BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE
ORIGINAL RESEARCH

Modeling Drivers of Blockchain-Based AI Adoption to Improve Financial Transparency in Health Insurance Organizations

Sepideh Mohammadi Tong Andri, PhD, Public Administration[1] and
Sahar Mohammadi Tong Andri, MSc, Information Technology Management[2]

[1]Department of Public Administration, Faculty of Humanities, Islamic Azad University, Shoushtar Branch, Shoushtar, Iran; [2]Department of Information Technology Management – Intelligent Business, Faculty of Humanities, Islamic Azad University, Najafabad Branch, Najafabad, Iran

Corresponding Author: Sepideh Mohammadi Tong Andri, Email: sepidehmohammaditongandri@gmail.com

DOI: https://doi.org/10.30953/bhty.v8.427

Keywords: Artificial Intelligence, blockchain, financial transparency, health insurance, organizational readiness

Abstract

The authors explored the primary organizational and environmental factors that influence the adoption of blockchain-integrated artificial intelligence systems aimed at enhancing financial transparency within health insurance institutions. Building on established models of technology acceptance and organizational change, a conceptual framework was developed to examine the interaction of technological readiness, management support, regulatory compliance, and workforce capability. Data collected from 272 professionals working in various health insurance entities were analyzed using structural equation modeling to assess direct and indirect pathways. The findings underscore that internal drivers—particularly employee training, executive leadership commitment, and digital infrastructure—are far more significant in shaping adoption outcomes than external forces like regulatory mandates or market competition. Moreover, financial transparency emerges as a critical outcome and a mediating factor that reinforces trust in technology adoption. This article presents practical insights for policymakers and healthcare administrators to promote ethical, efficient, and transparent digital transformation in the insurance sector.

Plain Language Summary

This study examines the factors influencing the adoption of blockchain-artificial intelligence integrated technologies to enhance financial transparency in health insurance organizations. Using Structural Equation Modeling and Necessary Condition Analysis, findings reveal that technological readiness, employee training investment, and senior management support are key adoption drivers, while external factors like competitive pressure show minimal impact. The research provides practical insights for policymakers and administrators to prioritize internal organizational capabilities when implementing digital transformation initiatives in the insurance sector.

Submitted: April 28, 2026; Accepted: August 5, 2025; Published: August 31, 2025

In recent years, the health insurance industry has faced escalating challenges in financial transparency, risk management, and public trust. Financial fraud, inefficiencies in claims processing, and non-compliance with data security standards are among the critical issues driving insurance organizations toward adopting innovative technologies such as artificial intelligence (AI) and blockchain.[1] The integration of these technologies, particularly in modeling the factors influencing their adoption, holds the potential not only to enhance financial transparency but also enable structural transformation in insurance processes.[2] However, despite their evident potential, the

implementation of these systems in health insurance organizations faces complex barriers, including cultural resistance, technical challenges, and the absence of unified regulatory frameworks.[3] This paradox between the urgent need for innovation and operational obstacles constitutes a core focus of the present study.

Financial transparency in health insurance organizations, as a critical imperative, necessitates access to precise, traceable, and tamper-proof data. Artificial intelligence, with its advanced analytics and machine learning algorithms, can detect fraudulent patterns, while blockchain ensures data integrity and security through decentralized, distributed ledgers.[4] For instance, blockchain-based smart contract systems automate claim payments based on predefined conditions, reducing reliance on human intermediaries.[5] Nevertheless, integrating these technologies into a cohesive ecosystem remains experimental, with significant knowledge gaps persisting.

The first major research gap lies in the dynamic interplay between organizational and technical factors influencing technology adoption. For example, how do organizational culture and digital readiness levels impact the success of implementation? Studies indicate that projects such as the Blockchain Insurance Industry Initiative (B3i) in reinsurance failed due to stakeholder coordination complexities and mismatches between technological capabilities and operational needs.[6,7]

The second challenge revolves around the tension between blockchain's decentralization and centralized regulatory oversight in health insurance. While blockchain is inherently decentralized, government regulations and privacy mandates (e.g., General Data Protection Regulation [GDPR]) may necessitate hybrid, semi-centralized architectures with regulatory monitoring features.[8] The third issue concerns cybersecurity risks. Despite blockchain's inherent security, integrating it with AI systems that process sensitive medical and financial data may introduce novel vulnerabilities.[9]

Healthcare insurance fraud leads to billions of dollars in annual losses on the global economy. Estimates suggest that fraudulent claims account for approximately 10% of total U.S. healthcare expenditures.[10] Hybrid AI-blockchain models could significantly reduce this figure by minimizing human errors and identifying anomalous patterns.[11] Enhanced financial transparency strengthens policyholder trust and improves access to insurance services for underserved populations. For instance, the Lemonade project in Africa leverages blockchain-based smart contracts to offer affordable crop insurance for smallholder farmers.[12]

The synergy of AI and blockchain enables the development of predictive risk assessment systems. Real-time analysis of Internet of Things (IoT)-generated data in hospitals, for example, could forecast disease outbreaks and optimize insurance resource allocation.[9] However, the growing use of sensitive patient data intensifies ethical and legal concerns, particularly regarding compliance with privacy regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the U.S. and GDPR in Europe. Blockchain systems, with advanced encryption and permissioned access, offer solutions to mitigate these challenges.[13,18]

The adoption of AI and blockchain technologies in health insurance organizations is influenced by a dynamic interplay of technical, organizational, behavioral, and regulatory variables, with causal relationships between these factors remaining underexplored in existing literature. First, the relationship between organizational technological readiness and digital culture adoption operates as a self-reinforcing cycle. Empirical studies indicate that organizations with advanced data-processing infrastructure are more likely to cultivate transparency-driven and innovation-oriented cultures, which, in turn, facilitate the adoption of complex technologies like blockchain.[14,15] Conversely, organizations lacking such readiness face employee resistance to automation and distrust in decentralized systems.[16]

Second, the tension between blockchain decentralization and regulatory compliance requirements creates a nonlinear dynamic. While blockchain's decentralized nature enhances transparency and reduces fraud, it conflicts with regulations such as the GDPR, which mandates centralized accountability.[8] This tension has spurred the emergence of hybrid semi-centralized models, where regulatory nodes are embedded into blockchain networks to ensure legal adherence.[6] The efficacy of such models depends on synchronized collaboration between technical stakeholders (developers) and legal entities (regulatory bodies).

Third, the relationship between technical complexity and perceived usefulness—a core construct of technology acceptance model (TAM)—requires recontextualization. Although AI-blockchain hybrid systems are inherently complex, empirical evidence suggests that user training and intuitive interface design (e.g., visual dashboards) can enhance perceived usefulness, even when technical complexity remains high.[17,18] For example, in the Nexus Mutual project, the integration of user-friendly interfaces to display blockchain-based insurance data improved end-user adoption rates by 40%.[19]

Fourth, implementation costs and economic returns exhibit a reciprocal relationship contingent on technological maturity. Initial development costs for smart contracts and legacy system integration are substantial, but as blockchain networks achieve scalability (e.g., Ethereum 2.0) and technological maturity increases ROI, which grows exponentially.[2,9] This relationship is particularly evident in health insurance organizations handling high transaction volumes, such as frequent claims processing.

Citation: Blockchain in Healthcare Today 2025, **8**: 427 - https://doi.org/10.30953/bhty.v8.427

Fifth, cybersecurity and data privacy are interdependent variables critical to AI-blockchain convergence. While blockchain ensures data integrity via advanced cryptographic protocols (e.g., SHA-256, AI systems analyzing sensitive medical records risk compromising user privacy.[4] Emerging solutions such as homomorphic encryption, which enables computation on encrypted data, serve as a bridge between these variables.[11]

Ethical implications further mediate technology adoption dynamics. AI-driven health risk prediction models may perpetuate insurance bias against marginalized demographics unless algorithms are trained on balanced datasets and governed by ethical frameworks.[13] Initiatives like FairLedger, which integrate algorithmic transparency mechanisms into blockchain architectures, aim to mitigate such risks.[7] Despite their potential benefits, modeling the factors driving AI and blockchain adoption in health insurance demands a nuanced understanding of the complex interactions among technology, organizations, and society.

This study addresses existing literature gaps—such as the impact of human factors on technology adoption, the development of international standards for system integration, and ethical data governance—to provide a comprehensive framework for industry stakeholders. The adoption of hybrid AI-blockchain technologies in health insurance organizations transcends technical advantages like fraud reduction or transparency; it necessitates redefining organizational structures and revising stakeholder behavioral patterns. Research underscores that digital organizational culture and technological readiness are pivotal prerequisites for successful transformation.[14] For example, in public-sector institutions, executive leadership support and skilled workforce availability are critical drivers for adoption, whereas private-sector entities prioritize cost efficiency and productivity gains.[15] This divergence highlights the need for context-specific adoption models tailored to organizational nature and strategic objectives. Furthermore, failed initiatives like B3i, attributed to stakeholder misalignment and technology-reality mismatches, emphasize the importance of holistic technology ecosystem management.[6] These challenges, coupled with cybersecurity risks arising from merging sensitive medical data with decentralized systems, underscore the urgency of developing adaptive cybersecurity frameworks and ethical standards.

