

Impact of using cryptocurrency to maintain cyber security blockchain innovations and applications

Debajyoti Sarkar

Department of Commerce, Rajiv Gandhi University, Itanagar, Arunachal Pradesh, India

ABSTRACT

Purpose: Cryptocurrency has been identified as a form of currency that can be transferred through a “Digital platform.” Such “cryptocurrencies” are presented in the form of a large amount of data that can be leveraged through networks. Due to the presence of key gaps and a lack of strong authentication of these networks, both the data and the transaction details of the users are easily available and accessible to the hackers. **Methodology:** A deductive approach has been used in the present study to generate hypotheses and variables from the previous studies. For this study, the authors developed a survey questionnaire and collected data from 50 potential respondents sampled through simple random sampling method. After the data were collected, the researcher analyzed the data using paired sample test, correlation, one-sample T test, and F-test **Findings:** The present study findings infer that cryptocurrency has a positive impact on development and innovation of blockading technologies and cybersecurity. Most of the participants were unaware that clicking on malicious websites may provide accessibility to hackers. The study found that there is a huge increase experienced in the number of malicious actions, phishing attacks, cyber threats, scams, and financial frauds. Henceforth, the growth of cryptocurrency has enforced companies to develop and innovate blockchain applications to increase the integrity and security of transactions. **Implications:** Cyber security plays a key role in ensuring the integrity, transparency, authentication, and reliability of the data and networks, especially in the case of Fintech organizations. The primary aim of the study was to analyze the impact of using cryptocurrencies to achieve cyber security, maintain blockchain innovations, and secure other technological applications. **Originality:** The originality of the study is fully authentic.

Key words: Authentication, blockchain, cryptocurrency, cyber security, cyber threats, transparency

INTRODUCTION

The term “Crypto currency” can be explained as a “digital currency” that has been used across the world as an alternative method of payment with the help of encryption algorithms. After it was introduced in the

year 2009, the exchange value of cryptocurrency has increased by 300% in the year 2020 (Varghese et al., 2021). According to (Ramos et al., 2022), “encryption technologies” has also been used in cryptocurrencies so that they can be used both as a currency as well as a virtual accounting system.

*Corresponding author:

Debajyoti Sarkar, Department of Commerce, Rajiv Gandhi University, Itanagar, Arunachal Pradesh, India.

E-mail: mithumimi9@gmail.com

Received: April 17, 2023; **Revised:** June 19, 2023; **Accepted:** August 20, 2023

DOI: 10.18843/ijcms/v14i3/02

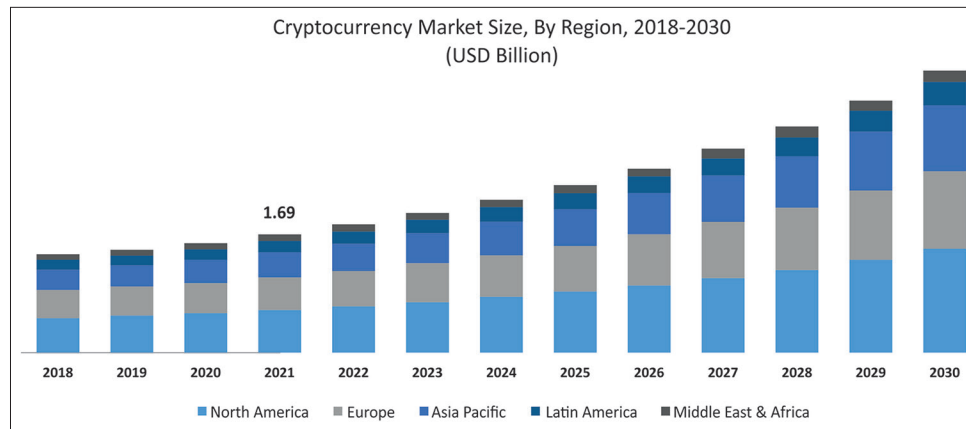


Figure 1: Market of cryptocurrency on a global scale from July 2018 to March 2030
Source: (Debajyoti, 2023)

Figure 1 provides an overview on the growing market of cryptocurrencies across the world, which has been estimated to be “1.69 billion USD. Moreover, the growth rate of crypto currency has also been accounted at a rate of 7.2% CAGR (Research and Markets, 2022). However, the main support for this growth stems from the fact that blockchain technologies and applications have been widely adopted for security and protection of the transactions that handle cryptocurrencies. The cryptocurrency trading has been valued at 2 Trillion USD as on June 2023 (Onyekwere et al., 2023).

