Anusandhanvallari
Vol 2024, No.1
November 2024
ISSN 2229-3388

Enablers And Barriers to Blockchain-Enabled Cybersecurity Adoption: A Study of Organizational Readiness

[1]Dr. H.B. Priyanka, [2]Dr. Nayana Kumari J, [3]Vimala B S, [4]Sumithra K S

Assistant Professor, Department of Commerce, SGT College, Bellary, Karnataka, India – 583103

Assistant Professor, Department of Commerce, SJR College of Science, Arts & Commerce, Bangalore, Karnataka, India

Assistant Professor, Department of Commerce, SJR College of Science, Arts & Commerce, Bangalore, Karnataka, India

Assistant Professor, Department of Commerce, SJR College of Science, Arts & Commerce, Bangalore, Karnataka, India

Abstract: Business entities are under growing pressure to strengthen their cyber defences, and blockchain is often put forward as a means of doing so on account of its distributed record keeping, its resistance to tampering and the shared view of data it offers to every participant. This paper is an attempt to study the factors that drive organizational readiness to adopt blockchain-enabled cybersecurity solutions. Data was collected from 119 respondents through a structured questionnaire. Six constructs were measured, namely blockchain awareness, security confidence, data integrity, organizational trust, adoption readiness and implementation challenges. Descriptive statistics, the Shapiro-Wilk test of normality, Spearman rank correlation, hierarchical multiple linear regression and the one-way ANOVA of Welch were used to analyse the data. It was found that blockchain awareness, security confidence, data integrity and organizational trust together explain 49.1 per cent of the variance in adoption readiness, and that all four constructs make a positive and statistically significant contribution, with blockchain awareness being the strongest single predictor. Implementation challenges was found to be negatively and significantly correlated with adoption readiness when taken on its own, but its contribution ceased to be significant once the other four constructs were held constant. No significant difference was observed across qualification groups for any of the six constructs, which indicates that these relationships hold uniformly across educational backgrounds. The findings suggest that implementation challenges act as a background drag that overlaps with the enabling perceptions rather than as an independent barrier. The results are of relevance to information technology managers, security practitioners and researchers who are attempting to decide where to invest while building a case for blockchain-enabled cybersecurity adoption.

Keywords: Blockchain adoption, cybersecurity, organizational readiness, security confidence, implementation challenges, organizational trust

1 Introduction

Cybersecurity has moved from being an operational matter handled within the information technology department to a matter that is taken up at the board level. As business entities digitize a larger share of their operations, the surface available for data breaches, insider misuse and transaction fraud widens, and centrally administered security controls do not always keep pace with it.

Blockchain is one of the technologies that is proposed as a remedy. It distributes trust across a network instead of concentrating it in a single administrator, it makes records difficult to alter once they have been written, and it provides every participant with a shared and verifiable view of the same data.

The presence of these properties does not by itself lead a business entity to adopt a blockchain-based security tool. Awareness of the technology, confidence that it improves security in practice, the belief that it protects the integrity of data, and trust in the ability of the organization to implement it responsibly all have to be present before adoption becomes a realistic step. Cost, complexity, the shortage of skilled personnel and the difficulty of integrating with legacy systems work in the opposite direction. Readiness is therefore not a single switch but the net outcome of enabling perceptions pulling in one direction and practical obstacles pulling in the other.

This paper studies that balance using survey data collected from 119 respondents. It examines how blockchain awareness, security confidence, data integrity and organizational trust relate to organizational readiness to adopt blockchain-enabled cybersecurity solutions, and separately how implementation challenges affect the same readiness. The paper does not set out to argue that blockchain is good or bad for security. It attempts to give information technology managers and researchers a clearer and evidence-based picture of what is, and what is not, associated with the readiness of an organization to move forward with it.

2 Review of Literature

Clohessy, T., & Acton, T. (2019) conducted a multi-case study of Irish business entities using the Technology-Organization-Environment (TOE) framework. It was found that top management support and organizational readiness were consistent enablers of blockchain adoption, and that smaller firms were less likely to adopt the technology than larger ones.

