Risk management in blockchain

إدارة المخاطر في المعاملات الرقمية (البلوك تشين)

by

SULTAN AL HOULI

Dissertation submitted in fulfilment
of the requirements for the degree of
MSc PROJECT MANAGEMENT
at
The British University in Dubai

October 2018

DECLARATION

I warrant that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.

I understand that a copy of my research will be deposited in the University Library for permanent retention.

I hereby agree that the material mentioned above for which I am author and copyright holder may be copied and distributed by The British University in Dubai for the purposes of research, private study or education and that The British University in Dubai may recover from purchasers the costs incurred in such copying and distribution, where appropriate.

I understand that The British University in Dubai may make a digital copy available in the institutional repository.

I understand that I may apply to the University to retain the right to withhold or to restrict access to my thesis for a period which shall not normally exceed four calendar years from the congregation at which the degree is conferred, the length of the period to be specified in the application, together with the precise reasons for making that application.

_____

Signature of the student

COPYRIGHT AND INFORMATION TO USERS

Abstract

The aim of the research is to identify the different concepts of blockchain which helps in easier identification of the different risks and the issues associated with blockchain technology. Blockchain is an emerging concept and therefore, it is necessary to identify the different risks and the issues associated with the blockhain technology. The research involves an extensive literature review that aims in thorough understanding of the different concepts and the structure of blockchain architecture. The data collection and data analysis is an important chapter of this research project since it aims in providing an accurate knowledge about the effectiveness of the different risk mitigation approaches that is identified in the literature review section. The research objective is to identify the different risks and the issues associated with a blockchain technology, its system and applications along with the recommendation of the strategy that will help in easier management of the risk and different issues associated with the use of blockchain. It is essential to identify the different risks associated with the use of blockchain and its application and the use and adoption of the blockchain technology is expected to increase in future

نبذة مختصرة

الهدف من البحث هو التعرف على المفاهيم المختلفة لتقنيةالبلوكتشين مما يساعد في التعرف على المخاطر المختلفة والمسائل المرتبطة بتكنولوجيا البلوك تشين. البلوك شين هو مفهوم ناشئ وبالتالي ، فمن الضروري تحديد المخاطر المختلفة والقضايا المرتبطة بتقنية البلوك تشين . اختار الباحث نهجًا أساسيًا لجمع البياناتالأولية لهذه الدراسة. يتضمن البحث مراجعة شاملة للدراسات السابقة والتي تهدف إلى فهم شامل للمفاهيم المختلفة وهيكل بنية البلوك تشين. يعتبر قسم مراجعة الدراسات السابقة جزءًا مهمًا من هذا المشروع البحثي حيث يهدف إلى تحليل المفاهيم المختلفة والقضايا المرتبطة بتكنولوجيا البلوك تشين. يتبعه قسم مراجعة الدراسات السابقة في البحث ، يهدف البحث إلى جمع البيانات الأولية وتحليل البيانات إحصائياً. يمثل جمع البيانات وتحليل البيانات فصلاً هامًا من هذا المشروع البحثي ، حيث يهدف إلى توفير معرفة دقيقة حول فعالية أساليب تخفيف المخاطر المختلفة التي تم تحديدها في قسم مراجعة الدراسات السابقة. الهدف من البحث هو تحديد المخاطر المختلفة والقضايا المرتبطة بتكنولوجيا البلوك تشين جنباً إلى جنب مع توصية الاستراتيجية التي ستساعد في سهولة إدارة المخاطر والقضايا المختلفة المرتبطة باستخدام البلوك تشين. من المهم أن نفهم الحاجة إلى إدارة مختلف القضايا والمخاطر المرتبطة بالبلوك تشين ضخمة لأنها تستخدم من قبل عدد من منظمات الأعمال في الآونة الأخيرة. هناك عدد من التطبيقات لتكنولوجيا البلوك تشينالتي تشمل العملة الرقمية (بتكوين) ، والعقود الذكية ، ايثريوم وهلم جرا. من الضروري تحديد المخاطر المختلفة المرتبطة باستخدام البلوك تشين وتطبيقاته ومن المتوقع أن يزيد استخدام وتبني تقنية البلوك تشين في المستقبل. وقد تم اتباع نهج منظم للبحث للتوصل إلى أسئلة البحث المحددة والإجابة عليها

