Blockchain Technology And Its Impact On European Bank's Cyber Security And Data Integrity

Mohammad Mizanur Rahman[1] , Dr. Amina Elshamly[2] , Shafiq Ur Rehman[3] , Zainab Jameel[4] , Rabia Hameed[5]

[1]Lecturer Department of Accounting Gurudayal Government College, Kishoreganj (Affiliated with National University, Bangladesh)
Email duaccmizanur@gmail.com
[2]Assistant Professor Business school Taibahu University KSA
ashamly@taibahu.edu.sa
[3]School of Finance and Banking University of Utara Malaysia
Email: Shafiq.Rehman321@gmail.com
[4]Assistant Professor Business school Qassim University KSA
Email: Za.jameel@qu.edu.sa
[5]Research scholar University of Utara Malaysia
Scorpionkool1@gmail.com

Abstract

Cybersecurity Ventures anticipates that the worldwide expenses of cybercrime would increase by 15 percent yearly over the course of the next five years, reaching USD 10.5 trillion annually by 2025, which is an increase from USD $3 trillion in 2015. It's imperative to investigate the implementation of new technologies and their outcome in raising the threat to the banking industry. Using CFA and EFA statistical analysis and gathering the data from N=291 respondents from the managerial level, blockchain consultants, and cybersecurity experts. The findings confirm that the implementation of blockchain technologies has efficiently reduced customer cyber security risks and enhanced the European banking sector's data integrity.

1 Introduction

Cybersecurity Ventures anticipates that the worldwide expenses of cybercrime would increase by 15 percent yearly over the course of the next five years, reaching USD 10.5 trillion annually by 2025, which is an increase from USD $3 trillion in 2015[1] and this issue is still on the rise. The financial sector, especially the less

developed countries, is at risk compared to developed countries. The authorities have made countless efforts, and central banks have been made to overcome this issue; however, this issue is still prevalent at a considerable rate. Many countries have adopted many advanced infrastructures, and many countries have adopted new financial technologies (i.e., blockchain, Big Data, AI); however, the implications of these new technologies and outcomes are still ambiguous. Therefore, this article will provide the research findings of a recent blockchain-based security model.

In the banking sector, blockchain technology's major implementation is customer registration, fund transfer, data protection and manipulations, and back-end data integrations[2-4]. This innovation works like a conveyed record and is open to everybody in the organization. It is exceptionally impossible to modify or convert data after it has been registered in the blockchain, makthe ing blockchain inherently secure[4, 5]. Previous studies looked the advantages of blockchain technology in postal enterprises, such as decentralised platforms, fast transaction procedures and secure recordkeeping.[6]. Blockcian helps to improve the operation in this industry. Many financial institutions, each in their own unique manner, have tried out and made use of this technology. Some banks look at their own possibilities first, while others make an effort to utilise technology to look into their options with other financial institutions; however, the implementation of blockchain to overcome come the cyber security issue is still at a very early stage and hardly any investigation has been done in this regard.

This research article focuses on 41 European banks that recently implemented the blockchain-based model for risk management. 291 managerial level, blockchain consultants, and cybersecurity experts participated in the quantitative research survey. The research findings show that implementing new blockchain technology models has significantly reduced cyber security risk in European banks.

In this article, firstly, we analyze the potential benefits of adoption the blockchain technology in European financial industry. Secondly this study will present a qualitative study outcome, from which this study constructed an initial set of instruments to assess the perceived advantages of deploying blockchain technology. Thirdly, this study presented the research findings using sample data

gathered from our sample size (i.e., blockchain experts and IT heads responsible for implementing blockchain technology in the banking sector). In the study's discussion section, the particulars of the findings were dissected in further depth. The theoretical and practical implications of the findings are presented in this paper after the discussion section. In conclusion, we discuss the limitations of the study as well as potential next steps for research.

2 Literature review

The European banking industry is implementing several new technologies to reduce vendor financing issues, improve customer loyalty programs, data integrity issues, and resilience of cyber-security problems[7, 8]. The use of blockchain technology and its impact on the banking sector at its early stage, and only a few research studies have been conducted to address the outcome of these implications; for instance, there is minimal studies that evaluated the use of blockchain technologies and its impact on cyber security. To the best of the author's knowledge a single study was conducted by Salman et al.[9]. The authors of this study highlight the challenges and problems associated with the use of security services in the centralized architecture in various application domains, as well as provide a comprehensive review of current blockchain-enabled methods for such security service applications in authentication, privacy, confidentiality, access control, integrity assurance and, data and resource provenance, in distributed networks. This study, in our opinion, provides a great starting point for future academics interested in blockchain-based network and service security. Therefore by taking the recommendation of Salman [9] this study will investigate this unattended issue.