Lustenberger, M., et al. (2021) extended the TOE framework into a Blockchain Adoption Model using survey data collected from firms in the DACH region. The study concluded that adoption is driven less by internal readiness on its own and more by the ecosystem surrounding the organization, which includes stakeholder pressure and regulatory clarity.

Bui, Q. T., & Le, S. T. (2025) surveyed small and medium logistics enterprises in Vietnam and used structural equation modelling to identify six significant barriers to blockchain adoption. High investment cost, weak cooperation among stakeholders and a shortage of skilled personnel were among the barriers identified, which establishes implementation challenges as a distinct and measurable brake on adoption.

Anomah, S., & Ayeboafo, B. (2026) studied blockchain audit readiness among financial professionals in Ghana, Egypt and Kenya. Organizational readiness and cybersecurity maturity were found to be the strongest predictors of readiness, while institutional pressures were found to act only indirectly.

Fang, Y., et al. (2026) examined blockchain adoption among small and medium e-commerce enterprises in China. It was observed that digital readiness reshapes the manner in which firms weigh the perceived benefits and costs of blockchain, rather than adding a uniform positive push towards adoption.

Chen, L., & Wong, K. (2024) combined the UTAUT and TOE models to study blockchain adoption in supply chains. It was found that cybersecurity concerns spanning the technological, organizational and environmental dimensions had a significant bearing on the adoption decision.

Queiroz, M. M., et al. (2020) examined the barriers present within a securities services value network through qualitative interviews. The obstacles were classified into internal-psychological, internal-functional, external-psychological and external-functional categories. The study argued that psychological resistance can matter as much as technical limitations.

Kouhizadeh, M., et al. (2019) analysed the barriers to blockchain implementation across industry and service sectors. Scalability concerns and market-based risk were identified as the most influential obstacles to successful adoption.

Okafor, C., et al. (2025) reviewed 28 peer-reviewed studies on blockchain barriers in logistics and grouped them into technical, economic, legal and organizational dimensions. It was observed that organizational and legal barriers are frequently underestimated when compared with technical barriers.

Al-Rakhami, M., & Al-Mashari, M. (2024) carried out a systematic literature review of blockchain technology adoption in organizations and proposed an augmented TOE framework in which improved security through smart contracts acts as an enabler, while scalability and regulatory limitations act as barriers.

Ibrahim, R., et al. (2026) proposed a decentralized trust framework that combined blockchain, anomaly detection based on artificial intelligence and a lightweight consensus mechanism. The authors argued that cybersecurity, data integrity and trust management have to be addressed together rather than as separate design problems.

Hassan, A., & Farooq, S. (2026) surveyed university students in a South Asian setting on blockchain adoption, perceptions of data security and cybersecurity awareness. It was found that cybersecurity awareness partially mediates the relationship between blockchain adoption and the perception of data security and privacy.

Bansal, P. (2020) reviewed the role of blockchain in cybersecurity. The study concluded that the decentralized and tamper-resistant properties of blockchain support data integrity and trust management, and that adoption by an organization still depends to a large extent on the perceived cost and complexity of implementation.

3 Research Gap

The existing literature examines the drivers of blockchain adoption and the barriers to blockchain adoption largely in isolation from each other. Much of the empirical work relies on qualitative interviews, single case studies, or samples drawn from one industry such as logistics or finance. There are few studies that bring the perception side, which is made up of awareness, security confidence, data integrity and organizational trust, together with the obstacle side, which is made up of implementation challenges, within a single quantitative model of organizational readiness. This paper is an attempt to fill this void using primary survey data collected on blockchain-enabled cybersecurity adoption.

4 Objectives of the Study

(a) To examine the influence of blockchain awareness, security confidence, data integrity and organizational trust on organizational readiness to adopt blockchain-enabled cybersecurity solutions.

(b) To assess the impact of implementation challenges on organizational readiness to adopt blockchain-enabled cybersecurity solutions.