Acknowledgement

The research study has considerably helped me in improving my knowledge and ability. This has been possible as the research project have helped me in facing the challenges and conquering them. It would not have been possible for me to conduct the research without the significant direction of my professors, companions and every one of who have added to this advancing knowledge. I want to thank my supervisor **Dr Maria Papadaki** for helping me in my research work as well as for giving their full support during the research study. I would also thank all the participants within this study for giving their time and helping me out with the project. From the support of people, I am inspired to work on further researches in this subject area. Finally, thank you to my family members who always encouraged me. Thank You.

CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

CHAPTER 1: INTRODUCTION

1.1. BACKGROUND OF THE RESEARCH STUDY

Blockchain is an ingenious invention and is an incorruptible digital ledger facilitating the economic transactions that can be programmed for recording every sort of transactions. The information that is held by blockchain technology mainly exists as a shared and continually reconciled database (Swan 2015). Blockchain can therefore be described as digital ledger which is associated with bitcoin and transaction with other cryptocurrencies. These transactions are recorded in chronological order and can be accessed by public. Blockchain is a technology behind bitcoin and other cryptocurrencies as it enables a user to share their ledger of transaction through this technology. Each transaction in a blockchain is recorded in blocks and each block is linked with the previous block thus forming a chain. These records or block of information gets distributed to all the participants in a particular network thus making the transaction public (Zyskind and Nathan 2015). One significant feature of blockchain technology is that the records can be updated only by the consensus from the majority of the participants of the transaction and therefore this is one of the most secure transactional processes. Bitcoin is one of the mostly used applications of blockchain technology and has gained strong focus across the financial institution. There are a number of factors that makes the technology of blockchain a leading one. Blockchain transactions do not require any intermediaries, which make the technology quite cost efficient (Kosba*et al.* 2016). This in turn lowers the risk of corruption and in turn reduces the transaction costs. The technology further supports real time data processing that increases the transparency in each transaction. The blockchain transaction further ensures improved control as it avoids data duplications. Every blockchain transaction ensure higher data security and data encryption and therefore blockchain technology can be securely used in payments, settlements, capital market,

smart contracts trade finance, digitization and record keeping. Blockchain technology indeed has a bright future.

Blockchain functions as a distributed ledger that is responsible for maintaining a permanent and tamper proof record associated with transactional data (Underwood 2016). This decentralized database of blockchain is managed by the computers that belong to peer to peer network and therefore each computer in a distributed network has to maintain a copy of the digital ledger which prevents a single point failure (Iansiti and Lakhani 2017). These copies of transaction are validated as well as updated simultaneously in order to eliminate the chances of error. A blockchain is a distributed database of records and is a technology where each transaction in the public ledger is verified (Pilkington 2016). Since the entered information of a blockchain technology cannot be erased, blockchain is considered one of the leading technologies of recent times. Blockchain establishes a system of distributed consensus in a digital world (Crosby*et al.* 2016). This technology opens the door for development of a scalable and democratic digital economy. This is possible as blockchain contains a verifiable record of each transaction. However, there are certain risks associated with the use of blockchain technology that is needed to be evaluated.

There are certain technologies, that not only improves the speed or efficiency of a process but also revolutionize an existing paradigm. Blockchain technology is a similar technology where the data is secured with the help of encrypted blocks that are accessed via a peer to peer network. Since the transactions are recorded in a distributed network instead of centralized systems, there are very less chances of risk in the system (Peters and Panayi 2016). Blockchain has a number of applications out of which the cryptocurrency is one of the most widely used applications of blockchain (Walch 2015). It will therefore be interesting to observe the development and sophistication of this technology. Before that, it is necessary to understand and manage the risks

