ZKG INTERNATIONAL

ISSN: 2366-1313

Cognizance of Block chain Data Security in Censorious Comprehensiveness

Abdul Khadeer, Research Scholar, Department of CSE , J.S University, Shikohabad.

Dr. Badarla Anil ,Professor ,Supervisor, Department of CSE, J.S University,Shikohabad.

Abstract - The major purpose of this study is to collect the opinions of professionals working in the field of cyber security on the topic of the potential of blockchain technology to serve as a suitable alternative for already established data security methods. A literature analysis was performed to evaluate previous research on Cyber Security, its infrastructure, and the essential components of Blockchain Technology. The review was carried out at the beginning of the project. The discovered themes that arose from the interviews make it clear that the participants do not regard blockchain technology to be a trustworthy alternative for the current security infrastructures and processes. This is evident based on the identified themes that surfaced from the interviews. The immutability and security characteristics of blockchain technology have proved a high degree of tampering resistance, making it a viable solution for the information security business. Despite the fact that blockchain technology has a number of benefits and optimistic components, its immutability and security features have demonstrated this. If blockchain technology can overcome its current limitations, it has the potential to become a tool that cannot be ignored when it comes to protecting the confidentiality and safety of user data.

It was decided to conduct a research study using qualitative methods in order to investigate the participants' points of view. Individual interviews with each participant, all of whom have professional competence in the field of cyber security, were carried out in order to give a better level of specificity in the report. During the course of the interview process, five distinct themes emerged as a result of the utilization of open-ended questions and dialogue with the participants.

Keywords: Information Systems, Informatics, Qualitative Research, Block chain, Cyber Security, Data Security, ICT, Privacy.

1. INTRODUCTION

Over the course of the past two decades, the sector of cybersecurity has undergone expansion and development as a result of these trends. The author Beynon-Davies (2020) suggests that the concept in issue may be better understood if it were referred to as data security. The rise in the number of people who work remotely and participate in communication practices that are analogous to those practices has resulted in an increase in the need for risk-mitigation measures that are linked with remote communication. According to Naidoo et al.'s (2020) findings, hackers are taking advantage of the increased dependence on virtual environments that

ISSN: 2366-1313

has developed as a direct consequence of the COVID-19 epidemic. The data suggests a considerable rise in phishing attempts related with the pandemic, indicating a huge increase of 667%, while the FBI has documented a major spike in cyber-crime. In light of the afore mentioned increase, it is very necessary for businesses to put in place the precautions that are necessary to protect their data. It is of the utmost importance for businesses to ensure that their data is secure, which calls for a diverse range of technical and non-technical precautions to be taken. In accordance with the findings of Beynon-Davies (2020).

According to Beynon-Davies (2020), there are three basic technical dimensions that may be used to classify different aspects of data security. These aspects include the following:

In this context, the three most important areas of concern are the formation of efficient personal identity management, the safeguarding of stored data, and the protection of transactional data. Managing personal identities effectively, safe-guarding stored data, and protecting transactional data are all interrelated.

The identification of a participant in traditional forms of interpersonal communication is accomplished via the use of nonverbal indicators. Beynon-Davies (2020) asserts that the usage of physical identities is impractical in long-distance communication; hence, the practice of using artificial identifiers, such as personal identification numbers (PINs) and passwords, is widespread.
The existence of a wide variety of outside dangers adds another layer of difficulty to the already difficult task of protecting sensitive data that has been saved. Theft of electronic equipment, invasions of personal privacy, and breaches of integrity are a few instances. A competent computer-based countermeasure would be one that entails the employment of an authorization approach for the use of databases and information and communication technology (ICT) systems. In accordance with the findings of Beynon-Davies (2020).

In conclusion, it is important to highlight the fact that the business sector of e-commerce has seen a sizeable expansion in recent years. The realm of financial data transactions is an extremely important one that calls for severe precautions to be taken in order to protect the security of the data and prevent unwanted access to it.
According to Beynon-Davies's research from 2020, some of the more common practices for protecting data transfers include using encryption, digital signatures, tunneling technologies, and firewalls. According to Beynon-Davies's research from 2020, firewalls are deployed in both the hardware and software that make up private networks in order to protect these networks from a variety of dangers.
The traditional methods used so far for the purpose of protecting and maintaining data security are demonstrative of the tactics utilized by cybersecurity firms to assure the safety of the sensitive information of their customers. These strategies will be discussed in further depth in the following paragraphs.