5 Hypotheses

The following hypotheses were derived to meet the objectives of the study.

H0a: Blockchain awareness, security confidence, data integrity and organizational trust are not significantly associated with organizational readiness to adopt blockchain-enabled cybersecurity solutions.

H0b: Implementation challenges are not significantly associated with organizational readiness to adopt blockchain-enabled cybersecurity solutions once blockchain awareness, security confidence, data integrity and organizational trust are held constant.

6 Scope of the Study

The study covers organizational readiness to adopt blockchain-enabled cybersecurity solutions, examined through the perception of the respondents on blockchain awareness, security confidence, data integrity, organizational trust and implementation challenges. The findings are intended to help information technology professionals,

security practitioners and decision makers understand what is, and what is not, associated with readiness for blockchain-enabled cybersecurity adoption.

7 Research Methodology

The study is based on both primary and secondary data. The primary data was collected through a structured questionnaire and the secondary data was drawn from published literature. The questionnaire covered six constructs, namely blockchain awareness, security confidence, data integrity, organizational trust, adoption readiness and implementation challenges, and it yielded 119 usable responses on blockchain-enabled cybersecurity adoption. Each of the six constructs was measured using three Likert scale items ranging from 1 to 5, and the item scores were averaged into a construct level mean score for every respondent. Descriptive statistics, the Shapiro-Wilk test of normality, Spearman rank correlation, hierarchical multiple linear regression and the one-way ANOVA of Welch were used to analyse the data.

8 Analysis and Interpretation

8.1 Demographic Profile

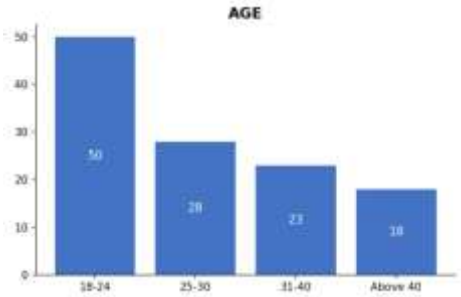
Table 1: Frequency table of age

Age	Counts	% of Total
18 to 24	50	42.0%
25 to 30	28	23.5%
31 to 40	23	19.3%
Above 40	18	15.1%
Total	119	100.0%

Source: Primary Data

It is observed that 42.0 per cent of the 119 respondents fall in the age group of 18 to 24 years, followed by 23.5 per cent between 25 and 30 years, 19.3 per cent between 31 and 40 years, and 15.1 per cent above 40 years. The sample is tilted towards younger respondents but is reasonably spread across the age brackets, with roughly a third of the respondents aged 31 years and above. This gives the analysis a mix of early career and more experienced perspectives.

Graph 1: Frequency of age



The bar chart depicts the same distribution as Table 1, with a steady decline in the count of respondents across the higher age categories. A meaningful share of the respondents, at 15.1 per cent, are above 40 years of age, which enables the survey to capture the views of more experienced staff alongside those of younger respondents.

Table 2: Frequency table of qualification

Qualification	Counts	% of Total
Master's Degree	55	46.2%
Working Professional	38	31.9%
Bachelor's Degree	26	21.8%
Total	119	100.0%

Source: Primary Data

It is observed that 46.2 per cent of the respondents hold a Master's degree, 31.9 per cent identify themselves as working professionals and 21.8 per cent hold a Bachelor's degree. The sample is well educated, which suggests that the respondents bring a reasonable baseline of formal knowledge to their views on blockchain-enabled cybersecurity, along with a meaningful share of respondents who have direct exposure to the workplace.

Graph 2: Frequency of qualification



The bar chart depicts the same pattern as Table 2. Holders of a Master's degree form the largest group, working professionals account for close to a third of the sample, which points to practical exposure to industry, and holders of a Bachelor's degree make up the smallest group.