associated with the blockchain technology. The research will mainly highlight the risk management process that will help in easier use and application of the technology. Although the distributed network of blockchain looks quite promising to eliminate certain existing risks in the transactional process, it does not guarantees the elimination of the new set of risks from the system (Zhenget al. 2016). Since it is not possible to anticipate all the risks that are associated with blockchain, risk management associated with the blockchain technology is essential. There are a number of risks or certain causes of risks that is needed to be addressed in order to ensure successful implementation of blockchain applications. These risks mainly arise because blockchain is a decentralized technology and there are no intermediaries to handle a particular risk or dispute the resolution in times of needs. The absence of an intermediary controller might lead to accidental loss of the private keys which in turn might result in certain irretrievable loss (Heires 2016). Furthermore, sourcing the blockchain technology might result in a significant third party risk exposure and therefore, the process of risk management in blockchain becomes a necessary need.

One of the essential aspects of scrutinizing the risk management process in blockchain is scrutinizing the cryptocurrencies since it is one of the most widely used applications of blockchain technology. The successful adoption and operation of a new technology like blockchain require appropriate management of the risks associated with the technology. This concept is particularly true when a distributed ledger like blockchain is in question. The technology of distributed ledger has potential to be used as the backbone of many core platforms in future and therefore, risk assessment and risk management for this technology is quite essential (Iansiti and Lakhani 2017). Blockchain as a whole helps the organizations in minimizing the risks associated with a system and therefore it is essential to evaluate the risks associated with this technology.

The security in the technology of blockchain can be ensured by properly plan methods and technologies. The strategies of risks management in blockchain will be discussed and evaluated in this research study. The need for risk management in blockchain is integral as it is one of the leading technologies of recent times (Iansiti and Lakhani 2017). Furthermore the blockchain technology is considered as a foundational technology for the future of risk management. The research study will be evaluating the different causes of risks and will try to find out the strategies that might help in risk management and mitigation of the risk.

1.2. AIMS OF THE STUDY

The research aims at analyzing the concept of blockchain technology and the risks associated with this technology. Blockchain is expected to be one of the leading technologies in future and is expected to form the base of secure transactions. It is therefore essential to identify and understand the risks associated with the blockchain technology so that the proper use of same can be established. However, in order to understand the risks associated with the system, it is essential to understand the technology of blockchain and this research study aims at evaluating the same. The research report further aims at identifying the different strategies of risk management so that the identified risks can be eliminated. For that a primary research will be performed as the research report aims at collection of primary data for analysis of the research problem that is to be identified (Lindman, Tuunainen and Rossi 2017). The aim of the research is to investigate the different features of blockchain technology in order to identify the risks that are associated with this blockchain. The research study will be performed according to the objectives of the research that is identified in the following section.

1.3. OBJECTIVES OF THE STUDY

The objectives of this research report as identified are as follows-

1. To understand the technology of blockchain

2. To identify the risks associated with the blockchain technology.

3. To assess the risk management process in blockchain.

4. To recommend certain strategies to eliminate the risks associated with blockchain technology.

The above points are the identified objectives of the research project. Based on these objectives, the research questions for this research study are formulated that will lead the project in a particular direction.

1.4. RESEARCH QUESTIONS

The research questions that give an idea of the identified research problem that this research project will address are as follows-

1. What is the technology behind blockchain?

2. What are the major risks associated with a blockchain?

3. What is the different risk mitigation approaches that can be employed to address the different risks associated with blockchain?

4. What are the strategies that can ensure secure use of blockchain technology?

1.5. RATIONALE OF THE STUDY

Blockchain is a new technology that is capable of revolutionizing the future of transaction. Therefore it become essential to identify the risks associated with this technology so that the mitigation of same becomes easier. Blockchains are of two types, which are permission-less blockchain and permissioned blockchain. The permission-less blockchain allow any party to participate in a network while that of a permissioned blockchain can only be formed by consortiums or administrator who evaluates the participation of an entity in a blockchain network. The risks in both permissioned and permission-less block chain is needed to be evaluated and therefore this research project has been undertaken. Blockchain technologies in recent times are appearing in a variety of commercial applications (Iansiti and Lakhani 2017). It is expected that blockchain applications will be increasing in recent years and therefore, this research project is justified as it will be unveiling the issues associated with the blockchain applications. The use of Bitcoin which is one of the main technological innovations of blockchain is expected to increase as well and therefore, it is essential to address the risks associated with the blockchain and the application.

