as a major threat to cryptocurrency ecosystems. This research confirmed that the general public understands that user errors, such as falling for phishing scams, can lead to substantial losses in digital currency, especially since cryptocurrency transactions often make user data publicly accessible, increasing vulnerability (Khonji et al., 2013).

Man-in-the-middle attacks are another prevalent threat, where attackers intercept communications to steal cryptocurrency information (Shaik, 2021). As the results showed, public awareness of such risks is growing, aligning with the literature on how malware can compromise sensitive information without detection (Mallik, 2019). This increasing awareness is crucial, as public networks used for cryptocurrency transactions can easily become entry points for these kinds of attacks. The high level of public concern over these risks reinforces the findings that 2FA, which provides an additional layer of security by requiring both a password and a secondary verification method (such as a hardware token), is recognized as an effective protective measure (Reese et al., 2019). The positive impact of 2FA on security awareness demonstrated in this study aligns with its established role in preventing unauthorized access to accounts, as discussed by Shaik (2021).

The lack of sufficient regulatory oversight in the cryptocurrency market continues to be a challenge, contributing to unethical practices such as wash trading and fake cryptocurrency exchanges (Human, 2023). This research indicated that the public is increasingly aware of the risks posed by scam exchanges, with Xia et al. (2020)

documenting a high number of scam domains and fake exchange apps in circulation. The study's results highlight the vital role of security programs in addressing these risks by detecting fraudulent websites and emails (Mirčevski et al., 2023). Security programs, as demonstrated by the positive regression results in this study, significantly contribute to public awareness by identifying potential threats before users engage in cryptocurrency transactions.

Education also emerged as a critical factor in mitigating security risks. As Camp (2024) highlighted, the lack of knowledge can make users more vulnerable to sudden market shifts and regulatory changes. This study found that public education about cryptocurrency significantly enhances awareness, allowing users to make informed decisions and avoid falling prey to scams. Educated investors are better equipped to recognize the risks involved in cryptocurrency transactions and are more likely to adopt preventive measures such as 2FA and security programs. The positive impact of education on awareness in this study corroborates Shahzad et al. (2024), who argued that educational initiatives such as workshops, campaigns, and conferences can significantly improve public trust and comprehension of cryptocurrency.

The implications of these findings are far-reaching. For cryptocurrency adoption to grow sustainably, it is imperative that the public not only understands the basic mechanics of digital currencies but also the security risks and protections associated with them. The significant impact of security programs, 2FA, and education in this study suggests that stakeholders—including financial institutions, governments, and educators—should prioritize these areas to foster a secure and informed environment for cryptocurrency users. Collaborative efforts to provide educational resources and promote awareness can enhance the public's confidence in cryptocurrencies, ensuring a safer and more resilient cryptocurrency ecosystem for the future.

In conclusion, this research reinforces the importance of a multifaceted approach to enhancing public awareness of cryptocurrency security risks. By addressing the significant factors of security programs, 2FA, and education, key stakeholders can effectively reduce the risks associated with digital currencies and promote more secure investment practices in the ever-evolving cryptocurrency landscape.

CONCLUSION

The research has highlighted key characteristics of public awareness in Malaysia regarding cryptocurrency security risks. A significant portion of the general public is already familiar with cryptocurrencies, and some have actively engaged with them. It is encouraging that respondents demonstrate a satisfactory level of awareness about security risks associated with cryptocurrency investments. Many understand the inherent risks and are taking necessary precautions to protect their digital assets, recognizing that threats such as phishing, man-in-the-middle attacks, and fake cryptocurrency exchanges are ever-present and can lead to substantial financial losses.

In response to these risks, several important recommendations can be made. First and foremost, there is a need to strengthen public education and awareness initiatives around cryptocurrencies. Publicity campaigns, workshops, and educational modules should be designed to equip investors with a deep understanding of how cryptocurrencies operate, the characteristics of the market, and the associated risks. This knowledge will empower investors to make informed decisions, remain vigilant, and invest prudently. As the cryptocurrency market grows and evolves, continuous education will be crucial in helping users adapt to new developments, trends, and emerging threats.