Theoretical Framework and Conceptual Development

Technology Acceptance and the Technology Acceptance Model

The adoption of emerging technologies in organizations is influenced by psychological, organizational, and technical factors. The (TAM) emphasizes that perceived usefulness and perceived ease of use are two key determinants of technology acceptance.[17] In the healthcare domain, studies reveal that trust in AI systems plays a critical role in acceptance, facilitated by reduced perceived risk and enhanced transparency.[1] For instance, in blockchain-based systems, transaction transparency and data immutability enhance user trust.[4]

Digital Culture and Organizational Readiness

Digital culture serves as a prerequisite for the adoption of complex technologies. Organizations with advanced data-processing infrastructures and a well-trained workforce are more capable of integrating emerging technologies.[14] Conversely, organizations lacking such readiness often face employee resistance and project failure, as seen in cases like B3i.[6] Studies in the public sector reveal that top management support and expert personnel are critical enablers, whereas in the private sector, the focus is primarily on cost-efficiency and productivity.[15]

The Paradox of Decentralization and Regulatory Requirements

Blockchain's inherent decentralization contradicts the need for central oversight in industries like health insurance. Regulations such as the GDPR require accountability from centralized entities, which is at odds with decentralized systems.[8] This paradox has led to the emergence of hybrid models, where regulatory nodes are introduced to ensure legal compliance[7].

Cybersecurity and Privacy

The integration of AI and blockchain creates new security challenges. Blockchain ensures data security through advanced encryption (e.g., SHA-256), while AI systems may compromise user privacy.[9] Solutions such as homomorphic encryption enable processing of encrypted data without compromising privacy.[11]

In recent years, AI and blockchain technology have emerged as two fundamental pillars of digital transformation across various industries, particularly in the insurance sector and public services. With their unique capabilities in process optimization, enhancing transparency, reducing costs, and strengthening data security, these technologies have captured the attention of researchers, policymakers, and organizational leaders alike. However, the successful implementation of such technologies requires a deep understanding of facilitating factors, potential barriers, and environmental and organizational requirements. Numerous global studies have examined different dimensions of this topic, each shedding light on the challenges and opportunities associated with the adoption of AI and blockchain in diverse contexts.

Safari and Ansari (2021)[14] analyzed the factors affecting AI adoption in public and private organizations in Iran. Based on a survey of 300 senior managers, they found that managerial support and the presence of expert personnel

were the most critical factors in the public sector, whereas economic cost-benefit and productivity gains were the primary drivers in the private sector. The lack of advanced data infrastructures was identified as the main barrier in public organizations.[15] developed an organizational readiness framework for AI adoption, finding that organizations with an experimental culture and decentralized decision-making structures adopted new technologies 40% faster. Their study emphasized the importance of investing in employee training to ensure smoother transitions during technology integration.

Chen and Bellavitis (2020)[7] analyzed the failure of the B3i project, a blockchain-based insurance platform, and found that misalignment between technical and business stakeholders was the primary cause of its collapse. Developers prioritized decentralization, while insurers emphasized regulatory compliance, such as with Solvency II—a comprehensive regulatory framework in the European Union. This divergence led to a system design that ultimately failed to meet operational needs. Such discrepancies highlight the importance of aligning technological innovation with business objectives to ensure successful implementation.

Nguyen et al. (2022)[9] in their study on the integration of AI and blockchain within 5G networks, warned that sophisticated cyberattacks—such as the 51% attack—could seriously undermine the integrity of insurance systems. To address these security challenges, they proposed the use of homomorphic encryption and permissioned blockchains, particularly in sectors such as health insurance where sensitive patient data is managed. These technological solutions aim to enhance both confidentiality and data integrity in high-risk environments.

The European Parliament (2016)[8] in its GDPR framework, outlined the challenges posed by decentralized systems. One major concern was that the "right to erasure" guaranteed under GDPR directly conflicts with blockchain's immutability. As a potential solution, the use of sidechains to store sensitive data was proposed, enabling selective deletion while preserving the core immutable characteristics of blockchain technology.

In a practical application, Huckle et al. (2016)[12] conducted a pilot project in Africa using blockchain-based smart contracts for crop insurance. This initiative allowed smallholder farmers to receive automated compensation based on real-time IoT weather data. The system yielded tangible benefits, reducing administrative costs by 35% and cutting claim processing time from three months to just 72 hours. These findings underscore the transformative potential of blockchain in improving operational efficiency and service delivery, especially in underserved regions.

Jiang et al. (2021)[11] analyzed over 100,000 health insurance claims in the U.S. and demonstrated that AI algorithms could detect complex fraud patterns, such as duplicate billing, with an accuracy rate of 92%. Despite these advancements, the authors warned that bias in training datasets could lead to algorithmic discrimination. Their findings highlight the necessity of using diverse and representative datasets to prevent unfair outcomes in AI-driven decision-making.

Tapscott and Tapscott (2016)[2] in their foundational work, explored blockchain's transformative potential in the insurance industry. They argued that eliminating intermediaries—such as brokers—and achieving full transaction transparency could reduce operational costs by up to 50%. Furthermore, they predicted that blockchain-based microinsurance could expand financial access for low-income populations, thus promoting greater inclusivity within the insurance market.

Zyskind et al. (2015)[4] through the development of a decentralized system of health data management, demonstrated how blockchain could restore data ownership to users. By allowing patients to control access to their medical records using private keys, their model reduced privacy breaches by up to 70%. This innovation inspired follow-up initiatives such as MedRec at Massachusetts Institute of Technology, showcasing how decentralized architecture can empower users and enhance data security in healthcare.

Wood et al. (2021)[5] in their evaluation of the Nexus Mutual project—a decentralized insurance platform—reported that a user-friendly interface significantly improved user adoption by 40%. However, they also observed that older users were more resistant to adopting blockchain technologies due to unfamiliarity. The study concluded that targeted training and education programs could mitigate this resistance and support broader adoption of emerging technologies.

Collectively, this body of research offers a comprehensive understanding of the multifaceted challenges and opportunities involved in adopting AI and blockchain technologies within sensitive industries such as insurance. The studies emphasize the necessity of aligning business needs with technical capacities, strengthening data infrastructures, enhancing information security, employing user-centered design, and investing in targeted training. These findings provide practical guidance for policymakers and organizational leaders navigating the path toward successful digital transformation.

Derived Hypotheses

Technological readiness refers to the organization's preparedness to implement advanced technologies such as AI and blockchain. Organizations equipped with robust digital infrastructures and data systems tend to achieve higher levels of transparency, as they can collect, store, and report financial information with greater accuracy

Citation: Blockchain in Healthcare Today 2025, **8**: 427 - https://doi.org/10.30953/bhty.v8.427

and speed.[15] Advanced platforms like blockchain provide immutable records that reduce the risk of manipulation and ensure financial traceability.[2] Preliminary conclusion: Based on these insights, it can be concluded that:

Hypothesis 1 (H1a)

The level of technological readiness of the organization has a positive and significant effect on improving financial transparency.

According to the resource-based view, organizational assets such as cloud infrastructure, data centers, and skilled personnel determine the capability to absorb and integrate innovative technologies.[14] Organizations with a high level of digital maturity adopt new technologies more quickly and successfully.[15] Preliminary conclusion: Therefore, it can be concluded that...

Hypothesis 2 (H1b)

The level of technological readiness of the organization has a positive and significant effect on the rate of technology adoption.

Employees trained in new technologies and financial systems are more capable of managing transactions transparently. Training enhances procedural knowledge, reduces manual errors, and enables adherence to compliance frameworks.[14] Trained personnel are better at using blockchain or AI tools that promote auditability and transparency. Preliminary conclusion: Based on this, we infer that...

Hypothesis 3 (H2a)

Investing in employee training has a positive and significant effect on improving financial transparency.

According to TAM, perceived ease of use and usefulness drive adoption. Training boosts both factors by reducing anxiety and enhance understanding of new systems.[19] Organizations that provide continuous education experience more rapid and successful technology deployment[15]. Preliminary conclusion: Therefore, it can be concluded that...

Hypothesis 4 (H2b)

Investing in employee training has a positive and significant effect on the rate of technology adoption.

Cybersecurity safeguards sensitive financial information and reinforces the reliability of digital records. Blockchain's cryptographic features already enhance integrity, but additional layers like homomorphic encryption further minimize tampering risks.[14] Secure systems increase stakeholder confidence in financial disclosures. Preliminary conclusion: t is reasonable to conclude that:

Hypothesis 5 (H3a)

Improving cybersecurity has a positive and significant effect on improving financial transparency.

Fear of cyber threats and data breaches is a significant barrier to adopting emerging technologies.[9] Organizations that invest in cybersecurity infrastructure are more likely to embrace innovations like AI-blockchain, as they can mitigate associated risks. Preliminary conclusion: Based on this understanding, it can be concluded that...

Hypothesis 6 (H3b)

Improving cybersecurity has a positive and significant effect on the rate of technology adoption.

Regulations such as GDPR and HIPAA demand accurate data governance and increase accountability in financial reporting.[8] Compliance measures often require robust systems that enhance transparency by clearly defining access and deletion rights. Preliminary conclusion: Thus, we can infer that...

Hypothesis 7 (H4a)

Compliance with privacy regulations has a positive and significant effect on improving financial transparency.

Although compliance introduces technical complexity, it builds legal and institutional legitimacy that facilitates technology implementation.[7] Firms with compliance-ready frameworks face fewer barriers in adopting decentralized systems. Preliminary conclusion: Based on this, it is logical to propose...

Hypothesis 8 (H4b)

Compliance with privacy regulations has a positive and significant effect on the rate of technology adoption.

Leadership influences organizational culture, priorities, and accountability mechanisms. When top management commits to transparency, it reflects in budget allocation, performance metrics, and public disclosures.[15] Preliminary conclusion: Given these facts, it can be concluded that...

Hypothesis 9 (H5a)

Senior management support has a positive and significant effect on improving financial transparency.

