National College of Ireland

Understanding the impact of Blockchain Technology in shaping future for Business Cyber-Security.

MSc Research Project
MSc in Cyber Security

Prathmesh Tambe
Student ID: x22244182

School of Computing
National College of Ireland

Supervisor: Mark Monaghan

Table of Content

Introduction

Background

Blockchain technology is a distributed database that stores and records transaction dated on several computers hence providing a high level of security, transparency and once recorded cannot be altered. Each transaction or 'block' occurs in a set time and it is connected to the preceding block hence making it a 'chain' (Saeed et al., 2023). These prospects eradicate the risk of several control mechanisms per central authorities thus making a network hard to manipulate. Stacks' significance is in improving security and confidence in specific uses. For the business, it offers a reliable ground for any transactions which shields data from unauthorized access by hackers. Blockchain transparency makes all the participants be able to view and check all the transactions and encourage more accountability (Demirkan, et. al, 2020).

Moreover, the long-term and complete digital contracts, smart contracts, that contain the terms of the agreement encoded, minimize human influence and time. In addition to finance, blockchain technology is disrupting supply chain, healthcare, identity in variety of applications (Miracle, 2024). That it can produce better security, clarity and efficiency in systems defines why it is such a vital tool in the production of the kind of world that business and technology will create.

Problem Domain

Though legacy centralized systems have been implemented in many organizations, they are becoming more vulnerable to cyber threats such as, hacking, data theft, anonymity, and the likes which results to high losses and compromises organizational stand (Etemadi et al., 2020). I have seen these centralized systems which are controlled from a single point; it is from this that hackers feast on. In addition, the current security mechanisms offer little visibility and Governance into security breaches hence posing significant challenges to the detection and prevention of such incidents (Prakash et. al, 2022). The approach to be taken in the study would be to understand how these properties of blockchain can help improve the modality, security and automaticity of the processes that are affected by the aforementioned problems (De Nicola and Raja, 2022). Thus, the study will examine the possibility of applying blockchain in an effort to contribute to the creation of better and stronger cybersecurity models for business management.

Aim and Objectives

The aim for the study is to understand the impact of Blockchain Technology in shaping future for Business cyber-Security.

The objectives for the study are;

- To evaluate the present state of cybersecurity practices in Businesses
- To identify common problems which blockchain technology could address for enhancing entire security concerns.
- To assess the practical implementation as well as benefits of Blockchain technology in business security

Rationale

The justification for analysing the influence of blockchain technology on the business cybersecurity comes from the increased intensity and complexity of the cyber-incidents threatening the business information. The conventional security strategies are proven inadequate when handling the breaches resulting to heavy losses both financially and in terms of reputation. Such characteristics of blockchain technology as decentralisation, impossibility to change data and openness of transactions are viewed to mitigate these challenges (Tibrewal, et. al, 2022). With decentralization, lack of a single point that can be hacked or modified, and the impossibility of changing data without its being noticed, blockchain will improve the protection of business processes. Also, they eliminate some of the human errors and possible loopholes in security since security measures involve smart contracts. The purpose of this research is to identify how and in what manner' blockchain is already being utilized to address cybersecurity challenges and to analyse the direct advantages that are available to business in their attempts to protect their digital assets. It is imperative to know how blockchain can transform the world of cybersecurity in order to improve defence initiatives and construct a safer business landscape.

Literature review

Evaluate the present state of cybersecurity practices in Businesses

According to Lee and Kim (2021) in the modern world where organization activities are done through the Internet, cyber security has become an important component of the organizations. In the current world, the number of threats, and the level of sophistication of these threats are on the rise and this has put a lot of pressure on businesses to protect their critical assets such as data, IT systems, and networks. Cyber threats are evolving and cyber criminals are employing various strategies such as phishing, ransom ware, advance persistent threats and so on. In addition, Chidukwani et al. (2022) these attacks can be very destructive and impact the organization through loss of data, funds and damage to reputation. The nature of these threats is such that they are likely to be subtle to be unveiled, which makes them an unending headache to business organizations. The parameters of the risk picture also indicate that, despite growing awareness, human error is still a chief Cybersecurity threat. In this context, even the workers can make a mistake and click a link, use unsafe password and do not obey security measures.

In addition, as per Khan et al. (2022) despite the most rigorous training and constant awareness campaigns, most employees are a vulnerability to any organisation's security. Technological development is good but fast and this is a two-edged sword. The IT revolution and introduction of other new technologies add value to the business operations but come with other risks. Organizations fail to apply the latest security updates as and when released hence expose their business to the risk of getting attacked. Also, more and more rules appear regarding data shield and privation like GDPR or CCPA which businesses need to meet. It can be resource demanding and difficult especially for SMEs, to make sure that the set compliance is achieved.

Today's businesses are choosing a layered security strategy, where multiple security levels are put up in one business. These are the firewalls, intrusion detection systems (IDS), the antivirus and the encryption (Uchendu et al., 2021). This way, firms seek to achieve a cumulative effect, meaning that by applying multiple layers of defences businesses get an enhanced security environment. Understanding that factors such as human fault contribute towards cyber threats, organizations are focusing on preparing their personnel. These programs inform the employees on the new threats and how to handle them, for instance, dealing with phishing and ways of creating and using passwords. Incident response plan for a cyber-attack is essential to ensure that its effect is reduced to the barest minimum. Enterprises are creating and refining the guidelines of what should be done in the case of data loss, included in incident response plans. As per the work of Taherdoost (2022), these are the phases of threat management that involves threat identification and isolation, communication of the threat to those affected, and recovery of the affected systems. Modern technologies like artificial intelligence, (AI) and machine learning (ML) are being used to improve cybersecurity. In addition, as per Demirkan et al. (2020) these technologies are useful to decide big amounts of data to define irregularities that could suggest a cyber threat. Among the biggest advantages of threat intelligence automation, there is the faster reaction to threats.

According to Habib et al. (2022) the concept of the Zero Trust security model is becoming rather popular as a method of improving cyber protection. Technology such as the blockchain has the potential of enhancing the general aspect of cybersecurity. Its decentralised and also non-modifiable characteristic provides inherent protection against the data manipulation by attackers. Blockchain can bring benefits in terms of transparency, traceability of events, and safety helping different sectors and industries such as the supply chain management and the digital identities (Saeed et al, 2023) Due to the evolution of cybersecurity attacks, several organizations are considering Cybersecurity as a Service providers. These providers provide MSS – managed security services which include threat intelligence, incident handling, and penetration testing. This means that a business can tap a specific field of specialization and obtain vital resources it may not otherwise have the capacity for. More and more organisations are facing data breaches which in turn increases the focus on data privacy (Ghelani, 2022). There is heightened awareness in businesses' data protection where specific measures like encryption and anonymization of data are observed. Besides, they are extending privacy by design principles that imply the inclusion of data protection actions at the stage of creating products and services.