8.2 Descriptive Statistics and Normality

Table 3: Descriptive statistics and test of normality

Construct	Mean	SD	Shapiro-Wilk W	p
Blockchain Awareness	3.48	0.744	0.933	< .001
Security Confidence	3.52	0.659	0.929	< .001

Data Integrity	3.69	0.625	0.942	< .001
Organizational Trust	3.41	0.677	0.940	< .001
Adoption Readiness	3.46	0.826	0.946	< .001
Implementation Challenges	2.87	0.760	0.947	< .001

Source: Primary Data

Data integrity recorded the highest mean score at 3.69, followed by security confidence at 3.52, blockchain awareness at 3.48, adoption readiness at 3.46 and organizational trust at 3.41. Implementation challenges recorded the lowest mean at 2.87, which means that the respondents did not in general rate the obstacles to implementation as severe when compared with the enabling constructs. The Shapiro-Wilk test is significant for every construct at $p < .001$, which confirms that none of the six variables is normally distributed. This supports the use of a non-parametric measure of correlation alongside regression in the analysis that follows.

8.3 Spearman Rank Correlation

Table 4: Spearman rank correlation matrix

Construct	BA	SC	DI	OT	AR	IC
Blockchain Awareness (BA)	1.000	0.274**	0.299**	0.325**	0.576**	-0.115
Security Confidence (SC)	0.274**	1.000	0.347**	0.275**	0.427**	-0.184*
Data Integrity (DI)	0.299**	0.347**	1.000	0.266**	0.414**	-0.064
Organizational Trust (OT)	0.325**	0.275**	0.266**	1.000	0.454**	-0.175
Adoption Readiness (AR)	0.576**	0.427**	0.414**	0.454**	1.000	-0.219*
Implementation Challenges (IC)	-0.115	-0.184*	-0.064	-0.175	-0.219*	1.000

*Source: Primary Data. * p < .05, ** p < .001*

It is observed that adoption readiness correlates positively and significantly with all four enabling constructs. The correlation is strongest with blockchain awareness at rho = 0.576 and $p < .001$, followed by organizational trust at rho = 0.454 and $p < .001$, security confidence at rho = 0.427 and $p < .001$, and data integrity at rho = 0.414 and $p < .001$. Implementation challenges is the only construct that correlates negatively with adoption readiness, at rho = -0.219 and p = .017, and it also correlates negatively with security confidence at rho = -0.184 and p = .045. The four enabling constructs correlate positively with one another, with rho ranging between 0.266 and 0.347,

which points to some shared underlying variance. This shared variance is accounted for directly in the regression analysis that follows.

8.4 Multiple Linear Regression

Table 5: Model fit, predictors of adoption readiness

Model	R^2	Adj. R^2	F	df1	df2	p
1	0.491	0.473	27.50	4	114	< .001

Table 6: Model coefficients, dependent variable is adoption readiness

Predictor	B	SE	t	p
(Constant)	-0.740	0.426	-1.74	.085
Blockchain Awareness	0.432	0.081	5.32	< .001
Security Confidence	0.255	0.093	2.74	.007
Data Integrity	0.224	0.097	2.30	.023
Organizational Trust	0.286	0.089	3.21	.002

Source: Primary Data

The four predictors together explain 49.1 per cent of the variance in adoption readiness, with an R-square of 0.491 and an adjusted R-square of 0.473, and the model as a whole is significant at $F = 27.50$ and $p < .001$. All four coefficients are positive and statistically significant. Blockchain awareness is the strongest predictor at $B = 0.432$ and $p < .001$, which means that a one point increase in awareness is associated with an increase of 0.432 points in adoption readiness while the other three constructs are held constant. Organizational trust at $B = 0.286$ and $p = .002$, security confidence at $B = 0.255$ and $p = .007$ and data integrity at $B = 0.224$ and $p = .023$ follow, each with a significant positive effect. This meets the first objective of the study. We reject H0a, since blockchain awareness, security confidence, data integrity and organizational trust each make an independent and statistically significant contribution to organizational readiness to adopt blockchain-enabled cybersecurity solutions.