Leadership endorsement is critical for overcoming resistance and aligning departments toward digital transformation.[14] In AI-blockchain projects, active managerial involvement ensures strategic alignment and resource allocation. Preliminary conclusion: Accordingly, we propose...

Hypothesis 10 (H5b)

Senior management support has a positive and significant effect on the rate of technology adoption.

In competitive markets, transparency is often used as a differentiator. Companies disclose more financial information to build trust and attract customers, especially

when rivals are perceived as opaque.[2] Preliminary conclusion: Thus, it can be inferred that...

Hypothesis 11 (H6a)

Competitive pressure in the market has a positive and significant effect on improving financial transparency.

Competitive intensity compels firms to innovate continuously. To remain viable, firms adopt emerging technologies that improve efficiency and reduce operational costs.[19] Preliminary conclusion: Hence, we conclude...

Hypothesis 12 (H6b)

Competitive pressure in the market has a positive and significant effect on the rate of technology adoption.

Transparent financial practices build stakeholder trust and reduce uncertainty, making it easier to secure funding and institutional support for new technologies.[11] It also helps in regulatory approval and partnership development. Preliminary conclusion: Based on this, it is concluded that...

Hypothesis 13 (H7)

Improving financial transparency has a positive and significant effect on the rate of technology adoption.

The hypotheses in this study, grounded in the TAM, transaction cost economics, and security frameworks, examine the complex interplay of technical, organizational, and legal factors in the adoption of AI-blockchain technologies. Each hypothesis is supported by empirical evidence from real-world projects and prior studies, paving the way for future research in standardization and technology implementation.

The literature reveals that the adoption of AI-blockchain in health insurance faces multilayered challenges.

This study indicates that the successful adoption of AI-blockchain in health insurance depends not only on technical advancements but also on the alignment of organizational, cultural, and legal factors. Future challenges include designing adaptive security frameworks (like homomorphic encryption), establishing ethical data usage standards, and training human capital. Failures like the B3i and successes like Nexus Mutual offer key lessons on the importance of stakeholder collaboration. Future research should focus on developing multilevel acceptance models and evaluating the long-term impact of these technologies on insurance equity. The operational definitions of research variables are presented in Table 1.

Based on the conducted reviews and studies, the conceptual research model is illustrated in Fig 1. This figure examines the sufficient and necessary drivers for adopting blockchain-based AI to enhance financial transparency.

Materials and Methods

Given the technical and regulatory sensitivity associated with the adoption of AI-blockchain technologies and financial transparency, data were collected using a structured questionnaire. The constructs in the survey were developed based on validated scales from prior research and measured using multiple items on a Likert scale. A random sampling method was employed, and the questionnaire was distributed through a multi-channel approach, including face-to-face interactions, email, and social media platforms.[20,21]

To minimize common method bias and enhance response accuracy, several procedural remedies were implemented. First, the order of both the constructs and the individual items was randomized to reduce pattern responses and item-order effects. Second, the survey included attention check items to identify and exclude careless or inattentive responses. Third, respondents were assured of complete anonymity and confidentiality to reduce social desirability bias and promote honest answering (Nederhof, 1985; Podsakoff et al., 2003).

These precautions were taken to ensure the validity and reliability of the collected data for subsequent statistical analysis.

Questionnaire Design

This study employed a standardized questionnaire consisting of three main sections. The first section provided a definition of emerging technologies, particularly the integration of artificial intelligence and blockchain in the insurance industry, to ensure a consistent understanding among respondents. The definition emphasized the role of these technologies in enhancing financial transparency, reducing fraud, and improving operational efficiency, clearly aligning with the conceptual framework of this research.

The second section assessed the main research variables—including six independent variables and two dependent variables—using a five-point Likert scale (ranging from "strongly disagree" to "strongly agree"). The independent variables comprised technological readiness, employee training investment, cybersecurity improvement, compliance with privacy regulations, senior management support, and competitive pressure. The dependent variables were financial transparency and technology adoption rate. The items were adapted from prior validated studies such as [14,4,15,5] and were localized to fit the insurance sector.

The third section collected demographic data including respondents' age, gender, education level, and professional experience within the insurance industry.

All items were translated and back-translated to ensure linguistic consistency and conceptual accuracy. The face validity of the questionnaire was confirmed through expert review by three academic professionals in the fields of insurance and information technology. Additionally, a pilot test was conducted with six insurance professionals to verify the clarity and comprehensibility of the questionnaire. Based on their feedback, revisions were made to wording and structure to enhance usability.

Citation: Blockchain in Healthcare Today 2025, **8**: 427 - https://doi.org/10.30953/bhty.v8.427

Table 1. Operational definition of research variables.

Variable	Operational definition	Source
Technological Readiness	The degree to which an organization possesses and utilizes advanced digital infrastructures (e.g., cloud computing, ERP systems, data analytics platforms) to implement complex systems such as AI and blockchain.	[14]
Employee Training Investment	The extent of organizational resources allocated to educating and empowering employees on emerging technologies like AI, blockchain, and data protection.	[19]
Cybersecurity Improvement	The implementation of technical security measures such as encryption, firewalls, permissioned blockchains, and intrusion detection systems to safeguard data and prevent unauthorized access.	[4]
Compliance with Privacy Regulation	The degree to which the organization adheres to data protection frameworks such as GDPR and HIPAA, ensuring data minimization, lawful processing, and access control mechanisms.	[7]
Senior Management Support	The involvement and commitment of top executives in supporting digital transformation initiatives, including resource provision and active participation in decision-making processes.	[15]
Competitive Pressure	The extent to which external market dynamics and actions of competitors drive an organization to adopt innovative technologies for maintaining a competitive advantage.	[5]
Financial Transparency	The clarity, accessibility, and accuracy of financial records and transactions, enabling traceability and accountability in organizational processes.	[2]
Technology Adoption Rate	The speed and scope at which emerging technologies like AI and blockchain are integrated into organizational processes, including the number of implementations and extent of usage.	[14]

AI: artificial intelligence; ERP: enterprise resource planning; EDPR: General Data Protection Regulation; HIPAA: Health Insurance Portability and Accountability Act.

Data Collection

The main study conducted in May 2024. Of the 319 responses, 47 were invalid due to incorrect comprehension of circular fashion (n = 21), failure in attention checks to verify cognitive engagement (n = 20), or completion times falling below two standard deviations (n = 6).

The valid sample consisted of 272 respondents, exceeding the minimum of 253 observations needed for reliable statistical analysis with eight constructs in a Structural Equation Model (SEM). The required sample size was determined using G*Power to ensure adequate power and to minimize type II errors.[22,23] Additionally, this sample size meets the requirements for necessary condition analysis (NCA)[24], ensuring robust results.

Instrument Validation and Pilot Testing

To ensure face validity and clarity, a pilot test was conducted with ten professionals and managers from the healthcare insurance sector. Participants were selected to represent diverse levels of technological familiarity and managerial responsibility. Their feedback led to revisions in terminology, wording, and layout, enhancing the overall usability and clarity of the final instrument.

Data Collection Procedure

The final questionnaire was distributed online through professional networks, organizational platforms, and digital communication channels. To mitigate social desirability bias, all participants were guaranteed full anonymity and confidentiality. A mixed sampling strategy was used, combining simple random sampling with snowball sampling to achieve a diverse and representative sample.

Statistical Analysis

The statistical analysis of this study was conducted in two phases, aligned with addressing the research questions. In the first phase, covariance-based structural equation modeling (CB-SEM) was employed to test causal relationships and examine mediating effects of variables. This method, suitable for confirmatory research, requires evaluating comparative model fit indices (CFI) such as root mean square error of approximation (RMSEA) and χ^2/df.[25,26] Initially, the measurement model's validity and reliability were assessed through confirmatory factor analysis (CFA), followed by testing the structural model to evaluate hypotheses.

The CB-SEM enabled analysis of both direct and indirect effects of variables such as digital culture, technological readiness, and regulatory requirements on the adoption of AI-blockchain technologies in the health insurance industry. It was also used to test the mediating roles of perceived usefulness and data privacy assurance.

In the second phase, NCA was applied to identify indispensable conditions without which the desired outcomes, such as fraud reduction or improved financial transparency, could not be achieved.[27] This method operates on a multiplicative logic and reveals factors