Rationale

Various challenges have been raised in the use of cryptocurrencies such as lack of understanding, lack of regulatory frameworks, volatility, security risks, transaction irreversibility, and uncertainty regarding taxation and scalability issues. According to (Choithani et al., 2022), there has been a significant increase in fraud cases, misleading transactions, and the theft of digital currencies around the world due to the lack of proper regulatory frameworks. The number of scams has increased in cryptocurrency from October 2020 to March 2021. The total loss was found to be 80 Million USD lost by 7000 people (Weichbroth et al., 2023).

Figure 2 provides an overview on market capitalization of cryptocurrencies from 2010 to 2023. There has been a significant growth in the market capitalization of digital currencies from 250.82 billion US Dollars to 869.37 US Dollars. Moreover, the market capitalization also has been estimated to be 1851.2 billion US dollars in September 2021 (Debajyoti, 2023).

Objectives

The objectives of the study are as follows:

- To provide a broad scope on the use of cryptocurrency to enhance the security of blockchain innovation and other applications
- To critically evaluate the challenges faced by the business organizations to adopt blockchain applications and innovative tools
- To provide a set of strategies that can be used by the companies to increase the effectiveness of cryptocurrency, blockchain applications, and innovations.

Literature Review

Impact of cryptocurrency on blockchain technologies and cyber security

Cryptocurrency is creating a positive impact on the adoption and innovation of blockading technologies and cyber security. (Deshmukh et al., 2022) mentioned that cryptocurrency has imposed several threats on the users due to which the development of blockchain has become a norm in the modern era. In this same context, blockchain technologies and other innovative applications are also playing a huge role to protect the digital transactions.

In addition to this, blockchain innovation implies that the financial and transactional data are encrypted and the public and private data are maintained in the most secure form to protect the digital assets such as cryptocurrency. Besides that, blockchain allows the users to send money or transact the payment under strong protection and high-security networks. Cybercrime has increased a lot though various measures have been taken by the regulatory authorities (Sailaja and Thamodaran, 2016). On the other hand, cyber

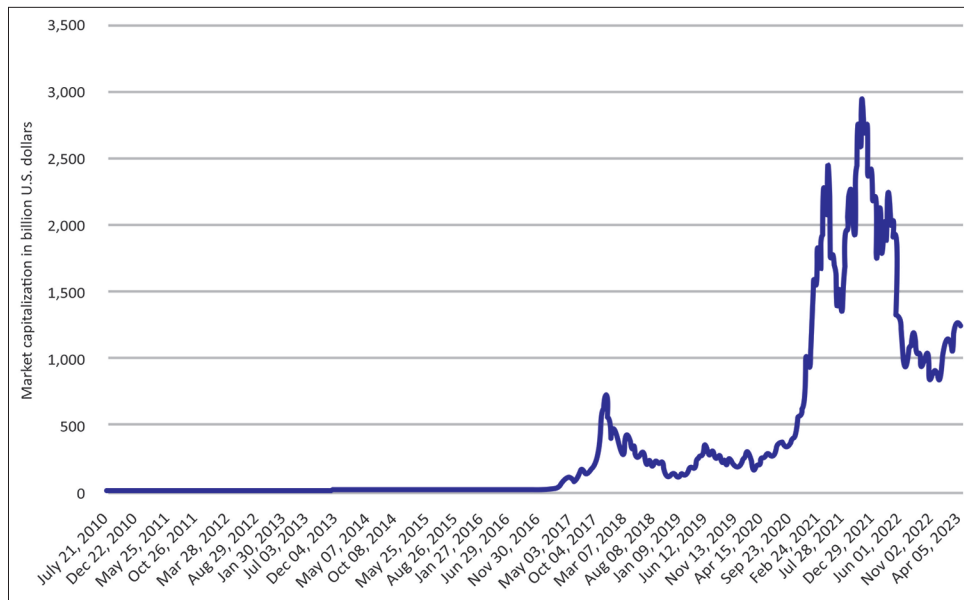


Figure 2: Overall market capitalization of cryptocurrency
Source: (Statista, 2023)

security measures have also increased their standards so that the cyber threats can be get rid of and the data can be secured.