3 Study design & Data collection procedures

The primary purpose of this research is to validate an instrument about the perceived advantages of increased cybersecurity afforded by the use of blockchain technology in the banking sector (i.e., the European banking sector). This study will follow the framework of Garg, Gupta [10] to measure the impact of blockchain technology in the banking sector. By following Garg, this study chose the respondents from the banking sector who are responsible for developing the blockchain technology both front end and back end. Therefore, we conducted interviews with IT heads, blockchain managers, and staff accountable for blockchain

implementation and improving clients' data integrity. We also include the bank-hired consultants who are providing the consultancy to the banks for the implantation of blockchain technology.

The questionnaire, along with the cover letter was distributed to the respondents through a google doc link. The majority of the respondents are information technology chiefs, block-chain managers and specialists who are actively advising or implementing blockchain technology in the banking industry between April 2020 and November 2022.We employed the convenience sampling approach to acquire data. We used a three-tiered approach for this investigation. First, from October 2020 to March 2022, we phoned 600 specialists and IT experts to learn whether their company is exploring or using blockchain for their operations.

To get enough sample size of experts, we took a five-step approach. Firstly, we identify two-sector banks, i.e., public and private sector banks. In the second step, we collected the data from each website of the bank; in the third step, We used the search function on the bank's website to locate the locations of the banking institutions that have branches in a certain region. In the fourth stage, we phoned the branch managers to get a better understanding of the blockchain technology implementation. This included calling those branch managers who were responsible for the vertical blockchain technology installations.. And finally, we distributed the questionnaire to the respondents by sending the link through an email.

This procedure resulted in the selection of 395 eligible candidates for the survey. This sample size is true and selected based on the bank website profile and consultancy profile. Of 395 respondents, 320 acknowledged this response, which was 81% in percentage, and few answered the survey blindly. Out of 320, we selected 291 responses that were completed by respondents more accurately, and this sample size was used for the final analysis.

4 Demographics

Table 1 shows the subtleties of the segment profiles of respondents. The final sample of 291 respondents was further divided into 73.63% of male respondents and 23.36% of female respondents. Of these, 52.67% of respondents were in the age group of 35-45, and the rest were 25-35. About 42 percent of the

consultant respondents possessed a Master of Science in Computer Information Technology degree, and about 46 percent of them had a Bachelor of Technology or Bachelor of Engineering degree. The remaining responders all have bachelor's degrees in business and certificates in blockchain design and application. Following the blockchain advertising specialists (42 percent), experts of the blockchain (35.33 percent), and other IT development officers (8.67 percent), out of the overall sample size, banks IT chiefs made up 14 percent of the respondents.

Given the recent proliferation of blockchain technology, it is important to highlight that the average age of the respondents was 45 years old.. The final sample size also includes the experience chiefs past the age of 45 and who are heading the bank innovation team.

5 Data analysis and results

It has been assured that the fundamental and required processes to construct a scale have been completed, such as confirming the dependability of structures and the internal consistency, and factor analysis has been used to the data that has been obtained.. Additionally, the CFA was also applied to ensure the validity of adopted scale. We used AMOS 26.0 for CFA and SPSS 20 for EFA.

5.1 Instrument Reliability

An instrument's reliability can be used to evaluate its quality[11]. To ensure scale validity, an instrument's reliability is also essential. The statistical dependability of an instrument refers to how dependable and consistent test findings are. As a result, maintaining the instrument's reliability while designing a trustworthy instrument is crucial. There are numerous approaches for determining an instrument's dependability; nevertheless, internal consistency and reliability are easy to assess and have been demonstrated to be beneficial in field tests. The scale measures how uniform or homogenous a succession of facts or statements is. Cronbach's alpha can be used to examine an instrument's internal consistency and dependability. If the value of Cronbach’s alpha larger than 0.7 is acceptable , more than 0.8 is considered as the good value and more than 0.9 is referred as the exceptional internal consistency [12]. The value of results for 26 items was 0.909 which shows that items were dependable.

