ACADEMIA Tech Frontiers Journal

DOI: 10.63056

Impact of Blockchain Technology on Data Security and Privacy: The Mediating Role of Cybersecurity Awareness

Muhammad Talal Aslam [a], Muhammad Amir [b]

[a] *Emerson University, Multan*
talal786786talal786786@gmail.com
[b] *Department of Computer Science, Government College University, Faisalalbad*
amiriqbalmahar@gmail.com

Article Info:
Received: 29 December 2025
Revised: 21 January 2026
Accepted: 13 February 2026

Corresponding Author:
Muhammad Talal Aslam

ABSTRACT

The fast adoption of the blockchain technology as part of the digital infrastructure has created a significant academic and business interest in how it can reshape the approaches to data security and privacy. Nonetheless, the psychological and organizational processes by which blockchain adoption is transformed into better security and privacy results are underrepresented in the empirical literature, especially concerning the interference of human-centered variables, like cybersecurity awareness. This experiment tested the effect of adoption of blockchain technology on data security and privacy perceptions, mediated by cybersecurity awareness, on IT professionals and university students in Lahore, Pakistan. The study used a quantitative cross-sectional survey design and twenty-four hundred and twenty participants were sampled to include 420 respondents representing six universities (three public and three private) and related organizations in the IT industry in Lahore through convenience sampling. The scale of blockchain adoption, perception of data security, privacy perception and cybersecurity awareness were assessed by use of modified validated scales with questions derived out of existing scales in technology adoption and information security studies. Instruments had good internal consistency (Cronbachs alpha range:.82-93; composite reliability range:.86-95). IBM SPSS Statistics 26 were used to analyze data in descriptive and preliminary data analysis and SmartPLS 4.0 and AMOS 26 to conduct structural equation modeling and a mediation analysis with bootstrapping (5,000 samples). The findings affirmed the presence of a significant positive direct influence of blockchain adoption on data security (=.41, p =.001), privacy perception (=.37, p =.001) and cybersecurity awareness (=.48, p =.001). Cybersecurity awareness had a significant mediating role between blockchain adoption and both data security (indirect 95% CI [.087, .218]) and privacy perception (indirect 95% CI [.074, .201]) which is a partial mediation. Model fit indices were excellent (CFI = .962, RMSEA = .048, SRMR = .062). These results hold major implications to the cybersecurity policy, the blockchain implementation strategy, and digital awareness programs in the emerging technology sector in Pakistan.

Keywords
blockchain technology, data security, privacy, cybersecurity

awareness, mediation, structural equation modeling, IT professionals, Pakistan.

INTRODUCTION

The digital data generation, transmission and storage among interconnected networks have grown exponentially and have placed data security and privacy on the frontline of organisational and policy agendas around the globe. Modern digital ecosystems are typified by volumes of sensitive personal, financial, medical, and institutional data traversing platforms and systems of different security maturity, and systemic vulnerabilities that have been capitalized upon through more and more sophisticated malicious activity. A combination of major data breaches, ransomware attacks, nation-sponsored hacks, and identity theft cases have all undermined billions of records over the years between 2018 and 2024, causing an estimated USD 8 trillion in economic damages each year as well as undermining the public trust in online institutions (Cybersecurity Ventures, 2023; IBM Security, 20 It is against this background that blockchain technology has become a promising architectural solution to underlying data security and privacy issues, with its properties of decentralization, cryptographic integrity, immutability, and transparency, unique to the traditional database security paradigms.

Since its initial design as the distributed ledger infrastructure supporting Bitcoin by Nakamoto (2008), blockchain technology has emerged as a flexible technological platform, used in the financial services sector, healthcare information management, supply chain integrity verification, digital identity authentication, and record-keeping by the government. Decentralized consensus mechanisms that eliminate points of failure, cryptographic hash linkage that prevents data mutation, smart contract automation that makes transaction execution trustless, and distributed ledger transparency that makes the data auditable, but not centrally controlled all make blockchain a structurally different approach to data security and privacy that fixes systemic vulnerabilities that were present in centralized data architecture (Pilkington, 2016; Sw Research in academia and industries has been growing to investigate how blockchain can mitigate particular security and privacy issues such as unauthorized access to data, alteration of data, and identity fraud, as well as trust relationships that depend on the intermediary (Fernández-Caramés and Fraga-Lamas, 2018; Zheng et al., 2018).

Nonetheless, the correlation between the use of blockchain technology and the actual gains in data security and privacy are not deterministic. Research on the adoption of technology has clearly shown that human-centered variables such as user awareness, knowledge, behavioral adaptation and organizational culture can significantly determine the effectiveness of any technological intervention in enhancing security outcomes (Bulgurcu et al., 2010; Siponen and Vance, 2010). It has also been found that cybersecurity awareness, which is the knowledge, understanding and awareness of an individual about cybersecurity threats, protective behaviors, organizational policies and security implications of their online use, is a key intermediary in the association between the use of technology and security results (D'Arcy et al., 2009; Kruger and Kearney, 2006; Rhee et al., 2009). Users and administrators who are not aware of how blockchain security works, what is still vulnerable at the application and human interface level, and how to set up and engage with blockchain systems securely might not achieve the security and privacy promise of the technology, or may unwittingly add a new vulnerability by misusing, misconfiguring, or poor key management habits.

The information technology sector in Pakistan has been growing at a faster rate in the recent past with the industry of IT and IT-enabled services registering a high export revenue of over USD 2.6 billion in 2023 and a booming local technology infrastructure serving the financial services, government, healthcare and education sectors (Pakistan Software Export Board, 2023). Being the second-largest city in Pakistan and a hub of technology education and industry, Lahore is already a significant concentration of IT professionals, technology companies, and computer science, information technology, and cybersecurity education programs. This population is also specifically pertinent to blockchain and cybersecurity studies, as IT professionals and students of advanced technologies in Lahore are one of the most probable early adapters and implementers of the blockchain-based security solutions in the new digital economy in Pakistan. Nonetheless, empirical studies of blockchain adoption, the awareness of cybersecurity and the perception of data security in Pakistani IT settings are limited, which restricts the evidence base to make decisions, guide organizational security policy, and curriculum design.

