DOI: https://doi.org

ComputeX - Journal of Emerging Technology & Applied Science

Journal homepage: https://rjsaonline.org/index.php/ComputeX

Blockchain Security and Financial Transaction Trust: The Mediating Role of Data Integrity and the Moderating Role of Regulatory Compliance

Daniyal Zaheer [1], Dur-E- Adan [2]

[1] Department of computer science, Virtual University, Islamabad, Pakistan

[2] Department of Computer Science, National University of Modern Languages, NUML Islamabad, Pakistan

Email: daniyalzaheer139@gmail.com

ARTICLE INFO

Received:
April 17, 2026
Revised:
May 12, 2026
Accepted:
May 26, 2026
Available Online:
June 07, 2026

Keywords:

blockchain security, financial transaction trust, data integrity, regulatory compliance, PLS-SEM, fintech, banking, mediation, moderation, digital trust.

Corresponding Author:
daniyalzaheer139@gmail.com

ABSTRACT

It's a study on financial transaction trust for banking and fintech players, with the data integrity as mediator and the regulatory compliance as moderator in the relation between these two. The design of the research is aimed at explaining and quantitative research paradigm. For the study they were sampled banking profession, fintech profession, compliance profession and IT security profession and the combined total respondents were 412 subjects with multi-stage purposive sampling method for collecting the data for the study from the subjects. The analysis was done in several steps: First data screening of missing data; outlier, violation of normality; second data by validating measurement model using Confirmatory Factor Analysis (CFA); finally data solving by Partial Least Squares Structural Equation Modeling (PLS-SEM) with 5000 bootstrap resamples in the software of smartPLS 4.0. The Standardized Root Mean Square Residual (SRMR) was used to assess model fit and predictive relevance was assessed using blindfolding model identification (Q2) values. Data integrity and financial transactions trust were partially mediated (indirect effect $\beta = 0.241$, $p < 0.001$) or completely mediated (indirect effect $\beta = 0.312$, $p < 0.001$), respectively, for security of blockchain on financial transactions trust.Data integrity and financial transactions trust were partially mediated (indirect effect $\beta = 0.241$, $p < 0.001$) or completely mediated (indirect effect $\beta = 0.312$, $p < 0.001$), respectively, for security of blockchain on financial transactions trust. The moderation analysis results reaffirm that the impact of blockchain security on magnitude of trust for financial transactions holds when the regulatory compliance frameworks in the financial sector are robust enough (interaction $\beta = 0.187$, $p < 0.01$). The study offers guidance on the adoption way, design of financial regulation and digital trust management for the dynamic fintech industry.

Introduction

Overall, the digitalisation of financial services has given rise to the significant transformation of the structure of trust in financial transactions. The use of decentralized technologies is impacting traditional financial systems by bringing questions to the forefront on questions of trust, assumptions that were foundational to financial exchanges a long time ago. In this suite of technologies, codesvelopment has begun between blockchain, a distributed ledger technology supporting the financial blockchain applications such as cryptocurrencies, smart contracts, and new fintech software, and all participants of the financial industry—including banks, fintech companies and regulators—and blockchain has reached unprecedented status among financial sector academics for its ability to increase the security, transparency and efficiency of financial transactions. It's specifically the fundamental architecture of the blockchain, where the entries have to be immutable, cryptographic hashes have to link the blocks, distributed consensus mechanisms are used, and decentralized validation processes must validate the entries, that make it an inherently trust-relevant technology, with its security properties as key to its value proposition, in financial contexts in particular.

The trust in financial transactions as a multidimensional phenomenon consists of trust in security of transactions, in trustability and accuracy of financial elements and in faith that transactions will take place as planned without disruption, fraud and manipulation. No one invests in a financial system that they don't trust, the World Economic Forum (2020) have said, and trust is a precondition of financial system stability, particularly for traditional banking, payment systems and the new financial system decentralised finance. However, security – cryptographic security of transactions, network security against 51% attacks, smart contract security and node security – is a key technical feature needed to establish this trust on transactions when applying the blockchain in a financial context.

But there is no one-to-one correlation between security of the blockchain and security of the financial transaction. This has been emphasised through several theoretical and empirical arguments regarding the link between the security and hygiene properties of blockchain technology and the level of trust stakeholders place in blockchain. Data integrity is one of the intermediate variables which make sure the information throughout the blockchain about the financial transactions is legitimate, accurate, complete and dependable. Because they ensure data integrity – that transaction records cannot be altered by anyone who isn't supposed to, that all participants have access to the same version of the ledger and have an "auditable trail" of all transactions over the years – blockchain's cryptographic and consensus-based security attributes are beneficial for financial transaction trust. The data integrity secured, then in turn supports the trust of financial transaction for the relevant parties and performs well to ensure the accuracy and reliability of financial transaction records. This data-integrity mediation of the security–trust relationship on the blockchain connects the technical security aspects of blockchains with stakeholder trust while providing a theoretically satisfying and practical account of how this occurs.

The regulation compliance further complicates the relationship. Undoubtedly, compliance is already one of the most tightly-regulated sectors in all economies, and the financial sector is currently seeing an increasingly complex patchwork of anti-money laundering (AML), know your customer (KYC), data compliance (GDPR/PDPA) and even, in some areas, specific regulations for blockchain from a number of jurisdictions such as the Financial Action Task Force (FATF), Securities and Exchange Commission (SEC) of the United States (USA), and the European Union (MiCa regulation). Thus the compliance factor of blockchain influences the security–legitimacy relationship, by giving the blockchain an external institutional engagement: compliance aspect of blockchain's implementations gives the parties and in particular banking customers institutional parties, institutional validation and measurement mechanism, thus establishing an additional layer of trust (security) and accountability, beyond that which it brings by itself due to the blockchain, as a consequence of respecting a regulatory framework. However, in a similar fashion, a Blockchain technologies implementation without or contrary to the regulatory regime can offer technically secure solutions, but at a deeper level, regulatory moderation analysis can identify a loss of institutional confidence in a Blockchain implementation.