Despite the fact that the aforementioned tactics have been evaluated and have shown to provide acceptable security to the companies who use them, there is a growing body of evidence that supports the use of Blockchain technology as an efficient solution for the protection of data and the processing of transactions.

The most popular form of decentralized digital money, Bitcoin, utilizes the blockchain to function as its main ledger. Bitcoin was first invented in 2008 by an unknown person who went by the alias "Satoshi Nakamoto." In 2009, the term "blockchain" was first used to refer to a

ISSN: 2366-1313

specific technology that was later applied in a variety of sectors.

In spite of the assertion made earlier that blockchain technology represents a significant impetus for contemporary networking and security research, there is a paucity of information concerning the perspectives of employees working in the aforementioned fields with regard to the possible adoption of blockchain-based applications.

In light of this assumption, the major purpose of this master's thesis is to investigate the perspectives of cyber security experts on the use of blockchain technology as an alternative approach to the protection and transmission of secret information. Therefore, it is essential for the aforementioned cohort and the scope of this study to determine the perceptions of prospective users regarding the implementation of blockchain technology, to solicit their unbiased viewpoints, and to obtain input on potential applications and advancements that could propel the research. In addition, it is imperative that this study obtain input on potential applications and advancements that could propel the research.

The current study tries to establish the scope of the research endeavor as well as the constraints that it faces.

The perspectives of the participants on blockchain technology and its possible applicability to current information and communications technology (ICT) systems are the primary subject of this research. As a consequence of this, the scope of this study will not be restricted to the investigation of a certain hardware or software system that is often used in the industry. The purpose of this research is to evaluate the notion of requesting input from participants evaluating the existing ICT infrastructure and their perceptions of whether or not a blockchain solution would serve as an alternative that is feasible.

In addition, the current investigation includes participants who have past experience working in the security industry. This is because having an in-depth grasp of how traditional cybersecurity systems and the monitoring services connected with them operate is essential for the success of the investigation.

To elaborate more on the aforementioned remark, certain limitations will be placed in order to bring the master's thesis into alignment with its various characteristics. It is strongly suggested that participants have at least one year of professional experience in the area of cyber security, especially in jobs that are connected to monitoring, engineering, or management. In addition, it is important to remember that the data managed by the aforementioned organizations and systems is of a sensitive nature. Because of this, there are a number of rules in place that are designed to protect the confidentiality and safety of both the workers and the consumers. As a result, neither specific examples nor statistical data will be provided. The overall notion of how blockchain technology may appropriately serve the function of preserving the sensitive data that was discussed before will continue to be the primary focus of attention.

2. METHODOLOGY

➢ Philosophical Paradigms

Within the realm of information systems, Klein and Myers (1999) identified three primary epistemological classifications that are commonly used in qualitative research. Positivism, interpretivism, and critical inquiry are the three schools of thought in philosophy that are being taken into account.

ISSN: 2366-1313

Positivism, often known as post-positivism, is one of the paradigms that is being taken into account. According to Creswell and Creswell's (2017) study, post-positivists often explore deterministic issues, the consequences of which may be quantified using preset and stable techniques that are related to the underlying causes of the problem. Creswell and Creswell (2017) also state that post-positivists typically investigate deterministic problems. This is quite similar to the process that is used in experimental research.

In contrast to positivism, the interpretative paradigm is most often used to qualitative research as opposed to quantitative research. This is due to the former's emphasis on the researcher's experience and perspective. According to Klein and Myers (1999), information systems research is considered interpretative when it incorporates the investigation of social constructs, tools, and artifacts in order to gain understanding of reality. Interpretive research, as described by Klein and Myers (1999), is said to provide results that are not preconceived and are instead based upon the human perception of a scenario as it develops. According to Creswell and Creswell (2017), the application of this paradigm by researchers is highly dependent on the viewpoints of the persons engaged. According to Creswell and Creswell's (2017) research, the participants in a study are the ones who build the meaning of a scenario via interaction based on how they interpret the open-ended questions posed by the researcher.
The critical inquiry or transformational paradigm is the third and last paradigm that has been outlined here. According to Klein and Myers (1999), research in the area of Information Systems may be categorized as "critical" when its major purpose is to investigate social phen-omena, structures, and situations that contribute to alienation. This is the case when the primary objective of the study is to critique these factors. According to Creswell and Creswell (2017), this specific philosophical paradigm is centered on meeting the needs of groups and people who may have been excluded or disenfranchised from our cultural standards. Creswell and Creswell argue that this particular philosophical paradigm concentrates on addressing the requirements of these groups and individuals. According to Creswell and Creswell (2017), the researcher is the one who identifies the most important aspect of the research project. Following this, the researcher works with the participants to create questions, collect data, and conduct an analysis of the material.