Challenges of using cryptocurrency

The prevalence of using cryptocurrencies has also increased in the recent decade. According to (Bhardwaj et al., 2022), financial transaction is neither governed, monitored nor controlled by a regulatory authority, due to which the cryptocurrency has been leading to the growth of cyber threats. Moreover, the use of cryptocurrency has also given rise to the growth of illegal trading platforms that are used for financial frauds by cybercriminals. On the other hand, hackers use phishing attacks in which whenever a user clicks a malicious link or a website, sent by the hackers, the details of the crypto users get hacked and their digital assets are stolen.

Strategies to improve cryptocurrency and blockchain

Crypto users need to make sure that they are well aware of and have in-depth insights about cryptocurrency to make safe transactions. Besides that, the governments also need to adopt various policies and adhere to regulations to strictly regulate, monitor and control the transactions, and punish the cybercriminals. (Fahmi et al., 2023) mentioned that the users must avoid clicking and trusting unknown parties or web links without proper verification of their profiles, as these websites may be malicious and a trap for the users to steal their valuable information. In addition to these, the governments should also develop a regulatory framework for addressing the trading

of illegal platforms and tools by hackers. Furthermore, the blockading application should be developed in a way such that it would not allow access to third parties.

Theoretical framework

For this study, the Short Interest Theory has been adopted as it is appropriate for stock market investments. (Sakas et al., 2022) mentioned that short interest has been considered as a precursor, when the value of cryptocurrency increases. However, greater the interest is, higher the risk would be. On the other hand, a high short interest implies that due to lack of accuracy and transparency, most of the investors tend to sell their stocks.

This is mainly due to the fact that traders and investors use different tools to generate the predicted results. As a result, it helps the traders to make a profitable investment. In addition to this, the short sellers also create a pressure on huge supplies and buying to reduce the value of cryptocurrencies. Yu et al. (2022) noted down that Short Interest Theory also focuses on buying and selling decisions of crypto currencies, which results in the action of threats.

METHODOLOGY

Research Approach

In the present study, a deductive approach has been used to generate different types of hypotheses and variables from

the existing studies. This type of deductive approach helps the researchers to focus on the existing literature reviews.

Research Philosophy

Positivism philosophy has been adopted for the study as it allows the researchers to adhere to the scientific viewpoint of the data. Moreover, this philosophy also allows the research to provide only factual, scientific, and truthful data, which in turn provide an objective perspective to the entire study.

Research Design

The present study follows the descriptive design so that it can develop a better understanding about the situation, phenomena, and entire population. Descriptive design also allows the study to use different kinds of techniques, approaches, and procedures.

Sample Size and Technique

The authors made use of survey-based data collection process. The total number of members surveyed for this research was 50. A simple random sampling technique was used to determine the participants from the total population.

Data Collection

In this research, primary methods were used for data collection process. However, the strategy of the research has

been to extract quantitative data directly from the primary sources, in line with (Tibrewal et al., 2022). The main purpose of using a primary method is that it helps the researchers in gathering real, universal, and truthful data. As a result, these research methods have also helped to enhance the validity, and reliability of the data. In addition to these, the authors developed a survey questionnaire as a research tool to collect the data. However, the questionnaires would be provided to the participants with the help of Google Forms.

Data Analysis

The authors made use of Google Forms to collect the responses from the respondents. After data collection, SPSS was used to analyze the quantitative data. In this study, the authors conducted F test, t-test, Chi-square test, sample test, and correlation analysis. The main purpose of using SPSS is to determine the influence of independent variables on the dependent variables (Garg, 2022).