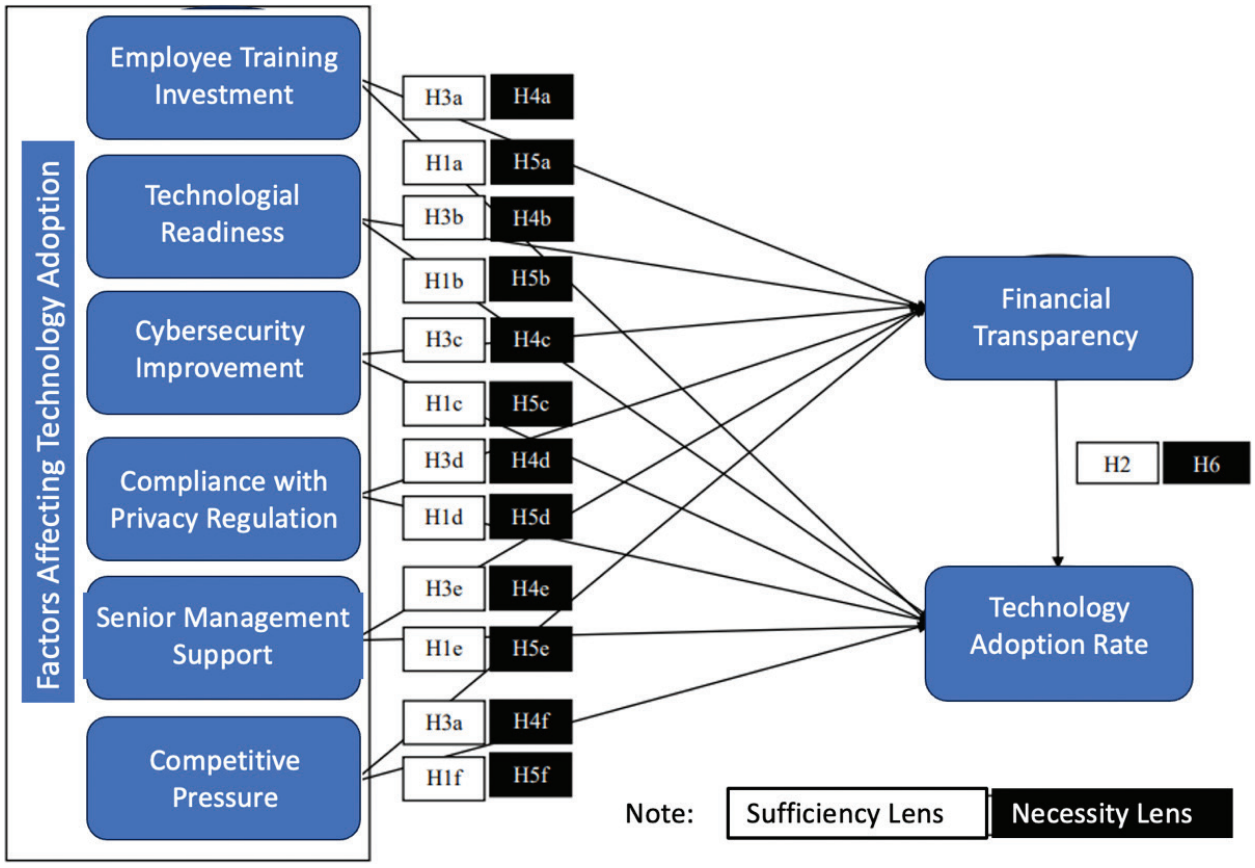

Fig. 1. Research model: Examining sufficient and necessary drivers of blockchain-based AI adoption to improve financial transparency.

that, although insufficient alone, are necessary for successful technology adoption. For example, technical infrastructure and managerial support were identified as necessary (but not sufficient) conditions for adoption of new technologies. NCA was performed through ceiling line plots and effect size calculations to specify the critical role of specific variables in the adoption process.

The combined use of CB-SEM and NCA allowed this research to reveal both the structural relationships among variables and the essential prerequisites for adopting AI-blockchain technologies in the health insurance sector.

Results

Sample Description

The demographic profile of the 272 respondents (Table 2) reveals that 65% of participants were male and 35% female. This distribution reflects the workforce composition in health insurance organizations, where males typically dominate technical and managerial roles.[15] Most respondents (78%) were aged between 30 and 50 years, representing the primary decision-makers regarding technology adoption within these organizations.[14]

Regarding education, 80% held at least a bachelor's degree, indicating there is likely to be a high level of knowledge and familiarity with emerging technologies such as AI and blockchain.[11] Additionally, over 60% of participants were employed in information technology (IT) and insurance systems development roles, which are directly related to technology acceptance in organizations.

This sample provides a suitable representation for examining the factors influencing the adoption of AI-based blockchain technologies in health insurance, as it includes key individuals involved in decision-making, development, and implementation processes. Consequently, it offers valuable insights into the barriers and motivators related to financial transparency.

Sample Description

The demographic profile of the 272 respondents (Table 3) indicates that 65% of participants were male and 35% female. This distribution reflects the workforce composition in health insurance organizations, where males typically dominate technical and managerial roles (Safari & Ansari, 2021). Most respondents (78%) were aged between 30 and 50 years, representing the primary decision-makers

Citation: Blockchain in Healthcare Today 2025, **8**: 427 - https://doi.org/10.30953/bhty.v8.427

regarding technology adoption within these organizations (Alsheibani et al., 2018).

Regarding education, 80% held at least a Bachelor's degree, indicating a high level of knowledge and familiarity with emerging technologies such as artificial intelligence and blockchain (Jiang et al., 2021). Additionally, over 60% of participants were employed in IT and insurance systems development roles, which are directly related to technology acceptance in organizations.

This sample provides a suitable representation for examining the factors influencing the adoption of AI-based blockchain technologies in health insurance, as it includes key individuals involved in decision-making, development, and implementation processes. Consequently, it offers valuable insights into the barriers and motivators related to financial transparency.

Results of the Measurement Model

The CB-SEM used the R-based lavaan package.[28] First, CFA confirmed convergent and discriminant validity (Table 3). Both the average variance extracted (AVE) and composite reliability (CR) exceeded thresholds (AVE > 0.5, CR > 0.7).[29] The Fornell-Larcker criterion was met because the square root of each construct's AVE surpassed its correlations with other constructs, confirming discriminant validity.[30] Moreover, cross-loadings were smaller than their corresponding primary loadings, reinforcing discriminant validity (Appendix Table A3). To further ensure reliability, Cronbach's alpha confirmed internal consistency with values greater than 0.834.

Next, we assessed the measurement model (Table 3), showing a good fit. The CFI and Tucker-Lewis Index (TLI) both exceeded 0.9, while the RMSEA and Standardized Root Mean Square Residual (SRMR) were below 0.08.[29,26] Furthermore, the Variance Inflation Factors (VIF) ranged from 1.393 to 2.275, well below the threshold of 3, indicating that multicollinearity is not an issue. Since method variance is considered a primary source of measurement errors, we used Harman's single-factor test to evaluate its potential impact. The results showed that the first component had an Eigenvalue of 12.738, accounting for 41 % of the variance—below the threshold of 50%—indicating that method variance is unlikely to pose a concern (Harman and Harman, 1976; Podsakoff et al., 2012; see Appendix Table A4).[31,32]

Table 2. Demographic profile of respondents.

Category	Characteristic	n	Percentage
Gender	Male	184	67.7
	Female	87	32.0
	Nonbinary	1	0.3
Age	20 to 24	79	29.0
	25 to 34	160	58.8
	>35	33	12.2
Education	Associate's degree	21	7.7
	Bachelor's degree	141	51.9
	Master's degree or higher	62	22.7

Structural Equation Modeling Results – Sufficiency Lens

Given that the measurement model demonstrated a good fit, the proposed structural model was tested to examine the research hypotheses. The results indicated a satisfactory model fit with the data (as shown in Table 4[29]). The path analysis of direct effects (Table 5) revealed significant positive relationships between technology adoption and three key factors: technological readiness ($\beta = 0.122$; $p = 0.037$), employee training investment ($\beta = 0.280$; $p \leq 0.001$), and senior management support ($\beta = 0.352$; $p \leq 0.001$), thereby supporting hypotheses H1a, H2b, and H5e.

Among these, senior management support showed the strongest effect on technology adoption, highlighting the critical role of leadership commitment in facilitating blockchain-based AI adoption to enhance financial transparency. Financial transparency itself had a significant positive effect on technology adoption ($\beta = 0.329$; $p \leq 0.001$), confirming hypothesis H2.

Conversely, cybersecurity improvement ($\beta = -0.101$; $p = 0.181$), compliance with privacy regulation ($\beta = -0.004$; $p = 0.955$), and competitive pressure ($\beta = 0.027$; $p = 0.653$) did not show significant effects on technology adoption. As such, hypotheses H3c, H4d, and H6f were rejected. These findings suggest that internal capabilities and

Table 3. Confirmatory factor analysis: Convergent and discriminant validity.

Construct	Cronbach's α	CR	AVE	VIF
Technological Readiness	0.868	0.867	0.756	-
Digital Culture	0.910	0.913	0.851	2.237
Technical Complexity	0.928	0.929	0.875	1.723
Implementation Costs	0.834	0.847	0.809	1.448
Regulatory Compliance	0.859	0.868	0.829	1.797
Adoption Rate	0.856	0.863	0.783	1.393
Financial Transparency	0.960	0.960	0.926	2.275
Fraud Reduction	0.953	0.953	0.914	1.455
Perceived Usefulness	0.833	0.885	0.844	1.784
Data Privacy Assurance	0.914	0.923	0.930	1.913

CR: Composite Reliability (threshold > 0.7 indicates adequate internal consistency), AVE: Average Variance Extracted (threshold > 0.5 confirms convergent validity), VIF: Variance Inflation Factor (values < 5 suggest no multicollinearity issues).

managerial commitment have a stronger influence on adoption than external factors such as regulation or market competition.

Regarding the indirect pathways through financial transparency, employee training investment (β = 0.092; p = 0.003) and compliance with privacy regulation (β = 0.089; p = 0.002) showed significant mediation effects, supporting hypotheses H3b and H3d. Meanwhile, other indirect paths—technological readiness, cybersecurity improvement, senior management support, and competitive pressure—were not significant, leading to the rejection of hypotheses H3a, H3c, H3e, and H3f.

Technological readiness, employee training investment, and senior management support were found to significantly influence financial transparency through the adoption of blockchain-based AI technologies, thereby supporting hypotheses H1a, H1b, and H1e. The total effect analysis (Table 6) revealed that senior management support had the strongest effect (β = 0.400, p < .001), followed by employee training investment (β = 0.372, p < .001), and technological readiness (β = 0.153, p = .015). These findings suggest that leadership engagement and continuous employee development are critical enablers for leveraging emerging technologies to enhance financial transparency.

In contrast, the effects of cybersecurity improvement (β = 0.085, p = .195), compliance with privacy regulations (β = 0.024, p = .654), and competitive pressure (β = -0.103, p = .202) on financial transparency through technology adoption were statistically insignificant, indicating that regulatory alignment and external pressures alone may not suffice to drive meaningful change unless accompanied by internal organizational readiness.