The approach used in terms of methodology.

Creswell and Creswell (2017) have identified three main methodological approaches or strategies of inquiry that are often used in the area of information systems (IS) research. These methods may be broken down into two categories: qualitative and quantitative. The qualitative, the quantitative, and the mixed methodologies are all included in these approaches.
Researchers that use quantitative methods first attempt to examine a theory by developing hypotheses, and then, using the data that they collect, they either confirm or disprove the assumptions. In most cases, the data is collected in a numerical format, and then it is put through various statistical techniques and tested against various hypotheses in order to conduct an analysis (Creswell & Creswell, 2017).

On the other hand, researchers who use qualitative approaches attempt to appreciate the importance of an event by looking at it through the eyes of the persons who are engaged in it. Participant observation is a technique that is widely used in this approach to the collecting of data. In this method, researchers watch

ISSN: 2366-1313

participants as they are engaged in a variety of activities (Creswell & Creswell, 2017).

The mixed method approach is a research technique that includes both quantitative and qualitative methods and designs. This strategy utilizes both primary and secondary sources of data. According to Creswell & Creswell's (2017) argument, this method provides a more in-depth understanding of a study topic.

The interpretative paradigm of this master's thesis requires the use of a qualitative research strategy in order to be successful. As was said before, this methodology seeks to understand the importance of an event from the views of the participants. Because of this, it has been determined to be a suitable technique. The selection of this methodology was made in line with the criteria proposed by Creswell and Creswell (2017). These factors include the research questions, the author's own experience, and the audience for whom the study was conducted. The preceding criteria have their origins in the field of computer and network security.

The procedures that are followed in order to get information.

The interpretative paradigm serves as the theoretical foundation for the research approach that was taken in the form of a qualitative methodology for this master's thesis. According to Creswell and Creswell (2017), the methods that are used in qualitative research include participant observation, qualitative interviews, qualitative documents, audiovisual material, and digital material. Because of the interpretative nature of this research, the researchers decided to gather their data via the use of unstructured qualitative interviews. According to Creswell & Creswell (2017), the current investigation is thought to be suitable for conducting face-to-face interviews with the participants. These interviews would make use of semi-structured and open-ended questions to extract the participants' opinions and viewpoints.

The current restrictions that have been implemented in order to battle the widespread Covid-19 epidemic are putting a limit on the practicability of this choice in terms of the well-being of myself and the other persons involved. The interviews were carried out using several approaches, each of which was modified to cater to the specific requirements and preferences of the participants. Conducting the interview via video conference was the strategy that I suggested using because it would make it easier for the interviewer to take notes and also enable the interviewee to provide additional details regarding their nonverbal cues and gestures that they were displaying. The interviewees were asked for their permission before their phone calls were recorded for the purpose of making it easier to analyze the information that was gleaned from the interviews. The findings were obtained from the notes that were collected throughout the interview in the event that the interviewee chose not to go with the alternatives that were presented before and instead opted for an audio call or an unrecorded iteration of a video call.

In relation to the inquiry prompts of this master's thesis, it is very necessary for the interviewers to display certain characteristics in order to guarantee the validity of the sample. The aforementioned characteristics were discussed in passing in the part that dealt with the scope and the restrictions, specifically: Regardless of the participants' employment roles, they must all have a minimum of one year of professional experience in the subject of cyber security to be eligible to participate in the training. The aforementioned restriction was put into place to guarantee that persons have an adequate awareness of the way in which modern cyber security

ISSN: 2366-1313

systems operate. It is recommended that people hold an academic background in the area of information technology or information systems in order to promote a better grasp of the operational mechanics of blockchain technology. This will allow users to better comprehend how the technology works.

Drawing from the aforementioned information and subsequent outreach to a subset of the subjects, it was seen that owing to the fledgling nature of blockchain technology, some people demonstrated a lack of full comprehension of the working of the technology. This was observed despite the fact that the information had been provided. As a consequence of this, it is important for me to compile a full exposition on various blockchain mechanisms. These mechanisms include, but are not limited to, blockchain classifications, consensus protocols, as well as permissioned and permissionless blockchains. Moreover, it is imperative that I do this as soon as possible. The aforementioned subject was brought up in response to questions on an understanding of how blockchain technology works.

The presentation was provided in the style of a lecture, and it lasted for around a quarter of an hour. It was done separately during each interview, and its purpose was to provide the participants with further information on the subject of blockchain technology in a more broad sense.