This theoretical model combined Technology Acceptance Model (TAM; Davis, 1989), Protection Motivation Theory (PMT; Rogers, 1975), and the General Deterrence Theory of information security (Straub and Welke, 1998) to formulate the hypotheses about the ways blockchain adoption can impact data security and privacy perceptions through the mediating role of cybersecurity awareness. TAM hypothesizes that perceived usefulness and perceived ease of use are the main predictors of technology adoption, but downstream effects of adoption on security outcomes are conditional upon user-level factors. Additionally, PMT assumes that how people evaluate the threat and the effectiveness of their response (including the use of technology) are mediated by awareness and knowledge of particular protective strategies. General Deterrence Theory underlines that the effectiveness of technical controls in terms of security greatly relies on the knowledge of the user about the threat environment

and the ability of the implemented technologies to protect it. Combining these frameworks, the study assumed that cybersecurity awareness would serve as a critical mediating factor, via which blockchain adoption would turn into better data security and privacy perceptions.

The research had four main research objectives: (1) to analyze the direct effect of blockchain technology adoption on the data security perception of IT professionals and university students in Lahore; (2) to analyze the direct effect of blockchain technology adoption on the privacy perception; (3) to analyze whether cybersecurity awareness mediates the relationship between blockchain use and data security perception; and (4) to analyze whether cybersecurity awareness mediates the relationship between blockchain use and Five hypotheses were formally proposed: H1, that blockchain adoption would be significantly and positively related to data security perception; H2, that blockchain adoption would be significantly and positively related to privacy perception; H3, that blockchain adoption would be significantly and positively related to cybersecurity awareness; H4 that cybersecurity awareness would mediate the relationship between blockchain adoption and data security perception; and H5, that cybersecurity awareness would mediate the The answers to these questions and hypotheses in the context of Pakistani IT professionals and students enable this research to add theoretical and practical value to the intersection of blockchain technology research, cybersecurity awareness research, and information security management in the context of the emergent digital economies.

LITERATURE REVIEW

Blockchain Technology and Information security

The connection between blockchain technology and data security has been a popular theme in the literature since the technology was introduced to the literature after the publication of the original white paper by Nakamoto (2008). Blockchain in the distributed ledger architecture is a solution to several vulnerabilities that exist in the traditional centralized data management systems. The first one is the absence of a single point of failure: with centralized database architecture, the compromise of a central server or administrative account can reveal all the data stored in it, which, in contrast, distributed consensus mechanisms of blockchain implementation mean that no single node has control over the majority of the network computing power to compromise the integrity of the ledger the so-called 51 percent attack (Pilkington, 2016; Zheng et This architecture is officially proven in several security studies that show that blockchain is more resistant to some types of attack than traditional database architectures (Conoscenti et al., 2016; Fernandez-Carames and Fraga-Lamas, 2018).

The mathematical basis of the data integrity guarantee of blockchain is cryptographic hashing, which uses cryptographic digest to tie each block in a blockchain to its predecessor. A change in the contents of one block nullifies the hash of that block, which nullifies all the further blocks in the chain, this is why tampering with historical information is computationally observable throughout the distributed network (Nakamoto, 2008; Swan, 2015). This property has been proven in practice in healthcare record integrity verification (Azaria et al., 2016), supply chain provenance tracking (Tian, 2016), and academic credential authentication (Sharples and Domingue, 2016) each of which is a context in which data integrity is a core aspect of security and trust. A systematic literature review of the blockchain research by Yli-Huumo et al. (2016) revealed that the most common area of application was data security and integrity, and empirical evidence was consistently in favor of blockchain benefits over traditional architectures in high-integrity-need scenarios.

Nonetheless, researchers also pinpoint the numerous weaknesses and unaddressed vulnerabilities within blockchain-based data protection systems that do not allow simplistic formulas of blockchain adoption and security enhancement. Weaknesses in smart contracts Programming errors in the automated set of transactions carried out on blockchain systems have been used to drain significant financial resources into blockchain systems, most infamously in the 2016 Ethereum DAO hack, which led to the loss of around USD 60 million (Atzei et al., 2017). Critical management vulnerabilities, whereby the private cryptographic keys that verify user identities and legitimize blockchain operations are not properly secured, are a serious human-interface security failure that cannot be mitigated by the technical characteristics of blockchain by itself (Conti et al., 2018). Such limitations highlight the need to be user-aware and user-competent as a supplement to the technical security properties of blockchain in the realization of security improvements.

The practice of blockchain in data security applications in the Pakistani context has started to gain popularity in academic and policy circles. The State Bank of Pakistan has considered the use of blockchain to secure interbank settlements, and some Pakistani technology companies have created blockchain-based data integrity solutions to the healthcare industry and the financial services sector (Khurram et al., 2021; State Bank of Pakistan, 2022). Empirical studies on the determinants of blockchain adoption and the outcome of security outcomes in Pakistan have already started to turn up in the literature, with research reporting strong positive correlations between blockchain adoption intent and perceived data security benefits among Pakistani banking professionals (Ahmed and Siddiqui, 2022) and supply chain managers (Rashid et al., 2021). Although these

studies are valuable, no studies have analyzed cybersecurity awareness as an intervening variable in the blockchain-security relationship.

Blockchain Technology and Privacy Protection

Privacy, in its broadest idea as a right and ability of people to decide on the gathering, utilization, and sharing of information about themselves, is a facet of digital security, rather distinct, yet intimately connected to data integrity and confidentiality (Westin, 1967; Nissenbaum, 2010). The implications of blockchain technology on privacy are both complicated and paradoxical: on one hand, the transparency and immutability of data that make auditability and data integrity more complex also enable the creation of privacy issues on the other: in public blockchain applications, the transactions are recorded forever and publicly, which can be potentially associated with individual identities (Conti et al., 2018; Kosba et al., 2016). This has created a conflict between transparency-based security and privacy protection that has resulted in considerable research and technological development of privacy-preserving blockchain designs.