This study falls under two theoretic framework. When investigating the factors leading to the adoption of financial technology that impact perceived ease of use and perceived usefulness (PUE) underpinned by perceived security and trust, one can draw on the Technology Acceptance Model (TAM) (Davis 1989). In the blockchain space, security has been the top perceived attribute that impacts intentions to adopt and confidence in the blockchain. Institutional Trust Theory (Zucker, 1986) brings complementing elements to TAM, and co-opts it into the concepts of process trust in technological systems caused by institutional practices such as compliance, or legal and professional requirements for accountability. The amalgamation of these frameworks affords a theoretically significant analysis of how blockchain security brings about trust via data integrity mediation, and how compliance helps moderate trust-building. The study then contributes to the adoption of blockchain research and the fintech literature regarding trust since it builds a theoretically integrated and empirically rigorous test of the relationship between blockchain security and trust and takes into account mediation and moderation effects.

There are four major contributions of the study. It is to provide empirical studies of the massive financial services blockchain industry by testing the mechanism that links data integrity with the security–trust relationship of the blockchain, rather than the prevailing empirical study on blocks chain industry, which centered around a model-based approach.Turning to the empirical study of the condition of use of the blockchain in financial services sector, it is one of the first quantitative studies to examine the security–trust relationship between the two entities, deviating from the previously predominant "direct effects" model which has given the subject of blockchain trust a purely theoretical focus.Turning to the empirical study of the condition of use of the blockchain in this financial services sector it is one of the first quantitative studies to test the data integrity mechanism by observing the security–trust relationship between the two entities, and stops the models and approaches that were to date purely theoretical and thus strongly focussed on the field of "direct effects" in the trusts research on blockchain. Second, it is important to grasp the institutional context of the WEB3 sector in relation to blockchain use, where regulatory compliance is one of the most important moderators of the blockchain security–trust relationship and consequently of the designs of blockchain-friendly regulations that support trust-building blockchain implementation. Third, it was thought to apply methodological robustness taking into account the complexity of the model tested in the present study, the PLS-SEM with bootstrapping and the model fit assessment by SRMR and the predictive relevance by Q^2. The informants in the banking and fintech sector included banking professionals, fintech executives, compliance officers, and IT security specialists and thus constituted an organisationally diverse sample to provide a multi-faceted insight into the voices of stakeholders, but also enhanced the relevance of the study with respect to its application to practice in the area of blockchain under security and trust aspects.

Literature Review

The model was borrowed from the two prevailing models, the first one is the Technology Acceptance Model (TAM) and the second one is the Institutional Trust (IT) Theory. Davis (1989) suggested in his “Technology Acceptance Model” that, through attitudes and behavioral intentions of the users, the usage of IT depends on the perceived usefulness and perceived ease of use. Gefen et al. (2003) modified TAM to fit the financial technology context and added the domain of technology acceptance (trust) so they can examine the moderating role that the concept of trust plays in the relationship between the technology quality and the intention to adopt the technology in the context of ecommerce. Other research studies concerning financial technologies related to TAM, including studies on mobile banking (Luo et al., 2010), Internet banking (Yoon, 2010), and Digital payment systems (Oliveira et al., 2016), generally confirmed that security perceptions were the major determinant in trust, and trust was the major determinant of intention to use. The present study applies this TAM trust continuum as a theoretical basis, to analyze financial transaction trust of blockchain security. Institutional trust theory suggests that there were three types of trust: characteristic trust – relying on personal attributes, historical trust – relying on experience and past events, and institutional trust – relying on formal institutional structures, rules and certificates (Zucker, 1986). The problem of trust is relevant, particularly in cases of blockchain, as it is with regards to regulatory compliance – institutions that can generate trust in financial blockchain-based architectures without relying on a specific financial transaction or on specific individuals.

Since the original Bitcoin paper by Nakamoto et al., 2008, the literature on blockchain has grown significantly in financial service research, covering such topics as payment settlements (Bech & Garratt, 2017), trade finance (Guo & Liang, 2016), know your customer (KYC) verification and security (Sullivan & Burger, 2017), and central bank digital currency (Auer & Böhme, 2020). The value proposition of blockchain in financial applications depends on how well blockchain's security is addressed, with Narayanan et al. (2016) giving a detailed description of the security mechanisms in blockchain such as cryptographic hash functions (SHA-256 and Keccak), digital signatures, Merkle tree structures and a number of distributed consensus algorithms (PPoW, PoS, and Practical Byzantine Fault Tolerance [PBFT]). Financial Use Cases: The three most significant characteristics of blockchain, that are relevant to the security of a financial system, are summarized by Pilkington (2016) – immutability, transparency and decentralization, (which is the root of blockchain), that all mitigate fraud, error and counterparty risk – all the issues that cause distrust in traditional financial systems. However, security of blockchain cannot be taken for granted: In an important 2017 report, Atzei et al., highlighted 46 classes of cryptographic vulnerabilities that were targeted by attacks in the wild against smart contracts; in another report in 2020, Saad et al., systematically listed the different classes of blockchain network attack, including, amongst others, eclipse, routing, Sybil and 51% attacks, being each an attack vector.

In the information systems and financial sense of the word, data integrity is the accuracy, completeness, consistency and reliability of the data throughout its lifecycle from entry to storage, processing to retrieval. Data integrity was formally defined by Wang and Strong (1996), which equated with conceptual notions of data quality by an information system to 4 dimensions—intrinsic quality, contextual quality, representational quality and accessibility quality. Data integrity is critical in financial services too – risk data aggregation and reporting requirements outlined in the BCBS 239 principles are stringent with regards to data integrity for systemically important banks and IFRA and GAAP accounting requirements require data integrity requirements for financial reporting. Blockchain drew a higher level of data integrity assurance than traditional centralized system of database however, as Evans et al (2017) proved, an auditor trail process (building an immutable, timestamped record of all data entries and changes) of blockchain directly supports the data integrity requirement by financial regulators and auditors, as shown by Peters and Panayi (2016).