RESULTS

Demographic Analysis

Sample test

Table 1 shows the differences in relationship between the variables under consideration. As mentioned earlier, the authors made use of SPSS to compare the relationship between the variables. The mean value of the first pair from sample test was found to be -1.180 . Moreover, the standard deviation value of the first pair was 1.004 . The mean value

Table 1: Paired sample test

| | Paired sample test | | | | | t | df | Sig. (2-tailed) |
|---|--------------------|-------|-----------------|---|--------|--------|----|--------------------|
| | Paired differences | | | | | | | |
| | Mean | SD | Std. error mean | 95% confidence interval of the difference | | | | |
| | | | Lower | Upper | | | | |
| Pair 1 | | | | | | | | |
| What is your gender? | -1.180 | 1.004 | 0.142 | -1.465 | -0.895 | -8.312 | 49 | 0.000 |
| Do you think that cryptocurrency has a positive effect on the development and innovation of blockading technologies and cyber security? | | | | | | | | |
| Pair 2 | | | | | | | | |
| What is your age? | -0.340 | 1.272 | 0.180 | -0.701 | 0.021 | -1.891 | 49 | 0.065 |
| Do you consider that use of cryptocurrencies has been increasing the number of cyber threats? | | | | | | | | |

Table 2:

Correlation test

| | What is your gender? | What is your age? | Do you think that Crypto currency has a positive effect on the development and innovation of Block chain technologies and cyber security? | Do you believe Block chain allows users to make safe and secure transaction? | Do you consider that use of crypto currencies has been increasing the number of cyber threats? | Do you agree that by clicking on malicious websites, it gives accessibility to the third parties and Hackers? | Do you think that Block chain applications has been playing a key role to increase the integrity and security of transactions? | Do you believe that the growth of fraud cases, hacking, and theft of digital currencies has been due to the growth of cryptocurrency? | Do you consider that regulatory framework is very important for the crypto users in order to eliminate the trading of illegal platforms and tools by hacker? |
|--|----------------------|-------------------|---|--|--|---|--|---|--|
| What is your gender? | 1 | 0.170 | 0.197 | -0.030 | 0.043 | -0.204 | -0.180 | 0.279* | -0.078 |
| Pearson correlation | | | | | | | | | |
| Sig. (1-tailed) | | 0.118 | 0.085 | 0.418 | 0.384 | 0.077 | 0.106 | 0.025 | 0.295 |
| n | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 |
| What is your age? | 0.170 | 1 | 0.349** | 0.367** | 0.294* | 0.202 | 0.244* | 0.193 | 0.032 |
| Pearson correlation | | | | | | | | | |
| Sig. (1-tailed) | 0.118 | | 0.006 | 0.004 | 0.019 | 0.079 | 0.044 | 0.089 | 0.412 |
| n | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 |
| Do you think that Crypto currency has a positive effect on the development and innovation of Blockading technologies and cyber security? | | | | | | | | | |

(Contd...)

Table 2: (Continued)

| | | Correlation test | | | | | | | | | |
|---|--------|------------------|---------|---------|--------|-------|---------|--------|--------|----|----|
| Pearson correlation | 0.197 | 0.349** | 1 | 0.422** | 0.274* | 0.057 | 0.100 | 0.122 | -0.078 | | |
| Sig. (1-tailed) | 0.085 | 0.006 | | 0.001 | 0.027 | 0.348 | 0.244 | 0.199 | 0.295 | | |
| <i>n</i> | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 |
| Do you believe that Block chain allows users to make safe and secure transaction?? | | | | | | | | | | | |
| Pearson correlation | -0.030 | 0.367** | 0.422** | 1 | 0.095 | 0.199 | 0.216 | 0.275* | 0.051 | | |
| Sig. (1-tailed) | 0.418 | 0.004 | 0.001 | | 0.255 | 0.083 | 0.066 | 0.027 | 0.363 | | |
| <i>n</i> | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 |
| Do you consider that use of crypto currencies has been increasing the number of cyber threats? | | | | | | | | | | | |
| Pearson correlation | 0.043 | 0.294* | 0.274* | 0.095 | 1 | 0.200 | 0.138 | 0.075 | 0.039 | | |
| Sig. (1-tailed) | 0.384 | 0.019 | 0.027 | 0.255 | | 0.082 | 0.170 | 0.301 | 0.394 | | |
| <i>n</i> | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 |
| Do you agree that by clicking on malicious websites, it gives accessibility to the third parties and hackers? | | | | | | | | | | | |
| Pearson correlation | -0.204 | 0.202 | 0.057 | 0.199 | 0.200 | 1 | 0.500** | 0.271* | 0.097 | | |
| Sig. (1-tailed) | 0.077 | 0.079 | 0.348 | 0.083 | 0.082 | | 0.000 | 0.028 | 0.252 | | |
| <i>n</i> | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 |