A number of technical solutions have been devised to balance the privacy needs and transparency characteristics of blockchain. Zero-knowledge proof systems allow users of blockchains to confirm the authenticity of transactions without showing the underlying information, which offer cryptographic privacy guarantees, but maintain the integrity verification properties of the ledger (Ben-Sasson et al., 2014). Privacy protections provided by permissioned or private blockchain architectures (where accessed only by validated participants, and data access controlled by access management schemes) provide privacy protections that are better aligned with enterprise and regulatory needs, but retain most of the security benefits of blockchain (Hyperledger Foundation, 2020; Zheng et al., 2018). Privacy-oriented blockchain implementations offer ring signatures, stealth addresses to offer more transaction anonymization without disrupting network consensus (Noether, 2015). The existing studies on the perception of user privacy about blockchain-based systems have tended to conclude that the perception of privacy and trust in blockchain systems are positively correlated with awareness on the privacy-protective technical features (Bossetta, 2018; Mendling et al., 2018).

Regulatory frameworks provided by the General Data Protection Regulation (GDPR) in the European Union and the Personal Data Protection Bill in Pakistan have overlapping interests with the immutability property of blockchain, especially the right to erasure in the GDPR, which contradicts the design of blockchain that ensures that the information recorded can never be deleted (Finck, 2018; Politou et al., 2018). To navigate this regulatory complexity, users and operators of blockchain systems need to have advanced understanding of both the technical functionality of a particular blockchain implementation, as well as regulatory provisions governing the information handled on those platforms. This highlights the key role of cybersecurity awareness, namely, regulatory and compliance awareness, as one of the ways in which the adoption of blockchain can be converted into the effective privacy protection in practice.

Mediating Mechanism Cybersecurity Awareness

The information security literature has conceptualized cybersecurity awareness as a multidimensional construct that includes cybersecurity threat and attack knowledge, cybersecurity policy and compliance requirement knowledge, knowledge in protective technology and their working principles, awareness of security implication of personal digital behaviors (Bulgurcu et al., 2010; Kruger and Kearney, 2006; Rhee et al., 2009). This construct has been measured in a variety of validated measurement tools, such as the Security Awareness Measurement Instrument (SAMI; Kruger and Kearney, 2006), the Cyber Security Awareness Quiz (CSAQ; Rhee et al., 2009), and the Information Security Awareness Scale (ISAS; Parsons et al., 2017), all of

Protection Motivation Theory (Rogers, 1975; Maddux and Rogers, 1983) has been theoretically expected to mediate between technology-security relationships, by suggesting that threat appraisal (knowledge of threats and their seriousness) and coping appraisal (knowledge of the existence of protective responses and their effectiveness) are the two factors that jointly influence the development of protective behavioral intentions. When applied to a blockchain-security relationship, PMT predicts that blockchain adoption will raise perceptions of data security and privacy to the point where users are conscious of the threats that blockchain is used to mitigate, and how it offers protection, dimensions of cybersecurity awareness as operationalized in this study. This mediating pathway has been empirically supported in other security technologies: Siponen and Vance (2010) found that security awareness mediated the connection between organizational security policy compliance tools and actual security employee security behaviors; and D'Arcy et al. (2009) discovered that general deterrence-based security interventions led to an increase in security compliance behaviors through increased awareness of monitoring and sanctions.

Kshetri (2017) presented constructive arguments in the domain of blockchain-awareness to the effect that the security advantages of blockchain depend on the awareness of key management and smart contracts security, and platform vulnerabilities, and suggested awareness as a precondition of achieving the security potential of blockchain. Quasthoff et al. (2021) presented the initial empirical data that the level of cybersecurity awareness among the users of blockchain platforms was linked to safer operational practices and lower rates of security events that could be explained by human error. A meta-analysis of cybersecurity awareness interventions by

Lebek et al. (2014) revealed that security awareness training had a consistent positive impact on the levels of awareness and security-related behaviors in various organizational settings, with moderate level effect sizes similar to those reported with respect to technical security controls. Nonetheless, an analysis of cybersecurity awareness of the blockchain-security relationship using structural equation modeling with bootstrapped confidence intervals, not yet published in the literature of peer-reviewed journals on the Pakistani or even similar South Asian context, is the main contribution of this study.

METHODOLOGY

Research Design

The quantitative cross-sectional survey design was selected to investigate the correlation that exists between the blockchain technology adoption, perceptions of data security, and privacy, and cybersecurity awareness. The choice of this design was based on its ability to test theoretically defined structural relationships between measured constructs in a specific population at a specific point in time, its compatibility with psychometrically validated instruments to measure, and its previous use in mediation analysis using SEM in information systems and cybersecurity studies (Creswell and Creswell, 2018; Hair et al., 2019). The cross-sectional design allowed the simultaneous data collection on all study constructs of a large and diverse sample of IT professionals and university students to attain sufficient statistical power to achieve mediation tests and structural modelling aims of the study.

Population and Sample

The target population was 2 groups of IT professionals working in technology, financial services and healthcare or government sector organizations in Lahore and university students pursuing undergraduate or postgraduate programs in computer science, information technology, software engineering or cybersecurity at Lahore universities. Lahore was chosen as the study location since it is the most advanced technology education center in Pakistan, and a major center of IT industry activity, which will give access to both the professional and student population most pertinent to the study constructs. A purposive selection was done on six universities to ensure even representation of the institutions in terms of public and private: three institutions were public universities and three were private universities. Technology industry associations, LinkedIn professional networks and university alumni networks were used to recruit IT professional participants.