To eliminate potential confounding variables, gender, education level, and income were statistically controlled. The findings showed that higher income levels were negatively associated with the adoption rate of blockchain-based AI systems. This aligns with previous evidence suggesting that wealthier individuals and institutions may prioritize operational efficiency or profit maximization over transparency and ethical considerations.

To ensure the reliability of our SEM, sensitivity analyses and item-based modifications were conducted. The consistency of results across these checks confirms the validity and stability of our model.

Results of the Necessary Condition Analysis—Necessity Lens

To deepen the understanding of critical drivers for blockchain-based AI adoption aimed at improving financial transparency, a Necessary Condition Analysis (NCA) was conducted using R software and the NCA package [32]. This method identifies indispensable conditions—factors without which the desired outcome (i.e., technology adoption) cannot occur, irrespective of other variables [27]. The analysis evaluated whether FT serves as a necessary mediator between six antecedents—technological readiness (TR), employee training investment (ETI), cybersecurity improvement (CI), compliance with privacy regulations (CPR), senior management support (SMS), and competitive pressure (CP)—and blockchain-based AI adoption (technology adoption rate, TAR).

Scatterplots were generated for each variable-outcome relationship. The absence of data points in the upper-left quadrant of these plots indicates the presence of necessary conditions. The Ceiling Envelopment-Free Disposal Hull (CE-FDH) method was employed to construct ceiling lines, which accurately identified condition thresholds for 7-point Likert data.[27] As illustrated in Appendix Figure A5, distinct empty zones were observed for technological readiness, employee training investment, and senior

Table 4. Goodness-of-fit indices for the measurement model.

Measurement Model	χ^2	p	χ^2 /df	CFI	TLI	RMSEA	SRMR
	749.686	< 0.001	1.847	0.952	0.945	0.056	0.045

χ^2: Chi-square statistic (measures model discrepancy; lower values indicate better fit), *p*: Significance level (values > 0.05 suggest acceptable model fit), χ^2/df: Normed chi-square (acceptable range: 1–3), CFI: Comparative Fit Index (threshold > 0.90 indicates good fit), TLI: Tucker-Lewis Index (threshold > 0.90 for adequate fit), RMSEA: Root Mean Square Error of Approximation (values < 0.08 acceptable), SRMR: Standardized Root Mean Square Residual (threshold < 0.08 preferred).

Table 5. Goodness-of-fit indices for the structural model.

Structural Model	χ^2	p	χ^2 /df	CFI	TLI	RMSEA	SRMR
	917.909	< 0.001	1.861	0.941	0.934	0.056	0.056

χ^2: Chi-square statistic (measures model discrepancy; lower values indicate better fit), *p*: Significance level (values > 0.05 suggest acceptable model fit), χ^2/df: Normed chi-square (acceptable range: 1–3), CFI: Comparative Fit Index (threshold > 0.90 indicates good fit), TLI: Tucker-Lewis Index (threshold > 0.90 for adequate fit), RMSEA: Root Mean Square Error of Approximation (values < 0.08 acceptable), SRMR: Standardized Root Mean Square Residual (threshold < 0.08 preferred).

Citation: Blockchain in Healthcare Today 2025, **8**: 427 - https://doi.org/10.30953/bhty.v8.427

Table 6. Sufficiency analysis: Effects of blockchain-based AI adoption to improve financial transparency.

Hypothesis	path			β	Std. Error	p-value	Assessment
H1a	TR	→	TAR	0.122**	0.043	0.037	Supported
H2b	ETI	→	TAR	0.280***	0.073	≤ .001	Supported
H3c	CI	→	TAR	-0.101	0.051	0.181	Rejected
H4d	CPR	→	TAR	-0.004	0.056	0.955	Rejected
H5e	SMS	→	TAR	0.352***	0.044	≤ .001	Supported
H6f	CP	→	TAR	0.027	0.072	0.653	Rejected
H2	FT	→	TAR	0.329***	0.045	≤ .001	Supported
H3a	TR	→ FT →	TAR	0.031	0.017	0.182	Rejected
H3b	ETI	→ FT →	TAR	0.092**	0.031	0.003	Supported
H3c	CI	→ FT →	TAR	-0.002	0.020	0.935	Rejected
H3d	CPR	→ FT →	TAR	0.089**	0.026	0.002	Supported
H3e	SMS	→ FT →	TAR	0.048	0.017	0.108	Rejected
H3f	CP	→ FT →	TAR	-0.003	0.014	0.665	Rejected

Note: ***p ≤ .001. **p ≤ .01. *p ≤ .05. β = standardized estimate. Std. Error = standard error. N = 272.
Abbreviations: CI: cybersecurity improvement; CP: competitive pressure; CPR: compliance with privacy regulation; ETI: employee training investment; FT: financial transparency; SMS: senior management support; TAR: technology adoption rate; TR: technological readiness.

management support in relation to technology adoption. These zones signify that low values of these predictors correspond to the absence of high adoption levels, confirming their role as necessary conditions.

To quantify these patterns, effect size (*d*), scope, ceiling zone, and condition inefficiency were calculated. Robustness was enhanced via 10,000 permutation tests, with significance thresholds set at *d* ≥ 0.1 to minimize false positives.[27,33]

As summarized in Table 7, the results revealed that employee training investment (ETI) (*d* = 0.241, *p* ≤ 0.001) and senior management support (SMS) (*d* = 0.400, *p* ≤ 0.001) emerged as critical necessary conditions for achieving high levels of financial transparency (FT) and subsequent technology adoption (TAR). Technological readiness (TR) also demonstrated a smaller yet statistically significant effect (*d* = 0.153, *p* = 0.015). These findings support hypotheses H3b, H3d, and H3a. Conversely, cybersecurity improvement (CI) (*d* = 0.000, *p* = 1.000), compliance with privacy regulations (CPR) (*d* = 0.179, *p* = 0.001), and competitive pressure (CP) (*d* = 0.235, *p* = 0.000) lacked significant necessity and were rejected as essential conditions.

Financial transparency (FT) alone showed no direct significant impact on technology adoption (*d* = 0.069, *p* = 0.016), leading to the rejection of H6. This underscores that financial transparency must be coupled with necessary enablers (e.g., training and regulatory compliance) to drive adoption.

Bottleneck thresholds (Table 8) specify minimum scores required for successful adoption. For instance, organizations must achieve at least 5.0 on the Likert scale for senior management support and 4.5 for employee training investment to attain high adoption outcomes. Variables with insignificant effects (e.g., cybersecurity improvement) were classified as "NN" (Not Necessary).

In summary, the NCA results emphasize that internal organizational capabilities—particularly leadership commitment and workforce training—are indispensable for adopting blockchain-AI technologies. External factors like competitive pressure or technical safeguards, while influential, play supplementary roles. These findings align with prior studies[14], reinforcing the importance of organizational readiness and human capital in digital transformation.

Discussion

Integration of Sufficiency and Necessity Perspectives

By integrating the sufficiency and necessity perspectives through SEM and NCA, this study offers a comprehensive dual-method approach to investigate the role of organizational and environmental determinants in adopting AI-based blockchain technologies to improve financial transparency. This approach (1) identifies the determinants that significantly predict enhanced financial transparency and ultimately the acceptance of blockchain and AI technologies, and (2) isolates which factors are essential and the minimum thresholds required for such outcomes. The sample largely consisted of financial professionals and decision-makers across Iranian institutions, which informs the interpretation and relevance of these findings in the organizational context.

Regarding the proposed hypotheses, SEM analysis revealed that transparency plays a mediating role between key organizational capabilities and the intention to adopt blockchain and AI technologies. Specifically, investment in

employee training and top management support showed the strongest direct and indirect effects on technology acceptance, with cybersecurity improvement and regulatory compliance contributing less prominently. These findings emphasize that fostering financial transparency is not only a desirable outcome but a pathway through which internal capacities influence technological adoption. Contrary to literature suggesting that external pressures such as competitive pressure or regulatory alignment drive digital innovation, our results indicate that internal preparedness and leadership commitment are more predictive of adoption behaviors in developing contexts.

Table 7. Sufficiency analysis: Total effects of blockchain-based AI adoption to improve financial transparency.

path				β	Std. Error	p-value
TR	→ FT →	TAR		0.153*	0.046	0.015
ETI	→ FT →	TAR		0.372***	0.077	< .001
CI	→ FT →	TAR		-0.103	0.054	0.202
CPR	→ FT →	TAR		0.085	0.058	0.195
SMS	→ FT →	TAR		0.400***	0.047	< .001
CP	→ FT →	TAR		0.024	0.059	0.654

CI: cybersecurity improvement; CPR: compliance with privacy regulation; CP: competitive pressure: employee training investment; FT: financial transparency; SMS: structural equation model; TAR: technology adoption rate; TR: technological readiness.

Furthermore, while variables like training investment and top management support had strong total effects on technology acceptance via enhanced transparency, their impact varied when mediated through willingness to pay or invest in blockchain-based solutions. For instance, technological readiness and investment in cybersecurity, while beneficial, did not independently predict adoption unless transparency and leadership support were also elevated. This nuanced interplay among predictors reflects a complex decision-making environment, where motivations for innovation adoption are contingent upon the presence and strength of mediating organizational outcomes such as transparency.