(Contd...)

of the second pair was found to be 0.23. Further, the sample test was conducted to have a better understanding about the effectiveness and relationship of both the hypotheses.

Statistical Analysis

Table 2 shows the results from Pearson's correlation. The correlation test was conducted to measure the value of the variables under study. In general, if the test generates a value <0.05 nb, then it denotes the existence of a significant relationship between the variables. In the present study, the correlation analysis outcomes establish the presence of a significant positive relationship among age, gender, and use of cryptocurrency. In correlation test, one-tailed factor was used.

According to the outcomes from statistical analyses, the study participants firmly believe that cryptocurrency has a positive impact on development and innovation of blockading technologies and cybersecurity. This finding aligns with that of the literature (Caporale et al., 2020) whom mentioned about the significant negative effects of cyberattacks on the probability for cryptocurrencies. Most

of the participants were unaware that clicking on malicious websites may provide accessibility to hackers. In the study conducted earlier (Zwilling et al., 2022), though the participants were adequately aware about the cyberattacks, they failed to install protective measures.

One-Sample Test

Table 3 shows the outcomes of T-test while the primary purpose of performing T-test is to compare two different mean values. In the present study, the one sample T-test value was found to be 3.280. On the other hand, the mean difference was found to be 1.220. The correlation value was found to be significant at both 0.05 and 0.01 levels. This infers that most of the study participants acknowledged their interest toward cryptocurrency which got reflected in the T-test outcomes as well.

Table 4 shows the F-test analysis outcomes and in this study, the F-test achieved a mean square of 0.223 for the first two groups. Furthermore, the mean age value was found to be 1.343. The results derived from the F-test reflected that the

Table 3: One sample t test

| | Test value=0 | | | | | |
|---|--------------|----|-----------------|-----------------|---|-------|
| | t | df | Sig. (2-tailed) | Mean Difference | 95% confidence interval of the difference | |
| | | | | | Lower | Upper |
| What is your gender? | 3.280 | 49 | 0.002 | 0.180 | 0.07 | 0.29 |
| What is your age? | 9.254 | 49 | 0.000 | 1.220 | 0.96 | 1.48 |
| Do you think that Crypto currency has a positive effect on the development and innovation of blockading technologies and cyber security? | 9.566 | 49 | 0.000 | 1.360 | 1.07 | 1.65 |
| Do you believe that blockchain allows users to make safe and secure transaction? | 9.430 | 49 | 0.000 | 1.400 | 1.10 | 1.70 |
| Do you consider that use of cryptocurrencies has been increasing the number of cyber threats? | 9.342 | 49 | 0.000 | 1.560 | 1.22 | 1.90 |
| Do you agree that by clicking on malicious websites, it gives accessibility to the third parties and hackers? | 8.161 | 49 | 0.000 | 1.420 | 1.07 | 1.77 |
| Do you think that blockchain applications have been playing a key role to increase the integrity and security of transactions? | 7.972 | 49 | 0.000 | 1.340 | 1.00 | 1.68 |
| Do you believe that the growth of fraud cases, hacking, and theft of digital currencies has been due to the growth of cryptocurrency? | 10.253 | 49 | 0.000 | 1.580 | 1.27 | 1.89 |
| Do you consider that regulatory framework is very important for the crypto users to eliminate the trading of illegal platforms and tools by hacker? | 8.012 | 49 | 0.000 | 1.300 | 0.97 | 1.63 |