The methods that are used in the data analysis process.

According to Creswell and Creswell (2017), while doing qualitative research, it is essential to provide an overview of the processes that are involved in interpreting the various kinds of qualitative data that have been collected. An explanation of the data will be produced as a result of the analysis of the data, which will take into account the aspects of the study as well as the qualitative research methods that were used. The analysis of data is an essential part of qualitative research, and it is tightly entwined with the other aspects of the study. This close intertwining makes the data analysis an indispensable component. According to Creswell and Creswell (2017), researchers have the capacity to do an analysis of an initial interview and afterwards write memoranda that can be integrated into the final report, even when further interviews are still being conducted at the same time. Creswell and Creswell (2017) also argue that researchers have the ability to undertake an analysis of an initial interview. Creswell and Creswell (2017) referred to this process as simultaneous processes in their definition of the term.
In order to successfully organize and interpret the data that has been obtained, the process of data analysis requires that a certain order of sequential actions be adhered to. Creswell & Creswell (2017) provided a set of sequential instructions, and the current experiment will follow those guidelines.

The first stage is to organize and make the data ready for analysis. This will be done at the beginning. When all of the necessary materials, including notes and recordings, have been compiled, they will then be systematically categorized based on the sources from which they originated.

The second phase is carefully going over all of the data that is available and interpreting it. During this stage, an assessment will be made regarding the veracity and significance of the information that was provided by the participants, as well as the overall message that was conveyed.

The third step is to get started on the coding process for all of the data that is now at your disposal. In order to denote the preliminary category that the material falls under, a code word that is enclosed in

ISSN: 2366-1313

brackets will be placed next to each and every transcript.

The production of a detailed description and the determination of recurring themes is the fourth phase in the process. Overarching themes will be developed via the use of the coding framework that was outlined before for the purpose of future application in the study inquiry. According to the findings of the research conducted by Creswell & Creswell (2017, page 313)

In qualitative research, the aforementioned topics usually emerge as noteworthy discoveries, and researchers frequently use them as headers in the results sections of research papers, dissertations, or theses. It is advised that the presentation of different points of view should have several facets and be supported by a range of citations as well as tangible facts.

The fifth stage is the process of representing the description and the themes. The decisive interpretation of the findings and patterns that were gleaned from the investigation is the last step in this guide's process, and it is followed by the presentation of those findings and investigations. The conclusions of the final report are going to be presented in the form of a narrative passage.

In the realm of academic research, the principles of reliability and validity are of the utmost importance.

In this part, we are going to offer an examination of the reliability and validity of the procedure that was used to collect the data and analyze it in connection to the qualitative study that was carried out. It is necessary that the researcher follow to certain processes in order to guarantee the authenticity of the results obtained from the investigation.
The meaning of the term "validity" varies significantly depending on whether a qualitative or quantitative research approach was used to collect the data. The capacity of qualitative research to preserve validity is one of the most significant advantages of this kind of study. The correctness of the results from each of the several points of view will determine whether or not the study may be considered legitimate. According to Creswell (2014), the views expressed in the aforementioned statement were derived from the viewpoints of the researcher, the people who participated in the study, and the readers of the academic publication.

According to Creswell (2014), the researcher's preconceived notions have a major influence on the validity of the study. My past knowledge as a cyber security analyst is used extensively throughout the whole of my master's thesis. In addition, the people who took part in the research are experts in the field of cybersecurity; as a result, their perspectives are congruent with mine on a personal level about issues that are solely focused on modern frameworks and methods of cybersecurity.

When conducting academic research or studies, it is imperative to keep in mind the moral and ethical implications of one's actions.

Respect for the people who take part in research is one of the most important ethical factors to take into account while doing research. Before beginning the research, the participants were given enough notice that their participation was fully voluntary and that they kept the choice to withdraw from the study at any point in time. The identity of those who took part will not be made public in this article under any circumstances. Utilizing their designation was the appropriate course of action to take in order to protect their anonymity.

Aside from that, the individual conduct of interviews was primarily aimed at safeguarding the participants' privacy and

ISSN: 2366-1313

confidentiality as the primary concerns during the course of the interviews. This helped to create a safe environment in which the participants felt comfortable being open and honest about their thoughts and feelings about the issues that were being discussed. As a result, the participants were able to freely express themselves and share their perspectives.

Additionally, it is important to note that the recordings and transcripts were stored on separate electronic devices as well as physical notepads; however, no corresponding backup files were kept. After the research has been concluded, the material will be discarded in order to protect the participants' right to confidentiality as well as their personal privacy.