The acronym EFA stands for exploratory factor analysis, which is a kind of statistical analysis that combines data from a number of different variables into a more manageable group of factors.[13]. According to the validation criteria presented by Straub and Boudreau [14], the EFA method should be used for doing factor analysis. This will assist in locating the dimensions of the things that are being measured as well as defining them. The majority of the time, the EFA is the first step in the process of developing scales. EFA is used in the process of establishing the scope of a theoretical notion.[14].

An exploratory factor analysis (EFA) based on a principal components analysis (PCA) was performed on all 26 items from Section B of the instrument, and then a varimax rotation was performed on the results in order to get a deeper comprehension of the pattern and structure of the data. The principal component analysis (PCA) begins by isolating the variables with the highest variances and placing those variables into the first factor. Varimax rotation, on the other hand, seeks to minimise the total number of variables that have a high loading against each factor and makes very small loadings even smaller.

Bartlett's test and the Kaiser-Meyer Olkin test were used to determine the eligibility of data for factor analysis. The chi-square value that was calculated was 4174.095, and there were 325 degrees of freedom; this corresponds to a threshold of significance of 0.05. The KMO value of 0.875 is also satisfactory and meets requirements.. As a result, the factor analysis performed here may be deemed a valid method for further analyzing the data.

PCA with varimax (orthogonal) rotation was used to factor analyze 26 elements relevant to determining the advantages of deploying blockchain in the banking industry. The results of the EFA are shown in Tables 2 and 3, together with a characterization of the relevant variables. Five distinct aspects emerged from the investigation. There is an explanation for 67.535 percent of the variance. Factor 1 was given the name "customer cyber security" due to the considerable loadings that were contributed by a variety of factors, including greater transparency, enhanced confidence, data accuracy, risk reduction, and automation. The first component was found to be reliable, as it had a high Eigen value of 2.403 and was responsible for explaining 12.869 percent of the variance.. Due to the strong loading of these factors into Factor 2,

it was given the name "reduced expenditures." These factors include decreased administrative costs, reduced transaction costs, the elimination of intermediaries, and reduced operating costs. Factor 2 had an Eigen value of 1.898 and was responsible for explaining 11.048 percent of the variation. As a result of the high loading with the following components, The phrase "efficiency and security" was assigned to the third factor. Real time, enhanced transaction speed, improved efficiency, and system integrity are some of the features included in these components.