Table 4: F test outcomes

| | Sum of Squares | df | Mean Square | F | Sig. |
|---|----------------|----|-------------|-------|-------|
| What is your gender? | | | | | |
| Between groups | 0.106 | 3 | 0.035 | 0.223 | 0.880 |
| Within groups | 7.274 | 46 | 0.158 | | |
| Total | 7.380 | 49 | | | |
| What is your age? | | | | | |
| Between groups | 4.028 | 3 | 1.343 | 1.602 | 0.202 |
| Within groups | 38.552 | 46 | 0.838 | | |
| Total | 42.580 | 49 | | | |
| Do you think that cryptocurrency has a positive effect on the development and innovation of blockading technologies and cyber security? | | | | | |
| Between groups | 4.303 | 3 | 1.434 | 1.459 | 0.238 |
| Within groups | 45.217 | 46 | 0.983 | | |
| Total | 49.520 | 49 | | | |
| Do you believe that blockchain allows users to make safe and secure transaction? | | | | | |
| Between groups | 2.783 | 3 | 0.928 | 0.833 | 0.482 |
| Within groups | 51.217 | 46 | 1.113 | | |
| Total | 54.000 | 49 | | | |
| Do you consider that use of cryptocurrencies has been increasing the number of cyber threats? | | | | | |
| Between groups | 1.370 | 3 | 0.457 | 0.314 | 0.815 |
| Within groups | 66.950 | 46 | 1.455 | | |
| Total | 68.320 | 49 | | | |
| Do you agree that by clicking on malicious websites, it gives accessibility to the third parties and hackers? | | | | | |
| Between groups | 8.563 | 3 | 2.854 | 2.001 | 0.127 |
| Within groups | 65.617 | 46 | 1.426 | | |
| Total | 74.180 | 49 | | | |
| Do you think that blockchain applications have been playing a key role to increase the integrity and security of transactions? | | | | | |
| Between groups | 2.724 | 3 | 0.908 | 0.628 | 0.601 |
| Within groups | 66.496 | 46 | 1.446 | | |
| Total | 69.220 | 49 | | | |
| Do you believe that the growth of fraud cases, hacking, and theft of digital currencies has been due to the growth of cryptocurrency? | | | | | |
| Between groups | 6.800 | 3 | 2.267 | 2.029 | 0.123 |
| Within groups | 51.380 | 46 | 1.117 | | |
| Total | 58.180 | 49 | | | |

null hypothesis is rejected. In other terms, the alternative hypothesis has been accepted in the F-Test. The variables,

that is, the dependent and independent variables were found to have a significant relationship with each other.

Chi-square T-test

The outcomes from the Chi-square test are shown in Table 5. Pearson Chi-square value was determined to be 3.410a. On the other hand, the Pearson Chi-square value was found to be 3.410a for another variable. In general, the primary goal of using Chi-square test is to determine the influence of independent variables on the independent variables. The minimum expected value was found to be 0.54. The results of this test reflect that most of the participants agreed to the viewpoints. The present study outcomes are in line with the conclusion of the systematic literature review conducted earlier. In this study (Batubara et al., 2018), the authors mentioned that security, scalability, and flexibility are predominant

Table 5: Chi-square tests

| | Value | df | Asymp. Sig. (2-sided) |
|------------------------------|--------------------|----|-----------------------|
| Pearson Chi-square | 3.410 ^a | 2 | 0.182 |
| Likelihood ratio | 4.130 | 2 | 0.127 |
| Linear-by-linear association | 1.896 | 1 | 0.169 |
| <i>n</i> of Valid cases | 50 | | |
| Pearson Chi-square | 1.228 ^a | 3 | 0.746 |
| Likelihood ratio | 1.585 | 3 | 0.663 |
| Linear-by-linear association | 0.090 | 1 | 0.765 |
| <i>n</i> of valid cases | 50 | | |
| Pearson Chi-square | 2.275 ^a | 3 | 0.517 |
| Likelihood ratio | 3.255 | 3 | 0.354 |
| Linear-by-linear association | 2.045 | 1 | 0.153 |
| <i>n</i> of valid cases | 50 | | |
| Pearson Chi-square | 1.829 ^a | 3 | 0.609 |
| Likelihood ratio | 2.662 | 3 | 0.447 |
| Linear-by-linear association | 1.581 | 1 | 0.209 |
| <i>n</i> of valid cases | 50 | | |
| Pearson Chi-square | 7.393 ^a | 3 | 0.060 |
| Likelihood ratio | 5.951 | 3 | 0.114 |
| Linear-by-linear association | 3.813 | 1 | 0.051 |
| <i>n</i> of valid cases | 50 | | |