Analyse the Features and Mechanisms of Blockchain Technology

Blockchain is a distributed digital ledger that has brought great changes to the sphere of storing, safeguarding, and validating the data (Gurdgiev and Fleming, 2021). This system runs in a multi-node environment; therefore, there is no central point of failure as seen in the centralized systems. The work of Zeng et al. (2020) discusses every node contains the whole copy of the blockchain and all nodes approve the transactions, which makes the network immune to the attacks and prospective alteration of the data. Its major characteristics like decentralization, its ability to not be altered, and the ability for the public to verify it make it stronger. In addition, as per Ruan (2023) the application of cryptographic hash and consensus algorithms keeps transaction records unchangeable and tamper-proof is

accomplished through cryptographic hashing and consensus mechanisms. Transparency entails that all the parties involved have an opportunity to look at the transactions in other parties in a ledger hence providing an independent means of verification and indeed auditing.

According to Garg et al. (2021) different consensus algorithms are used in blockchain and the most typical ones are the proof of work and the proof of stake. In PoW miners are involved in solving the difficult mathematical problems to add the new blocks, it demands a large processing power but offers greater security. In PoS, the choice of the validators is dependent on how many tokens the validators are willing to stake they offer higher security and less energy consumption. Last but not the least; smart contracts–program code embedded in the blockchain protocols that contain the terms of an agreement that are also coded, to eliminate the need for middlemen and to cut off the possibilities of cheating. The work of Lim et al. (2021) has characteristics make blockchain quite versatile as an instrument of improving security, lack of opacity, and effectiveness in various application fields ranging from the financial sector to supply chains.

Nevertheless, this book revealed that blockchain technology has limitations such as scalability and interoperability. The topic of scalability describes the ability of a cryptocurrency to handle more and more transactions and is currently solved through techniques like sharding, off-chain solutions, and Layer 2 solutions. The addition of work Zhu et al. (2021) have discussed about smart contracts is a blockchain interchangeability that is a method of allowing different blockchain networks to share information with each other and has seen cross chain protocols and standard frameworks to boost this. Cryptographic security with using public and private keys in the construction of blockchain and its decentralized nature make it very hard to hack and perform frauds. However as per Idrees et al. (2021), in attaining ubiquitous acceptance on blockchain technology, these issues of scalability as well as interoperability, have to be solved. All in all, the fundamental elements and processes of blockchain give it effective solutions for strengthening the security, effectiveness, and credibility of various applications to drive positive change in the modern digital world.

Assess the practical implementation as well as benefits of Blockchain technology in business security

The concept of applying the blockchain solution in business security entails a number of certain procedures and it has many advantages that greatly improve the security conditions of numerous enterprises. The work of Idrees et. al. (2021) has showcased the process of using blockchains starts with comprehending its fundamental concepts and choosing the proper type of blockchain – public, private, or consortium to fulfil the enterprise needs. Some types of blockchain are public, like Bitcoin and Ethereum, which means that they are as transparent and safe as possible but they take more resources. Consortium and private blockchain offer more control and are more appropriate for business use to achieve higher transaction speed and increased privacy.

The process usually comprises the adoption of service-oriented architectures where blockchain interacts with the existing systems via APIs and middleware. Smart contracts on the other hand are executed to achieve specific operations and regulate functioning based on set programs without the intervention of the individuals (Zidan et al., 2023). For example, in the supply chain, the contract can be programmed to release payment when goods are at a particular stage. Entities also require a governance structure that also fixes permissions and roles for the permit action in the blockchain system. The work of Feng et al. (2020) effective key management procedures that involve the use of effective access keys to Blockchain assets are also crucial. Another advantage of using the blockchain technology in business security is that it increases the data accuracy and discourages its alteration. The permanency of the record immobilises data from being amended or deleted since the blockchain technology is majorly based on a definite record.

Compared to the centralized architecture where usually there are weak links in the system, Blockchain has minimal or almost no single point failure element, due to its distributed structure. In a decentralization network, data is processed in many different nodes so that even if a single node is infiltrated the whole network will not be overrun (Mark and Joe, 2024). It is important for the business to minimize the vulnerability of such information from hackers and maintain the operations of the business when the hacking attempt occurs. Additionally, blockchain can help eliminate paper records and automate identity check since. Blockchain allows for the creation of secure and tamper-proof digital identity which will minimize identity theft and only authorized persons would have access to important information. The third beneficial aspect of blockchain implementation is the financial aspect, and more specifically the cost-effectiveness aspect. Speaking of the improved business operations due to the smart contracts' usage, the elimination of middlemen and the automation of various operations seem to contribute to the decrease in business costs and the increase in productivity (Abu-Elezz et al. 2020). For instance, in a financial industry, Blockchain

technology is capable of enabling cross border fast and cheap compared to banking sectors. In SCM it will increase the level of accuracy and decrease length of time it takes to complete a transaction hence cut costs.

Therefore, it can be stated that the application of blockchain technology in business security is quite intricate, and it is necessary to take into account certain factors and coordinate the employed technology with the current business systems (Safitra et al., 2023). The advantages such as, improved quality of the data, decreased amount of fraud, distributed safeguard, easy identification process, and less cost makes the blockchain as a strong tool for business who wants to upgrade their security measure and productivity. Technology is gradually advancing and thus its integration is likely to grow in the future cutting across different sectors.

Research Methodology

The following is the study's research method which describes the scientific approach adopted in this study to analyses the effect of blockchain technology to business cybersecurity. The approach used in the paper is both qualitative, and quantitative, which allows for the richest impact of the given subject.

Research Philosophy

The research is justified within the framework of such an epistemology as pragmatism which recognizes that the studied phenomenon is infinitely multifaceted and requires the use of various research methodologies (Leng et al., 2020). Thus, pragmatism aligns well with this research approach because it deals with real-life results and their practical use, which is suitable for considering the rapidly developing sphere of blockchain in cybersecurity. This view implies that the provision of mixed results is useful to present a broader picture based on the purpose of blockchain for practical applications of businesses.

Research Approach

This study uses qualitative data with the integration of deductive and inductive approaches. Hypothesis testing is done within the context of the deductive research approach, whereby the review of the literature involves the analysis of the different theories and frameworks existing within the context of blockchain and cybersecurity. It formulates specific hypotheses and directs the survey design while conducting this review. At the same time, an inductive technique is used to dissect the survey data, which helps to describe new patterns and make additional observations that enhance comprehension of the research issue.

Data Collection

Data collection for this study involved two primary sources: Admittedly, the two studies comprised of a literature review and an online survey. The literature review was carried out using a review of published studies, conference papers, white papers, and industry reports (Taherdoost, 2021). It was useful that this secondary data gave a theoretical framework and background to the context by which primary research methodology and identification of its themes and holes could be distinguished. An online survey was developed with 15 questions; the research questions focused on perceptions, experience, and opinion on the application of blockchain in improving business cybersecurity. Thus, the obtained 132 valid responses represent a sample derived from a population of cybersecurity professionals, IT managers, and business leaders. After carrying out a literature review, the questions that were created were in line with the research objectives.

Data Analysis

Comparing the two contexts, the data analysis process included both quantitative and qualitative methodological approaches. Content analysis on survey responses was done using descriptive statistics The results were analyzed to provide key findings. Frequency tables, percentage analysis, and cross-tabulations were then used in the analysis of the respondent's perception of blockchain as a cybersecurity solution. Concerning the qualitative data analysis, the open-ended responses were analyzed using thematic analysis. This entailed processes of coding and analysis of the data to look for patterns in the participants' perceptions about the benefits, limitations, and possibilities of blockchain technology in cybersecurity. The combination of both analytical and narrative data enabled the researchers to create a complex picture of the investigated question.