In fact, there is empirical evidence that data integrity/efficiency is also linked to trust not only of the data, but of the financial transaction in different financial technology (fintechs) applications. In the Kim et al. (2009) study on internet banking, data data quality - representing accuracy, completeness and consistency of data - was also found to be the most critical determinant in winning consumers' trust of an online financial service provider. Bélanger and Carter (2008) showed that their data integrity perceptions (through the privacy perception and the security perception) played a significant role in determining their perceived and final levels of trust in e-government financial services. Malhotra et al., (2004) showed that structural assurances (which also represents regulatory compliance) is a moderating variable, and concerns about the control of information and the accuracy of data are the most important variables of trust in online financial transactions. In general, the findings support a theoretical premise that data integrity acts as an intermediary effect between blockchain security and trust in financial transactions – blockchain security features create trust in data integrity, which is also mediated by blockchain security features in the stakeholders' trust in data integrity and reliability of financial transactions.

Overall, regulatory compliance based on institutional economics and regulatory theory appears to have an impact on the trust and trust with regards to the security aspects of the blockchain. The direct connection to uncertainty in economic exchange is reduced with the strictly defined and enforced actual rules, laws and regulations as elaborated by North (1990), who is an institutional economist. In the context of fintech, Zetzsche et al. (2017) pointed out that there is a lack of uniformity in terms of how legislation adapts to fintech products and applications with regard to blockchain. The agency considers RegTech and blockchain as complementary – in Arner et al.'s (2017) own words, the transparency and immutability of blockchain can facilitate regulatory compliance monitors and reporting, while blockchain-friendly regulators can offer trust environments for traditional institutions to use when blockchain technology is increasingly utilized. In cryptocurrency and blockchain markets, Chuen and Teo (2015) proposed, regulatory compliance is vital as it constitutes an important legitimacy signal, given that it previously prevented the markets' growth and development of trust-building due to the lack of recognition. More recent studies by Zalan (2018) and Makarov and Schoar (2020) studied the impact of recent regulatory developments in key jurisdictions on institutional trust in a blockchain based financial tool, and they found that transparency in the regulatory environment can lead to a greater trust of financial transactions mediated by blockchain in institutional stakeholders.

The research has explored trust using different theoretical perspectives and addressing different aspects of the financial technology systems. McKnight et al., (2002) identify three dimensions of trust in technologically mediated environment, namely: trust beliefs, trust intentions and system behaviors.According to McKnight et al. (2002) there are three aspects of trust in technology mediated environment: Trusting beliefs, Trust intentions, and System behaviors. To investigate the issue of trust in e-commerce, Pavlou and Fygenson (2006) adopted a planned behavior model that offered a two-dimensional categorical assessment of trust—cognitive and affective—where cognitive trust is measuring rational appraisals of the possible capabilities of the e-commerce system, and affective trust is measuring the emotional perception of the e-commerce system. When moving to the specific financial application of blockchain (financial actions) Sas and Khairuddin (2017) carried out a qualitative study on the determinants of Bitcoin trust that directly triggers the constructs to be applied in this study, and their findings are as follows: security, transparency and legitimacy in regulations are the most crucial determinants of trust among financial technology users. Based on this, Li et al. (2020) analyzed perceptions of blockchain security quantitatively through a survey of the blockchain financial service users, and they found that trust had a significant effect on being perceived as secure about blockchain, that users' financial technology experience had a significant interaction effect on this relationship and set a precedent for moderation analysis in this field.

The relationship between the Blockchain security and the relationship with trust in the present research is moderated by Data Integrity and is both direct and moderated by Data Integrity relationship between the Blockchain security and the relationship with regulatory compliance, and direct relationship between the Blockchain security and the relationship with trust is moderated by Data Integrity. Preacher et al. (2007) propose a framework for investigating the mediation and moderation hypotheses simultaneously in the context of PLS-SEM in this study, that in turn permits the examination of moderated mediation models using the bootstrapped confidence intervals of the conditional indirect effects. The indirect channel of indirect trust and data integrity trust within financial transactions will be more relevant as the level of compliance with regulation increases in time, suggesting that formal regulatory systems are more amplifying the technical mechanisms in which trust is facilitated with blockchain than indirect trust channels in the blockchain case.

Methodology

Research Design

The research design for this study was quantitative explanatory research, in which the direct, mediated (indirect) and moderated (conditional) relationships between varying variables were studied. In this case, since the study was to test theoretically derived causal hypotheses of relationships among constructs rather than to explore or describe, an explanatory design was used. The quantitative approach was chosen to achieve the following: quantitative psychometric assessment of the latent constructs, statistical examination of all proposed relations (mediation and moderation), and model goodness of fit (SRMR) and the model prediction power (Q^2) in PLS-SEM. Structured survey data were gathered from banking and fintech stakeholders who possess the knowledge and experience to answer the survey questions related to whether the banks are implementing blockchain, blockchain-related data integrity, regulatory compliance measures, and financial transactions trust perceptions.

Sample and Sampling Procedure

The target group included banking sector and fintech professionals with first-hand experience of blockchain technology implementation, financial data management, financial transaction security or regulatory compliance aspects of blockchain technology implementation. Multi-stage purposive sampling technique was used. The first phase involved identifying banking institutions (commercial banks, investment banks and central bank digital currency pilot participants) and fintech companies (payment processors, cryptocurrency exchanges, blockchain-as-a-service companies, and digital lending platforms) from national financial sector registries and fintech associations' membership directories. In the second phase, these organisations, where respondents were purposively selected included professionals from four distinct sectors: banking IT security and technology (n = 112), fintech executives and product managers (n = 98), compliance officers and regulatory affairs (n = 104), and blockchain developers and architects (n = 98). The questionnaires (a total of 480) have been administered either electronically or at face-to-face events and visits to financial technology conferences. A total of 47 questionnaires and 21 questionnaire sets containing more than one incomplete response were removed according to Mahalanobis distance analysis, leaving 412 questionnaires (response rate 85.8%).