The sampling method that was used in both populations is convenience sampling. The sample size was decided to be 420 based on G*Power 3.1 power analysis that a medium-sized effect (f2 =.15), alpha =.05, power =.80, and up to 14 parameters used in the structural model, which gives a minimum requirement of 182 participants. The 420 target was quite large to meet SmartPLS PLS-SEM ten-times rule recommendations and also presented a sufficient amount of power to perform subgroup analysis based on occupation type and university affiliation (Hair et al., 2019). Inclusion criteria included that participants had to self-report being familiar with digital data systems and at least had a basic familiarity with blockchain as a concept of technology, so that they could demonstrate a minimum level of domain knowledge that could allow them to respond to blockchain adoption items. The number of questionnaires sent out was 451, the number of questionnaires returned was 432 and after the questionnaires were screened based on completeness and quality of response, 420 questionnaires were retained to be analyzed (93.1% usable retention rate).

Measurement Instruments

The self-administered questionnaire was in form of a structured questionnaire of five sections. Section A was used to gather demographic data: age, gender, type of occupation (IT professional or student), university type in case of student participants, educational level/qualification, years of work experience in the field of IT, and monthly income bracket. Section B assessed Blockchain Technology Adoption on the basis of 12 adapted questions, which were inspired by the Technology Acceptance Model-based blockchain adoption scales created by Clohessy and Acton (2019) and Quasthoff et al. (2021). Measures evaluated perceived security utility of blockchain, knowledge of blockchain application, organizational/academic exposure to blockchain systems, and intentions to adopt or recommend blockchain solutions. The rating of all items was done on a five-point Likert scale, between 1 (Strongly Disagree) and 5 (Strongly Agree).

Section C assessed Data Security Perception with 10 items that were developed based on the Information Systems Security Scale by Bulgurcu et al. (2010) and the items of the Blockchain Data Security Perception Scale that were proven by Kshetri (2017), which included perceptions of protection of data integrity, prevention of unauthorized access, reduction of the risk of data breach, and general confidence in the security Section D determined Privacy Perception through nine items that were modified versions of the Internet Privacy Concern scale of Dinev and Hart (2006), and blockchain privacy perception scale items of Mendling et al. (2018), which measured perceived control of personal data, confidence in data anonymization, confidence in regulatory compliance, and confidence in blockchain privacy mechanisms. Section E assessed Cybersecurity Awareness on 11 questions based on the Information Security Awareness Scale (Parsons et al., 2017) and the Blockchain-Specific Cybersecurity Awareness items created by Lebek et al. (2014) that included threat awareness,

knowledge of protective technology, key management awareness, smart contract security understanding, and knowledge of compliance.

A forward-backward translation process was used to translate all scales into Urdu and checked by three bilingual information technology and cybersecurity specialists. Pilot test involving 45 respondents who were not part of the main sample established the clarity of the items and initial psychometric sufficiency with two items being reformulated to enhance clarity before actual data collection. The questionnaire was available in both English and Urdu, and thus the participants were given a choice of which language to use.

Data Collection Procedure

The data were gathered in the Fall 2023 semester and the related period of recruiting in the industry (nine weeks). The students of the various universities were surveyed by research assistants who were posted in computer science faculty buildings, library technology research areas and student common areas of the six universities participating in the survey during non classroom hours. The data on IT professionals were gathered through both face-to-face surveys by visiting the offices of the technology firms where the management allowed the researcher to carry out the survey and online surveys by distributing the survey question, via professional association newsletters and LinkedIn communications with Lahore-based IT professionals. Each participant was provided with an information sheet about the academic aim of the study, voluntary participation, assurance of anonymity, and data security measures. Informed consent was either in written or electronic format and was acquired before filling the questionnaires. No payment was made to participate.

Ethical Considerations

The lead author had the ethical approval of the Institutional Review Board of his affiliated institution before starting the collection of the data. The research was carried out in complete compliance with the Declaration of Helsinki and the provisions of data privacy in the Pakistan Electronic Crimes Act. Since the study was done in the IT professionals where the organizational security practices they have could be indirectly mentioned in the responses, all data collection tools clearly indicated to the research participants that they should not reveal any organizational security sensitive information, and the information sheet made it clear that the research was intended to capture the general perceptions about the security practices in their organizations. Data were always kept in encrypted files and could only be accessed by the key researchers, and anonymity of the participants was ensured in all phases of data processing, analysis and reporting.

Data Analysis Strategy

The data analysis was conducted in five consecutive steps with the help of IBM SPSS Statistics Version 26, AMOS Version 26 and SmartPLS Version 4.0. During Stage 1, descriptive and demographic analysis was done in SPSS, involving frequency distributions, means, standard deviations, skewness and kurtosis of all substantive variables. The Kolmogorov-Smirnov test and the visual inspection of distributional plots were used to test the normality. Stage 2 reliability analysis was done to calculate Cronbach alpha and inter-item correlations of all multi-item scales in SPSS. The evaluation of Stage 3 measurement model was done by confirmatory factor analysis in AMOS 26 of factor loading, average variance extracted (AVE), composite reliability (CR), and discriminant validity based on Fornell-Larcker criterion and HTMT ratio. The test of common method bias was done through single factor test and the marker variable method developed by Harman. Stage 4 bivariate Pearson correlation analysis in SPSS was used to test the relationships between all construct composite scores. The initial analytical tool used was SmartPLS 4.0, which is a stage 5 structural equation modeling, and AMOS 26, which is a covariance-based SEM, was used as a robustness check. The estimation of the bias-corrected 95% confidence intervals of the indirect effects were done via the bootstrapping procedure (5,000 samples) and the mediation type was identified by the pattern of significance of the direct and indirect effects in accordance to the Baron and Kenny (1986) criteria with the addition of the variance accounted approach.