Ethical Consideration

The focus was placed on the ethical issues in the course of the research from the beginning. All persons completing surveys were briefed on the research study and its intent or purpose and signed consent forms that provided them with their rights as participants such as their right to withdraw from the study at any time. The survey filled did not require participants to reveal their identity; thus, the survey ensured that the participants' identity was not revealed. Also, the study followed the standards and guidelines on data management and analysis in research wherein all the collected data were secured and privy only to the research team. The statistics were represented with accuracy and honesty and any possibility of bias or presentation of the data in a favorable/unfavorable light of our research methodology was never considered.

Data Analysis

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not familiar at all	3	2.3	2.3	2.3
	Not very familiar	6	4.5	4.5	6.8
	Somewhat familiar	13	9.8	9.8	16.7
	Very familiar	110	83.3	83.3	100.0
	Total	132	100.0	100.0	

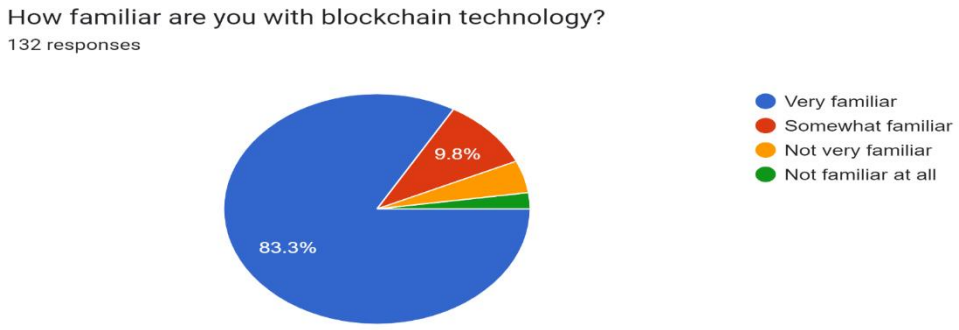

Figure 1: Response of question 1

It is easy to determine the amount of knowledge that the respondents had with blockchain technology by looking at the table. Due to the fact that the majority of the individuals in the sample (83.3% of them) are highly acquainted with the contents of the sample, it would seem that the individuals who are a part of the sample have a greater degree of knowledge or use. The percentage of people who are completely unfamiliar with the topic is just 2.3%, while 4.5% are only marginally unfamiliar with it. The percentage of persons who have a moderate degree of acquaintance with the subject is just 9.8 percent. As can be seen from the cumulative percentage, this group has a significant amount of interest in blockchain technology. This interest reflects a clear trend of acquiring a grasp of how blockchain technology operates.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	24	18.2	18.2	18.2
	Not sure	2	1.5	1.5	19.7
	Planning to	13	9.8	9.8	29.5
	Yes	93	70.5	70.5	100.0
	Total	132	100.0	100.0	

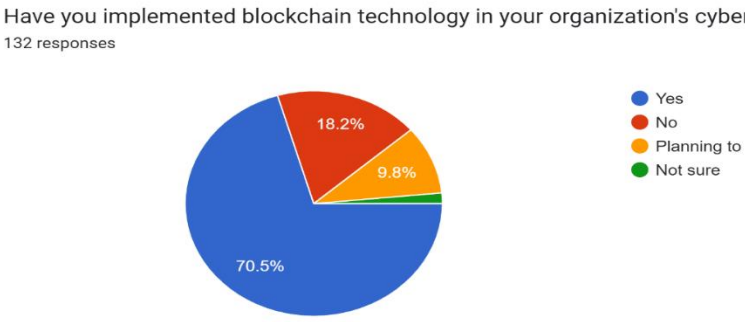

Figure 2: Response of question 2

The information that is shown in this table indicates that a large fraction of respondents has used blockchain technology, with 75% of them having successfully accomplished such an undertaking inside their respective organizations. There are also 18.2% of individuals who have not yet embraced it, while 9.8% of people have the intention of doing so in the near future. The present condition of its implementation is something that just 1% of people are currently uncertain about. Taking into consideration these findings, it would seem that blockchain technology is being widely embraced in commercial settings, with just a small percentage expressing concerns about its application or choosing not to use it.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Enhanced data integrity	88	66.7	66.7	66.7
	Improved transparency	26	19.7	19.7	86.4
	Reduced fraud and tampering	18	13.6	13.6	100.0
	Total	132	100.0	100.0	

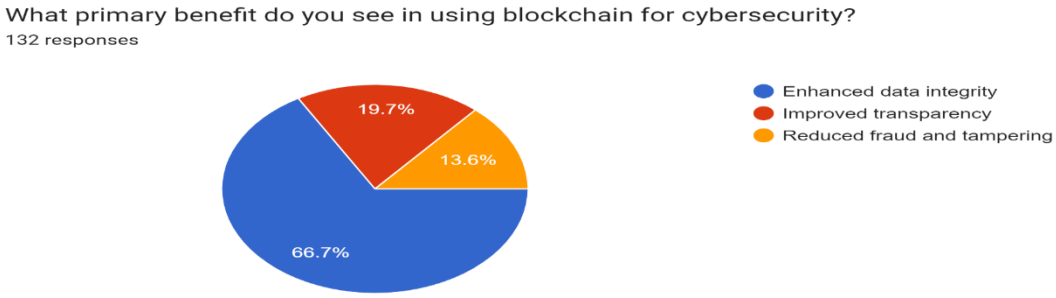

Figure 3: Response of question 3

When questioned about the benefits of using blockchain technology for cybersecurity, 66.7% of respondents selected greater data integrity as the key benefit of using this technology. This occurred when they were asked about the advantages of using this technology. 27% of those who have examined the advantages say that increased transparency is the most significant, while 13.6% believe that reduced instances of fraud and meddling are the most essential among the benefits. However, the distribution shows the significance of data integrity as a critical component for blockchain's attractiveness in the area of cybersecurity. This is despite the fact that the openness of blockchain technology and its capacity to prevent fraud are generally regarded as two of its most important features.

		Frequency	Percent	Valid	Cumulative

				Percent	Percent
Valid	Data security	85	64.4	64.4	64.4
	Financial transactions	27	20.5	20.5	84.8
	Identity verification	5	3.8	3.8	88.6
	Supply chain management	15	11.4	11.4	100.0
	Total	132	100.0	100.0	

