Spring 3-16-2024

Does Blockchain Technology Adoption Matter To Data Breaches?

Kyungmyung Jang
Mississippi State University

Merrill Warkentin
Mississippi State University

Does Blockchain Technology Adoption Matter to Data Breaches?

Kyungmyung Jang
Mississippi State University
kj1350@msstate.edu

Merrill Warkentin
Mississippi State University
m.warkentin@msstate.edu

ABSTRACT

Firms adopt blockchain technology to provide secure digital transactions using cryptographic hashes. However, blockchain systems in firms can encounter a series of hacks and attacks because of vulnerabilities. The extant studies on blockchain technology and information security suggest conflicting perspectives regarding the legitimacy of blockchain security through qualitative research. In essence, we have a lack of quantitative research that can shed light on conflicting perspectives. Therefore, we examine the relationship between blockchain technology adoption and information security through empirical research using data breaches. We utilized institutional theory to develop our hypotheses and employed the staggered difference-in-differences design to test the proposed hypotheses. The findings indicate that substantive blockchain technology adoption reduces data breaches. Our study provides revelatory insights that not all blockchain technology adoptions affect data breaches based on sophisticated research methods.

Keywords

Blockchain Technology Adoption, Data Breaches, Institutional Theory, Difference-in-Differences, A Quasi-Experiment

INTRODUCTION

Blockchain technology employs cryptographic hashes assigned to individual nodes using the peer-to-peer network architecture, providing more secure digital transactions based on a consensus mechanism (Chanson, Bogner, Bilgeri, Fleisch, & Wortmann, 2019). The fundamental core of blockchain technology is trustworthy consensus systems engaging multiple stakeholders within an open architecture. The trust-based blockchain systems operate on permissionless digital transactions, eliminating the need for third-party interventions to complete digital transactions (Catalini & Gans, 2020). In this sense, scholars have defined blockchain technology as a disruptive innovation that fundamentally transforms business operations (Constantinides, Henfridsson, & Parker, 2018; Hendershott, Zhang, Zhao, & Zheng, 2021; Warkentin & Orgeron, 2020).This blockchain-based disruptive innovation yields two primary economic advantages: (1) the cost reduction of verification and (2) the cost reduction of networking (Catalini & Gans, 2020). In line with the economic advantages of blockchain technology, prior studies on blockchain economics have focused on investigating diverse economic advantages resulting from blockchain technology adoption such as total productivity factor (Xu & Guan, 2022), firm performance (Sheel & Nath, 2019), and market value (Jeong & Lim, 2023). The findings from these studies demonstrate the positive effects of blockchain technology adoption on total productivity factors, firm performance, and market value. Consequently, a large number of firms have adopted blockchain technology as a strategic tool to increase their revenues, productivity, and the efficacy of business routines (Janssen, Weerakkody, Ismagilova, Sivarajah, & Irani, 2020; Toufaily, Zalan, & Dhaou, 2021).

However, the extant studies have given a lack of attention to information security risks associated with blockchain technology adoption. A series of hacks and attacks on blockchain systems raise concerns about the data security of blockchain systems (Li, Jiang, Chen, Luo, & Wen, 2020; Rasi, Rakiman, Radzi, Masrom, & Sundram, 2021). Information security risks regarding blockchain technology adoption can lead to data breaches within firms because of vulnerabilities in blockchain systems operations. This leads to increased concerns about the reliability and integrity of blockchain systems. Conversely, other scholars have proposed that blockchain technology could enhance data security because of cryptographic hashes (Catalini & Gans, 2020; Toufaily et al., 2021). As a result, the prior studies on blockchain technology adoption and information security suggest a conflicting perspective. Therefore, we propose the following research question to extend the literature on blockchain technology and information security through empirical research using data breaches:

RQ: What is the relationship between blockchain technology adoption and data breaches?

To answer the research question, we utilize institutional theory to explain the relationship between blockchain technology adoption and data breaches within firms. Institutional theory distinguishes between symbolic and substantive adoption to assess how accurately a firm's activities are mirrored in the signals it conveys to stakeholders. Symbolic adoption, akin to a house having an alarm sticker but lacking an actual security system, aims to enhance a firm's external validation or legitimacy rather than obtaining specific technological benefits (Angst, Block, D'arcy, & Kelley, 2017). In contrast, substantive adoption, the extreme end, involves signals that precisely reflect the adopted practices, tightly integrated into the organization's core operations. This means that substantive adoption, akin to an actual security system, aims to enhance a firm's internal validation to obtain specific technological benefits. We classify symbolic or substantive blockchain technology adoptions using a firm's public disclosures from EDGAR (https://www.sec.gov/edgar/search/).