8.5 Hierarchical Regression

Table 7: Model fit with implementation challenges added

Model	R^2	ΔR^2	F	ΔF	p (ΔF)
2 (Model 1 + Implementation Challenges)	0.495	0.004	22.16	0.91	.342

Table 8: Model coefficients, dependent variable is adoption readiness

Predictor	B	SE	t	p
(Constant)	-0.457	0.519	-0.88	.381
Blockchain Awareness	0.424	0.081	5.20	< .001
Security Confidence	0.243	0.094	2.59	.011
Data Integrity	0.226	0.097	2.32	.022
Organizational Trust	0.281	0.089	3.15	.002
Implementation Challenges	-0.071	0.075	-0.95	.342

Source: Primary Data

The addition of implementation challenges to the model raises the explained variance only marginally, from 49.1 per cent to 49.5 per cent, with a change in R-square of 0.004, and this increase is not statistically significant at a change in F of 0.91 and p = .342. Implementation challenges carries a negative coefficient, which is consistent with its negative correlation with readiness in Table 4, but the effect is small and is not significant once blockchain awareness, security confidence, data integrity and organizational trust are held constant, at B = -0.071 and p = .342. The four enabling predictors all remain significant and change little in size. This meets the second objective of the study. We accept H0b, since implementation challenges is significantly and negatively related to adoption readiness on its own, but its influence overlaps heavily with that of the enabling constructs, and once those constructs are accounted for it does not add a meaningful independent drag on readiness.

8.6 One-Way ANOVA

Table 9: One-way ANOVA of Welch across qualification groups

Construct	F	df1	df2	p
Blockchain Awareness	0.43	2	69.2	.655
Security Confidence	0.05	2	61.1	.952
Data Integrity	0.01	2	66.1	.992
Organizational Trust	0.05	2	70.5	.948
Adoption Readiness	0.50	2	67.4	.610
Implementation Challenges	1.90	2	63.3	.158

Source: Primary Data

The one-way ANOVA of Welch finds no statistically significant difference across the three qualification groups, which are Bachelor's degree, Master's degree and working professional, for any of the six constructs, since all the significance values are greater than .15. Implementation challenges comes closest to a group difference at F = 1.90 and p = .158, but it does not cross the conventional threshold of significance. It can therefore be deduced that the significant relationships identified in Tables 4 to 8 hold uniformly across educational backgrounds and are not driven by any one qualification group.

9 Findings and Suggestions

The sample is tilted towards younger respondents, with 42.0 per cent aged between 18 and 24 years, and is well educated, with 46.2 per cent holding a Master's degree. This gives a mix of theoretical familiarity with the concepts of blockchain and, in the case of the working professional segment, direct exposure to the workplace. Data integrity was rated the highest among the six constructs at a mean of 3.69 and implementation challenges the lowest at a mean of 2.87. All six constructs departed significantly from a normal distribution.

The Spearman correlations show that all four enabling constructs relate positively and significantly to adoption readiness, with rho ranging between 0.41 and 0.58, while implementation challenges relates negatively and significantly at rho = -0.219. The multiple regression run for the first objective found that the four enabling constructs together explain 49.1 per cent of the variance in adoption readiness, with all four predictors individually significant and blockchain awareness the strongest at B = 0.432. The hierarchical regression run for the second objective found that implementation challenges adds only marginally to the explained variance once the four enabling constructs are controlled for, and that its own effect is not significant in the full model, even though it is significantly and negatively correlated with readiness on its own. The one-way ANOVA of Welch showed no significant difference in any of the six constructs across the qualification groups.

It is suggested that initiatives to build blockchain awareness be taken up first, since awareness is the single strongest predictor of adoption readiness in this sample. Training, briefings and internal communication that raise a genuine understanding of the mechanics of blockchain are likely to yield the largest marginal payoff. It is further

suggested that organizations invest in organizational trust and security confidence alongside awareness, since both remain independently significant predictors even after awareness and data integrity are accounted for. Visible commitment from the leadership and a transparent record on security can help build both.