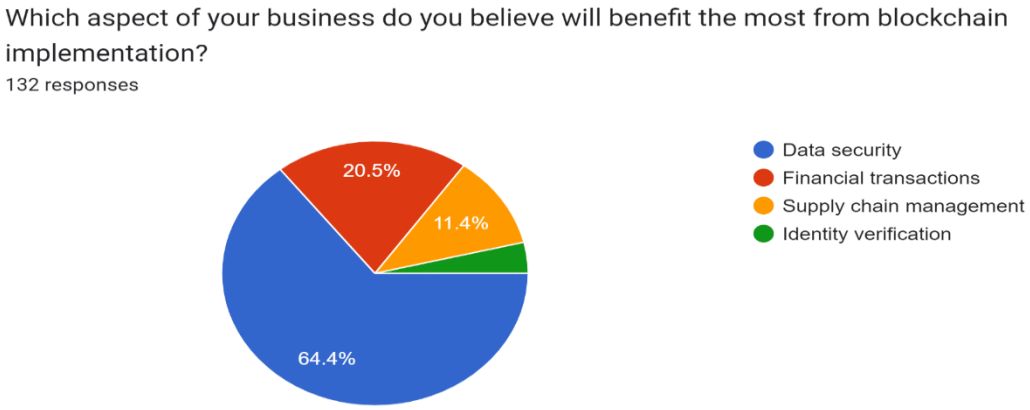

Figure 4: Response of question 4

It is clear from the image that 64.4% of respondents feel that blockchain technology will be the most effective in improving data security. This illustrates how vital people perceive it to be for the purpose of security. In spite of the fact that 25% of respondents felt that financial transactions are the most major benefit, 11.4% said that identity verification was more important, and 3.8% believed that supply chain management was less important. The findings give proof that there is a significant correlation between blockchain technology and enhanced data security when compared to other technologies.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Complexity of integration	35	26.5	26.5	26.5
	High costs	75	56.8	56.8	83.3
	Lack of expertise	21	15.9	15.9	99.2
	Regulatory uncertainties	1	.8	.8	100.0
	Total	132	100.0	100.0	

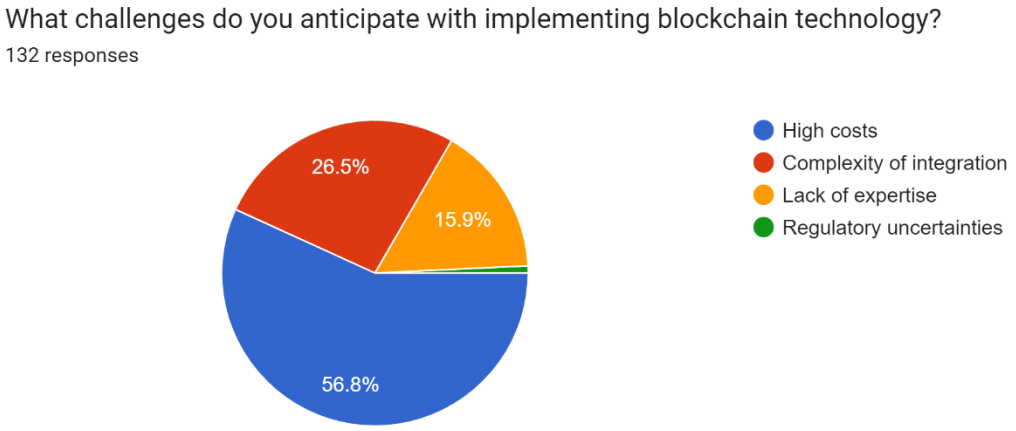

Figure 5: Response of question 5

According to the information shown in the table, 56.8% of those who participated in the survey cited high cost as the most major expected obstacle to the use of blockchain technology. In addition, 26.5% of those who participated in the survey are very worried about the difficulties of the process of integrating. Concerns about regulatory issues are the cause of worry for the least number of respondents, which is 8%. A lack of understanding is a source of anxiety for 15% of those who responded to the survey. According to these results, the bulk of the difficulties that are related with the deployment of blockchain technology are of a technical and financial character.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Extremely important	80	60.6	60.6	60.6
	Moderately important	16	12.1	12.1	72.7
	Not important	4	3.0	3.0	75.8
	Very important	32	24.2	24.2	100.0
	Total	132	100.0	100.0	

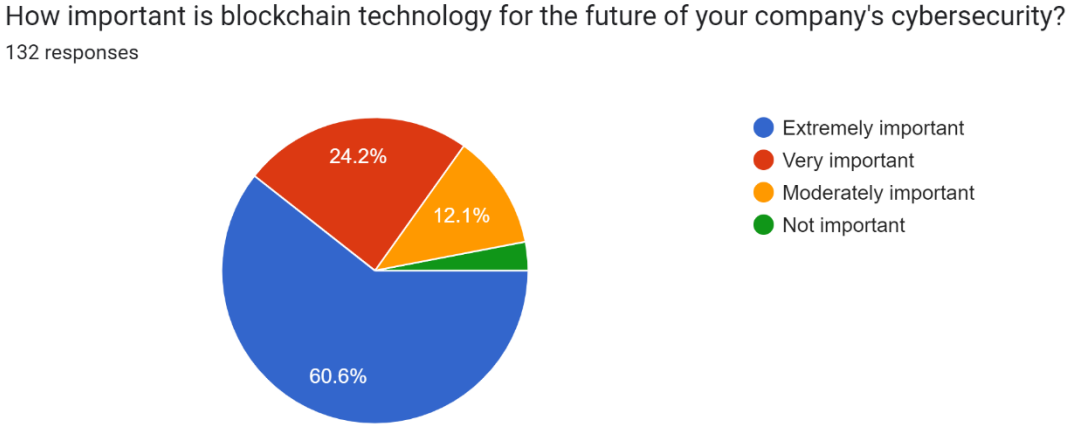

Figure 6: Response of question 6

According to the data shown in the table, sixty-six percent of persons are of the opinion that blockchain technology will be a vital component to the success of their company in the years to come. A further 24.2% of individuals are of the opinion that it is of utmost significance, while 12.1% are of the opinion that it is of considerable significance. A mere 3% of individuals are of the opinion that it is of no significance. The results of the survey indicate that these companies are totally in agreement with the notion that blockchain technology will play a big role in the plans that they want to put into action in the future.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Data privacy	33	25.0	25.0	25.0
	Energy consumption	17	12.9	12.9	37.9
	Lack of interoperability	2	1.5	1.5	39.4
	Scalability issues	80	60.6	60.6	100.0
	Total	132	100.0	100.0	

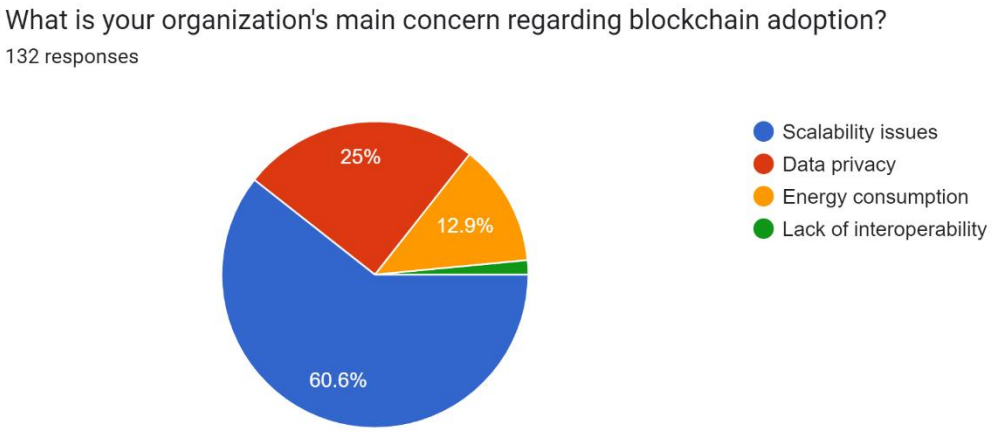

Figure 7: Response of question 7

As far as the use of blockchain technology is concerned, the research suggests that sixty-six percent of respondents are worried about the scalability of the platform. 12.9% of respondents are concerned about the amount of energy they use, and the next most common issue is the security of one's data, which accounts for 25% of respondents. Only 1.5% of the issues are brought on by incompatibility with other systems, which is one of the many issues that might arise. Taking into consideration this distribution, it is evident that companies who are using blockchain technology are concerned about a range of issues. The most important of these issues are associated with the difficulties that are associated with technology; nevertheless, problems pertaining to privacy and the environment also play a considerable influence.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	6	4.5	4.5	4.5
	Unsure	1	.8	.8	5.3
	Yes, significantl	83	62.9	62.9	68.2