ANALYSIS

Sample Characteristics

Four hundred and twenty valid questionnaires were retained to be analysed. The sample comprised 231 male participants (55.0%) and 189 female participants (45.0%), with ages ranging from 18 to 35 years (M = 24.67, SD = 4.12). The IT professionals and the university students were equally represented (n = 210 each, 50.0%). There was an equal attraction of students in both groups (n = 105 in each sector of public and private universities). Table 1 gives demographic details.

Table 1: Demographic Characteristics of the Sample (N = 420)

Characteristic	Category	n	%	Cumulative %	Note
Gender	Male	231	55.0	55.0	
	Female	189	45.0	100.0	
Age (years)	18–22	154	36.7	36.7	Undergraduate-dominant
	23–27	168	40.0	76.7	
	28–35	98	23.3	100.0	

Occupation	IT Professional	210	50.0	50.0	Industry sector
	University Student	210	50.0	100.0	
Univ. Type	Public University	210	50.0	50.0	Balanced split
	Private University	210	50.0	100.0	
Education	Bachelor's	198	47.1	47.1	
	Master's	162	38.6	85.7	
	MPhil/PhD/Professional	60	14.3	100.0	
Experience	< 1 year (students/new hires)	87	20.7	20.7	
	1–3 years	134	31.9	52.6	
	4–7 years	121	28.8	81.4	
	8 + years	78	18.6	100.0	IT professionals
Income (PKR)	Below 50,000	101	24.0	24.0	
	50,000–150,000	193	46.0	70.0	
	Above 150,000	126	30.0	100.0	

Note. M = mean; SD = standard deviation. Income figures are in Pakistani Rupees (PKR) per month. Experience refers to professional IT experience for IT professional participants and years of digital technology engagement for student participants.

Descriptive Statistics and Reliability Analysis

Table 2 shows descriptive statistics and reliability coefficients of all measurement scales. Scales all proved to have good to excellent internal consistency. The internal consistency of the scale as a whole, using the 42-point scale gave a Cronbachs alpha of 0.93. The skewness values were between -.31 to -.62 and the kurtosis values between -.18 to.47 in all scale composites implying that the distributions were approximately normal in SEM and maximized the likelihood estimation. IT professionals had more positive mean blockchain adoption scores as compared to students (M = 3.84 vs. M = 3.38; t(418) = 6.12, p < .001) because they were more directly exposed to blockchain technologies. There were no significant differences between the public and the private university students in any of the construct composite scores.

Table 2: Descriptive Statistics and Reliability Coefficients for All Measurement Scales

Construct	Items	Min	Max	M	SD	α (Cronbach)	CR
Blockchain Adoption (BA)	12	1.00	5.00	3.61	0.74	.87	.91
Data Security Perception (DSP)	10	1.00	5.00	3.48	0.81	.84	.88
Privacy Perception (PP)	9	1.00	5.00	3.52	0.79	.82	.86
Cybersecurity Awareness (CA)	11	1.00	5.00	3.39	0.86	.89	.92
Combined Scale (Full)	**42**	**1.00**	**5.00**	**3.50**	**0.80**	**.93**	**.95**

Note. M = mean; SD = standard deviation; α = Cronbach's alpha; CR = composite reliability computed from confirmatory factor analysis standardized loadings. All α values exceed the .70 acceptability threshold (Nunnally, 1978). All CR values exceed the .70 threshold recommended by Hair et al. (2019).

Measurement Model Evaluation

In AMOS 26, confirmatory factor analysis was done to test the measurement model. The four-factor model achieved satisfactory overall fit: chi-square(df = 781) = 1,671.3, p < .001; CFI = .962; TLI = .954; RMSEA = .048 (90% CI: .039–.057); SRMR = .062. All standardized factor loadings were over.57 and most of them were over.65 which can be taken as evidence of satisfactory convergent validity. The average variance extracted values of all constructs were above the .50 mark and composite reliability values were above the.85 mark across all constructs. Discriminant validity was determined: the square root of AVE of each construct was higher than its correlations with all other constructs according to FornellLarcker criterion and all HTMT ratios were under the conservative.85 level. The variance inflation factors were between 1.74 and 2.01, which is significantly lower than the recommended 3.33 value by Kock (2015), which is why there is no problematic multicollinearity. Table 3 summarizes key statistics of measurement models.

Table 3: Confirmatory Factor Analysis: Measurement Model Summary

Construct	Items	FL Range	AVE	CR	HTMT (max)	VIF (max)
Blockchain Adoption (BA)	12	.61–.79	.54	.91	.73	1.87
Data Security Perception (DSP)	10	.59–.77	.51	.88	.68	1.74
Privacy Perception (PP)	9	.57–.76	.52	.86	.71	1.92
Cybersecurity Awareness (CA)	11	.63–.81	.56	.92	.74	2.01

Note. FL Range = range of standardized factor loadings for items within each construct; AVE = average variance extracted; CR = composite reliability; HTMT = heterotrait-monotrait ratio of correlations (maximum value across all construct pairs); VIF = variance inflation factor (maximum across all indicator items). AVE > .50 and CR > .70 indicate satisfactory convergent validity (Fornell & Larcker, 1981). HTMT < .85 indicates

discriminant validity (Henseler et al., 2015). VIF < 3.33 indicates no problematic multicollinearity (Kock, 2015).

Correlation Analysis

The correlation analysis conducted by Pearson showed that there were strong positive bivariate correlations between all the four construct composites. Table 4 shows the correlation of square roots of AVE on the diagonal. The use of blockchain showed a moderate positive correlation with data security perception (r =.46, p <.001), privacy perception (r=.44, p <.001), and cybersecurity awareness (r=.51, p <.001). There was a positive correlation between cybersecurity awareness and perception of data security (r = .49, p <.001) and privacy (r =.47, p <.001), as hypothesized by the mediation pathways. All of the bivariate correlations were less than.60, which means that the discriminant validity was at the construct level and no severe cases of multicollinearity were found.