3. EMPIRICAL FINDINGS

Following the completion of six interviews comprised of free-flowing questioning and conversation, a number of parallels and contrasts were discovered. The primary ideas that emerged from the analysis of the patterns are the focus of the fourth chapter's discussion. In order to accomplish this goal, the strategies for data collection and analysis that were discussed in the part that came before this one were used. The layout of this chapter is based on the chronological order in which the interviews were conducted, beginning with the respondents' first impressions of the data security architecture and policies that are now in place. An explanation of the Blockchain technology and an analysis of its potential repercussions will follow immediately after that. This thesis investigates a number of open-ended questions about blockchain technology, the culmination of which is an investigation into whether or not cyber security experts perceive blockchain technology as a viable alternative and their thoughts on the possible future uses of this technology. The following section will provide a condensed summary of the five overarching themes that emerged throughout the course of the analysis of the data that was acquired.

- Current Data Security Infrastructure and Methods
- Blockchain Operation and Understanding
- Blockchain Scalability and Sustainability
- Security of Blockchain
- Blockchain Implementation on Data Privacy and Security

4. DISCUSSION

➢ Opinion on current Data Security infrastructure and methods

On this section the opinions of the Cyber Security professionals in regards to the current systems and methods used on Cyber Security in order to protect sensitive data are summarized according to the first research question:

RQ1: How satisfied are Cyber Security Professionals with the current data security infrastructures and methods?

The results are briefly presented on the table below in order to be used in the following discussion.

Table 1: Opinion on current Data Security infrastructure and methods

ISSN: 2366-1313

1	The current systems are on a really good level. Improvements could still be made
2	Transition to Cloud-based systems is seen positively
3	Security level depends on each individual organizations' infrastructure and expertise
4	The human error can create gaps in the security control systems
5	Being Pro-active generally prevents succesfull attacks
6	Multifactor Authentication is perceived as extremely secure
7	2FA is usefull but frequent changes of passwords is tiresome for the users
8	Current Encryption methods are adequate and promote trust
9	Encryption adds an extra layer of security
10	People are careless when it comes to security and privacy. Lack of awareness and training is causing most of the security issues
11	Devices are rarely at fault. Most of the times security gaps are caused due to misconfigurations or human errors

The general consensus among those with a stake in the matter is that the modern security control systems are trustworthy when it comes to safety. The wide variety of devices are functioning at a high level, so significantly decreasing the impact of any hostile efforts conducted against a business. According to Beynon-Davies's (2020) hypothesis, some of the most recent methods that are used to protect sensitive data include firewalls and permission mechanisms. The participants are in agreement with the aforementioned concept and say that the common trend towards cloud-based solutions would further strengthen the existing security architecture.

The people who were interviewed believe that the execution of an organization's security control systems and the members' commitment to the rules of the organization are two of the most important factors that determine how effective an organization's security measures are. Human mistake, as opposed to a lack of effective device protection mechanisms inside an enterprise, is often the cause of security flaws that are later exploited by hostile actors. According to what was mentioned earlier in the literature review that was carried out by Acar et al. (2016), the reason for this occurrence is attributed to the significant disparity between the theoretical security capabilities of these devices and the inadequate implementation of security measures in real-world usage scenarios. In other words, the inadequate implementation of security measures in real-world usage scenarios is the cause of this occurrence.

An additional major claim was that the use of a proactive strategy has the ability to improve the reaction time that a business has when confronted with harmful assaults. In order to reduce the likelihood of fraudulent actions and unauthorized access to sensitive information, it is essential to be able to predict the ways that hostile actors may use to exploit security flaws.

Beynon-Davies (2020) has indicated in the past that the adoption of authorization procedures is of the highest significance in the preservation of sensitive information belonging to workers or customers. The participants have given their resounding endorsement to the notion that the existing implementations of two-factor authentication and multi-factor authentication are absolutely necessary in order to protect an organization from hostile actors and efforts at social engineering. In spite of what was said above, one member shared their opinion that forcing users to often change their passwords may be a cumbersome experience for them. After multiple failed tries, people may give up on their efforts to create a unique and secure password,

ISSN: 2366-1313

choosing instead for a password that is easy to remember but also vulnerable to being guessed. This is because simple passwords are easier to remember than complex passwords, but they are also easier to crack. Another possibility is that they may continue to use their original password but will make some modest adjustments to it. There is a possible danger to the corporation as a whole as a result of individual individuals having their accounts hacked.