	y				
	Yes, to some extent	42	31.8	31.8	100.0
	Total	132	100.0	100.0	

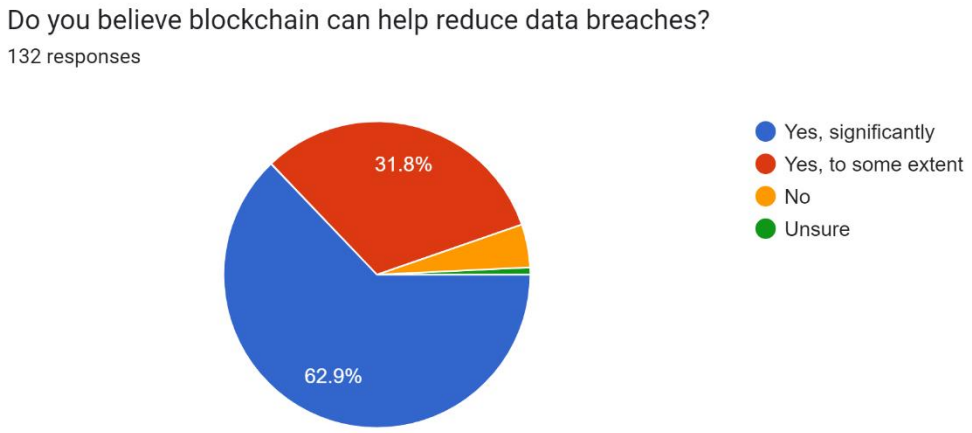

Figure 8: Response of question 8

According to the statistics shown in the table, 62.9% of respondents are of the opinion that blockchain technology has the potential to be of significant aid in the fight against data breaches. A mere 4.5% of respondents are of the opinion that it is not capable of reducing the amount of data breaches, while 0.8% are uncertain about this. Nevertheless, 31.8% of people are of the opinion that it could be helpful to some extent. Based on the findings presented here, it would seem that there is a substantial degree of confidence in the capability of blockchain technology to improve data security and reduce the number of breaches that take place.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Financial services	91	68.9	68.9	68.9
	Healthcare	29	22.0	22.0	90.9
	Retail	9	6.8	6.8	97.7
	Technology	3	2.3	2.3	100.0
	Total	132	100.0	100.0	

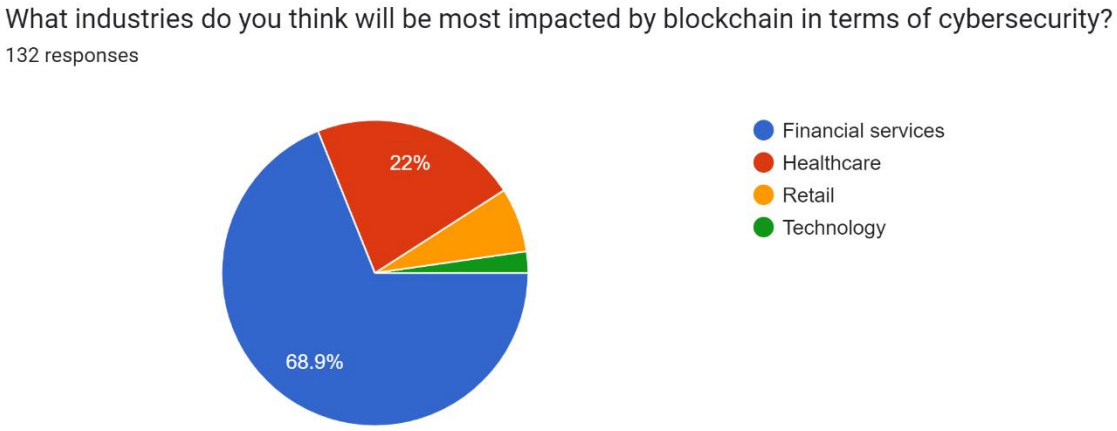

Figure 9: Response of question 9

According to the data shown in the table, the majority of respondents (68.9%) are of the opinion that the commercial sector of the financial services industry will be the one to see the most significant influence from the implementation of blockchain technology. The next industry on the list is healthcare, which accounts for 22% of the total, followed by retail, which accounts for 6.8%, and technology, which provides 2.3% of the total. When this is taken into consideration, it is probable that the sectors that place a high priority on efficiency, transparency, and security are the ones that are most likely to see the most substantial benefits from blockchain technology.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	External courses/workshops	37	28.0	28.0	28.0
	Industry partnerships	15	11.4	11.4	39.4
	Internal training	77	58.3	58.3	97.7
	No specific approach	3	2.3	2.3	100.0
	Total	132	100.0	100.0	

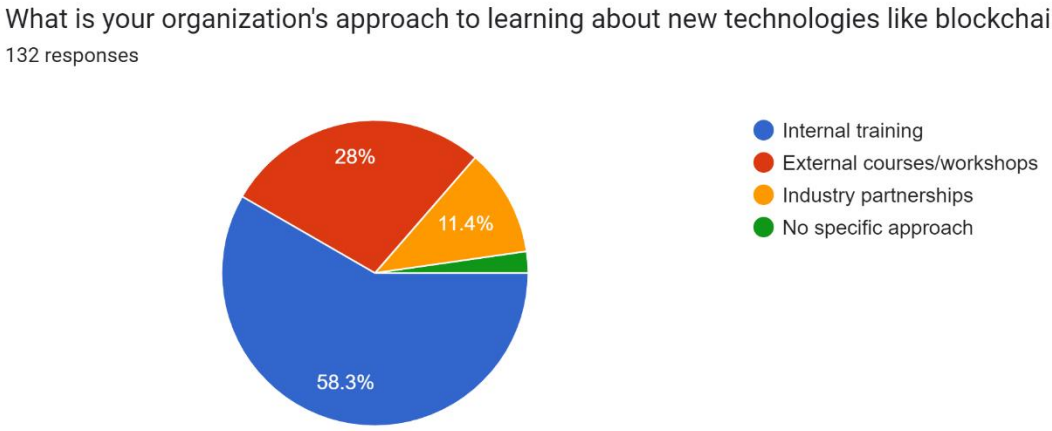

Figure 10: Response of question 10

The data shown in the table indicates that the most prevalent approach of acquire information about emerging technologies is via the use of internal training. This approach is utilized by 58.3 % of the organizations that all of the respondents are linked with. 25% of the population makes use of resources obtained from external sources, such as classes or seminars, while another 25% of the population relies on industrial connections. Only 2.3% of individuals do not have a detailed strategy, which is a very small percentage. In light of the fact that this is the situation, it is reasonable to assume that the great majority of companies would prefer to build their own technical competence inside their own organization, while at the same time making use of resources from outside sources and creating strategic alliances.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not confident	8	6.1	6.1	6.1
	Somewhat confident	42	31.8	31.8	37.9
	Undecided	4	3.0	3.0	40.9
	Very confident	78	59.1	59.1	100.0
	Total	132	100.0	100.0	