Additionally, improving account security is essential. Investors should be encouraged to install robust security programs that can detect and prevent threats such as suspicious emails, phishing attempts, and fraudulent websites. The use of 2FA should also be promoted, as it provides an extra layer of security by requiring both a password and a second form of verification, such as a phone code or hardware token. These measures significantly reduce the likelihood of unauthorized access to crypto accounts and digital assets.

Another key recommendation is for investors to comply with local laws and regulations to mitigate risks associated with illegal activities. Regulatory frameworks can help curb unethical practices, such as market manipulation and fraudulent exchanges. Therefore, ensuring that cryptocurrency transactions align with legal requirements can provide investors with an additional layer of protection.

Online cryptocurrency platforms also have a responsibility to improve their security measures continuously. By investing in stronger security protocols and enhancing platform reliability, exchanges and wallets can safeguard user assets from cyberattacks. Moreover, platforms should allocate adequate resources to address the most critical factors affecting user trust, such as secure trading environments and transparent operations.

In line with these recommendations, business entities involved in cryptocurrency should regularly review and update their product descriptions, specifications, and pricing to maintain accuracy and consistency, as suggested by Gan et al. (2024). This will not only enhance the trustworthiness of cryptocurrency offerings but also contribute to more informed consumer decisions.

Looking to the future, the development of the cryptocurrency market should prioritize large-scale and sustainable growth while ensuring enhanced reliability and security. As more cryptocurrencies emerge, the ecosystem will become richer and more diverse, attracting a broader range of users. Sustainable growth will depend on fostering trust among investors and ensuring that technological advancements in security keep pace with market expansion.

Furthermore, consumer satisfaction will play a vital role in shaping the future of cryptocurrencies. As noted by Kee et al. (2023), customer satisfaction is closely linked to brand loyalty. Therefore, cryptocurrency platforms that deliver secure and reliable services are likely to build stronger customer relationships, driving long-term loyalty and contributing to the market's success.

In conclusion, while cryptocurrencies offer exciting opportunities, they also present significant security risks that require ongoing attention. A proactive approach—one that includes public education, improved security measures, regulatory compliance, and continuous platform enhancements—will help mitigate these risks. As the cryptocurrency ecosystem grows, it is vital to ensure that both individual investors and businesses are well-equipped to navigate the complexities of this rapidly evolving landscape. With these steps in place, the future of cryptocurrencies holds the promise of sustainable development, greater reliability, and a robust, trusted digital financial ecosystem.

ACKNOWLEDGMENT
N/A

DECLARATION OF CONFLICTING INTERESTS

The authors declared no potential conflicts of interest.

REFERENCES

Ajupov, A., Sherstobitova, A., Syrotiuk, S., & Karataev, A. (2019). The risk-management theory in modern economic conditions. In *E3S Web of Conferences* (Vol. 110, p. 02040). EDP Sciences. https://doi.org/10.1051/e3sconf/201911002040

Al-Amri, R., Zakaria, N. H., Habbal, A., & Hassan, S. (2019). Cryptocurrency adoption: current stage, opportunities, and open challenges. *International Journal of Advanced Computer Research, 9*(44), 293-307. http://dx.doi.org/10.19101/IJACR.PID43

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research, 48*(7), 953-977. https://doi.org/10.1177/0093650218800915

Bouri, E., Gabauer, D., Gupta, R., & Tiwari, A. K. (2021). Volatility connectedness of major cryptocurrencies: The role of investor happiness. *Journal of Behavioral and Experimental Finance, 30*, 100463. https://doi.org/10.1016/j.jbef.2021.100463

Breuer, F., Goyal, V., & Malavolta, G. (2021, September). Cryptocurrencies with security policies and two-factor authentication. In *2021 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 140-158)*. IEEE. https://doi.org/10.1109/EuroSP51992.2021.00020