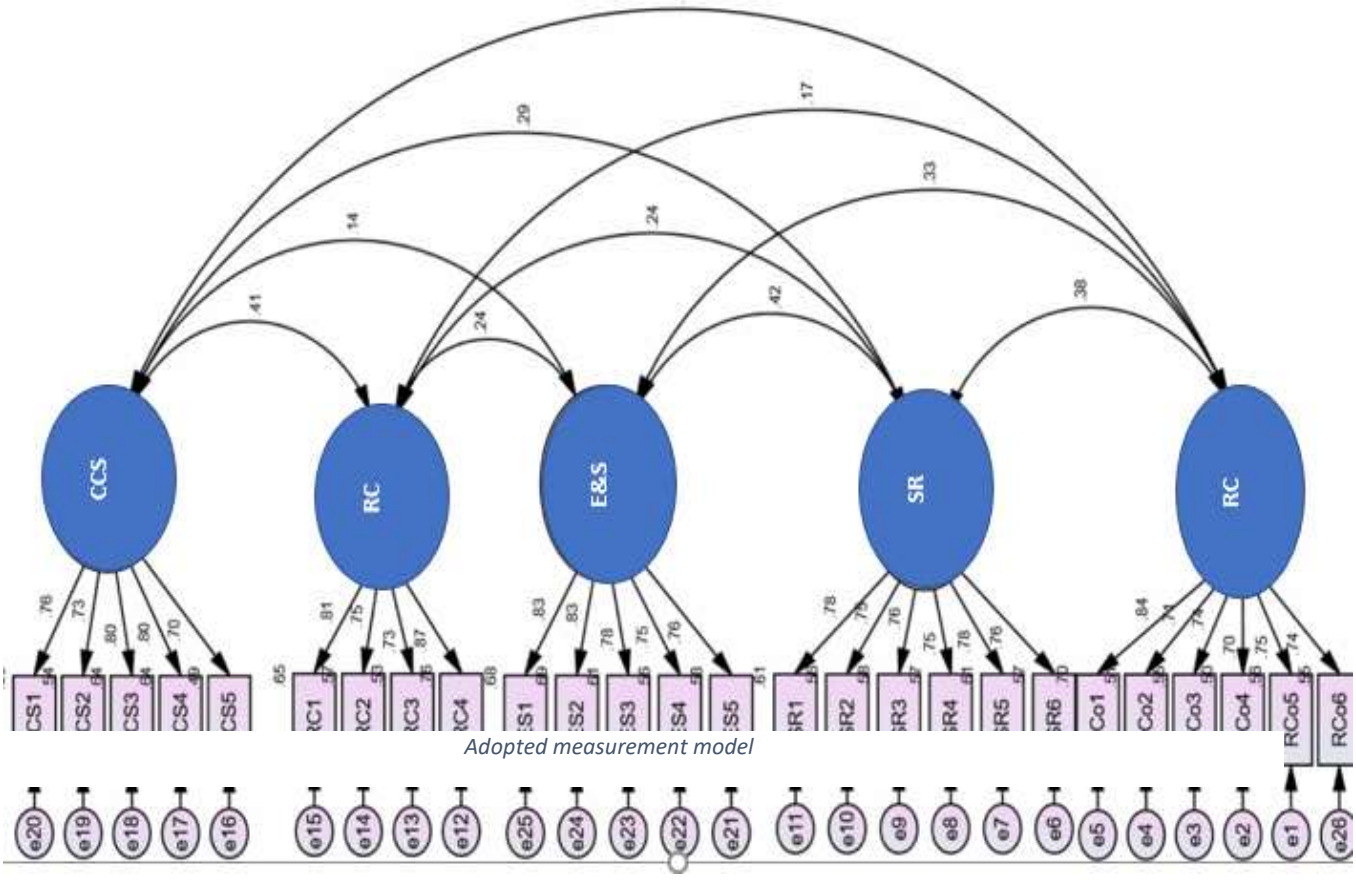
Table 1 Population classifications of respondents

POPULATION VARIABLE	CLASSIFICATIONS	RATE OF RESPONSE
GENDER	Male	76.63%
	Female	23.36%
AGE RANGE	35–45 years	52.67%
	25–35 years	47.33%
EDUCATION	MSC	43.00%
	B.E/B.Tech.	46.00%
	Business Graduate	12.00%
POPULATION	IT head of banks	14.00%
	BC Marketing experts BC consultants non classified reposndents	42.00%
		35.33%
		8.67%

Component 3 accounted for 13.657% of the variance and had an Eigenvalue of 2.66. Due to the high weighting of the following elements, Factor 4 was called "data integrity" Quicker settlements, increased traceability, immutable data record, more data management, increased robustness, and better system resiliency are all benefits of blockchain technology. This component's

Eigenvalue was 7.131, and it was responsible for explaining 15.077 percent of the total variance. Because it was substantially laden with the following elements, item 5 was prominently labelled "regulatory compliance." These items included smoothness of business process, decreasing fraudulent transactions, ensuring immutable business rules , data security and increasing regulatory compliance. This component has an Eigenvalue of 3.462, which indicates that it accounts for around 14.883 percent of the variance. To facilitate better understanding and to illustrate what their constituent parts imply, the five components have been developed.

F1: Customer Cyber Security (CCS): The elements in this category are connected to the advantages of high-quality customer service provided by the banking industry. F2: Cost Recudtion (RC): The components that make up this aspect are linked to the many benefits that come with having reduced expenses in the banking business.This component contains aspects that are associated to the advantages of efficiency and safety in the banking business. F4: Data Integrity for Safe Transfers: The components of this factor are tied to the benefits of safe transfers in the banking industry. F5: compliance regulatory (RC): The sub-factors that make up this factor are concerned with the positive aspects that come along with adhering to the regulations that govern the banking sector.



Adopted measurement model

Table 3

Table 2 Reliability and items loading.