The research study evaluates the concept, feature and structure of blockchain technology. The research project will be analyzing the various risks that a blockchain application might face so that the strategies for eliminating those risks can be identified. The risk mitigation approaches of blockchain technology will be evaluated in this research study.

1.5. SCOPE OF THE RESEARCH

The entire research project is divided into a number of chapters for evaluating the blockchain technology and the risks associated with the technology. Risk identification will be followed by proposing certain risk mitigation approaches that will help in eliminating the identifying risks. The overview and the brief content of each of the chapter of this research project is discussed in the following paragraphs-

***Chapter 1: Introduction*-** In this chapter, the topic of the research is proposed and brief introduction of the topic, background, aims and objectives of the research topic is proposed in this chapter. This chapter will be identifying the objectives of the research that will drive the researcher to the right direction. This is an important chapter as it forms the basis of the entire chapter as the objectives and the aims of the research will be identified in this chapter. This chapter will provide an idea of the aims and objectives of the research to the readers. Structuring the chapter to the best of knowledge of the researcher is essential in order to develop a clear base for the research that will be conducted. The research will be based on the topic of blockchain and risk management.

***Chapter 2: Literature Review*-**The literature review chapter will be discussing and analyzing the different theories associated with blockchain and risk management in blockchain. The purpose of the literature review chapter is to place each work or theory in the context of contribution to the detailed analysis of the identified research problem. This chapter will be locating the research within the context of the existing literature so that understanding the research problem is easier. The literature review chapter will be a great help of the researcher in analyzing the concept of blockchain and risk management. This chapter will not only evaluate the concept of blockchain but will also identify the risks associated with the use and operation of blockchain.

The existing literature will be evaluated so that the gaps between the real life implications and the theoretical evidences of the research study are assessed (Iansiti and Lakhani 2017). A detailed review of the literature will help the researcher in identifying and understanding the issues and challenges in use and adoption of blockchain technology and its different applications. The chapter provides a detailed understanding of the issues, features, advantages and the challenges associated with the technology of blockchain. This chapter is one of the most important chapters since it evaluates the previous researches that has been carried out in this topic. Furthermore, it is important to incorporate the comprehensive review of the researchers that have been performed in this field so that the future studies in this field are evaluated. The literature review chapter will be evaluating the books, scholarly articles and journals which are relevant to the topic of the research topic. Literature review is important to identify the data sources that the previous researchers have used so that evaluation of the research topic and the research problems become easier. Furthermore, the literature is important to record the thoughts and experiences which would otherwise have been inaccessible to others and therefore, this is an important chapter of the research project.

Chapter 3: Methodology- The research methodology chapter proposes the tools and techniques that will be followed while performing the research in the topic of blockchain and risk management. In this chapter the researcher identifies the process and method of data collection. The purpose of research methodology is to inform proper action that will help in conceptualizing the findings of the research in an appropriate manner. It is expected that a research project will be of high quality and will be used to create or produce a knowledge that will be applicable even outside the research setting and thus the research methodology chapter is an important consideration of the research. A primary research methodology will be followed in this project and primary data will be collected by conducting surveys.

Chapter 4: Data Analysis- This chapter of the research project is one of the important chapters of research project as this chapter provides the main findings of the research project. This chapter provides the highlights of the collected data and the analyses the same in order to find answers to the identified research questions. The chapter will help the researcher in collecting relevant information that is required to channelize the entire research work in a particular direction. The findings of this chapter will be discussed in details in the following chapter.

Chapter 5: Discussion- this chapter will provide a discussion on the findings of the previous chapter and the extent to which the undertaken research will be able to identify and analyze the problems that have been identified. This is an important chapter of the research project as it unveils the validity and the effectiveness of the research that has been performed.