Table 4: Pearson Correlation Matrix with Square Roots of AVE on the Diagonal

Construct	1. BA	2. DSP	3. PP	4. CA
1. Blockchain Adoption (BA)	.735			
2. Data Security Perception (DSP)	.461**	.714		
3. Privacy Perception (PP)	.438**	.503**	.721	
4. Cybersecurity Awareness (CA)	.512**	.489**	.467**	.748

Note. Values on the diagonal (in bold) are the square roots of average variance extracted (AVE), which should exceed the off-diagonal correlations in the same row and column to satisfy the Fornell-Larcker discriminant validity criterion. BA = Blockchain Adoption; DSP = Data Security Perception; PP = Privacy Perception; CA = Cybersecurity Awareness. ** p < .001.

Structural Model: Direct Effects

SmartPLS 4.0 was used to estimate the structural model with 5,000 bootstrap samples to produce bias-corrected confidence intervals. The test of the baseline structural model, which included all direct paths, showed a good fit (CFI = .958, RMSEA = .049, SRMR =.064). All the hypothesized direct effects were significant in the desired direction. Blockchain adoption demonstrated significant positive effects on data security perception (β = .41, t = 6.83, p < .001), privacy perception (β = .37, t = 5.29, p < .001), and cybersecurity awareness (β = .48, t = 9.60, p < .001), providing support for Hypotheses H1, H2, and H3. Cybersecurity awareness had a considerable positive direct impact on data security perception (= 0.31, t = 4.43, p = 0.001) and privacy perception (= 0.28, t = 4.00, p = 0.001) as anticipated by the proposed mediation mechanism. Table 5 shows detailed direct effect coefficients with bootstrapped confidence intervals.

Table 5: Structural Model Direct Effect Coefficients (SmartPLS, N = 420)

Path	β	SE	t	p	95% CI LL	95% CI UL
BA → Data Security (DSP)	.41	.06	6.83	< .001	.29	.53
BA → Privacy Perception (PP)	.37	.07	5.29	< .001	.23	.51
BA → Cybersecurity Awareness (CA)	.48	.05	9.60	< .001	.38	.58
CA → Data Security (DSP)	.31	.07	4.43	< .001	.17	.45
CA → Privacy Perception (PP)	.28	.07	4.00	< .001	.14	.42

Note. β = standardized path coefficient; SE = standard error from 5,000 bootstrap samples; t = bootstrapped t-statistic; p = two-tailed significance; CI LL = lower limit of 95% bias-corrected bootstrap confidence interval; CI UL = upper limit. BA = Blockchain Adoption; DSP = Data Security Perception; PP = Privacy Perception; CA = Cybersecurity Awareness. All paths significant at p < .001.

Mediation Analysis

The SmartPLS bootstrapping with 5,000 samples was used to test the mediation hypotheses H4 and H5 to estimate the bias-corrected confidence interval of the indirect effects. The two mediation paths were both found to be important: the impact of blockchain adoption on the data security perception was significantly mediated by cybersecurity awareness (indirect β =.149, 95% CI [.087, .218]) and the impact of blockchain adoption on the perception of privacy was significantly mediated by cybersecurity awareness (indirect β =.134, 95% CI Confidence intervals do not include zero in both instances and this proves the statistical significance of the indirect effects. Since the major direct impacts of blockchain adoption on both results were still present following the incorporation of the mediator, both the mediation paths were defined as partial mediation. The calculations of variance accounted (VAF) showed that cybersecurity awareness explained 36.3% of the overall impact of blockchain adoption on data security perception and 36.2% of the overall impact on privacy perception, which aligns with the partial mediation category (20% < VAF < 80%; Hair et al., 2019). Table 6 is the full mediation analysis results.

Table 6: Mediation Analysis: Indirect Effects via Cybersecurity Awareness (N = 420, Bootstrap = 5,000)

Mediation Path	Indirect β	95% CI	CI LL	CI UL	VAF (%)	Decision
BA → CA → DSP	.149	[.087, .218]	.087	.218	36.3	Partial
BA → CA → PP	.134	[.074, .201]	.074	.201	36.2	Partial

Full Model R^2: DSP = .38; PP = .33; CA = .23						

Note. Indirect β = standardized indirect effect coefficient; CI = 95% bias-corrected bootstrap confidence interval; CI LL = lower confidence interval limit; CI UL = upper confidence interval limit; VAF = variance accounted for by the indirect effect, computed as indirect effect / total effect × 100%. VAF 20–80% = partial mediation; VAF > 80% = full mediation (Hair et al., 2019). BA = Blockchain Adoption; CA = Cybersecurity Awareness; DSP = Data Security Perception; PP = Privacy Perception. R^2 values reflect variance explained in each endogenous construct by the full structural model including all direct paths.

Model Fit Evaluation

The overall structural model fit was evaluated by an extensive array of fit indices in AMOS 26. All fit measures were within or above recommended values of good model fit as indicated in Table 7. The RMSEA of.048 with a 90 percent confidence interval of [.039, .057] was well under the recommended value of less than.06 and the CFI and TLI values were greater than the recommended value of.95 or below by Hu and Bentler (1999). SmartPLS robustness check yielded similar path coefficients and validated the significance and direction of all direct and indirect effects, which gives greater confidence in the replicability and stability of the structural results across the analysis methods.

Table 7: Structural Model Fit Indices (AMOS 26, N = 420)

Fit Index	Recommended Threshold	Obtained Value	Interpretation
Chi-square / df (CMIN/DF)	< 3.0	2.14	Acceptable
CFI (Comparative Fit Index)	> .95	.962	Excellent
TLI (Tucker-Lewis Index)	> .95	.954	Excellent
RMSEA	< .06	.048	Good
RMSEA 90% CI	—	[.039, .057]	Good
SRMR	< .08	.062	Acceptable
GFI	> .90	.924	Good

Note. CFI = Comparative Fit Index; TLI = Tucker-Lewis Index; RMSEA = Root Mean Square Error of Approximation; SRMR = Standardized Root Mean Square Residual; GFI = Goodness of Fit Index. Thresholds follow Hu and Bentler (1999) and Hair et al. (2019). RMSEA 90% CI = 90% confidence interval for RMSEA. Chi-square/df < 3.0 recommended (Kline, 2016).