LITERATURE REVIEW

Institutional Theory

The fundamental core of institutional theory lies in the concept of institutional isomorphism to understand how organizational behaviors are shaped by institutional rules (DiMaggio & Powell, 1983). Institutional isomorphism manifests through three mechanisms: (1) coercive, (2) mimetic, and (3) normative. The coercive mechanism is the pressures firms face from external entities such as regulatory bodies, compelling them to conform to established norms and regulations. The mimetic mechanism refers to organizations imitating each other due to uncertainty. In contexts where organizational technologies, goals, or the environment are inadequately understood, leading to ambiguity, organizations tend to imitate other organizations. This mimetic behavior offers advantages, enabling organizations to identify practical solutions at minimal costs when dealing with highly uncertain issues. The normative mechanism emerges from the process of professionalization. This process entails individuals within a specific occupation collaborating to establish standards, define working conditions, and develop specialized techniques for the field.

Within the complex dynamics of institutional isomorphism, institutions are recognized as higher-order social structures that define the appropriate structures and behaviors essential for organizational operation (Angst et al., 2017; DiMaggio & Powell, 1983). Institutions influence organizational behavior not solely by enhancing performance but by conferring legitimacy within diverse social contexts. Consequently, organizations frequently adjust their strategies and behaviors to conform to these institutional norms, striving not only for enhanced performance but primarily for legitimacy in the eyes of varied stakeholders (Dahlin, Ekman, Röndell, & Pesämaa, 2020; DiMaggio & Powell, 1983; Truong, Mazloomi, & Berrone, 2021). For publicly traded firms, numerous stakeholder groups possess the potential authority to grant legitimacy. In this context of institutional theory, the decision to adopt blockchain technology within firms can be categorized as either symbolic or substantive adoption strategies.

Symbolic adoptions are intended to influence stakeholder perceptions without substantial implementation of technology, meaning the organizational routines are not altered because of the adoptions (Angst et al., 2017; Dahlin et al., 2020; Truong et al., 2021). In contrast to symbolic adoptions, substantive adoptions incorporate the actual implementation of technology in business routines to achieve technical benefits (Angst et al., 2017; Dahlin et al., 2020; Truong et al., 2021). In the realm of blockchain context, publicly listed firms encounter analogous pressures from stakeholders. There has been a push to adopt blockchain technology due to its potential to generate significant savings through operational efficiencies and decreased digital transaction costs (Hughes et al., 2019; Toufaily et al., 2021).

HYPOTHESIS DEVELOPMENT

Symbolic Blockchain Technology Adoption

Symbolic blockchain technology adoption aims to influence stakeholders' perceptions without making substantial changes to organizational routines. This strategic approach emphasizes the appearance of technological adoption rather than its substantive integration, allowing organizations to maintain their existing operational structures while projecting an image of blockchain technology advancement. In this sense, symbolic blockchain technology adoption does not empower firms to effectively counter external threats, as these adoptions lack substantial integration into their business operations. Therefore, we predict that symbolic blockchain technology adoption does not influence data breaches in firms.

Hypothesis 1: Symbolic blockchain technology adoption will not influence data breaches in firms.

Substantive Blockchain Technology Adoption

Substantive blockchain technology adoption aims at actual integration into organizational routines to gain tangible technical benefits, including enhanced security and reliability in a firm's blockchain systems. The incorporation of blockchain technology is integrated into the fundamental business practices and processes of organizations. Consequently, substantive adoptions of blockchain technology can lead to substantial and tangible modifications in organizational routines. By integrating blockchain technology into firms' operations, firms can create a robust security infrastructure, reducing vulnerabilities and enhancing resilience against information security threats. Therefore, we predict that substantive blockchain technology adoption will reduce data breaches in firms.

Hypothesis 2: Substantive blockchain technology adoption will reduce data breaches in firms.