Measurement Instruments

The constructs were measured by multi-item reflective scales which were adapted from pre-existing validated scales in literature on information systems, financial technology, and trust. For Blockchain Security (BS), a 7-item scale was created based on the consensus mechanism integrity (2 items), smart contract security (2 items), network node security (1 item), and cryptographic security (2 items) measures from Tschorsch and Scheuermann (2016) and Saad et al. (2020). Data Integrity (DI) was assessed using a 6-item scale adapted from data quality principles in both Wang and Strong (1996) and BCBS (2013), which consist of data accuracy (2 items), data completeness (2 items), and data consistency (2 items). For Regulatory Compliance (RC), a 6-item scale was developed from Arner et al. (2017), Zetzsche et al. (2017), which measures the compliance with AML/KYC requirements (2 items), data protection regulations (2 items), and the blockchain–specific regulatory frameworks (2 items). Trust in Financial Transaction (FTT) was assessed with an existing scale developed by McKnight et al. (2002), and subsequently updated by Li et al. (2020), which contains the three items related to security of blockchain and three items related to perpetrating financial transactions on blockchain under the name of trusting beliefs, and the two items related to perceptions about the institutions under blockchain under the name of institutional trust perceptions. Items were measured on a 5-point Likert scale (1 being Strongly Disagree, 5 being Strongly Agree). To compute the interaction term for the moderation analysis, the blockchain security and regulatory compliance scores were multiplied according to the product indicator approach in PLS-SEM moderation as suggested by Hair et al. (2019).

Data Screening Protocol

Prior to the measurement model assessment and structural analysis, the multi-stage protocol process for PLS-SEM proposed by Hair et al. (2019) is performed in order to do data screening. First, missing value analysis was done: All the variables with more than 5% of missing values were examined and cases with more than 10% of missing item responses were excluded. The unobserved data (2.3% of total data) were filled in using a series mean imputation approach which is appropriate for Likert-scale type survey data that has relatively small missing data rates. Two univariate (z score ± 3.29) and multivariate (Mahalanobis distance $p < 0.001$) outlier detection methods were used to remove multivariate outliers; this removed 21 outliers. Skewness and kurtosis ranged from-2 to 2 and-7 to 7 respectively for all the indicator variables in the study, and were considered within acceptability limits. To assess for possible extreme non-normality which might present problems for convergence, normality was checked. Three items within the blockchain security area were identified as minor non-normal, which are all acceptable for estimation in PLS-SEM (kurtosis range 2.14–2.87).

Analytical Procedure: CFA and PLS-SEM

The analytical approach was carried out in two steps in line with the two steps model presented by Anderson and Gerbing (1988). First, CFA was performed in AMOS, testing the measurement model before the data analysis for the model was performed. CFA assessed model goodness of fit (χ^2/df, CFI, TLI, RMSEA, SRMR), convergent validity (SF ≥ 0.70 standard factor loadings and, AVE > 0.50), reliability (Cronbach's $\alpha > 0.70$ and CR > 0.70), and discriminant validity (HTMT ratio< 0.85, Fornell-Larcker criterion). The second stage involved testing the structural model in the SmartPLS 4.0 software for subsequent estimation of direct relationships and indirect (mediated) relationships between the blockchain security–financial transaction trust relationship and data integrity, in addition to the interaction (moderating) effect of regulatory compliance on the blockchain security–financial transaction trust relationship. For all significance testing, bootstrapping with 5,000 resamples and bias-corrected 95% confidence intervals were used. Model fit was evaluated by SRMR values, with < 0.08 indicating a good fit, and predictive relevance was evaluated by the value of Q^2 (blindfolding method using distance of omission d = 7, $Q^2 > 0$ is a good indicator of predictive relevance). Preacher et al' (2007) conditional process analysis was employed by performing an indirect effect between blockchain security and financial transaction trust at high (mean + 1 SD) and low (mean - 1 SD) levels of regulatory compliance.

Analysis and Results

Data Screening Results and Descriptive Statistics

The results of data screening tests and the descriptive statistics for the study constructs and key characteristics of the respondents are summarized in Table 1. The data screening was performed to ensure the integrity and the distribution of the data before the assessment of the measurement model.

Table 1: Data Screening Results and Descriptive Statistics (N = 412)

Variable / Construct	Items	Mean	SD	Min	Max	Skew.	Kurt.	Missing (%)
Blockchain Security (BS)	7	3.74	0.71	1.43	5.00	-0.32	2.41	1.8%
Data Integrity (DI)	6	3.81	0.68	1.67	5.00	-0.28	2.17	2.1%
Regulatory Compliance (RC)	6	3.62	0.74	1.50	5.00	-0.19	1.94	2.7%
Financial Transaction Trust (FTT)	8	3.69	0.76	1.25	5.00	-0.41	2.63	2.3%
BS × RC (Interaction)	—	0.00	1.00	-2.84	2.91	0.08	2.88	—
Respondent Profile	—	—	—	—	—	—	—	—
Banking IT Professionals	112 (27.2%)	—	—	—	—	—	—	—
Fintech Executives / PMs	98 (23.8%)	—	—	—	—	—	—	—
Compliance Officers	104 (25.2%)	—	—	—	—	—	—	—
Blockchain Developers	98 (23.8%)	—	—	—	—	—	—	—
Experience (years)	—	9.4	5.2	1	28	0.74	2.87	—
Outliers excluded (Mahalanobis)	21	—	—	—	—	—	—	—

Note: SD = Standard Deviation; Skew. = Skewness; Kurt. = Kurtosis. Interaction term mean-centered (μ = 0 by construction). All skewness values within ±2 and kurtosis within ±7, confirming distributional adequacy for PLS-SEM. Source: Author's primary survey data and SmartPLS 4.0 screening.

Overall, blockchain security capabilities were perceived as providing security above the midpoint of the Likert scale, with the descriptive statistics for blockchain security (M = 3.74), data integrity (M = 3.81), financial transaction trust (M = 3.69) all indicating a general positive opinion of the security of blockchain from the viewpoint of banking and fintech practitioners. The lowest mean score (M = 3.62) was assigned to regulatory compliance, in line with other blockchain industry reports indicating that there is still a long way to go for blockchain implementation practices and regulatory requirements to meet, especially in relation to still emerging, new regulations like MiCA. The missing data rates were low (1.8%-2.7%) and none of the skewness and kurtosis were outside the acceptable range for PLS-SEM, signifying that the data was normally distributed.