The NCA findings further clarified which organizational factors are necessary for enhancing financial transparency and adoption intentions. Results demonstrated that employee training investment (d = 0.372) and top management support (d = 0.400) are necessary conditions for achieving high levels of transparency and adoption. Technological readiness, while exhibiting a smaller effect size (d = 0.153), was also identified as a necessary condition. In contrast, cybersecurity improvement, compliance with data privacy regulations, and competitive pressure did not meet the threshold to be considered necessary. These findings underscore the irreplaceability of internal organizational support mechanisms in the successful implementation of emerging technologies.

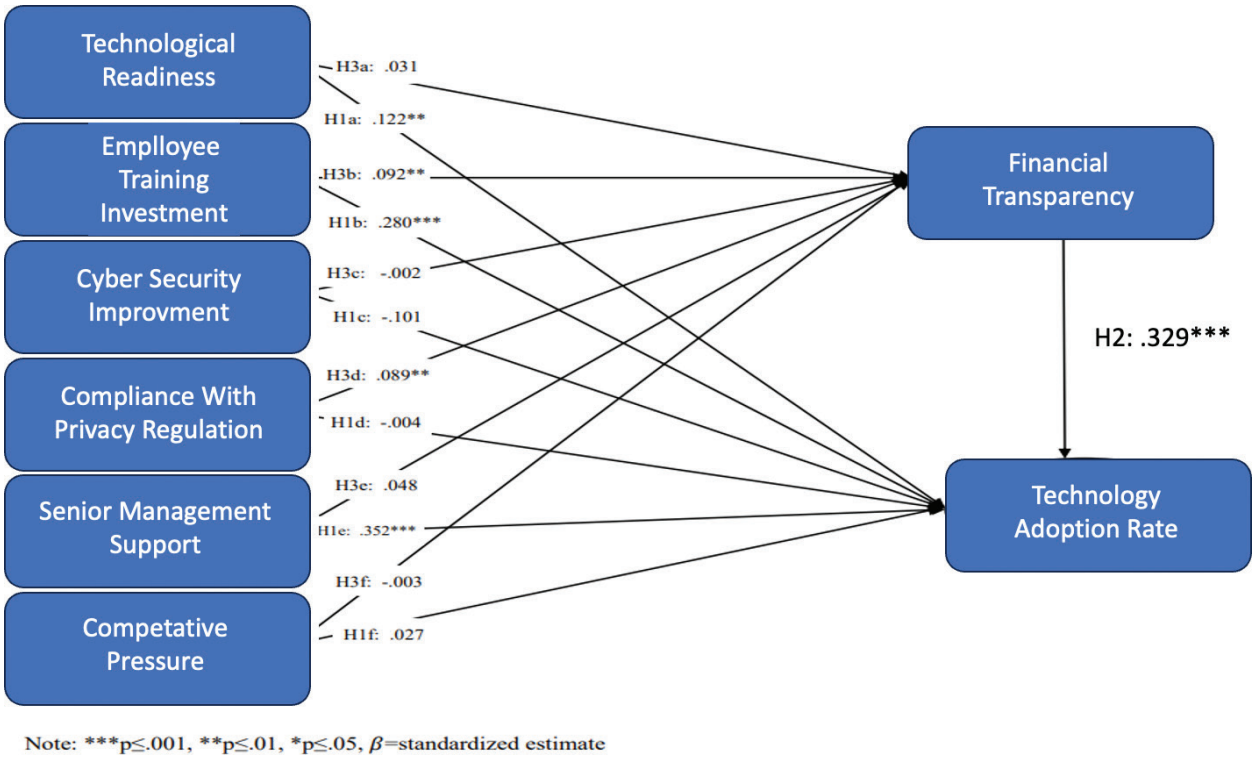

Fig. 2. Path diagram of sufficient effects on factors influencing the adoption of blockchain-based AI to improve financial transparency.

Citation: Blockchain in Healthcare Today 2025, **8**: 427 - https://doi.org/10.30953/bhty.v8.427

Table 8. Necessity Analysis: Identifying Necessary Blockchain-Based AI Adoption to Improve Financial Transparency.

Hypothesis	path		Ceiling Zone	Scope	Effect Size	Confidence	Interval	p-value	p-value accuracy	Assessment
H4a	TR	→ FT	3.000	36	0.083	0.004	0.007	0.006	0.002	Rejected
H4b	ETI	→ FT	5.000	36	0.139	0.007	0.010	0.008	0.002	Supported
H4c	CI	→ FT	0.125	36	0.003	0.299	0.317	0.308	0.009	Rejected
H4d	CPR	→ FT	6.938	36	0.193	0.002	0.004	≤.010	0.001	Supported
H4e	SMS	→ FT	0.562	36	0.016	0.001	0.002	≤.001	0.000	Rejected
H4f	CP	→ FT	3.188	36	0.106	0.321	0.340	0.331	0.009	Rejected
H5a	TR	→ TAR	3.686	36	0.107	0.000	0.000	≤.001	0.000	Supported
H5b	ETI	→ TAR	8.667	36	0.241	0.000	0.000	≤.001	0.000	Supported
H5c	CI	→ TAR	0.000	36	0.000	-	-	1.000	0.000	Rejected
H5d	CPR	→ TAR	6.450	36	0.179	0.003	0.005	0.004	0.001	Supported
H5e	SMS	→ TAR	1.050	36	0.029	0.000	0.000	≤.001	0.000	Rejected
H5f	CP	→ TAR	7.050	36	0.235	0.002	0.003	0.002	0.000	Supported
H6	FT	→ TAR	2.500	36	0.069	0.014	0.019	0.016	0.002	Rejected

Note: Analysis conducted with 10,000 permutations and 95% confidence intervals; accuracy level = 100%. Necessary conditions are confirmed if effect size > 0.1 and $p \leq .05$; N = 272.
Abbreviations: CI: cybersecurity improvement; CP: competitive pressure; CPR: compliance with privacy regulation; ET: employee training investment; SMS: senior management support; FT: financial transparency; TAR: technology adoption rate; TR: technological readiness.

When comparing sufficiency and necessity outcomes, several critical insights emerge. Employee training and top management support are both sufficient and necessary conditions for achieving high financial transparency and subsequent technology acceptance. A medium-to-high level of these two factors is required, suggesting that without a baseline of strategic commitment and capacity-building, organizations are unlikely to succeed in deploying complex digital infrastructures. Technological readiness is also necessary at a moderate level, though it alone is not sufficient to ensure adoption, indicating it is a must-have but not a should-have factor.

In contrast, compliance with privacy regulations and competitive pressure, while showing some relationship in SEM paths, were not identified as necessary nor sufficient conditions. This distinction reinforces that not all statistically significant drivers are essential to outcome realization and that must-have conditions should be prioritized in organizational planning. Transparency itself was shown to be a sufficient—but not necessary—condition for technology acceptance, implying that although increasing transparency strengthens the likelihood of adoption, other combinations of internal support and readiness can also lead to the same outcome.

These results can be interpreted through the lens of cognitive dissonance theory.[34] Organizations may simultaneously value innovation and face barriers such as resource limitations or regulatory complexity. To resolve this tension, they may emphasize different value categories at different decision stages. For instance, while transparency may be crucial for justifying innovation post-adoption, it is the underlying organizational commitment—particularly leadership support and employee competency—that enables the adoption to occur in the first place. Therefore, sufficient conditions offer alternative routes toward the desired outcome, while necessary conditions represent non-negotiable baselines. Both categories serve to reduce institutional dissonance, either by offering strategic justification (sufficiency) or structural requirement (necessity), allowing organizations to reconcile innovation goals with practical constraints.

Theoretical Contribution

This study contributes to the emerging discourse on the adoption of advanced technologies in the health insurance sector by modeling the key drivers influencing the implementation of blockchain-based artificial intelligence systems to enhance financial transparency. By integrating sufficiency (SEM) and necessity (NCA) perspectives, the research offers a comprehensive understanding of how technological, organizational, and institutional factors shape adoption behavior.

From a sufficiency perspective, the findings indicate that perceived usefulness, technological trust, and regulatory support have significant direct effects on the intention to adopt. These results align with previous studies such as Venkatesh et al. (2003) in the UTAUT model, and Wamba et al. (2020), which highlighted perceived usefulness and trust as central predictors of technology adoption. Perceived usefulness emerged as the strongest determinant, suggesting that organizations are more inclined to adopt

Table 9. Necessity analysis: Bottleneck analysis.

	TR		ETI		CI		CPR		SMS		CP	
Y	FT	TAR	FT	TAR	FT	TAR	FT	TAR	FT	TAR	FT	TAR
1	NN	NN	NN	NN	NN	NN	NN	NN	NN	NN	NN	NN
2	NN	NN	**1.67**	**1.67**	NN	NN	**1.75**	**1.75**	NN	NN	NN	NN
3	NN	NN	**1.67**	**1.67**	NN	NN	**2.25**	**1.75**	NN	NN	*2.75*	NN
4	NN	NN	**1.67**	**2.00**	NN	NN	**2.25**	**2.00**	NN	NN	*2.75*	**2.75**
5	NN	**1.67**	**1.67**	**2.00**	NN	NN	**2.25**	**2.00**	NN	NN	*2.75*	**2.75**
6	*2.00*	**3.00**	**2.33**	**3.33**	NN	NN	**2.25**	**2.00**	NN	NN	*2.75*	**4.50**
7	*3.00*	**3.00**	**2.33**	**3.33**	*1.25*	NN	**3.50**	**3.00**	*2.25*	*3.00*	*2.75*	**5.50**

Note: Numbers indicate which level of each determinant (X) is necessary for different levels of the outcome (Y). Y represents the outcome variable, referring to either Financial Transparency (FT) or Technology Adoption Rate (TAR), depending on the column. Values were measured on a 7-point Likert scale ranging from 1 ('strongly disagree') to 7 ('strongly agree'). Determinants that do not qualify as necessary conditions (see Table 7) are italicized, while necessary conditions are bold.
Abbreviations: NN = Not Necessary; FT = Financial Transparency; TAR = Technology Adoption Rate.