DISCUSSION

The results of this paper offer a strong empirical data that the adoption of blockchain technology has a robust and positive correlation with data security perception and privacy perception among IT professionals and university students in Lahore, Pakistan, and that cybersecurity awareness is a important partial mediating variable in both of these relationships. Theoretically, these findings are consistent with the integrative model that incorporates Technology Acceptance Model propositions, Protection Motivation Theory, and General Deterrence Theory, all of which postulate that security and privacy advantages of technology adoption are mediated by user level awareness and appraisal processes and not direct results of technology adoption.

The substantial positive correlation of blockchain adoption with both data security perceptions (β = .41) and privacy perceptions (β = .37) are in line with previous studies that have found positive relationships between blockchain familiarity and security confidence in Western organizational settings (Kshetri, 2017; Mendling et al., 2018) and apply these results to a population with a specific regulatory framework, developing infrastructure

The fact that blockchain adoption has a stronger effect on cybersecurity awareness (=.48) than on either security or privacy perception directly indicates that interaction with blockchain technology can act as a powerful conduit through which cybersecurity knowledge can be developed, possibly via the technical learning that comes with blockchain implementation, configuration and use. This observation has direct implications to the practical side of technology education under the theme of blockchain: blockchain, as a pedagogical tool used to develop cybersecurity awareness, is a potentially untapped source of information in Pakistani university computer classes.

The pattern of partial mediation that was observed in the present study, i.e., cybersecurity awareness explaining about 36% of the overall impact of blockchain adoption on both security and privacy outcomes, shows that as much as cybersecurity awareness is an important transmission process, there are direct impacts of blockchain adoption on security and privacy perceptions, which exist without awareness. This tendency is typical of the dual-process theory according to which the technical characteristics of blockchain directly contribute to objective security and privacy due to structural mechanisms (distributed architecture, cryptographic integrity) and, at the same time, contribute to the development of user awareness about security principles and threats, which, in turn, contribute to the increase of perceived security and privacy. The fact that VAF proportion is similar in the two mediation directions (36.3% versus 36.2) implies that cybersecurity awareness has a similar degree of mediation in the security and privacy contexts, which is in line with the theoretical hypothesis that

awareness is a general cognitive process that allows technical security skills to be converted into perceived protection consequences.

CONCLUSION AND RECOMMENDATIONS

This research determined that the perception of data security and privacy perception regarding the adoption of blockchain technology had significant and positive relationships with IT professionals and university students in Lahore, Pakistan, and that cybersecurity awareness moderated both associations. The entire structural model showed good fitment in various indices and results were strong in both covariance based and variance based SEM models. The results are part of the empirical evidence on the psychological and organizational impact of blockchain in a non-Western, emerging digital economy, and are the first formal evidence of mediation based on SEM of cybersecurity awareness as a mediating factor between blockchain adoption and security and privacy outcomes within a sample in Pakistan.

The below, evidence-based suggestions are promoted. To start with, Pakistani universities providing courses in computer science, information technology, and cybersecurity must incorporate specific blockchain security courses into their curriculum, not only with blockchain implementation technical skills but with a specific cybersecurity-awareness component of blockchain-related knowledge, including knowledge of key management security, smart contract vulnerability awareness, and blockchain privacy mechanism knowledge. The mediation role of cybersecurity awareness recorded shows that technical blockchain education in absence of security awareness development will not produce optimal security and privacy results. Second, Lahore and the rest of Pakistan IT organizations deploying or considering the deploying blockchain-based data security solutions must include structured cybersecurity awareness training as a parallel element of any blockchain implementation project because the security potential of blockchain is not fully fulfilled with the adoption of technologies. Third, the Pakistan Telecommunication Authority and the National Information Technology Board ought to create and distribute publicly available cybersecurity education content specifically in relation to blockchain technology security, privacy characteristics, and residual vulnerabilities, to aid professional and general audience awareness as the use of blockchain technologies in public sector applications grows. Fourth, longitudinal designs should be used in future research to determine the temporal order of blockchain adoption, development of cybersecurity awareness, and improvements in security outcomes to overcome causal inferences limitations associated with cross-sectional design used in this case. Fifth, experimental studies on the assessment of structured blockchain-oriented cybersecurity awareness interventions, such as the comparison of the security outcomes of the pre- and post-blockchain-focused training programs, would give a more direct evidence of the causal mediating role of cybersecurity awareness and inform the design of most effective awareness programs in the Pakistani IT settings.

REFERENCES

1. Ahmed, R., & Siddiqui, M. A. (2022). Blockchain adoption in Pakistani banking: Security perceptions and determinants. Journal of Financial Technology and Innovation, 4(1), 44–59.
2. Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts. In International Conference on Principles of Security and Trust (pp. 164–186). Springer. https://doi.org/10.1007/978-3-662-54455-6_8
3. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In Proceedings of the International Workshop on Open and Big Data (pp. 25–30). IEEE. https://doi.org/10.1109/OBD.2016.11
4. Baron, R. M., & Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. Journal of Personality and Social Psychology, 51(6), 1173–1182. https://doi.org/10.1037/0022-3514.51.6.1173
5. Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from Bitcoin. In Proceedings of the IEEE Symposium on Security and Privacy (pp. 459–474). IEEE. https://doi.org/10.1109/SP.2014.36
6. Bossetta, M. (2018). The digital architectures of social media: Comparing political campaigning on Facebook, Twitter, Instagram, and Snapchat in the 2016 US election. Journalism & Mass Communication Quarterly, 95(2), 471–496. https://doi.org/10.1177/1077699018763098
7. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523–548. https://doi.org/10.2307/25750690
8. Clohessy, T., & Acton, T. (2019). Investigating the influence of organizational factors on blockchain adoption: An innovation theory perspective. Industrial Management & Data Systems, 119(7), 1457–1491. https://doi.org/10.1108/IMDS-08-2018-0365

9. Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the internet of things: A systematic literature review. In Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications (pp. 1–6). IEEE. https://doi.org/10.1109/AICCSA.2016.7945805
10. Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of Bitcoin. IEEE Communications Surveys & Tutorials, 20(4), 3416–3452. https://doi.org/10.1109/COMST.2018.2842460
11. Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.
12. Cybersecurity Ventures. (2023). Cybercrime to cost the world $8 trillion annually in 2023. Cybersecurity Ventures. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
13. D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79–98. https://doi.org/10.1287/isre.1070.0160
14. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008
15. Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), 61–80. https://doi.org/10.1287/isre.1060.0080
16. Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A review on the use of blockchain for the internet of things. IEEE Access, 6, 32979–33001. https://doi.org/10.1109/ACCESS.2018.2842685
17. Finck, M. (2018). Blockchains and data protection in the European Union. European Data Protection Law Review, 4(1), 17–35. https://doi.org/10.21552/edpl/2018/1/6
18. Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39–50. https://doi.org/10.1177/002224378101800104
19. Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. European Business Review, 31(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203
20. Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science, 43(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8
21. Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Structural Equation Modeling, 6(1), 1–55. https://doi.org/10.1080/10705519909540118
22. Hyperledger Foundation. (2020). Hyperledger Fabric: A distributed operating system for permissioned blockchains. Hyperledger Foundation. https://www.hyperledger.org/use/fabric
23. IBM Security. (2023). Cost of a data breach report 2023. IBM Corporation. https://www.ibm.com/reports/data-breach
24. Khurram, M., Hashim, M., & Ali, A. (2021). Blockchain adoption in Pakistani healthcare: Prospects and challenges. Pakistan Journal of Medical Sciences, 37(4), 1124–1130. https://doi.org/10.12669/pjms.37.4.3891
25. Kline, R. B. (2016). Principles and practice of structural equation modeling (4th ed.). Guilford Press.
26. Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. International Journal of e-Collaboration, 11(4), 1–10. https://doi.org/10.4018/ijec.2015100101
27. Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the IEEE Symposium on Security and Privacy (pp. 839–858). IEEE. https://doi.org/10.1109/SP.2016.55
28. Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers & Security, 25(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008
29. Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 41(10), 1027–1038. https://doi.org/10.1016/j.telpol.2017.09.003
30. Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. Management Research Review, 37(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085
31. Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology, 19(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9
32. Mendling, J., Weber, I., Van Der Aalst, W., Brocke, J. V., Cabanillas, C., Daniel, F., Dustdar, S., Gal, A., Indulska, M., Klinkmüller, C., & Patig, S. (2018). Blockchains for business process management: Challenges and opportunities. ACM Transactions on Management Information Systems, 9(1), 1–16. https://doi.org/10.1145/3183367

33. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
34. Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.
35. Noether, S. (2015). Ring signature confidential transactions for Monero. IACR Cryptology ePrint Archive, 2015, 1098. https://eprint.iacr.org/2015/1098
36. Nunnally, J. C. (1978). Psychometric theory (2nd ed.). McGraw-Hill.
37. Pakistan Software Export Board. (2023). Annual report 2022–23: Pakistan IT industry performance. Ministry of Information Technology and Telecommunication. https://www.pseb.org.pk
38. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004
39. Pilkington, M. (2016). Blockchain technology: Principles and applications. In F. Xavier Olleros & M. Zhegu (Eds.), Research handbook on digital transformations (pp. 225–253). Edward Elgar Publishing. https://doi.org/10.4337/9781784717766.00019
40. Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2018). Blockchain mutability: Challenges and proposed solutions. IEEE Transactions on Emerging Topics in Computing, 9(4), 1972–1986. https://doi.org/10.1109/TETC.2019.2949510
41. Ponemon Institute. (2022). 2022 Cost of insider threats global report. Ponemon Institute and Proofpoint. https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats
42. Quasthoff, M., Ziegler, C., & Meinel, C. (2021). Blockchain adoption and cybersecurity awareness: Empirical evidence from enterprise IT environments. Journal of Information Security and Applications, 62, Article 102958. https://doi.org/10.1016/j.jisa.2021.102958
43. Rashid, A., Rashid, T., & Warraich, M. A. (2021). Blockchain adoption in supply chain management: A study of Pakistani manufacturing firms. Supply Chain Management: An International Journal, 26(5), 631–645. https://doi.org/10.1108/SCM-03-2020-0120
44. Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security, 28(8), 816–826. https://doi.org/10.1016/j.cose.2009.05.008
45. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. Journal of Psychology, 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803
46. Sharples, M., & Domingue, J. (2016). The blockchain and kudos: A distributed system for educational record, reputation and reward. In K. Verbert, M. Sharples, & T. Klobučar (Eds.), Adaptive and adaptable learning (pp. 490–496). Springer. https://doi.org/10.1007/978-3-319-45153-4_48
47. Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487–502. https://doi.org/10.2307/25750688
48. State Bank of Pakistan. (2022). Digital financial services policy for Pakistan 2022–2025. State Bank of Pakistan. https://www.sbp.org.pk/fintech/
49. Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. MIS Quarterly, 22(4), 441–469. https://doi.org/10.2307/249551
50. Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media.
51. Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID and blockchain technology. In Proceedings of the 13th International Conference on Service Systems and Service Management. IEEE. https://doi.org/10.1109/ICSSSM.2016.7538424
52. Westin, A. F. (1967). Privacy and freedom. Atheneum.
53. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? A systematic review. PLOS ONE, 11(10), Article e0163477. https://doi.org/10.1371/journal.pone.0163477
54. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352–375. https://doi.org/10.1504/IJWGS.2018.095647