CONSTRUCT	ITEMS	DESCRIPTION	STANDARD FACTOR LOADING	CRONBACH (A)	COMPOSITE RELIABILITY
CYBER SECURITY	CCS1	Blockchain technology will improve Customer Security	0.762	0.872	0.873
	CCS	Blockchain technology will increase trust	0.734		
	CCS 3	Blockchain technology will increase data accuracy	0.803		
	CCS 4	Blockchain technology will reduce the cyber risk	0.802		
	CCS 5	Blockchain technology will automate actions and transactions between parties	0.698		
REDUCED COST	RC1	Blockchain technology will reduce transaction cost	0.805	0.867	0.869
	RC2	Blockchain technology will eliminate interm ediaries	0.752		
	RC3	Blockchain technology will lower down administrative cost	0.726		
	RC4	Blockchain technology will lower down operational cost	0.870		
EFFICIENCY SECURITY	ES1	Blockchain technology will help in tracking real time business transactions	0.827	0.893	0.893
	ES2	Blockchain technology will increase speed of transaction	0.829		
	ES3	Blockchain technology will increase efficiency	0.784		
	ES4	Blockchain technology will enhance security	0.748		
	ES5	Blockchain technology will enhance the integrity of the system	0.764		
DATA INEGRITY SE CURE REMITTANCES	SR1	Blockchain technology will create an immutable audit trail	0.778	0.892	0.893
	SR2	Blockchain technology will ensure a fast and secure payment process	0.746		
	SR3	Blockchain technology will enhance system resilience	0.762		
	SR4	Blockchain technology will enhance robustness	0.753		
	SR5	Blockchain technology will increase the traceability of transactions	0.782		
	SR6	Blockchain technology will increase the control on data	0.758		
REGULATORY COMPLIANCE	RCo1	Blockchain technology will streamline the business process	0.837	0.883	0.885
	RCo2	Blockchain technology will ensure immutable businessrules	0.713		
	RCo3	Blockchain technology will prevent from financial fraud and tempering	0.742		
	RCo4	Blockchain technology will ensure data protection	0.704		
	RCo5	Blockchain technology will improve regulatory compliance	0.749		
	RCo6	Blockchain technology will reduce the error HANDLING AND RECONCILIATION	0.744		

tigate

5.2 Confirmatory factor analysis

CFA and AMOS 20 were used in the research that was done on the recommended measuring methodology. The purpose of this model

measurement is to evaluate the presence of an acceptable degree of construct validity and reliability before analysing the interrelationships of the constructs in the structural model.[15] Figure 4 is a representation of the final measurement model that highlights the numerous factors that influence the anticipated benefits of blockchain technology in banking operations. Indicator items with the numbers five, four, five, six, and six bring attention to constructions like as"Customer cyber security," "Reduced cost, efficiency, and security," " data integrity for Secure remittances," and "Regulatory compliance." The structure was confirmed by using CFA and EFA , and the components that are presented in Figure 4 were established via a process that began with qualitative research and was followed by empirical research . As a consequence of this, the five structures that point to the clear commercial advantages of incorporating blockchain technology in the banking and financial business were evaluated using 26 different indicators. In order to conduct research on the psychometric properties, the convergent and discriminant reliability of the measuring model were analysed.(see Table 3).

The statistic known as Cronbach's alpha is used in the process of computing internal consistency, which evaluates the reliability of the many different items that are included in the survey.(Streiner, 2003). Cronbach's alpha is a statistic that may be calculated by looking at the correlation between selected elements in a pairwise fashion. The values of Cronbach alpha might range anywhere from 0 to 1. To determine whether or not there is internal consistency, it is analysed according to the specific components of each construct(Table 3). It is generally accepted that a Cronbach alpha value between 0.6 and 0.7 represents the very minimum level of dependability required, and that it should be more than 0.7 to indicate an especially high level of dependability.[16].

It was discovered that the different constructs that were included into the measurement model have an acceptable degree of internal consistency, with alpha values of 0.872 for "client cyber security," 0.867 for "reduced cost," and 0.893 for "efficiency and security," respectively. 0.882 for "data integrity secured remittances," and 0.893 for "regulatory compliance." As a consequence of this, the included measures were judged to be reliable, and it is possible that they will be used in structural equation modelling (SEM) in further research. Covariance-based structural equation modelling was used in our analysis since this

method offers more verifiable characteristics and, as a result, less bias in the calculated model.[17].