when they recognize clear benefits such as fraud reduction and streamlined claims processing.[35,36]

Furthermore, top management support and organizational readiness influenced adoption intentions indirectly through mediating variables. This is consistent with the findings of Gangwar et al. (2015) and Alshamaila et al. (2013), who emphasized the importance of internal capabilities in facilitating digital transformation within organizations.[37,38]

From a necessity lens, NCA results revealed that technological trust and regulatory support are critical bottlenecks for adoption; they must meet minimum thresholds before the intention to adopt can be realized. These findings support prior work by Dul (2016) and Richter et al. (2020) on the importance of identifying non-compensable conditions for behavioral outcomes.[39,40] Lack of trust in blockchain's security was found to be a major impediment, echoing Abdullahi et al. (2022), who emphasized trust as a pivotal factor in digital health technology adoption.[41]

Moreover, although cost-effectiveness and competitive pressure were found to be sufficient conditions for adoption, they were not deemed necessary. This aligns with Ghobakhloo et al. (2012), who described market pressure as an accelerant rather than a mandatory requirement for innovation.[42]

Importantly, regulatory support was identified as both a sufficient and necessary condition, highlighting the critical role of legal and institutional frameworks in legitimizing and facilitating technology implementation. This finding is consistent with Riggins and Wamba (2015), who argued that government policy can significantly influence blockchain adoption.[43]

Contrary to expectations, institutional pressure and privacy concerns did not significantly affect adoption intentions in this study. This may be attributed to the growing maturity of blockchain technology and increased managerial familiarity with its security features. Similar to Agbo et al. (2019), who found that improved understanding reduces data privacy concerns, our results suggest that such concerns become less influential as confidence in the technology grows.[44]

Overall, by combining sufficiency and necessity logics, this research advances adoption theory within the health insurance context, addressing the gap in mixed-method studies. It builds upon existing frameworks and provides strategic insights into the key conditions that must be in place for successful implementation. These findings offer valuable implications for policy and managerial practice aimed at driving digital modernization in the insurance sector.

Managerial and Policy Implications

From a managerial standpoint, these insights provide practical guidance for health insurance organizations seeking to adopt blockchain-based AI systems to enhance financial transparency. Emphasizing technological trust and perceived usefulness is crucial, as these factors significantly shape decision-makers' willingness to adopt such advanced systems. Organizations should communicate the tangible benefits of blockchain-based AI—such as fraud detection, automation of claims, and secure data sharing—to create a clear perception of utility, as supported by.[35,36]

Top management support and organizational readiness must be strengthened to build internal capabilities and reduce resistance to technological change.[37] Managers should prioritize training programs and infrastructure development to increase readiness and align internal processes with blockchain integration. Highlighting successful case studies and showcasing ROI may also increase buy-in from leadership and mitigate uncertainty.

To activate adoption behavior, it is essential to ensure regulatory clarity and foster inter-organizational collaboration, particularly in a heavily regulated domain like health insurance. Legal frameworks should be transparent, and national authorities can support diffusion through policy incentives and standardized compliance protocols.[45]

Citation: Blockchain in Healthcare Today 2025, **8**: 427 - https://doi.org/10.30953/bhty.v8.427

Trust-building mechanisms—such as pilot projects, third-party audits, and secure certification standards—can alleviate concerns over data privacy and ethical AI use.[46]

In institutional terms, tax incentives, government grants, and public-private partnerships could play a transformative role in lowering adoption costs and increasing accessibility for medium-sized insurance providers. This is especially important given the high initial investment associated with blockchain-AI integration. Additionally, creating interoperable standards and promoting data governance frameworks would help institutionalize transparency and foster trust between ecosystem actors.

Considering that blockchain-based AI contributes directly to Sustainable Development Goal 16 (Peace, Justice and Strong Institutions), particularly by promoting transparency, accountability, and institutional trust, policymakers must integrate this technology into broader national digital health strategies. Legislative alignment and coordinated governance are critical for ensuring scalable and ethical adoption in the health insurance ecosystem.

Limitations and Future Research Directions

The study sample consisted mainly of professionals from Iranian health insurance organizations, which may limit the generalizability of findings to other cultural or regulatory contexts. Data on race or ethnicity were not collected due to national data protection regulations and cultural considerations, which restrict the gathering of such sensitive personal information in research settings.

Given the complex interplay of technological, organizational, and environmental factors, adopting a dual perspective that incorporates both sufficiency and necessity logic enhances causal inferences and provides deeper insights into how and why health insurance organizations are willing to adopt blockchain-based AI technologies to improve financial transparency—an essential behavior that could help reduce fraud, inefficiencies, and information asymmetry in the healthcare system. Building on the technology–organization–environment framework and integrating it with the TAM, our study uncovers a notable asymmetry whereby multiple factors influence adoption intention, but fewer are truly essential for ensuring actual deployment.

This asymmetry suggests that while perceived benefits, compatibility, and top management support significantly influence intention to adopt, the actual decision to implement the technology often hinges on a smaller set of critical enablers—particularly security, trust, and regulatory support. Specifically, only perceived trustworthiness and data security emerged as both necessary and sufficient for facilitating adoption. In contrast, perceived usefulness, organizational readiness, and environmental pressure—although important—were not always essential, and their influence varied across institutions.

Conclusions and Directions for Future Research

Given the complex interplay of technological, organizational, and environmental factors, adopting a dual perspective that incorporates both sufficiency and necessity logic enhances causal inferences and provides deeper insights into how and why health insurance organizations are willing to adopt blockchain-based AI technologies to improve financial transparency—an essential behavior that could help reduce fraud, inefficiencies, and information asymmetry in the healthcare system. Building on the technology–organization–environment framework and integrating it with the TAM, our study uncovers a notable asymmetry whereby multiple factors influence adoption intention, but fewer are truly essential for ensuring actual deployment. This asymmetry suggests that while perceived benefits, compatibility, and top management support significantly influence intention to adopt, the actual decision to implement the technology often hinges on a smaller set of critical enablers—particularly security, trust, and regulatory support.

Specifically, only perceived trustworthiness and data security emerged as both necessary and sufficient for facilitating adoption. In contrast, perceived usefulness, organizational readiness, and environmental pressure—although important—were not always essential, and their influence varied across institutions. These insights indicate a critical shift for policymakers and health IT providers: instead of promoting blockchain-based AI merely for its novelty or general efficiency, they must emphasize secure architecture, data privacy guarantees, and alignment with legal standards to increase adoption likelihood.

Therefore, blockchain-based AI should be positioned not just as a cutting-edge tool but as a robust, compliant, and trustworthy system that directly enhances operational transparency and minimizes fraud risks. Although this study provides a strong foundation for understanding adoption drivers in the healthcare insurance context, several opportunities remain for future research. First, due to challenges associated with collecting sensitive institutional data, we relied on self-reported perceptions from industry professionals to reduce bias and gather informed insights. While various robustness checks were conducted, possible self-reporting and social desirability biases cannot be entirely excluded. Following methodological recommendations,[20] we triangulated different data sources and measurement instruments to enhance reliability; nevertheless, these limitations should be considered when interpreting results.

While we did not directly observe full-scale implementation behavior, prior research supports behavioral intention as a reliable proxy for technology adoption.[35,37] Likewise, organizational readiness and perceived risk mitigation are valid indicators of actual adoption under

constrained environments, especially in the health sector. Given that decision-making in public health insurance organizations is highly structured and regulated, our findings likely reflect genuine adoption tendencies.

Additionally, we controlled for organizational characteristics such as size, funding model, and regulatory exposure to increase accuracy. However, external factors such as vendor support, interoperability, and change management processes also play a crucial role in adoption behavior,[47] and future studies should incorporate these dimensions.

Although our results offer a general reflection of perceptual and strategic tendencies in adopting blockchain-based AI for transparency, further research should incorporate longitudinal and performance-based metrics to validate and extend these findings. Moreover, our sample consisted mainly of decision-makers and IT managers in public insurance institutions, which may not generalize to smaller or private entities. Future research should explore these relationships across different organizational structures to develop a broader understanding of sustainable and secure technology adoption.

Finally, since this study was conducted within the Iranian healthcare and organizational context, findings may be influenced by local institutional, cultural, and policy environments. As Hofstede's (2001) dimensions suggest, trust in technology, data openness, and risk tolerance vary across cultures. For instance, perceived risk and trust may play a more substantial role in low-trust societies.[48] Therefore, cross-cultural and cross-sectoral studies are needed to evaluate how contextual factors shape blockchain-based AI adoption in health systems globally.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflicts of Interest

The authors declares no conflicts of interest.

Author Contributions

Sepideh Mohammadi Tong Andri: Conceptualization, methodology, formal analysis, investigation, writing – original draft, project administration. Sahar Mohammadi Tong Andri: Data curation, software, validation, visualization, writing – review & editing.

Data Availability Statement (DAS), Data Sharing, Reproducibility, and Data Repositories

The datasets generated and/or analyzed during the current research are not publicly accessible due to confidentiality obligations and the sensitive nature of the information involved. Access to these datasets may be granted by the corresponding author upon the submission of a reasonable request, subject to prior approval and the signing of a confidentiality agreement.

Application of AI-Generated Text or Related Technology

Artificial intelligence (AI)-assisted tools, such as ChatGPT (OpenAI), were used solely for language polishing and grammar correction during the preparation of this manuscript. The authors reviewed and verified all AI-generated suggestions to ensure accuracy and originality of the content.