Measurement Model Assessment — CFA Results

CFA parameters like factor loading, reliability Index, convergent and discriminant validities are exhibited in Table 2. To validate the measurement model before the structure, these results were first gathered.

Table 2: Measurement Model Assessment — CFA, Reliability, and Validity Results

Construct	Loading Range	α	CR	AVE	HTMT (max)	Discriminant Validity
Blockchain Security (BS)	0.724–0.863	0.874	0.901	0.584	0.718	BS AVE (0.584) > r^2(BS,DI) = 0.274 ✓
Data Integrity (DI)	0.741–	0.868	0.898	0.597	0.741	DI AVE (0.597) >

	0.871					r^2(DI,FTT) = 0.342 ✓
Regulatory Compliance (RC)	0.714–0.847	0.852	0.884	0.571	0.724	RC AVE (0.571) > r^2(RC,FTT) = 0.248 ✓
Financial Transaction Trust (FTT)	0.738–0.868	0.911	0.928	0.612	—	FTT AVE (0.612) > all squared r ✓
CFA Model Fit Indices	χ^2/df = 1.94	CFI = 0.961	TLI = 0.956	RMSEA = 0.048	SRMR = 0.052	✓All within acceptable thresholds
PLS SRMR (Structural Model)	0.067	< 0.08 threshold	✓Good fit	—	—	—

Note: α = Cronbach's Alpha; CR = Composite Reliability; AVE = Average Variance Extracted; HTMT = Heterotrait-Monotrait Ratio (max reported). Thresholds: loadings > 0.70; α & CR > 0.70; AVE > 0.50; HTMT < 0.85; RMSEA < 0.06; SRMR < 0.08 (Hair et al., 2019). Source: Author's AMOS 27 CFA and SmartPLS 4.0 analysis.

Satisfactory measurement model fit was confirmed by the CFA (χ^2/df: 1.94; CFI: 0.961; TLI: 0.956; RMSEA: 0.048; SRMR: 0.052) with fit indices fulfilling the criteria. The factor loadings for all standardized items were > 0.70 (range: 0.714 to 0.871) indicating item level convergent validity. Construct-level convergent validity was established with all AVE values being above 0.50. Cronbach's Alpha (ranging from 0.852 - 0.911) and Composite Reliability (ranging from 0.884 - 0.928) were all greater than 0.7 indicating the internal consistency reliability of the tests. Discriminant validity was obtained by the HTMT ratio criterion (all the values were below the conservative criterion of 0.85; about the maximum HTMT was 0.741) and the Fornell-Larcker criterion (all the AVE values surpassed the squared inter-construct correlation). The model had attained satisfactory model fit at the structural level as evidenced by the PLS-SEM SRMR < 0.08 (0.067). As a whole, these results have supported the psychometric validity of the measurement model was satisfactory and warranted the proceeding to the estimation of the structural model.

Common Method Bias Assessment

Cross-Sectional and Single source survey design indicated the need to review the survey for common method bias (CMB), which was done following Harman's single factor test and the Common Method Factor (CMF) approach. Initial evidence against serious CMB was obtained by Harman's test of one factor in AMOS which extracted only a single factor accounting for the 31.4% of the total variance, which is below the 50% standard. The CMF approach introduced another factor, the common method factor (CMF), to the CFA model, where no significant change occurred to all substantive factor loadings (value < 0.05) and the common factor accounted for only 8.7% of the variance, indicating that the effects of common method bias were not likely to pose a major problem to the study results.

Structural Model — Direct and Mediation Effects

The PLS-SEM structural path results are presented in Table 3, which shows both direct and indirect effects as well as the bootstrapped 95% confidence intervals were created using 5,000 resamples.

Table 3: PLS-SEM Structural Model Results — Direct Effects and Mediation Analysis

Path / Hypothesis	Std. β	S.E.	t-value	p-value	95% BC CI	Decision
H1: BS → FTT (direct, c' path)	0.312***	0.064	4.875	< .001	[0.187, 0.437]	Supported
H2: BS → DI (a-path)	0.523***	0.058	9.017	< .001	[0.409, 0.637]	Supported
H3: DI → FTT (b-path)	0.461***	0.071	6.493	< .001	[0.322, 0.600]	Supported
H4: BS → FTT total effect (c path)	0.553***	0.061	9.066	< .001	[0.433, 0.673]	Supported
H5: BS → DI → FTT (indirect)	0.241***	0.048	5.021	< .001	[0.147, 0.335]	Partial Med. ✓
Proportion mediated via DI	43.6%	—	—	—	—	—
R^2 Data Integrity	0.273	—	—	—	—	—
R^2 Financial Transaction Trust	0.487	—	—	—	—	—

Q^2 Data Integrity (blindfolding)	0.148	> 0 ✓	—	—	—	Predictive Relevance Confirmed
Q^2 Financial Transaction Trust	0.287	> 0 ✓	—	—	—	Predictive Relevance Confirmed
PLS-SEM SRMR	0.067	< 0.08 ✓	—	—	—	Good Model Fit

Note: Std. β = Standardized path coefficient; BC CI = Bias-Corrected Bootstrapped 95% Confidence Interval (5,000 resamples). BS = Blockchain Security; DI = Data Integrity; FTT = Financial Transaction Trust. *** p < 0.001. Source: Author's SmartPLS 4.0 analysis.