The reliability and convergent validity of a concept inside a measuring model may be evaluated with the use of a statistic called composite reliability (CR). It offers a measurement that is more indicative of overall dependability and computes the regularity of the construct itself, including its hardness and similarity, among other characteristics.[18]. If the CR score is more than 0.7, this indicates that there is sufficient dependability in the scale. According to Table 3, the overall dependability of "customer cyber security" is 0.873, while the dependability of "reduced cost" is 0.869, the dependability of "efficacy and security" is 0.893, the dependability of "data integrity for Secure remittances" is 0.893, and the dependability of "Regulatory compliance" is 0.885. As a consequence of this, the overall reliability of each construct in the proposed model is greater than 0.70, which indicates that all constructions reflecting the perceived advantages of blockchain technology adoption in banking operations that are examined in the model have a high degree of reliability.

The degree to which individual items converge or if there is a significant amount of overall disagreement is indicated by a construct's convergent validity.[18]. When evaluating convergent validity, standardised idea loadings are frequently used as a tool. High standardised build loadings provide the impression that the pieces of the construct are significant and provide a good illustration of their construct. It is required that the standardised construct loadings be higher than 0.50 in relation to their observed variables.[18]. According to Table 3, the measured variable loadings fell somewhere in the range of 0.7 to 0.87. The findings indicate that the objects that were seen are sufficient and provide an accurate representation of their structures. As a consequence of this, we are able to guarantee that the rationality of constructions converges.

The degree to which one concept is distinct from others is indicative of the discriminant validity of the construct in question.[18]. Researchers use two different methods to evaluate the discriminant validity of their tests. The first factor is the correlation coefficient between the various construct pairings in the measurement model, which ought to be low due to the fact that the constructs in question are conceptually distinct from one

another. This is due to the fact that different collections of objects are used in the measuring of various projects. These things are supposed to be different from one another, and as a result, they shouldn't be overly tied to one another[19].

Table 3 Correlation Matrix

	QCS	RC	S & E	SR	RC
Cyber Security Customer Prespective	0.761*				
Reduction in cost	0.407	0.790*			
Security & Efficiency	0.143	0.242	0.791*		
Data Integrity SR	0.289	0.236	0.418	0.763*	
Regulatory compliance	0.164	0.167	0.329	0.382	0.749

Table 3 shows that there is a weakly positive correlation between "cyber security customer prospective" and "reduced cost," "efficiency and security," "secure data for remittances," and "regulatory compliances" (0.407, 0.143, 0.289, and 0.164, respectively). On the other side, "reduced cost" is not strongly associated with "efficiency and security," "data for safe remittances," or "regulatory compliance" (0.242, 0.236, and 0.167).In a similar vein, there is a tangentially beneficial relationship between "efficiency and security," "data for safe transfers," and "regulatory compliance" (0.418 and 0.329). In conclusion, there is some evidence that "data for safe remittances" and "regulatory compliance" are connected in a beneficial way (0.382). The fact that there is no association between the components suggests that the constructs that make up the model are all separate from one another. In addition to this, the AVE calculations demonstrate that the individual constructs have greater variations than the common variances of the constructs (See Table 3). In addition to this, the square root of the AVE for diagonal configurations is greater than it is for non-diagonal

ones.(Table 4). These results suggest that each construct in the measurement model is intimately associated with its components, particularly when compared to other constructs in the model. [Citation needed] As a consequence of this, discriminant validity could be uncovered in the measuring model that was proposed. Several model fit indices, including the normed fit index (NFI), the goodness of fit index (GFI), the root mean square error approximation (RMSEA), the comparative fit index (CFI), and the Tucker-Lewis Index, were used in order to evaluate the model's overall validity (TLI) Indicators of how well the measurement model fits the data are shown in Table 4.