Britannica Money. (2024). *Cryptocurrency*. Britannica Money. https://www.britannica.com/money/cryptocurrency

Camp, S. (2024, August 1). *The importance of user education in crypto*. Fideum. https://www.fideum.com/blog/the-importance-of-user-education-in-crypto

Connecticut's Official State Website. (n.d.). *Cryptocurrency Risks*. Connecticut's Official State Website. Shttps://portal.ct.gov/dob/consumer/consumer-education/cryptocurrency-risks

Edeh, F. O., Aryani, D. N., Kee, D. M. H., Samarth, T., Nair, R. K., Tan, Y. S., & Teh, Y. C. (2021). Impact of COVID-19 pandemic on consumer behavior towards the intention to use E-wallet in Malaysia. *International Journal of Accounting & Finance in Asia Pasific, 4*(3), 42-59. https://doi.org/10.32535/ijafap.v4i3.1205

Eigbe, O. E. (2018). Investigating the levels of awareness and adoption of digital currency in Nigeria: a case study of bitcoin. *The Information Technologist, 15*(1), 75-82.

Extance, A. (2015). Bitcoin and beyond. *Nature, 526*(7571), 21. https://doi.org/10.1038/526021a

Fu, B., Yu, X., & Feng, T. (2022). CT-GCN: A phishing identification model for blockchain cryptocurrency transactions. *International Journal of Information Security, 21*(6), 1223-1232. https://doi.org/10.1007/s10207-022-00606-6

Gan, K. H., Lim, S. H., Aronkar, P., Lim, W. S., Lin, X., Hashim, M. B. M., ... & Kee, D. M. H. (2024). Investigating the relationship between key factors and customer satisfaction in an online shopping platform. *Journal of the Community Development in Asia, 7*(2), 149-162. https://doi.org/10.32535/jcda.v7i2.3213

Hayes, A. S. (2017). Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. *Telematics and Informatics, 34*(7), 1308-1321. https://doi.org/10.1016/j.tele.2016.05.005

Human, K. B. (2023). *A systematic review of cryptocurrencies use in cybercrimes* [Master's thesis, University of Central Florida]. STARS Library UCF. https://purls.library.ucf.edu/go/DP0028045

Kee, D. M. H., Lai, K. H., Lee, J. C., Lee, K. J., Lee, J. L., Yosanti, I., & Aryani, D. N. (2022a). Do you have a digital wallet? A study of e-wallet during the Covid-19 pandemic. *International Journal of Accounting & Finance in Asia Pasific, 5*(1), 24-38. https://doi.org/10.32535/ijafap.v5i1.1413

Kee, D. M. H., Ow, A. L., Ooi, Z. J., Sathiaseelan, P., Pang, K., Sathyan, K. A., & Madhan, S. (2022b). Have you touched? A case study of Touch n Go e-wallet. *International Journal of Accounting & Finance in Asia Pasific, 5*(1), 84-94. https://doi.org/10.32535/ijafap.v5i1.1416

Kee, D. M. H., Sin, L. G., Yuan, N. Z., Ni, N. L. Y., Wen, N. K., Fang, N. S., ... & Muhsyi, U. A. (2023). The influence of customer satisfaction, brand trust and brand loyalty on purchase intention: A study of McDonald's in Malaysia. *International Journal of Tourism and Hospitality in Asia Pasific, 6*(2), 88-101. https://doi.org/10.32535/ijthap.v6i2.2343

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: A literature survey. *IEEE Communications Surveys & Tutorials, 15*(4), 2091-2121. https://doi.org/10.1109/SURV.2013.032213.00009

Liu, K., Zhou, Z., Cao, Q., Xu, G., Wang, C., Gao, Y., ... & Xu, G. (2023). A robust and effective Two-Factor Authentication (2FA) protocol based on ECC for mobile computing. *Applied Sciences, 13*(7), 4425. https://doi.org/10.3390/app13074425