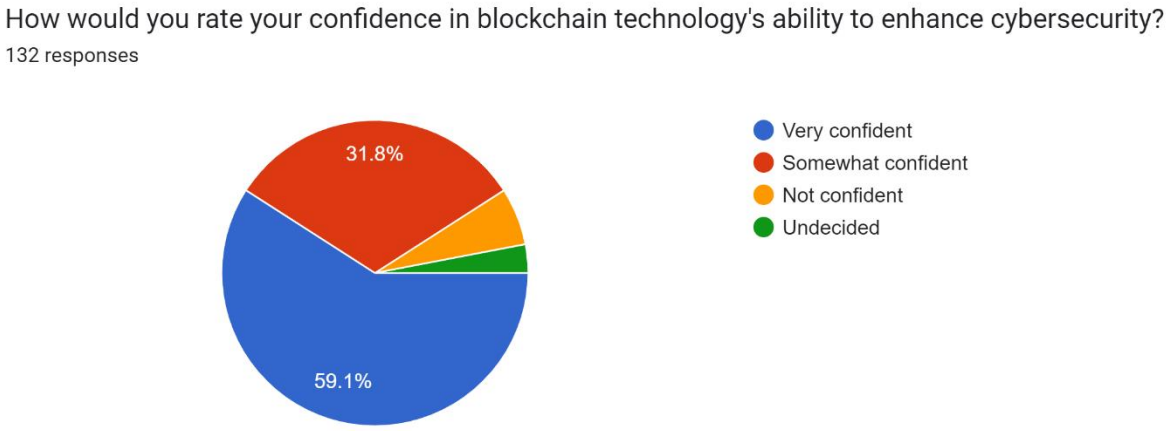

Figure 11: Response of question 11

In accordance with the information shown in the table, 59.1% of those who participated in the survey expressed a high degree of trust in the capacity of blockchain technology to improve security. In addition, 13% of people are hesitant of their decision, 6.1% are very uncertain, and 3% are not sure what they will do. It seems from the findings that people have a high degree of faith in the advantages that blockchain technology offers in terms of security. The vast majority of people either have a high degree of faith in its capabilities or a restricted amount of confidence in its capabilities.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Cryptographic security	16	12.1	12.1	12.1
	Decentralization	76	57.6	57.6	69.7
	Immutability	36	27.3	27.3	97.0
	Smart contracts	4	3.0	3.0	100.0
	Total	132	100.0	100.0	

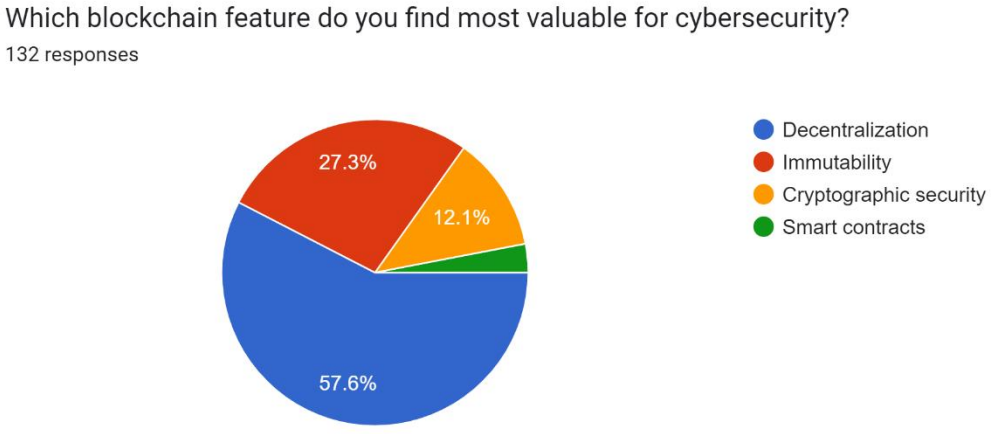

Figure 12: Response of question 12

As can be seen in the table, 57.6% of respondents are of the opinion that the most favourable aspect of blockchain technology in terms of security is its decentralized nature. On the other hand, the relevance of cryptographic security is scored at 12.1%, while the value of immutability is rated at 27.3%. A minority of individuals, namely fewer than three percent, are of the opinion that smart contracts provide significant benefits. As a result of these discoveries, it is abundantly evident that the decentralized nature of blockchain technology and its capacity to generate records that are both safe and immutable are highly significant components.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not sure	6	4.5	4.5	4.5
	Somewhat likely	48	36.4	36.4	40.9
	Unlikely	4	3.0	3.0	43.9
	Very likely	74	56.1	56.1	100.0
	Total	132	100.0	100.0	

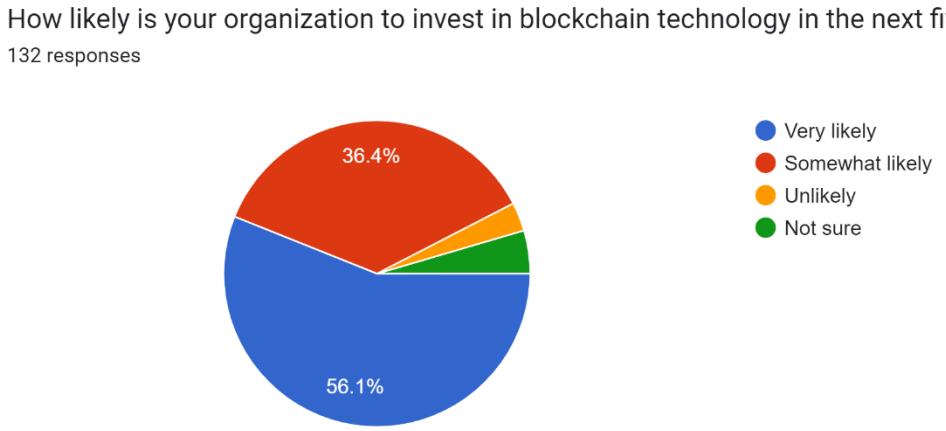

Figure 13: Response of question 13

The image illustrates that there is a significant trend toward the adoption of blockchain technology, as shown by the fact that 56.1% of respondents said that their organization is extremely likely to invest in blockchain technology. Nevertheless, 36.4% of individuals are doubtful about their decision, and 4.5% of people are also uncertain about their decision. Just 3% of individuals are of the opinion that it is very improbable. According to the data, it would seem that the majority of people are excited about the potential advantages that blockchain technology may give and have a good attitude about investing in it. This is the case since the majority of people are considering investing in blockchain technology.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Independent audits	72	54.5	54.5	54.5
	Internal testing	42	31.8	31.8	86.4
	Peer reviews	13	9.8	9.8	96.2
	Trust in the technology	5	3.8	3.8	100.0
	Total	132	100.0	100.0	