Acar et al. (2016) state that cryptographic algorithms are an essential component in the process of protecting sensitive information from being accessed by malicious parties. The respondents had a high degree of agreement and conviction on the effectiveness of modern encryption systems, which are seen to present a formidable barrier to unwanted access. They express this high level of agreement and conviction in a number of different ways.

The majority of participants in the discussion on modern cyber security systems and procedures are of the opinion that those systems are now operating at a highly competent level. This finding marks the end of the discussion. The observation that people working for an organization are reckless and make large mistakes as a consequence of insufficient knowledge and training is the key worry that is raising panic.

Table 2: Participants' perception on Blockchain technology and the way it operates

1	Most of the participants heard of the term Blockchain but corellate it to bitcoin mining andtransactions
2	Public permissionless blockchain is the most well-known form of blockchain due to its reputation
3	Private and consortium permissioned blockchains are perceived as secure and relatable tocurrent databases.
4	PoS is the most prefered consensus mechanism due to its high efficiency compared to the high cost PoW.
5	PBFT is perceived as really strict and not suitable for real life applications
6	Participants feel excited about the prospect of using smart contracts in the future.
7	Smart contracts are still not yet perceived as safe and secure and need improvements in orderto be trusted.
8	Blockchain immutability is perceived as extremely secure
9	Participants have shown little interest in the mining process
10	Blockchain's scalability is seen as a limitation by the participants
11	The power consumption of PoW is seen as a major issue
12	The cost of Blockchain systems is seen as forbidding for large scale implementation
13	Blockchain's transparency is perceived positively as long as non-sensitive data is visible
14	Blockchain systems need a central administration in order to be trusted

Notwithstanding the fact that the interviews were conducted with individuals who have amassed considerable experience in the IT and Cyber Security domains, the preponderance of respondents were only acquainted with blockchain as a nomenclature. Hughes and colleagues (2019) concur with the notion that only a limited number of individuals possess knowledge regarding blockchains, with the majority of such individuals being well-versed in the technical intricacies of the technology. It was noted that all participants, with the exception of one, were familiar with blockchains, primarily due to their widespread use in

ISSN: 2366-1313

cryptocurrencies such as Bitcoin. The public blockchain garnered the highest level of recognition from participants owing to its reputation.

Although the participants had prior knowledge limited to public blockchains, their keen interest in private and consortium blockchains was notable as they found them to be highly relatable. It is believed that the aforementioned blockchain variants are highly secure and bear close resemblance to the databases that are presently employed by various organizations.

Throughout the majority of the interviews, participants exhibited a notable level of enthusiasm upon being introduced to the concept of smart contracts and their operational mechanisms. Anticipated outcomes were observed as smart contracts exhibit analogous functionality to the correlation rules employed in Cyber Security for the purpose of log categorization. Although the participants initially displayed enthusiasm upon engaging in a discussion pertaining to a relatable topic, they were subsequently disheartened upon learning that smart contracts continue to encounter numerous security challenges, with various methods of exploitation being prevalent. Wang et al. (2018) identified Transaction-ordering dependence (TOD) and Timestamp-dependence as two commonly employed methods for perpetrating fraudulent activities. TOD enables a malevolent actor to manipulate the sequence in which transactions are executed, while Timestamp-dependence is utilized in timestamp-based smart contracts.

Consensus was reached among all participants regarding the high level of security provided by the immutability of the blockchain. Upon conducting a comparative analysis, the researchers were unable to identify any existing technology that could rival the tamper-resistant properties inherent in a blockchain system. Upon presentation of the mining process, the attendees exhibited a notable lack of interest. Two participants involved in Bitcoin transactions expressed that the expenses associated with mining are exorbitant and, as a result, they favor investing directly in Bitcoin rather than engaging in mining activities.

The considerable energy consumption associated with a Proof-of-Work (PoW) public blockchain, coupled with its limited scalability, has engendered reluctance among stakeholders to place their trust in it, as previously noted. In addition, it is believed that the expenses associated with operating a blockchain and establishing such systems are excessively high, thereby reducing their efficacy.

The study aims to investigate the perception of blockchain technology as a potential alternative to traditional data security systems and methods.

The focal point and fundamental essence of this Master's Thesis is encapsulated within this particular section. The present study integrates prior knowledge on contemporary security systems and methodologies with the recently acquired knowledge of participants on Blockchain technology, culminating in a comparative analysis. This study aims to evaluate the compatibility of Blockchain technology with Data Security by means of a comparative analysis of various technologies. Additionally, the research seeks to determine the most appropriate applications for Blockchain technology, should it prove to be a suitable fit for Data Security. This section pertains to the third and ultimate research inquiry of the paper, as indicated below:

Research Question 3: To what extent do Cyber Security Professionals endorse

ISSN: 2366-1313

Blockchain as a viable substitute for conventional data security systems and methodologies?