^a3 cells (50.0%) have expected count <5. The minimum expected count is 0.36. ^a6 cells (75.0%) have expected count <5. The minimum expected count is 0.36.

^a6 cells (75.0%) have expected count <5. The minimum expected count is 0.54. ^a6 cells (75.0%) have expected count <5. The minimum expected count is 0.36. ^a5 cells (62.5%) have expected count <5. The minimum expected count is 0.36.

issues that hinder the adoption of blockchain technologies. Further, change resistance and the lack of adoption governance models also prevent the migration to new technologies. In literature (Mohammad and Vargas, 2022), the challenges faced in the adoption of blockchain technologies have been categorized as three types such as technological, organizational, and environmental.

In this background, there is a need to develop security models to maintain integrity, consistency, reliability, and stability of the data. According to (Weichbroth et al., 2023), the usage of blockchain technologies alone cannot secure the data integrity. For the BC to be effective, the input data should be highly accurate. At present, the blockchain technology has been used by the major cryptocurrencies such as bitcoin and Ethereum. This technology has been a forerunner in other types of applications such as smart electric grids, smart healthcare, wireless sensor networks, cloud computing, and so on. In the future, artificial intelligence-based architecture can be developed to thoroughly analyze the network, the performance of the bitcoin and other such cryptocurrencies can be developed in terms of security.

CONCLUSION

The present study is an attempt to find out the impact of challenges faced by the business organizations in adopting blockchain applications and innovative tools and to provide a set of strategies to be used by companies to enhance their effectiveness in terms of cryptocurrency, blockchain applications, etc. The outcomes conclude that there has been a significant increase in the adoption of blockchain innovations and applications, as a result of threats imposed by cryptocurrency. Blockchain technologies have been largely applied in increasing the security and protection of transactions in cryptocurrencies like Bit coin. The main purpose for blockchain security is to make sure that the data, information, assets, systems, and networks of the users are secure and protected from cyber-attackers. As a result, this process creates a trust among the parties, while also building a high level of data integrity.

In the same context, the users also have been determined to decentralize their storage, which allows the blockchain application to encrypt every piece of information like a complete puzzle, which reduces the possibility of hacking. In such a way, the use of cryptocurrency can produce a positive impact on the development and innovation of cyber security and blockchain applications. In addition

to this, businesses need to focus on improving their data security infrastructure and protect their data and networks with innovative blockchain technologies and other applications.

AUTHOR'S CONTRIBUTION

Not applicable.

FINANCIAL SUPPORT

There is no financial support and sponsorship for this research.

ACKNOWLEDGMENT

Not applicable.

CONFLICTS OF INTEREST

This is to bring to your kind information that this research work has no conflicts of interest.