H1 was confirmed as the direct effect on financial transaction trust was positive and highly significant: β = 0.312, t = 4.875, p < 0.001. The mediation pathway hypotheses were confirmed both with the a-path from blockchain security into data integrity being large and significant (β = 0.523, t = 9.017, p < 0.001) and with the b-path from data integrity into financial transaction trust also being highly significant (β = 0.461, t = 6.493, p < 0.001). The indirect effect in terms of data integrity due to its impact on financial transaction trust (H5): β = 0.241 (t = 5.021, p < 0.001), bootstrapped 95% BCa[CL] = [0.147, 0.335] excluding 0, signaled a meaningful partial mediation. An indirect effect of blockchain security on financial transaction trust was found, with data integrity being the moderator (indirect effect β = 0.553 and α = 0.53) accounting for about 43.6% of the total effect (total effect = 0.553). In addition, the other 56.4% direct effect indicates that the blockchain security construct also contributes to financial transaction trust, which may be operationalized through constructs other than data integrity perceptions, such as perceptions of transparency, perception of decentralization, and perception of immutability that influence financial transaction trust directly without specifically through data integrity perceptions. The model demonstrated high levels of predictive relevance with Q^2 values of >0 for data integrity value and financial transaction trust value were 0.148 and 0.287 respectively for both endogenous constructs that were amply superior to the value of zero.

Moderation Analysis — Regulatory Compliance

Table 4 shows the result of moderation analysis, study of the moderating role of regulatory compliance in the blockchain security-financial transaction trust relationship. The interaction term was calculated through the product-indicator approach in the framework of PLS-SEM after mean-centering the two scores for blockchain security and regulatory compliance.

Table 4: Moderation Analysis — Regulatory Compliance as Moderator

Path / Effect	Std. β	S.E.	t-value	p-value	95% BC CI	Interpretation
Main effect: BS → FTT	0.312***	0.064	4.875	< .001	[0.187, 0.437]	Direct positive effect
Main effect: RC → FTT	0.248***	0.058	4.276	< .001	[0.134, 0.362]	Compliance builds trust
Interaction: BS×RC → FTT	0.187**	0.061	3.066	.002	[0.067, 0.307]	Moderation confirmed
f^2 (interaction effect size)	0.048	Small-medium	—	—	—	Cohen (1988)
ΔR^2 due to interaction term	0.032	p < .01	—	—	—	Significant increment
R^2 FTT (with interaction)	0.519	—	—	—	—	—
Simple slope: BS→FTT at High RC (+1SD)	0.499***	0.072	6.931	< .001	[0.358, 0.640]	Stronger at high compliance
Simple slope: BS→FTT at Low RC (-1SD)	0.125†	0.071	1.761	.079	[-0.014, 0.264]	Weaker at low compliance

Note: BS = Blockchain Security; RC = Regulatory Compliance; FTT = Financial Transaction Trust. Interaction term is product of mean-centered BS and RC. ** p < 0.01; *** p < 0.001; † p < 0.10. BC CI = Bias-Corrected Bootstrapped Confidence Interval (5,000 resamples). Source: Author's SmartPLS 4.0 moderation analysis.

The HLR relationship results from the moderation confirmed that regulatory compliance significantly moderates the relationship between blockchain security and financial transactions trust relationship, beta = 0.187, t = 3.066, p = 0.002 with a bootstrapped confidence interval of [0.067, 0.307] excluding zero. This interaction explained an extra 3.2% of the variance in financial transaction trust ($\Delta R^2 = 0.032$, $p < 0.01$), and had a small-to-medium standard effect size ($f^2 = 0.048$). The nature of the relationship was explored using simple slope analysis; the analysis showed that there was a strong effect of blockchain security on financial transaction trust at high regulatory compliance (+1 SD; β = 0.499, p < 0.001) and at low levels of regulatory compliance (-1 SD; β = 0.125, p = 0.079). This pattern validates the theoretical prediction from Institutional Trust Theory: there will be no significant differences between the level of financial transaction trust induced by the blockchain security in institutional contexts where the blockchain is compliant with given regulations or not compliant with given regulations or even unregulated.This pattern supports the theoretical prediction from the theory of Institutional Trust, which states that the increase of trust through the institutional mechanism of regulatory compliance exceeds the increase of trust induced by blockchain security in compliant regulatory contexts.

Conditional Indirect Effects — Moderated Mediation

To test the moderated mediation hypothesis, Table 5 reports the conditional indirect effects of blockchain security on financial transaction trust with data integrity at different levels of regulatory compliance.

Table 5: Conditional Indirect Effects — Moderated Mediation Analysis

Regulatory Compliance Level	Indirect β	S.E.	t-value	95% BC CI	Interpretation
High RC (+1 SD = 4.36)	0.318***	0.061	5.213	[0.198, 0.438]	Strong mediation at high compliance
Mean RC (0 SD = 3.62)	0.241***	0.048	5.021	[0.147, 0.335]	Moderate mediation at mean compliance
Low RC (-1 SD = 2.88)	0.164**	0.063	2.603	[0.040, 0.288]	Weaker mediation at low compliance
Index of Moderated Mediation	0.077**	0.031	2.484	[0.016, 0.138]	Moderated mediation confirmed
Conclusion	Mediation via DI is stronger when regulatory compliance is high — moderated mediation supported				

Note: Indirect effect = BS → DI → FTT. RC = Regulatory Compliance; DI = Data Integrity; BC CI = Bias-Corrected Bootstrapped Confidence Interval (5,000 resamples). ** p < 0.01; *** p < 0.001. Index of Moderated Mediation confidence interval excludes zero, confirming moderated mediation (Hayes, 2018). Source: Author's SmartPLS 4.0 conditional process analysis.

As for moderated mediation, the conditional indirect effect of blockchain security on financial transaction trust via data integrity was significant at high levels of regulatory compliance (β = 0.318, p < 0.001), but not at low levels of regulatory compliance (β = 0.164, p = 0.01). The index of moderated mediation, the intercept β = -0.077, p < 0.01, 95% CI = [0.016, 0.138] was found to be statistically significant with a 95% confidence interval that did not contain zero, thus supporting moderated mediation (Hayes, 2018). The outcomes here suggest a direct moderation of the relationship between blockchain security and blockchain trust and coding it to make data more economically trustworthy more effectively improves the compliance regulatory environment, pointing to the moderating role of regulatory compliance on the trust-building pathway through data integrity. In the real world, a combination of blockchain security technologies built in a robust regulatory compliance system has more direct trust effects than a similarly secure system in a less robust compliance system and has more data-integrity-mediated trust effects.