Luchkin, A. G., Lukasheva, O. L., Novikova, N. E., Melnikov, V. A., Zyatkova, A. V., & Yarotskaya, E. V. (2020, August). Cryptocurrencies in the global financial system: problems and ways to overcome them. In *Russian Conference on Digital Economy and Knowledge Management (RuDEcK 2020)* (pp. 423-430). Atlantis Press. https://doi.org/10.2991/aebmr.k.200730.077

Madavaram, R. (2022, May 16). *Malaysia's crypto scene is booming. What are the risks?.* NST Online. https://www.nst.com.my/business/2022/05/796525/malaysias-crypto-scene-booming-what-are-risks

Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi, 2*(2), 109-134. http://dx.doi.org/10.22373/cj.v2i2.3453

Mirčevski, J., Popović, N. B., Andrić, M., & Stanojev, B. (2023). Security of financial software to support cryptocurrency trading. In *BISEC'22: 13th International Conference on Business Information Security, December 03, 2022, Belgrade, Serbia*.

Notabene. (2023, June 6). *Travel Rule Crypto regulation in Malaysia*. Notabene. https://notabene.id/world/malaysia

Oswego State University of New York. (n.d.). *The Basics About Cryptocurrency*. Oswego State University of New York. https://www.oswego.edu/cts/basics-about-cryptocurrency#:~:text=A%20cryptocurrency%20is%20a%20digital,you%20need%20a%20cryptocurrency%20wallet.

Pacheco, R. (2024, April 24). *Cryptocurrency Security in 2024: Essential Guide to Protecting Your Crypto.* Swiss Money. https://swissmoney.com/cryptocurrency-security/

Peter, J. A., & Ogunlade, O. O. (2024). Connectivism theory in education and its applications to curriculum and instruction. *ASEAN Journal of Educational Research and Technology, 3*(3), 215-222.

Rahman, I. A., & Wulandari, H. D. (2022). Cryptocurrency price volatility analysis on bitcoin and altcoins before and during the COVID-19 Pandemic in Indonesia. *Journal of International Conference Proceedings, 5*(5), 182-194. https://doi.org/10.32535/jicp.v5i5.2008

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A usability study of five {two-factor} authentication methods. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)* (pp. 357-370).

Rice, M. (2019). *Cryptocurrency: History, advantages, disadvantages, and the future* [Senior honor theses, Liberty University Honors Program]. Scholars Crossing: The Institutional Repository of Liberty University https://digitalcommons.liberty.edu/honors/933

Roppelt, J. C. (2019). *Security risks surrounding cryptocurrency usage: a study on the security risks of cryptocurrencies and how security perception affects usage* [Master's thesis, University of Twente]. University of Twente Student Theses. http://essay.utwente.nl/79471/

Shahzad, M. F., Xu, S., Lim, W. M., Hasnain, M. F., & Nusrat, S. (2024). Cryptocurrency awareness, acceptance, and adoption: The role of trust as a cornerstone. *Humanities and Social Sciences Communications, 11*(1), 1-14. https://doi.org/10.1057/s41599-023-02528-7

Shaik, C. (2021). Defeating MITM attacks on cryptocurrency exchange accounts with individual user keys. *International Journal of Network Security & Its Applications, 13*(1).

Suruhanjaya Sekuriti. (n.d.). *The trading, issuance and safekeeping of Digital Assets in Malaysia are regulated by the Securities Commission.* Suruhanjaya Sekuriti. https://www.sc.com.my/digital-assets

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

Zaineldeen, S., Hongbo, L., Koffi, A. L., & Hassan, B. M. A. (2020). Technology acceptance model'concepts, contribution, limitation, and adoption in education. *Universal Journal of Educational Research, 8*(11), 5061-5071. http://dx.doi.org/10.13189/ujer.2020.081106

Zubir, D. A. S. B. H. M., Aishah, D. N., Ali, D. A., Mokhlis, D. S., & Sulong, D. F. (2020). Doing business using cryptocurrency in Malaysia. *International Journal of Management and Humanities, 4*(9), 148-157. https://doi.org/10.35940/ijmh.I0899.054920