REFERENCES

- Batubara, F., Ubacht, J., & Janssen, M. (2018). Challenges of Blockchain Technology Adoption for E-government: A Systematic Literature Review. In: *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*. doi: 10.1145/3209281.3209317
- Bhardwaj, J., Negi, R., Nagrath, P., & Mittal, M. (2022). *Applications of Blockchain in Various Domains*. Cham: Springer Nature. p. 1-30. doi: 10.1007/978-3-030-71485-7_1
- Caporale, G. M., Kang, W. Y., Spagnolo, F., & Spagnolo, N. (2020). Non-linearities, cyber attacks and cryptocurrencies. *Finance Research Letters*, 32, 101297. doi: 10.1016/j.frl.2019.09.012
- Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., & Shah, M. (2022). A comprehensive study of artificial intelligence and cybersecurity on bitcoin, crypto currency and banking system. *Annals of Data Science*, doi: 10.1007/s40745-022-00433-5
- Debajyoti, S. (2023). Impact of using crypto currency to maintain cyber security blockchain innovations and applications. *International Journal of Science and Research*, 12(5), 319-325. doi: 10.21275/SR23414204106
- Deshmukh, A., Sreenath, N., Tyagi, A. K., & Abhichandan, U. V. E. (2022). Blockchain Enabled Cyber Security: A Comprehensive Survey. In: *2022 International Conference on Computer Communication and Informatics (ICCCI)*. p. 1-6. doi: 10.1109/ICCCI54379.2022.9740843
- Fahmi, N., Hastasakti, D. E., Zaspigi, D., & Saputra, R. K. (2023). A comparison of blockchain application and security issues from Bitcoin to Cybersecurity. *Blockchain Frontier Technology*, 3(1), 81-88. doi: 10.34306/bfront.v2i2.231
- Garg, R. (2022). Ethereum based smart contracts for trade and finance. *International Journal of Economics and Management Engineering*, 16(11), 619-629. doi: 10.5281/zenodo.5854730
- Mohammad, A., & Vargas, S. (2022). Challenges of using blockchain in the education sector: A literature review. *Applied Sciences*, 12(13), 6380. doi: 10.3390/app12136380
- Onyekwere, E., Ogwueleka, F. N., & Irhebhude, M. E. (2023). Adoption and sustainability of bitcoin and the blockchain technology in Nigeria. *International Journal of Information Technology*, 15, 1-12. doi: 10.1007/s41870-023-01336-1
- Ramos, S., Mélon, L., & Ellul, J. (2022). Exploring Blockchains Cyber Security Techno-Regulatory Gap. An Application to Crypto-Asset Regulation in the EU. In: *10th Graduate Conference in Law and Technology, Sciences Po* (2022).
- Research and Markets. (2022). *Cryptocurrency Market Size, Market Share, Application Analysis, Regional Outlook, Growth Trends, Key Players, Competitive Strategies and Forecasts, 2022 to 2030*. Ireland: Research and Markets.
- Sailaja, P., & Thamodaran, V. (2016). Customer perception on security system in E-banking services with special references to EDC. *Indian Journal of Commerce and Management Studies*, 7(2), 66-72.
- Sakas, D. P., Giannakopoulos, N. T., Kanellos, N., & Migkos, S. P. (2022). Innovative cryptocurrency trade websites' marketing strategy refinement, via digital behavior. *IEEE Access*, 10, 63163-63176. doi: 10.1109/ACCESS.2022.3182396
- Statista. (2023). *Overall Cryptocurrency Market Capitalization Per Week from July 2010 to June 2023*. Hamburg: Statista.
- Tibrewal, I., Srivastava, M., & Tyagi, A. (2022). *Blockchain Technology for Securing Cyber-Infrastructure and Internet of Things Networks*. Singapore: Springer.

- p. 337-350. doi: 10.1007/978-981-16-6542-4_17
- Varghese, H. M., Nagoree, D. A., Anshu, & Jayapandian, N. (2021). Cryptocurrency Security and Privacy Issues: A Research Perspective. In: *2021 6th International Conference on Communication and Electronics Systems (ICCES)*. p. 902-907. doi: 10.1109/ICCES51350.2021.9489254
- Yu, F., G. Luo, A.A. Nair, K. Tsigaridis, and S.E. Bauer, (2022). Use of machine learning to reduce uncertainties in particle number concentration and aerosol indirect radiative forcing predicted by climate models. *Geophys. Res. Lett.*, 49, no. 16, e2022GL098551, doi:10.1029/2022GL098551
- Weichbroth, P., Wereszko, K., Anacka, H., & Kowal, J. (2023). Security of cryptocurrencies: A view on the state-of-the-art research and current developments. *Sensors (Basel)*, 23(6), 3155. doi: 10.3390/s230631553
- Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Çetin, F.,