METHODOLOGY

Data Collection

We collected data from multiple sources. First, data breach datasets were obtained from the Privacy Rights Clearinghouse (PRC). The PRC offers longitudinal datasets on data breaches spanning from 2005 to 2022. Second, we collected blockchain technology adoptions in the U.S. Securities and Exchange Commission websites (i.e., EDGAR), employing the keyword search mechanism as outlined in the literature (Cheng, De Franco, Jiang, & Lin, 2019). We categorized symbolic and substantive blockchain technology adoptions based on the definition in the prior literature (Dahlin et al., 2020; Truong et al., 2021). For example, if the adoption of blockchain technology descriptions contain "implement," "launch," and "operate," we assign these adoptions as substantive adoptions of blockchain technology. Otherwise, we assign symbolic adoptions of blockchain technology. The initial classification results could include minor errors. Descriptions such as "not implement," "not launch," and "not operate" could be falsely classified as substantive blockchain technology adoption. To address these issues, we proceeded with the data-cleansing and corrected any misclassifications to the extent possible. Third, we collected a firm's financial data sets from Compustat (i.e., Wharton Research Data Services) including the number of employees, research and development expenses, advertisement expenses, total assets, net income, sales, market value, and more. These variables are widely used as control variables in IS economics research (Kohli, Devaraj, & Ow, 2012; Mithas & Rust, 2016; Sabherwal, Sabherwal, Havakhor, & Steelman, 2019). Finally, we merged data on data breaches, blockchain technology adoptions, and financial information for firms, resulting in the creation of two-panel data sets at the firm-year level (Panel A contains symbolic adoptions of blockchain technology and Panel B contains substantive adoptions of blockchain technology). We have 103,310 firm-year observations of Panel A and 99,542 firm-year observations of Panel B, spanning from 2005 to 2022.

Descriptive Statistics

We reported the definitions of our variables in Table 1 and descriptive statistics of both Panels A and B in Table 2. In particular, Table 1 provides detailed explanations of variables and references. We perform a natural log transformation on Data Breaches, Size, R&D, Business Segment, Market Value, and Industry Sales. Utilizing the natural log transformation will enable a more intuitive interpretation of the regression coefficients.

Variable	Definition	Source
Data Breaches	A firm's number of data breaches per year	PRC
Symbolic BCT Adoption	The staggered interaction term between the symbolic treatment dummy and pre-post dummy	EDGAR
Substantive BCT Adoption	The staggered interaction term between the substantive treatment dummy and pre-post dummy	EDGAR
Size	Total assets that represent a firm's size (Haislip, Lim, & Pinsker, 2021; Higgs, Pinsker, Smith, & Young, 2016; Jang, Kim, & Kang, 2024)	Compustat
R&D	R&D expenses that capture a firm's R&D investment (Haislip et al., 2021; Higgs et al., 2016)	Compustat
Leverage	The ratio of total liabilities divided by total assets (Haislip et al., 2021; Higgs et al., 2016)	Compustat
Loss	An indicator variable equal to 1 if the firm reported negative net income in the current year, or 0 otherwise (Haislip et al., 2021; Higgs et al., 2016)	Compustat
Business Segment	The number of business segments (Aobdia, 2020)	Compustat
Market Value	Market capitalization (Guo, Walton, Wheeler, & Zhang, 2021)	Compustat
Industry Growth	Industry sales growth based on the two-digit GICS code	Compustat
Industry Sales	The sum of sales in each industry using the two-digit GICS code	Compustat

Table 1. Variables

Table 2 provides the number of observations, mean, and standard deviation of both Panels A and B.

	Panel A			Panel B		
Variable	**Observations**	**Mean**	**Std. dev.**	**Observations**	**Mean**	**Std. dev.**
Data Breaches	103,310	0.006	0.078	99,542	0.005	0.072
Symbolic BCT Adoption	103,310	0.008	0.089	-	-	-
Substantive BCT Adoption	-	-	-	99,542	0.001	0.037
Size	103,310	4.863	3.768	99,542	4.771	3.730
R&D	103,310	1.033	1.841	99,542	1.024	1.823
Leverage	103,310	0.798	3.627	99,542	0.790	3.621
Loss	103,310	0.283	0.450	99,542	0.282	0.450
Business Segment	103,310	1.031	0.989	99,542	1.017	0.985
Market Value	103,310	3.519	3.520	99,542	3.471	3.495
Industry Growth	103,310	0.029	0.104	99,542	0.029	0.104
Industry Sales	103,310	14.115	1.085	99,542	14.096	1.091