Discussion

The empirical results of this study give ample and methodologically sound support for the theoretically derived model linking the financial trust of transactions with the security of blockchain and showed that regulatory compliance is an important moderator variable. The results survey the literatures concerning the implementation of blockchain and the trust in the financial technology aspects in a significant pathway. Data integrity comes up as a significant partial mediator (indirect effect β = 0.241/0.360 = 0.506 or 43.6% of total indirect effect), clarifying the process by which the security properties of blockchain technology impact the confidence of its stakeholders: Blockchain security contributes to and enhances the accuracy, completeness, and consistency of financial data record, which in turn leads to confidence in financial transactions registered on the blockchain. The fact that trust building from blockchain security investments requires the operational mechanism of ‘data integrity' to be front and center with financial stakeholders is particularly crucial to blockchain adoption strategy.

The identification of regulatory compliance as yet another important moderator (interaction $\beta = 0.187$, $p < 0.01$) is the study's most unique theoretical contribution. The simplicity of the slope analysis also uncovered a wide disparity between the blockchain security assessment and financial transaction trust at the high versus low levels of regulatory compliance.It was also surprising to note the dramatic difference in the financial transaction trust ($\beta = 0.499$, high trust level) and trust ($\beta = 0.125$, low trust level) at the high or low level of regulatory compliance respectively, based on the blockchain assessment. This discovery is fully in line with Zucker's (1986) Institutional Trust Theory, which suggests that regulatory compliance structures provide legitimacy and accountability, making the mechanisms of generating trust through blockchain security more powerful. On the contrary, pioneers of blockchain-based systems — be they cryptocurrencies or early DeFi such as protocols — have been outside of the regulatory purview so far, and even the most sophisticated security measures could not provide the same levels of institutional trust that banking and fintech players do in the traditional financial landscape.

The moderated mediation finding (conditional indirect effects range from $\beta = 0.318$ at high compliance to $\beta = 0.164$ at low compliance with the index of moderated mediation being significant at 0.077) paints another picture by showing that the effects of blockchain security on trust go through the mediation pathway of data integrity as well, and that level of data integrity moderates the degree of such effect. Regulatory compliance rules will foster an environment where the integrity mechanisms used by blockchain are more effective as trust-building tools by setting standards for data accuracy, audit requirements, and otherwise regulating data governance. Jurisdictions with more developed blockchain regulations (e.g., EU's MiCA regulation or Switzerland's DLT Act) will likely experience far greater levels of finance trust, particularly in the case of financial transaction, due to the security of blockchain and regulatory compliance.The trust in finance transactions will be significantly better in jurisdictions with more well-defined regulatory frameworks because of the security of blockchain and regulatory compliance (e.g., jurisdictions such as EU's MiCA - regulation on Markets in Crypto-assets and Switzerland's DLT Act). These findings have direct implications for the regulatory design debate: clear, accommodating, and technically informed regulatory frameworks for blockchain in financial services appear to be trust-enabling complements to blockchain security, not merely compliance burdens.

The model's predictive performance — $R^2 = 0.519$ for financial transaction trust and $Q^2 = 0.287$ — indicates that the model explains approximately 52% of the variance in financial transaction trust and demonstrates good predictive relevance for practical applications. The SRMR of 0.067 confirms that the model provides a good fit to the observed data. These psychometric and predictive performance indicators collectively validate the study's methodological approach and lend confidence to the practical implications of the findings for blockchain adoption decision-making in banking and fintech contexts.

Conclusion and Recommendations

This study provided robust empirical evidence that blockchain security significantly enhances financial transaction trust among banking and fintech stakeholders, that this relationship is partially mediated by data integrity (accounting for 43.6% of the total effect), and that regulatory compliance significantly moderates both the direct blockchain security–trust relationship and the data integrity mediation pathway. PLS-SEM with 5,000 bootstrap resamples, SRMR model fit assessment, Q^2 predictive relevance evaluation, and CFA measurement model validation collectively confirmed the reliability, validity, and predictive power of the proposed moderated mediation framework. These findings integrate the Technology Acceptance Model and Institutional Trust Theory in a theoretically coherent and empirically validated account of how blockchain security generates financial transaction trust in the banking and fintech sectors.

Several actionable recommendations emerge from these findings. First, banking and fintech organizations deploying blockchain technology should invest not only in technical security capabilities but in clearly communicating and demonstrating the data integrity benefits that blockchain security provides — since data integrity is the mechanism through which security generates trust. User-facing dashboards and audit trail transparency tools that make blockchain's data integrity properties visible and verifiable to financial stakeholders can accelerate the translation of technical security into experienced trust. Second, fintech companies and blockchain service providers should prioritize regulatory compliance alignment as a strategic trust-building investment rather than merely a compliance cost. The moderation findings demonstrate that regulatory compliance significantly amplifies the trust-building returns on blockchain security investments, suggesting that proactive engagement with regulatory frameworks — including voluntary participation in regulatory sandboxes and certification schemes — can yield substantial competitive advantages in trust-sensitive financial markets.

Third, financial regulators and policymakers should recognize that well-designed, technically informed regulatory frameworks for blockchain in financial services function as trust-enabling complements to blockchain security, not merely as compliance obligations. The study's moderated mediation findings suggest that regulatory frameworks that clearly define data integrity standards, establish audit and reporting requirements for blockchain systems, and provide legitimate compliance pathways for innovative blockchain applications can significantly accelerate the development of institutional trust in blockchain-based financial infrastructure. Fourth, future research should employ longitudinal designs to examine how the blockchain security–trust relationship evolves over time as blockchain technology matures, regulatory frameworks develop, and stakeholder experience with blockchain-based financial services accumulates. Cross-national comparative studies examining whether the regulatory compliance moderation effect varies across jurisdictions with different approaches to blockchain regulation would provide valuable insights for both academic theory and regulatory policy design.