The findings are concisely displayed in the table presented below for utilization in subsequent discourse.

Table 3: Participants' view on Blockchain Technology as a substitute to the current systemsand methods.

1	Blockchain's immutability is classifying it as a great fit for an alternative database
2	Limited scalability is an issue that current systems do not face
3	Blockchain is still perceived as extremely secure, but claims were made that this stands due tothe fact that it has not yet been applied globaly as a solution
4	Being Trained and accustomed to Blockchain is a hindrance for the users that might also leadto unemployment
5	Consortium Blockchains are the prefered type since they could be a great fit for internal use within an organization, promoting secure communication with partners and customers.
6	PoS is the preffered consensus mechanism due to the fact that it could operate greatly within an organization, without the extreme costs of PoW.
7	The participants think that Blockchain is still not ready to be independently used, but they believe that it could partially become a part of the current infrastructure
8	Extra training needs to be previously done in case we decided to switch to Blockchains
9	Future implementation of Blockchain systems is seen in a positive light as long as the variousissues it currently faces are solved

In a nutshell, every individual who took part in the research agreed that one of the most important qualities of blockchain is its inability to be altered. They were led to mostly miss the possible problems originating from the immutability feature of the blockchain, which might hamper any efforts to change the blockchain as a result of the aforementioned observation, which led them to largely overlook the potential drawbacks resulting from the immutability feature. According to Zheng et al. (2017), blockchain technology is steadily progressing to a level where it already outperforms the effectiveness of the majority of Internet of Things (IoT) devices. This is mostly attributable to the immutability of the blockchain.

The scalability problems that public blockchains have are mostly attributable to the extravagant amounts of energy consumption and expenditures that are involved. As a result, the level of confidence that participants demonstrate is considerably hindered as a result of these problems. The already-in-place systems have been validated and shown to perform properly with just the barest of needs. Even though the majority of stakeholders believe that blockchain technology provides a higher level of security than existing systems, they are still hesitant to fully embrace it as a replacement for those systems until further advancements are made in this area.

The fact that blockchains have only been tested on a restricted number of low-scale applications is another issue that has been called into question in relation to this technology. During the course of the conversation, one of the participants voiced the opinion that if blockchain technology were to advance beyond the hype surrounding it at the moment and enter the stage of deployment, it would leave itself open to attack from malicious actors looking to take advantage of potential weaknesses. If the theory stated above is confirmed, it would indicate that there is no visible difference between modern systems and blockchains, since both would be subject to some type of cyber intrusion. This would be the case because both would be susceptible to being hacked.

ISSN: 2366-1313

Participants showed resistance toward using blockchains as autonomous security systems owing to the possibility for severe disruption to existing organizational processes. This was due to the fact that blockchains might be used to record transactions in real time. According to the statement, the deployment of the aforementioned systems would not only result in major cost repercussions for the company, but it will also need the firm to retrain its staff in order for them to be able to adjust to the changes. In addition to that, there is a possibility that this may cause a significant amount of people to lose their jobs. In the event that smart contracts are able to effectively handle the prevalent security issues, a variety of processes may be totally automated, which may lead to the displacement of individuals who are responsible for their implementation.

The widespread pessimism about blockchain technology was obviously casting a shadow on the possible advantages that might be gained by using this technology. In addition to the aforementioned, the respondents came up with a number of other industries that may be helped by the deployment of blockchain technology. The proponents of the consortium blockchain argue that it may be used as an ideal database for internal usage by workers and customers, as well as for the safe transmission of sensitive information with business partners and customers.

According to Christidis and Devetsikiotis (2016), concerns about security may be a major hurdle to the adoption of a public blockchain. As a result, they argue for the usage of a permissioned platform as an alternative to the use of a public blockchain.The participants have reached the consensus that the present iteration of blockchain technology is not in a stage where it can be regarded a practicable choice for autonomous operation. However, they do acknowledge that due to its immutable nature, it has the potential to add an additional layer of security when it is combined with systems that are already in place. As was said earlier, the folks are of the opinion that a certain level of education is required to achieve mastery in the operation of blockchain technology. Despite this, they continue to take a non-committal stance with regard to the implementation of it on a restricted, internal level.