Table 2. Descriptive Statistics

The Two-Way Fixed Effects Difference-in-Differences Through Staggered Treatment Timing

We utilized the two-way fixed effects (TWFE) difference-in-differences (DID) design using staggered treatment timing to test our hypotheses because the timing of a firm's blockchain technology adoption varies over the years. To do that, we formulated equation (1) as follows:

$$Data\ Breaches_{it} = \beta_0 + \beta_1 D_{it} + \beta_\zeta X_{it} + \alpha_i + \gamma_t + \varepsilon_{it} \quad (1)$$

, where α_i and γ_t are firms and years fixed effects that capture the main effects of treatment and pre-post dummies. X_{it} represents a vector of control variables, and D_{it} is the staggered interaction term to test our hypotheses. We used the equation (1) to get the estimand of β_1 using Panel A to test hypothesis 1 and Panel B to test hypothesis 2.

Entropy Balancing Matching

We utilized entropy balancing matching to balance covariates between the treatment and control groups at pre-treatment periods (i.e., before blockchain technology adoption either symbolic or substantive). Entropy balancing matching achieves balanced covariates by aligning the covariate distributions of the treatment and control group using a predetermined set of pre-treatment covariates (Hainmueller & Xu, 2013; McMullin & Schonberger, 2020). In this sense, entropy balancing matching is considered a multivariate matching approach that alleviates selection bias. We used the same covariates (See Guo et al., (2021)) that are determinants of blockchain technology adoption to utilize entropy balancing matching.

Empirical Results

We reported the results of staggered TWFE DID in Table 3. Model (1) represents the effects of symbolic blockchain technology adoption on data breaches and Model (2) illustrates the effects of substantive blockchain technology adoption on data breaches. The findings indicate that *Symbolic BCT Adoption* does not influence data breaches, which supports our hypothesis 1. Conversely, *Substantive BCT Adoption* significantly reduces data breaches ($p < 0.05$), which supports our hypothesis 2.

Variables	**Model (1)** **DV: Data Breaches**	**Model (2)** **DV: Data Breaches**
Symbolic BCT Adoption	0.01468 (0.00931)	-
Substantive BCT Adoption	-	-0.02534** (0.01147)
Size	0.00008 (0.00202)	-0.00639 (0.00466)
R&D	-0.00372**	0.01749*

	(0.00168)	(0.00918)
Leverage	0.00005 (0.00004)	-0.00015 (0.00012)
Loss	-0.00552 (0.00361)	-0.00411 (0.00263)
Business Segment	0.00970*** (0.00372)	0.00160 (0.00493)
Market Value	-0.00015 (0.00227)	0.00137 (0.00107)
Industry Growth	0.00911 (0.01497)	-0.00414 (0.02279)
Industry Sales	0.01446 (0.01228)	0.04269** (0.01904)
Constant	-0.19494 (0.16616)	-0.58027** (0.25639)
Observations	103,310	99,542
R-squared	0.254	0.173
Firm FE	Included	Included
Year FE	Included	Included
Panel	Panel A	Panel B
Note. *** p < 0.01; ** p < 0.05; *p < 0.1; Robust standard errors clustered by firm and year dummies		

Table 3. The Results of Staggered TWFE DID

CONCLUSION

This research examines the effects of blockchain technology adoption on data breaches through institutional theory. Based on symbolic or substantive blockchain technology adoption, we tested two primary hypotheses using the TWFE DID. We document that substantive blockchain technology adoption reduces data breaches. In this sense, this study provides revelatory insights that not all blockchain technology adoptions affect data breaches based on sophisticated research methods. Since symbolic blockchain technology adoption does not affect data breaches, managers need to consider alternative strategies to improve data security. This study has a limitation regarding the availability of financial data, and we have not considered a firm's approach to implementing blockchain technology. In addition, this study does not consider how blockchain technology aligns with and influences employee tasks that could affect data breaches. Future research should explore how blockchain technology aligns with and influences employee tasks that could affect data breaches. However, our empirical estimands are parsimonious to examine the effects of blockchain technology adoption on data breaches. We anticipate that future research can apply our study to examine the effects of blockchain technology adoption and data breaches based on private firms.