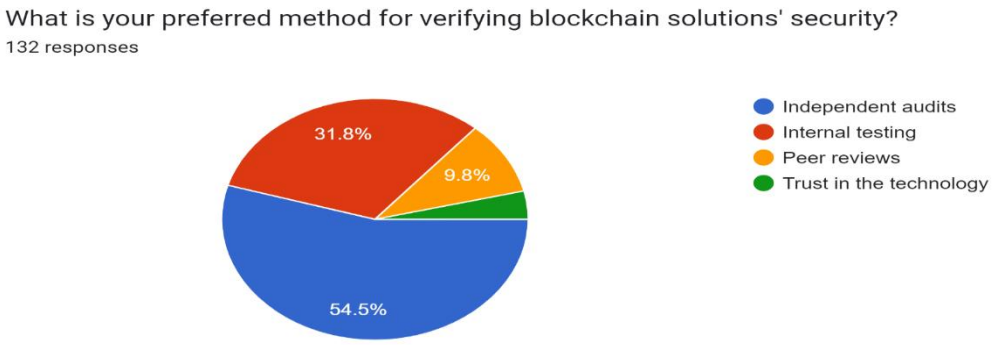

Figure 14: Response of question 14

As shown by the data presented in the table, 54.5% of respondents expressed a desire to have blockchain solutions examined by a third party that is not affiliated with the blockchain in order to ensure that these solutions are genuine. 9% of respondents want to have their work evaluated by their peers, while 13% like having their work evaluated internally. In situations when there is a dearth of more proof, just 3.8% of individuals still retain faith in the technique. In order to ensure that blockchain implementations continue to be reliable and secure, it is very vital to put in place stringent validation procedures.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Definitely	76	57.6	57.6	57.6
	Maybe	13	9.8	9.8	67.4
	Probably	38	28.8	28.8	96.2
	Probably not	5	3.8	3.8	100.0
	Total	132	100.0	100.0	

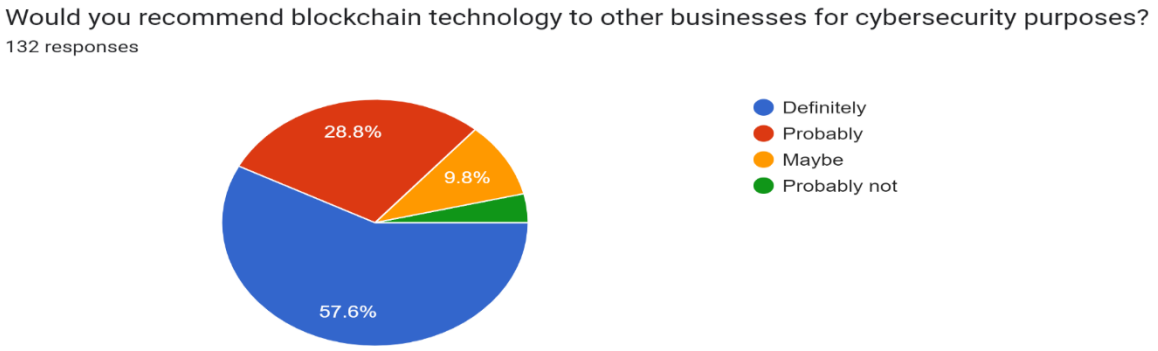

Figure 15: Response of question 15

Based on the data shown in the table, it is evident that 57.6% of the respondents who took part in the survey are sure that other companies should use blockchain technology for reasons related to safety. In conclusion, 28.8% of respondents would most likely put forth the proposition, 9.8% are unsure (maybe), and 3.8% would most likely not. The fact that the majority of respondents are prepared to advocate for the adoption of blockchain technology in other firms is evidence that there is a strong belief in the security advantages that blockchain technology brings.

Conclusion

The use of blockchain technology and specifics of employing the methods from the business security and other field as well as the significance of the technological and methodological progress in modern research and practice illustrate the changes that contemporary technology and methods bring to the theory and practice of security. The use of blockchain in that it offers decentralized, non-tamper able and transparent solutions to business' data management and utilization is set to be the hub that alters business' approaches towards data security, integrity and effectiveness. Hence, organizations can solve various security threats, avoid new risks, and increase the performance of existing ones with the help of decentralization, immutability, transparency, consensus mechanisms, smart contracts, and cryptographic security. However, issues like scalability and cross-compatibility are occasions that must be dealt with so as to fully unlock the potential of using supply chain finance.

The findings show that a large majority of the sample is well-informed on blockchain technology; in fact, 83.3% of respondents are very acquainted with it. The perceived relevance of blockchain in safeguarding data was shown when 66.7% of respondents named improved data integrity as the most essential advantage when questioned about its advantages in cybersecurity. Nevertheless, 56.8% of respondents identified the high cost as the primary obstacle to blockchain adoption, demonstrating the importance of financial considerations. Also, a majority of respondents believe blockchain's security capabilities; 62.9% are very confident in its ability to avoid data breaches. Although blockchain technology has gained recognition for its security features, the cost is still a major barrier affecting its adoption in the corporate sector, according to these studies. Real-world adoption of blockchain technology in business security requires knowledge of the concept's fundament and deciding on the right kind of blockchain – public, private, or consortium – for the given business case. When bringing blockchain into the current process environment, there is the need to adopt smart contract solutions, develop policy frameworks, and successfully manage the key infrastructure. The benefits of blockchain in business security are significant: it increases the reliability of data through its non-editable feature it decreases the chances of fraud through openness of every transaction and increases the chances of standing up to attacks by having no vulnerable link. In addition, the reduction of identity verification operations by adopting the solutions based on the blockchain and automation of numerous operations bring high value to the functioning of businesses.

In collecting data for this research, a survey was administered online as a means of recollecting information from the business professionals on the application of blockchain technology to cybersecurity. The survey that was conducted consisted of 15 well formulated questions that aimed at getting a broad response based on factors such as; awareness of the technology, perceived strengths and weaknesses, confidence in the paradigm's ability to offer security, and the probability of increased investment in the same. Carrying out the survey on the internet was helpful in the sense that the survey materials got to a large population and from different fields. The survey received 132 responses, which can be considered sufficient for analysis in terms of the number of subjects. The clear and relevant objectives prepared for the survey minimized the possibility of the respondents giving ambiguous or unconsciously skewed answers. Hiding the identity of participants probably had an influence on the bias of the comments received. This approach was useful in collecting both the amount and quality of information, thus providing a broad perspective of the current perceptions about blockchain in the context of secularity. The data collected was very helpful in the realization of the research objectives in providing information on the adoption of blockchain technology, perceived benefits and key challenges. Altogether, the process of data collection may be considered successful in given context to lay down the background for the further analysis of the blockchain potential in strengthening the cybersecurity of the business.

Integration of the state-of-the-art solutions such as blockchain and solid academic research approach constitutes a highly effective tool for improving organizational protection and gaining important insights. The idea of blockchain is based on decentralization, security, and high efficiency, which opens up amazing opportunities for data protection and optimization of work. However, proper choices of research strategies, emergent data collection, and proper analysis make sure that results of researches are accurate, relevant, and even more importantly conducted in a proper and ethical manner. Hence, adapting to these innovations and methodologies will be imperative for dealing with modern day problems and disseminating information in various disciplines.