In the end, the vast majority of those who participated in the survey had an upbeat perspective towards the possible course that blockchain technology may take. Many people feel that once blockchain technology has conquered the obstacles it is now facing, it will be an invaluable addition to the arsenal of tools that are used to protect sensitive and personal information.

5. CONCLUSION

In addition, since blockchain technology is still relatively new and has only a limited number of applications outside of the area of cryptocurrencies, it was important to offer participants with education about the basic functions of the technology. The procedure for gathering the necessary information consisted of conducting individual interviews with each participant, with each session lasting, on average, one hour. Within the process, there were a total of five people involved: one Cyber Security Engineer, four Cyber Security Analysts, and one Team Leader for the Security Operations Center. For the purpose of determining whether or not blockchain technology is appropriate for use in security systems, a thorough investigation and discussion were carried out. The research questions that were posed in the thesis were appropriately investigated.

ISSN: 2366-1313

Public blockchains are not considered appropriate for use by Cyber Security companies or the consumers they serve because of the high degree of secrecy that is required. The adoption of private blockchains and consortium blockchains is a possibility; nevertheless, a considerable number of stakeholders are of the opinion that more improvements are required before these alternatives can displace the current infrastructure. Therefore, according to their point of view, blockchains do have the potential to be useful, but not on their own as a replacement. The vast majority of responders pointed to the potential usefulness of a private blockchain as a very safe database, provided that it is connected with already existing technologies.

Even though there are a number of problems that have not been resolved, which have led to a feeling of mistrust among participants, it is interesting to note that the predominant opinion regarding blockchains is not entirely pessimistic. The possibility for blockchain technology to overcome the obstacles it is now facing and to be successfully used to take advantage of its benefits is a subject that is often brought up in conversation. In the event that this turns out to be true, it is possible that blockchain-based technologies may find some use in our particular industry in the not-too-distant future.

REFERENCES:

1) Abu-Salma, R., Sasse, M.A., Bonneau, J., Danilova, A., Naiakshina, A. and Smith, M., 2017, May. Obstacles to the adoption of secure communication tools. In 2017 IEEE Symposium on Security and Privacy (SP) (pp. 137-153). IEEE.

2) Acar, Y., Fahl, S. and Mazurek, M.L., 2016, November. You are not your developer, either: A research agenda for usable security and privacy research beyond end users. In 2016 IEEE Cybersecurity Development (SecDev) (pp. 3-8). IEEE.

3) Afanasyev, A., Halderman, J.A., Ruoti, S., Seamons, K., Yu, Y., Zappala, D. and Zhang, L., 2016, September. Content-based security for the web. In Proceedings of the 2016 New Security Paradigms Workshop (pp. 49-60).

4) Aitzhan, N.Z. and Svetinovic, D., 2016. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Transactions on Dependable and Secure Computing, 15(5), pp.840-852.

5) Al-Riyami, S.S. and Paterson, K.G., 2003, November. Certificateless public key cryptography. In International conference on the theory and application of cryptology and information security (pp. 452-473). Springer, Berlin, Heidelberg.

6) Beynon-Davies, P., 2020. Business information systems. Red Globe Press.

7) Boneh, D., Di Crescenzo, G., Ostrovsky, R. and Persiano, G., 2004, May. Public key encryption with keyword search. In International conference on the theory and applications of cryptographic techniques (pp. 506-522). Springer, Berlin, Heidelberg.

ISSN: 2366-1313

8) Brodie, C., Karat, C.M., Karat, J. and Feng, J., 2005, July. Usable security and privacy: a case study of developing privacy management tools. In Proceedings of the 2005 symposium on Usable privacy and security (pp. 35-43).

9) Christidis, K. and Devetsikiotis, M., 2016. Blockchains and smart contracts for the internet of things. Ieee Access, 4, pp.2292-2303.

10) Creswell, J. W., 2014. Research Design: Qualitative, Quantitative and Mixed Methods Approaches. London: Sage

11) Creswell, J. W., and Creswell, J. D., 2017. Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

12) Fischer-Hübner, S., 2001. IT-security and privacy: design and use of privacy-enhancing security mechanisms (No. 1958). Springer Science & Business Media.

13) Gambino, A., Kim, J., Sundar, S.S., Ge, J. and Rosson, M.B., 2016, May. User disbelief in privacy paradox: Heuristics that determine disclosure. In Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (pp. 2837-2843).

14) Gao, W., Hatcher, W.G. and Yu, W., 2018, July. A survey of blockchain: Techniques, applications, and challenges. In 2018 27th international conference on computer communication and networks (ICCCN) (pp. 1-11). IEEE.