REFERENCES

1. Angst, C. M., Block, E. S., D'arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly*, *41*(3), 893–916.
2. Aobdia, D. (2020). The economic consequences of audit firms' quality control system deficiencies. *Management Science*, *66*(7), 2883–2905.
3. Catalini, C., & Gans, J. S. (2020). Some simple economics of the blockchain. *Communications of the ACM, 63*(7), 80–90.
4. Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., & Wortmann, F. (2019). Blockchain for the IoT: privacy-preserving protection of sensor data. *Journal of the Association for Information Systems*, *20*(9), 1274–1309.
5. Cheng, S. F., De Franco, G., Jiang, H., & Lin, P. (2019). Riding the blockchain mania: Public firms' speculative 8-K disclosures. *Management Science*, *65*(12), 5901–5913.

6. Constantinides, P., Henfridsson, O., & Parker, G. G. (2018). Introduction—Platforms and infrastructures in the digital age. *Information Systems Research*, *29*(2), 381–400.
7. Dahlin, P., Ekman, P., Röndell, J., & Pesämaa, O. (2020). Exploring the business logic behind CSR certifications. *Journal of Business Research*, *112*, 521–530.
8. DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, *48*(2), 147–160.
9. Guo, F., Walton, S., Wheeler, P. R., & Zhang, Y. (2021). Early disruptors: Examining the determinants and consequences of blockchain early adoption. *Journal of Information Systems*, *35*(2), 219–242.
10. Hainmueller, J., & Xu, Y. (2013). Ebalance: A Stata package for entropy balancing. *Journal of Statistical Software*, *54*(7).
11. Haislip, J., Lim, J.-H., & Pinsker, R. (2021). The impact of executives' IT expertise on reported data security breaches. *Information Systems Research*, *32*(2), 318–334.
12. Hendershott, T., Zhang, X., Zhao, J. L., & Zheng, Z. (2021). FinTech as a game changer: Overview of research frontiers. *Information Systems Research*, *32*(1), 1–17.
13. Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems*, *30*(3), 79–98.
14. Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management*, *49*, 114–129.
15. Jang, K., Kim, H., & Kang, M. (2024). The effects of government labour intervention on firm performance and innovation. *Applied Economics*, 1–6.
16. Janssen, M., Weerakkody, V., Ismagilova, E., Sivarajah, U., & Irani, Z. (2020). A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. *International Journal of Information Management*, *50*, 302–309.
17. Jeong, A. Y., & Lim, J.-H. (2023). The Impact of Blockchain Technology Adoption Announcements on Firm's Market Value. *Journal of Information Systems*, *37*(1), 39–65.
18. Kohli, R., Devaraj, S., & Ow, T. T. (2012). Does information technology investment influence a firm's market value? A case of non-publicly traded healthcare firms. *MIS Quarterly*, *36*(4), 1145–1163.
19. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems*, *107*, 841–853.
20. McMullin, J. L., & Schonberger, B. (2020). Entropy-balanced accruals. *Review of Accounting Studies*, *25*(1), 84–119.
21. Mithas, S., & Rust, R. T. (2016). How Information Technology Strategy and Investments Influence Firm Performance. *MIS Quarterly*, *40*(1), 223–246.
22. Rasi, R. Z., Rakiman, U. S. B., Radzi, R. Z. R. M., Masrom, N. R., & Sundram, V. P. K. (2021). A literature review on blockchain technology: Risk in supply chain management. *IEEE Engineering Management Review*, *50*(1), 186–200.
23. Sabherwal, R., Sabherwal, S., Havakhor, T., & Steelman, Z. (2019). How does strategic alignment affect firm performance? The roles of information technology investment and environmental uncertainty. *MIS Quarterly*, *43*(2), 453–474.
24. Sheel, A., & Nath, V. (2019). Effect of blockchain technology adoption on supply chain adaptability, agility, alignment and performance. *Management Research Review*, *42*(12), 1353–1374.
25. Toufaily, E., Zalan, T., & Dhaou, S. B. (2021). A framework of blockchain technology adoption: An investigation of challenges and expected value. *Information & Management*, *58*(3), 103444.
26. Truong, Y., Mazloomi, H., & Berrone, P. (2021). Understanding the impact of symbolic and substantive environmental actions on organizational reputation. *Industrial Marketing Management*, *92*, 307–320.
27. Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management*, *52*, 102090.
28. Xu, R., & Guan, E. (2022). Can blockchain innovation promote total factor productivity? Evidence from Chinese-listed firms. *Applied Economics*, 1–18.