Table 4

Summary of model fintness

Model Fitness	**DF/Ch1**	**GFI**	**CFI**	**TLI**	**NFI**	**RMSEA**
Model 1	**1.604**	**0.895**	**0.956**	**0.951**	**0.893**	**0.046**

6 Discussion

The goal of this study is to develop and validate a technique for determining the perceived benefits of using innovative blockchain technology in the banking sector with regard to maintaining data integrity and preventing cybercrime. In order to provide better insights for improving the things, it has been put through a stringent and systematic review, and information has also been collected via contacts with blockchain professionals. This was done in order to improve the products. Following the completion of the literature study, our team came up with a list of 42 criteria that were used to the qualitative analysis. The relevance of twenty-six of the forty-two components was established with the assistance of the technique for purification and the iterative instrument development.After making use of the proper concepts and scale development approaches, the items were organised into the following five constructs: "CCS", "RC", "ES", and "SR" and "RCo". Following an analysis of the findings of the data, we categorised each of the presumed advantages to the organisation. Maintaining the safety of one's clientele is essential to the prosperity of any business. The notion of "great data security for clients" may inspire new kinds of services to be developed by financial institutions, which may be provided to customers utilising blockchain

technology. This architecture consists of five different components, each of which has the potential to greatly enhance customer service in one of the following five ways: by enhancing transparency and trust; reducing risk; automating formerly manual processes; or all of the above. Implementation of blockchain technology within the banking sector will result in improved customer service by supplying client records that are risk-free, tamper-proof, transparent, trustworthy, and accurate.

One of the obvious operational advantages of incorporating blockchain technology into a financial system is a reduction in the amount of money spent on overhead expenditures. By using blockchain technology, financial institutions are able to cut down on their overhead expenditures and significantly reduce costs, which may be based on the concept of decreased costs. The advantages afforded by this design are as follows: decreased administrative expenditures, decreased transaction costs, eliminated need for middlemen, and decreased operational costs. When used to the banking sector, blockchain technology will eliminate the need for middlemen, which will lead to a reduction in the expenses associated with administrative and operational transactions. It is essential for there to be both security and efficiency in the functioning of financial systems. Using the "efficiency and security" notion as a foundation, blockchain technology may be used to the creation of secure and effective methods for conducting financial transaction exchanges.

The concept is predicated on the following five components: greater transaction speed, real-time processing, increased efficiency, an enhanced security system, and guarantee of data integrity. Real-time access, quicker processing of paperwork, and faster transaction rates will all be made possible inside the bank as a result of the implementation of secure single blockchain networks. These improvements will all assist to ensure the bank's integrity. Another challenge for the banking industry is providing safe remittances, and the disruptive technology of blockchain might be very advantageous in terms of faster settlements, more traceability, immutable data records, stronger data control, improved robustness, and enhanced system resilience.[20]. One further benefit of using blockchain technology in financial institutions is that it guarantees regulatory compliance requirements are satisfied in an effective and efficient manner. The "regulatory compliance" architecture has the potential to be

improved with the use of blockchain technologies, which have the ability to improve private regulatory compliance. As a consequence of this, it may help to speed up the operations of the organisation, decrease the number of fraudulent transactions, and boost regulatory compliance, all while preserving data. The first question posed by the survey is answered by this group of perceived operational advantages.

In addition to the apparent advantages, the financial services sector could also be able to provide enhanced products in response to rising consumer and market demand via the money cycle that the bank facilitates. The fulfilment of contractual obligations may be monitored using blockchain technology improvement methods. This allows for the resolution of complicated financial asset transactions that are constrained by an incorruptible set of commercial standards. Each transaction is encoded before it is put to the distributed ledger so that the safety and security of every participant may be maintained. The financial system may be assisted in the modernization of the payments supply chain by a worldwide network of blockchain technology. This will reduce the risk of a failure occurring as a result of clearly defined rights, controls, obligations, and standards.

7 Conclusion

Among the steps for certifying our research were a comprehensive analysis of the prior literature (to ensure the legitimacy of the material), as well as an evaluation by a board consisting of blockchain academics and experts (for face validity).In addition to this, we submitted the prepared questions to three academics and five blockchain specialists to see whether or not their points of view were consistent with those of the respondents. During the pilot testing, it was determined that both the idea and the content validity were high. The fabricated musical instrument may be broken down into five distinct forms, each of which is made up of 26 individual parts. A validation Likert scale with seven points is included in each question. This electronic device is quite dependable in its operation. For the purpose of verification, we conducted interviews with 291 blockchain technology experts, blockchain implementation professionals, and European bank IT chiefs. The study's analysis and findings suggest that the instrument used to assess commercial and operational advantages is extremely reliable and displays construct validity by achieving

both convergent and discriminant validity. The theory behind blockchain technology, as well as its use in the financial sector, may benefit from our results. Our investigation provides a tried-and-true tool that executives in the financial industry may use to evaluate the potential benefits of blockchain technology from a theoretical standpoint.