References

Abu-Elezz, I., Hassan, A., Nazeemudeen, A., Househ, M. and Abd-Alrazaq, A., 2020. The benefits and threats of blockchain technology in healthcare: A scoping review. *International Journal of Medical Informatics*, *142*, p.104246. https://doi.org/10.1016/j.ijmedinf.2020.104246

Chidukwani, A., Zander, S. and Koutsakis, P., 2022. A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. *IEEE Access*, *10*, pp.85701-85719. **DOI:** 10.1109/ACCESS.2022.3197899

De Nicola, M. and Raja, C.D.D., 2022. Cybersecurity and Blockchain Impacts on Value Creation Process: Empirical Evidences From Non-financial Disclosure. *Journal of Modern Accounting and Auditing*, *18*(6), pp.251-263. https://www.davidpublisher.com/Public/uploads/Contribute/63d5dd217573a.pdf

Demirkan, S., Demirkan, I. and McKee, A., 2020. Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), pp.189-208. https://doi.org/10.1080/23270012.2020.1731721

Etemadi, N., Borbon, Y.G. and Strozzi, F., 2020. Blockchain technology for cybersecurity applications in the food supply chain: A systematic literature review. *Proceedings of the XXIV Summer School "Francesco Turco"—Industrial Systems Engineering, Bergamo, Italy*, pp.9-11. https://summerschool-aidi.it/images/papers/session_3_2020/ID-38.pdf

Feng, H., Wang, X., Duan, Y., Zhang, J. and Zhang, X., 2020. Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges. *Journal of cleaner production*, *260*, p.121031. https://doi.org/10.1016/j.jclepro.2020.121031

Garg, P., Gupta, B., Chauhan, A.K., Sivarajah, U., Gupta, S. and Modgil, S., 2021. Measuring the perceived benefits of implementing blockchain technology in the banking sector. *Technological forecasting and social change*, *163*, p.120407. https://drive.google.com/file/d/1mwlONCaJIxCho-ZITkVTaYYHNZmOlyic/view

Ghelani, D., 2022. Cyber security, cyber threats, implications and future perspectives: A Review. *Authorea Preprints*. https://www.techrxiv.org/doi/pdf/10.22541/au.166385207.73483369

Gurdgiev, C. and Fleming, A., 2021. Informational Efficiency and Cybersecurity: Systemic Threats to Blockchain Applications. *Innovations in Social Finance: Transitioning Beyond Economic Value*, pp.347-372. https://www.researchgate.net/profile/Dave-Gorman/publication/353563840_A_University_Model_of_Social_Finance_Reflections_on_the_University_of_Edinburgh%27s_Social_Investment_Fund/links/61ba08eb4b318a6970e30660/A-University-Model-of-Social-Finance-Reflections-on-the-University-of-Edinburghs-Social-Investment-Fund.pdf#page=365

Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S. and Ishfaq, M., 2022. Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. *Future Internet*, *14*(11), p.341. https://www.mdpi.com/1999-5903/14/11/341

Idrees, S.M., Nowostawski, M., Jameel, R. and Mourya, A.K., 2021. Security aspects of blockchain technology intended for industrial applications. *Electronics*, *10*(8), p.951. **https://doi.org/10.3390/electronics10080951**

Khan, A.A., Laghari, A.A., Shaikh, Z.A., Dacko-Pikiewicz, Z. and Kot, S., 2022. Internet of Things (IoT) security with blockchain technology: A state-of-the-art review. *IEEE Access*, *10*, pp.122679-122695. https://ieeexplore.ieee.org/iel7/6287639/6514899/09955535.pdf

Lee, S. and Kim, S., 2021. Blockchain as a cyber defense: opportunities, applications, and challenges. *Ieee Access*, *10*, pp.2602-2618. https://ieeexplore.ieee.org/iel7/6287639/6514899/09654201.pdf

Leng, J., Zhou, M., Zhao, J.L., Huang, Y. and Bian, Y., 2020. Blockchain security: A survey of techniques and research directions. *IEEE Transactions on Services Computing*, *15*(4), pp.2490-2510. https://www.computer.org/csdl/api/v1/periodical/trans/sc/5555/01/09271868/1p2RaCvQ7dK/download-article/pdf

Lim, M.K., Li, Y., Wang, C. and Tseng, M.L., 2021. A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries. *Computers & industrial engineering*, *154*, p.107133. https://doi.org/10.1016/j.cie.2021.107133

Mark, J. and Joe, B., 2024. Securing the Future: Exploring the Synergy of Business Analytics, Machine Learning, and Blockchain Applications in Retail Cybersecurity. *Journal Environmental Sciences And Technology*, *3*(1), pp.89-96. https://jest.com.pk/index.php/jest/article/download/95/89

Miracle, N.O., 2024. The impact of blockchain technology on improving cybersecurity measures. Https://www.researchgate.net/profile/osita-nwakeze/publication/382523859_the_impact_of_blockchain_technology_on_improving_cybersecurity_measures/links/66a14f3f27b00e0ca43e41a2/the-impact-of-blockchain-technology-on-improving-cybersecurity-measures.pdf

Prakash, R., Anoop, V.S. and Asharaf, S., 2022. Blockchain technology for cybersecurity: A text mining literature analysis. *International Journal of Information Management Data Insights*, *2*(2), p.100112. https://doi.org/10.1016/j.jjimei.2022.100112

Ruan, Z., 2023, November. Blockchain technology for security issues and challenges in IoT. In *2023 International Conference on Computer Simulation and Modeling, Information Security (CSMIS)* (pp. 572-580). IEEE. https://www.sciencedirect.com/science/article/pii/S187705091830872X/pdf?md5=e006dd5264e91074f3839985c03627d2&pid=1-s2.0-S187705091830872X-main.pdf

Saeed, S., Altamimi, S.A., Alkayyal, N.A., Alshehri, E. and Alabbad, D.A., 2023. Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), p.6666.**https://doi.org/10.3390/s23156666**

Safitra, M.F., Lubis, M. and Fakhrurroja, H., 2023. Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), p.13369. https://www.mdpi.com/2071-1050/15/18/13369

Taherdoost, H., 2021. Data collection methods and tools for research; a step-by-step guide to choose data collection technique for academic and business research projects. *International Journal of Academic Research in Management (IJARM)*, *10*(1), pp.10-38. https://hal.science/hal-03741847/document

Tibrewal, I., Srivastava, M. and Tyagi, A.K., 2022. Blockchain technology for securing cyber-infrastructure and internet of things networks. *Intelligent Interactive Multimedia Systems for e-Healthcare Applications*, pp.337-350. https://doi.org/10.1007/978-981-16-6542-4_17

Uchendu, B., Nurse, J.R., Bada, M. and Furnell, S., 2021. Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, p.102387.https://doi.org/10.1016/j.cose.2021.102387

Zeng, Z., Li, Y., Cao, Y., Zhao, Y., Zhong, J., Sidorov, D. and Zeng, X., 2020. Blockchain technology for information security of the energy internet: Fundamentals, features, strategy and application. *Energies*, *13*(4), p.881. **https://doi.org/10.3390/en13040881**

Zhu, P., Hu, J., Li, X. and Zhu, Q., 2021. Using blockchain technology to enhance the traceability of original achievements. *IEEE Transactions on Engineering Management*, *70*(5), pp.1693-1707. **DOI:** 10.1109/TEM.2021.3066090

Zidan, F., Nugroho, D. and Putra, B.A., 2023. Securing enterprises: harnessing blockchain technology against cybercrime threats. *International Journal of Cyber and IT Service Management*, *3*(2), pp.167-172. https://iiast.iaic-publisher.org/ijcitsm/index.php/IJCITSM/article/download/120/68