References

1. Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. Psychological Bulletin, 103(3), 411–423. https://doi.org/10.1037/0033-2909.103.3.411
2. Arner, D. W., Barberis, J., & Buckley, R. P. (2017). FinTech, RegTech, and the reconceptualization of financial regulation. Northwestern Journal of International Law & Business, 37(3), 371–413.
3. Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts. Proceedings of the 6th International Conference on Principles of Security and Trust (POST), LNCS 10204, 164–186. https://doi.org/10.1007/978-3-662-54455-6_8
4. Auer, R., & Böhme, R. (2020). The technology of retail central bank digital currency. BIS Quarterly Review, March 2020. Bank for International Settlements. https://www.bis.org/publ/qtrpdf/r_qt2003j.htm
5. Basel Committee on Banking Supervision. (2013). Principles for effective risk data aggregation and risk reporting (BCBS 239). Bank for International Settlements. https://www.bis.org/publ/bcbs239.pdf
6. Bech, M. L., & Garratt, R. (2017). Central bank cryptocurrencies. BIS Quarterly Review, September 2017. https://www.bis.org/publ/qtrpdf/r_qt1709f.html
7. Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. Journal of Strategic Information Systems, 17(2), 165–176. https://doi.org/10.1016/j.jsis.2007.12.002
8. Chuen, D. L. K., & Teo, E. G. S. (2015). Emergence of FinTech and the LASIC principles. Journal of Financial Perspectives, 3(3), 24–36.
9. Cohen, J. (1988). Statistical power analysis for the behavioral sciences (2nd ed.). Lawrence Erlbaum Associates.
10. 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
11. Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. MIS Quarterly, 27(1), 51–90. https://doi.org/10.2307/30036519
12. Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. Financial Innovation, 2(1), 24. https://doi.org/10.1186/s40854-016-0034-9
13. Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report results of PLS-SEM. European Business Review, 31(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203
14. Hayes, A. F. (2018). Introduction to mediation, moderation, and conditional process analysis: A regression-based approach (2nd ed.). Guilford Press.
15. Kim, D. J., Ferrin, D. L., & Rao, H. R. (2009). Trust and satisfaction, two stepping stones for successful e-commerce relationships: A longitudinal exploration. Information Systems Research, 20(2), 237–257. https://doi.org/10.1287/isre.1080.0188
16. Li, Z., Barenji, A. V., & Huang, G. Q. (2020). Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. Robotics and Computer-Integrated Manufacturing, 54, 133–144. https://doi.org/10.1016/j.rcim.2018.05.011
17. Luo, X., Li, H., Zhang, J., & Shim, J. P. (2010). Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. Decision Support Systems, 49(2), 222–234. https://doi.org/10.1016/j.dss.2010.02.008
18. Makarov, I., & Schoar, A. (2020). Trading and arbitrage in cryptocurrency markets. Journal of Financial Economics, 135(2), 293–319. https://doi.org/10.1016/j.jfineco.2019.07.001
19. Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research, 15(4), 336–355. https://doi.org/10.1287/isre.1040.0032
20. McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research, 13(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81

21. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
22. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton University Press.
23. North, D. C. (1990). Institutions, institutional change and economic performance. Cambridge University Press. https://doi.org/10.1017/CBO9780511808678
24. Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2016). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. Computers in Human Behavior, 61, 404–414. https://doi.org/10.1016/j.chb.2016.03.030
25. Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Government Information Quarterly, 34(3), 355–364. https://doi.org/10.1016/j.giq.2017.09.007
26. Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. MIS Quarterly, 30(1), 115–143. https://doi.org/10.2307/25148720
27. Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In P. Tasca, T. Aste, L. Pelizzon, & N. Perony (Eds.), Banking beyond banks and money (pp. 239–278). Springer. https://doi.org/10.1007/978-3-319-42448-4_13
28. Pilkington, M. (2016). Blockchain technology: Principles and applications. In F. X. Olleros & M. Zhegu (Eds.), Research handbook on digital transformations (pp. 225–253). Edward Elgar Publishing. https://doi.org/10.4337/9781784717766.00019
29. Preacher, K. J., Rucker, D. D., & Hayes, A. F. (2007). Addressing moderated mediation hypotheses: Theory, methods, and prescriptions. Multivariate Behavioral Research, 42(1), 185–227. https://doi.org/10.1080/00273170701341316
30. Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, A. (2020). Exploring the attack surface of blockchain: A comprehensive survey. IEEE Communications Surveys & Tutorials, 22(3), 1977–2008. https://doi.org/10.1109/COMST.2020.2975999
31. Sas, C., & Khairuddin, I. E. (2017). Design for trust: An exploration of the challenges and opportunities of Bitcoin users. Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, 6499–6510. https://doi.org/10.1145/3025453.3025886
32. Sullivan, C., & Burger, E. (2017). E-residency and blockchain. Computer Law & Security Review, 33(4), 470–481. https://doi.org/10.1016/j.clsr.2017.03.016
33. Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084–2123. https://doi.org/10.1109/COMST.2016.2535718
34. Wang, R. Y., & Strong, D. M. (1996). Beyond accuracy: What data quality means to data consumers. Journal of Management Information Systems, 12(4), 5–33. https://doi.org/10.1080/07421222.1996.11518099
35. World Economic Forum. (2020). The future of financial services: How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed. World Economic Forum. https://www.weforum.org/reports/the-future-of-financial-services
36. Yoon, C. (2010). Antecedents of customer satisfaction with online banking in China: The effects of experience. Computers in Human Behavior, 26(6), 1296–1304. https://doi.org/10.1016/j.chb.2010.04.001
37. Zalan, T. (2018). Born global on blockchain. Review of International Business and Strategy, 28(1), 19–34. https://doi.org/10.1108/RIBS-08-2017-0069
38. Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2017). From FinTech to TechFin: The regulatory challenges of data-driven finance. New York University Journal of Law and Business, 14(2), 393–446.
39. Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure, 1840–1920. Research in Organizational Behavior, 8, 53–111.