It is also suggested that implementation challenges not be treated as the primary lever for readiness on its own. Since the effect of implementation challenges disappears once the enabling constructs are controlled for, an effort to reduce cost, complexity or the skills gap is likely to pay off mainly by first improving awareness, confidence, the perception of data integrity and trust, rather than as an independent fix. A further suggestion is to measure implementation challenges in a more granular form, covering cost, shortage of skills, integration with legacy systems and regulatory uncertainty separately, since some of the sub-components may carry an independent effect that the pooled measure masks.

10 Conclusion

The study set out to examine what shapes organizational readiness to adopt blockchain-enabled cybersecurity solutions, using primary data collected from 119 respondents and structured around two objectives. On the first objective, blockchain awareness, security confidence, data integrity and organizational trust together explained close to half the variance in adoption readiness, and each made a positive and statistically significant contribution of its own, with blockchain awareness standing out as the strongest single predictor. On the second objective, implementation challenges was significantly and negatively correlated with readiness when considered alone, but once the four enabling constructs were held constant its independent contribution shrank to a small and non-significant effect. The comparison of groups by qualification level showed no meaningful difference, which indicates that these patterns are not driven by any one educational segment.

It was concluded that organizational readiness to adopt blockchain-enabled cybersecurity solutions is driven mainly by what people know and believe about the technology, that is, their awareness of it, their confidence in its security properties, their trust in the ability of the organization to implement it and their belief in its ability to protect the integrity of data, rather than by the practical obstacles standing in the way. Implementation challenges do matter, but the study suggests that they act as background friction that overlaps with weaker awareness and confidence rather than as a barrier standing on its own. For an organization attempting to build a business case for blockchain-enabled cybersecurity, this suggests that investment in education, transparent communication and the building of trust is likely to move readiness at least as much as an effort aimed narrowly at reducing the cost or complexity of implementation.

11 Limitations and Scope for Further Study

The study is based on the responses of 119 participants, which may not represent all industries or all sizes of organization. It measures readiness on the basis of perception rather than actual adoption behaviour, and the results therefore describe attitudes rather than confirmed outcomes of implementation.

There exists considerable scope for further study. The hierarchical regression could be replicated with a larger and more industry-diverse sample to confirm whether the marginal and non-significant contribution of implementation challenges holds outside this pool of respondents. Implementation challenges could be examined in a more granular form rather than as a single composite score. There is also scope to study whether the same relationships are observed across different countries and regulatory environments, and to follow respondents over time so that perception-based readiness can be compared with actual adoption.

12 References

[1] Al-Rakhami, M., & Al-Mashari, M. (2024). Exploring factors influencing blockchain adoption's effectiveness in organizations for generating business value: a systematic literature review and thematic analysis. Journal of Innovation and Entrepreneurship. https://doi.org/10.1080/17517575.2024.2379830

[2] Bansal, P. (2020). Blockchain for cybersecurity: A comprehensive survey. Proceedings of the International Conference on Data Science and Engineering.

[3] Chen, L., & Wong, K. (2024). Key determinants of blockchain adoption: A unified framework integrating UTAUT and TOE models. Proceedings of the 2024 7th International Conference on Blockchain Technology and Applications. https://doi.org/10.1145/3708622.3708629

[4] Clohessy, T., & Acton, T. (2019). Investigating the influence of organizational factors on blockchain adoption: An innovation theory perspective. Industrial Management & Data Systems, 119(7), 1457-1491.

[5] Kouhizadeh, M., Saberi, S., & Sarkis, J. (2019). Analysis of barriers to implement blockchain in industry and service sectors. Journal of Cleaner Production. https://doi.org/10.1016/j.jclepro.2019.06.099

[6] Lustenberger, M., Malešević, S., & Spychiger, F. (2021). Ecosystem readiness: Blockchain adoption is driven externally. Frontiers in Blockchain, 4, 720454. https://doi.org/10.3389/fbloc.2021.720454

[7] Queiroz, M. M., Fosso Wamba, S., & Branski, R. M. (2020). Barriers to blockchain adoption: Empirical observations from the securities services value network. Technological Forecasting and Social Change.