ABOUT THE AUTHOR(S)

1st Author
Azura Abdullah Effendi is a Senior Lecturer at Universiti Sains Malaysia. She teaches both undergraduate and postgraduate students Management and Organizational Behavior courses. She researches on Emotional Intelligence, Leadership, and various work values. She also supervises Master's and Doctoral candidates in these fields. Dr. Azura serves as a consultant for USM and the industry and external examiner to several universities. Member of the Malaysian Institute of Management (MIM), Malaysian Institute of Human Resource Management (MIHRM), and Asian Academy of Management (AAM). She has co-written books on Organizational Behaviour. She serves as a regular reviewer for World Applied Science Journal, Asian Academy of Management Journal, Universiti Tun Hussein Onn Malaysia Publishing Office, Asian Academy of Management Conference, and International Conference on Customer Service and Systems Management. Her research interest are Emotional Intelligence, Leadership and Work Values, Knowledge Sharing, Entrepreneurship and SMEs, Organizational Behavior
Email: azura_e@usm.my
Orcid ID: 0000-0003-3849-2912

2nd Author
Boon Keong Teow work in ViTrox College as a lecturer teaching Mathematics for Engineering and Computer Science students. He is also a trainer for Kangaroo Maths Competition and the Data Analysis with common softwares like Excel and Spreadsheets. He have one year experience in the production lead time analysis during my previous employment. He is responsible to look through the whole business processes while calculating the lead time for each of the single processes. Her research field is in Numerical Analysis. He is advanced in Data Analysis, Applied Mathematics field. He also possess intermediate knowledge in Finance field. Graduated in 2021 from UUM in Bachelor of Science (Hons.) Business Maths (Major Maths, minor Finance) with Vice Chancellor Gold Medal. He also graduated from Master in Maths in 2023 with CGPA 4.00. He is currently pursuing PhD in Applied Mathematics (Numerical Analysis).
Email: crowinxteow@gmail.com
Orcid ID:

3rd Author
Kai Guan The is an undergraduate student from USM who is studying the accounting course. He's passionate in accounting which hopes to grow as a balance in study and his interest.
Email: tehkaiguan1129@student.usm.my

4th Author
Yin Ann Tan is currently undergraduate student with disciplines on Materials Engineering at Universiti Sains Malaysia.
Email: yinann1130@student.usm.my

5th Author
Hsue Li Tay is currently undergraduate student at Universiti Sains Malaysia.
Email: hsueli@student.usm.my

6th Author
Yuxin Tang is currently undergraduate student at Universiti Sains Malaysia.
Email: tangyuxin@student.usm.my

7th Author
Simran Chaudhary is currently undergraduate student at IMS Engineering College.
Email: Simranchaudhary703@gmail.com

8th Author
Daisy Mui Hung Kee is an Associate Professor at the School of Management, Universiti Sains Malaysia. Her areas of interests are in Human Resource Management, Organizational Behavior, Work Values, Leadership, Entrepreneurship, and Psychosocial safety climate. Her current program of research focuses on Leadership and Psychosocial safety climate. She holds a PhD in Business and Management from International Graduate School of Business, University of South Australia. She was the secretary of Management Case Study Journal, Australia (2004-2006). She was award recipient of Merdeka Award 2006 from the Australia Malaysia Business Council of South Australia (AMBCSA) by former South Australia Governor Sir Eric Neal (2006). The award recognizes the Most Outstanding Malaysian University students in South Australia.She earned her MBA from School of Management, Universiti Sains Malaysia. She was awarded Dean's List for being one of the top MBA students (2003). Presently, she is an active academician and researcher supervising a numbers of MBA, MA and PhD candidates with working experience across diverse industries. She has published a good

numbers of journal papers during the course of her career. She has conducted series of training related to motivation and research in USM under Professional and Personal Development (PPD) workshop.

Email: daisy@usm.my
ORCID ID: 0000-0002-7748-8230