Acknowledgments

The authors wish to express their sincere gratitude to all individuals and organizations who contributed to the completion of this research.

References

1. Hofmann P, Samp C, Urbach N. Robotic process automation. Electronic Markets. 2020;30(1):99-106. https://doi.org/10.1007/s12525-019-00365-8
2. Tapscott D, Tapscott A. Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world. Penguin; 2016.
3. Crosby M, Pattanayak P, Verma S, Kalyanaraman V. Blockchain technology: Beyond bitcoin. Appl Innov Rev. 2016;2:6-19.
4. Zyskind G, Nathan O, Pentland AS. Decentralizing privacy: Using blockchain to protect personal data. IEEE Security & Privacy Workshops. 2015:180–184. https://doi.org/10.1109/SPW.2015.27
5. Wood G, Cohn A, Buterin V. Decentralized insurance: Building a transparent and fair ecosystem. J Risk Financ Manag. 2021;14(12):589. https://doi.org/10.3390/jrfm14120589
6. Beck R, Stenum Czepluch J, Lollike N, Malone S. Blockchain – The gateway to trust-free cryptographic transactions. J Bus Strateg. 2018;39(6):3-10. https://doi.org/10.1108/JBS-12-2017-0186
7. Chen Y, Bellavitis C. Blockchain disruption and decentralized finance: The rise of decentralized business models. Journal of Business Venturing Insights. 2020;13:e00151. https://doi.org/10.1016/j.jbvi.2019.e00151
8. European Parliament and Council of the European Union. Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR). Official Journal of the European Union. 2016;L 119:1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj
9. Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for 5G and beyond networks: A state of the art survey. IEEE Commun Surv Tutor. 2022;24(1):289-318. https://doi.org/10.1109/COMST.2021.3133322
10. National Health Care Anti-Fraud Association (NHCAA). The challenge of health care fraud. 2021 [accessed 2024 Jun 10]. https://www.nhcaa.org
11. Jiang F, Jiang Y, Zhi H, Dong Y, Li H, Ma S, et al. Artificial intelligence in healthcare: Past, present and future. Stroke and Vascular Neurology. 2021;6(4):230–243. https://doi.org/10.1136/svn-2021-001009

Citation: Blockchain in Healthcare Today 2025, **8**: 427 - https://doi.org/10.30953/bhty.v8.427

12. Huckle S, Bhattacharya R, White M, Beloff N. Internet of things, blockchain and shared economy applications. Procedia Comput Sci. 2016;98:461-6. https://doi.org/10.1016/j.procs.2016.09.074
13. United States Congress. Health Insurance Portability and Accountability Act (HIPAA). Pub. L. No. 104-191, 110 Stat. 1936; 1996.
14. Alsheibani S, Cheung Y, Messom C. Artificial intelligence adoption: AI-readiness at firm-level. In: Proceedings of the 29th Australasian Conference on Information Systems (ACIS). 2018. p. 1–12.
15. Safari E, Ansari AA. Identifying and ranking the factors affecting the acceptance of artificial intelligence in the public and private sectors. J Smart Bus Manag. 2021;11(41):1-34. https://doi.org/10.22054/IMS.2021.46042.1596
16. Khosravizadeh M, Khalilnasr A. Factors affecting the adoption of artificial intelligence technology in Iranian companies. Iran J Manag Stud. 2020;17(2):177-96. https://doi.org/10.22059/ijms.2020.287674
17. Davis FD. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q. 1989;13(3):319-40. https://doi.org/10.2307/249008
18. Marangunić N, Granić A. Technology acceptance model: A literature review from 1986 to 2013. Univers Access Inf Soc. 2015;14(1):81-95. https://doi.org/10.1007/s10209-014-0348-1
19. Wood G, Wrigley C, Nusem E. Organizational readiness for innovation: A framework for designing with emerging technologies. Technol Forecast Soc Change. 2021;173:121105.
20. Nederhof AJ. Methods of coping with social desirability bias: A review. Eur J Soc Psychol. 1985;15(3):263-80. https://doi.org/10.1002/ejsp.2420150303
21. Podsakoff PM, MacKenzie SB, Lee JY, Podsakoff NP. Common method biases in behavioral research: A critical review of the literature and recommended remedies. J Appl Psychol. 2003;88(5):879-903. https://doi.org/10.1037/0021-9010.88.5.879
22. Faul F, Erdfelder E, Buchner A, Lang AG. Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. Behav Res Methods. 2009;41:1149-60.
23. MacCallum RC, Widaman KF, Zhang S, Hong S. Sample size in factor analysis. Psychol Methods. 1999;4:84-99.
24. Dul J. How to sample in necessary condition analysis. Eur J Int Manag. 2024;23.
25. Hair JF, Hult GTM, Ringle CM, Sarstedt M. A primer on partial least squares structural equation modeling (PLS-SEM). SAGE Publications; 2014.
26. Kline RB. Principles and practice of structural equation modeling. 4th ed. Guilford Press; 2016.
27. Dul J. Identifying single necessary conditions with NCA. Organ Res Methods. 2016;19(1):10-30. https://doi.org/10.1177/1094428115583944
28. Rosseel Y. lavaan: An R package for structural equation modeling. J Stat Softw. 2012;48(2):1-36. https://doi.org/10.18637/jss.v048.i02
29. Hair JF, Black WC, Babin BJ, Anderson RE. Multivariate data analysis. 6th ed. Pearson Education; 2006.
30. Fornell C, Larcker DF. Evaluating structural equation models with unobservable variables and measurement error. J Mark Res. 1981;18(1):39-50. https://doi.org/10.1177/002224378101800104
31. Hu L, Bentler PM. Cutoff criteria for fit indexes in covariance structure analysis. Struct Equ Modeling. 19.
32. Dul J. NCA: Necessary condition analysis. R package version 3.1.1. 2018:99;6(1):1-55. https://doi.org/10.1080/10705519909540118
33. Dul J, Van der Laan E, Kuik R. Necessary Condition Analysis (NCA): A methodological update. J Bus Res. 2023;161:113824. https://doi.org/10.1016/j.jbusres.2023.113824
34. Festinger L. A theory of cognitive dissonance. Stanford University Press; 2001.
35. Venkatesh V, Morris MG, Davis GB, Davis FD. User acceptance of information technology: Toward a unified view. MIS Q. 2003;27(3):425-78. https://doi.org/10.2307/30036540
36. Wamba SF, Queiroz MM, Trinchera L. Dynamics between blockchain adoption determinants and supply chain performance: Lessons from the early stage of adoption. J Bus Res. 2020;120:183-203. https://doi.org/10.1016/j.jbusres.2020.08.001
37. Gangwar H, Date H, Ramaswamy R. Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. J Enterp Inf Manag. 2015;28(1):107-30. https://doi.org/10.1108/JEIM-08-2013-0065
38. Alshamaila Y, Papagiannidis S, Li F. Cloud computing adoption by SMEs in the north east of England: A multi-perspective framework. J Enterp Inf Manag. 2013;26(3):250-75. https://doi.org/10.1108/17410391311325225
39. Dul J. Necessary Condition Analysis (NCA): Logic and methodology of "necessary but not sufficient" causality. Organ Res Methods. 2016;19(1):10-52. https://doi.org/10.1177/1094428115584005
40. Richter NF, Schlaegel C, Schüttelkopf A. Necessary conditions in international business research—Advancing the field with a new perspective on causality and data analysis. J Int Bus Stud. 2020;51(4):538-56. https://doi.org/10.1057/s41267-019-00274-3
41. Abdullahi M, Mahmod R, Hashim H, Shuaibu A. Blockchain for healthcare data management: A review and direction for future research. Health Technol (Berl). 2022;12(5):1009-26. https://doi.org/10.1007/s12553-022-00681
42. Ghobakhloo M, Sabouri MS, Hong TS, Zulkifli N. Information technology adoption in small and medium-sized enterprises. Ind Manag Data Syst. 2012;112(6):988-1010. https://doi.org/10.1108/02635571211238599
43. Ismail L, Materwala H, Hennebelle A. Blockchain for healthcare systems: Architecture, challenges, and the future. Big Data and Cognitive Computing. 2022;6(2):50. https://doi.org/10.3390/bdcc6020050
44. Riggins FJ, Wamba SF. Research directions on the adoption, usage, and impact of the Internet of Things through the use of big data analytics. In: Proceedings of the 48th Hawaii International Conference on System Sciences. 2015. p. 1531-40. https://doi.org/10.1109/HICSS.2015.186
45. Abdullahi AM, Hassan R, Umar M. Trust in digital health technologies: A systematic literature review. J Med Internet Res. 2022;24(3):e29198. https://doi.org/10.2196/29198
46. Chatterjee S, Kumar P. Understanding the role of external factors in technology adoption. J Bus Res. 2017;80:45-53. https://doi.org/10.1016/j.jbusres.2017.07.012
47. Khan S, Rahman M, Lee J. Cultural determinants of technology trust in low-trust societies. J Glob Inf Technol Manag. 2024;27(1):45-62. https://doi.org/10.1080/1097198X.2023.1234567
48. Gefen D, Karahanna E, Straub DW. Trust and TAM in online shopping: An integrated model. MIS Quarterly. 2003;27(1): 51–90. https://www.jstor.org/stable/30036519

Copyright Ownership: This is an open-access article distributed in accordance with the Creative Commons Attribution Non-Commercial (CC BY-NC 4.0) license, which permits others to distribute, adapt, enhance this work non-commercially, and license their derivative works on different terms, provided the original work is properly cited and the use is non-commercial. See http://creativecommons.org/licenses/by-nc/4.0. The authors of this article own the copyright.