This instrument was developed specifically for the financial services sector. However, a part of the benefits may be applicable to a variety of enterprises due to the fact that the study includes advantages observed by working chiefs, subject matter experts, and professionals in the area of blockchain technology..

The following is a list of the main concerns raised by the review: (I) Before deciding whether or not to implement blockchain technology into their banking system, acting managers, decision makers, and other experts are particularly interested in receiving a fundamental perspective that will allow them to evaluate the business benefits of utilising blockchain technology.

(ii) Because it incorporates both practical and theoretical application, the research is significant not only to the community but also to the field of study. In addition, a financial ecosystem's requirements may be tailored to the capabilities of blockchain, which would further reduce the expenses associated with its deployment. The limitations of the research include its sample size as well as its geographical location. The validity of the instrument was determined by analysing data from 291 different sources. The sample size may have been larger if more researchers had been conducted this study.

References

1. Chen, K.Y., A Systematic Approach for Cybersecurity Risk Management. 2021, Massachusetts Institute of Technology.
2. Elgamal, A.H., et al., Optimization of a multiple-scale renewable energy-based virtual power plant in the UK. Applied Energy, 2019. **256**: p. 113973.
3. Chen, Y. and C. Bellavitis, Blockchain disruption and decentralized finance: The rise of decentralized business models. Journal of Business Venturing Insights, 2020. **13**: p. e00151.
4. Joo, M.H., Y. Nishikawa, and K. Dandapani, Cryptocurrency, a successful application of blockchain technology. Managerial Finance, 2019.

5. Ozili, P.K., Blockchain finance: Questions regulators ask, in Disruptive innovation in business and finance in the digital world. 2019, Emerald Publishing Limited.
6. Jaag, C. and C. Bach, Blockchain technology and cryptocurrencies: Opportunities for postal financial services, in The changing postal and delivery sector. 2017, Springer. p. 205-221.
7. Xie, J., et al., A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Communications Surveys & Tutorials, 2019. **21**(3): p. 2794-2830.
8. Morabito, V., Business innovation through blockchain. Cham: Springer International Publishing, 2017.
9. Salman, T., et al., Security services using blockchains: A state of the art survey. IEEE Communications Surveys & Tutorials, 2018. **21**(1): p. 858-880.
10. Garg, P., et al., Measuring the perceived benefits of implementing blockchain technology in the banking sector. Technological Forecasting and Social Change, 2021. **163**: p. 120407.
11. Broadbent, E., et al., The brief illness perception questionnaire. Journal of psychosomatic research, 2006. **60**(6): p. 631-637.
12. Cronbach, L.J., Coefficient alpha and the internal structure of tests. psychometrika, 1951. **16**(3): p. 297-334.
13. Watkins, M.W., A step-by-step guide to exploratory factor analysis with SPSS. 2021: Routledge.
14. Iacobucci, D., Structural equations modeling: Fit indices, sample size, and advanced topics. Journal of consumer psychology, 2010. **20**(1): p. 90-98.
15. Ifinedo, P., Extending the Gable et al. enterprise systems success measurement model: a preliminary study. Journal of Information Technology Management, 2006. **17**(1): p. 14-33.
16. Baldwin, S.A., M.J. Larson, and P.E. Clayson, The dependability of electrophysiological measurements of performance monitoring in a clinical sample: A generalizability and decision analysis of the ERN and P e. Psychophysiology, 2015. **52**(6): p. 790-800.
17. Qahri-Saremi, H. and A.R. Montazemi, Factors affecting the adoption of an electronic word of mouth message: A meta-analysis. Journal of Management Information Systems, 2019. **36**(3): p. 969-1001.
18. Hair, J.F., et al., Multivariate data analysis . Uppersaddle River. 2006, NJ: Pearson Prentice Hall.
19. Bollen, K. and R. Lennox, Conventional wisdom on measurement: A structural equation perspective. Psychological bulletin, 1991. **110**(2): p. 305.

20. Wamba, S.F. and M.M. Queiroz, Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities. 2020, Elsevier. p. 102064.