Chapter 6: Conclusion and Recommendations for further research: This will be the final chapter of the research project. This chapter will be concluding the findings of the research and will link the objectives with the data obtained from the research. The chapter will provide certain recommendations based on the obtained results of the research. The aim of this chapter is to summarize the contents and the findings of the research project.

CHAPTER 2: LITERATURE REVIEW

2.1. INTRODUCTION

The purpose of this chapter is to review the literature in the field of blockchain with an aim of identifying the issues and risks in blockchain technology. This will help in developing the base of the research as the literatures available in this field will be reviewed. Based on the findings of this chapter, the different risks associated with the use of blockchain will be identified. This would further help in collection of data for the research which will be performed in the later section of this research paper. This chapter of the research paper discusses and analyzes the different theories, principles and the concept associated with a blockchain technology. Blockchain is an emerging concept and therefore the review and the findings of the previous literature will help in understanding the concept of blockchain. Furthermore, it will provide a preliminary idea of the different risks associated with the different applications of blockchain. The literature review section of this research study will incorporate the current knowledge of the researcher and previously published literature along with practical findings. This will help in developing the base of the research topic.

2.2. THE CONCEPT OF BLOCKCHAIN

According to Scott(2016), Blockchain can be described as a digital ledger that deals with the transactions that are made with bitcoin and other cryptocurrencies. As per its design, blockchain is a decentralized technology used by a global network of computers that jointly manages the bitcoin transactions. It can be considered as an undeniably ingenious invention since the technology of blockchain created a new type of internet by allowing digital information to be distributed among the members. One of the greatest applications of blockchain technology is

bitcoin which is also referred to as digital gold. In the recent years, cryptocurrency has become a buzz worthy topic both in industrial sector and in academics. One of the most successful cryptocurrencies is bitcoin which reached a huge success as its capital market reaching 10 billion dollars in 2016 (Zheng*et al.* 2017). With a data storage structure that is specifically designed to operate with blockchain. Blockchain is a public ledger that stores all the transactional details in list of blocks. The security of blockchain technology is ensured by asymmetric cryptography and distributed consensus algorithm. The key characteristics of blockchain technology are decentralization, anonymity, auditability and persistency. These characteristics make the technology of blockchain effective and efficient.

Blockchain is an indestructible ledger (digital) of different economic transactions used for recording financial as well as all the virtual transactions. The information that is held with blockchain exists as a shared database so that the information is available to public. The database of blockchain is not stored in a single location and therefore the records are truly public and easily verifiable. Blockchain technology is similar to internet supported with the fact that has certain built in robustness (Crosby*et al.* 2016). The information is stored in form of blocks which are linked with its previous blocks. Since different blocks of information are stored across a network, the blockchain technology cannot be controlled by any single entity or authority and it has no single point of failure.

It is observed that the blockchain network or technology as a whole is transparent and incorruptible as it operates in a state of consensus where one automatically checks in with itself in every ten minutes. This is a system of self auditing as the blockchain system reconciles each and every transaction in an interval of ten minutes. Data transparency is embedded in the network as the definition is public (Wright and De Filippi 2015). The data stored in the blockchain network

cannot be corrupted and as altering any unit of information in blockchain is difficult. This is particularly because it requires a huge amount of computing power. Although theoretically it is possible, in practical, it is not most likely to happen. However, there are certain risks associated with the blockchain technology which is needed to be identified.

It can therefore be observed that the blockchain technology redefines the process by which the exchange sector operates, but also act in favor of the global financial economy as a whole (Wright and De Filippi 2015). This is possible mainly because the blockchain technology has an ability of optimizing the global infrastructure so that it can deal with the global issues associated with the financial transactions, more effectively than the current system.

Blockchain has gained a huge popularity in a limited time mainly because it solves a most basic problem of manipulation. This is possible because the network of computing nodes make up the network of blockchain. Blockchain is a decentralized technology used by a global network of computers that manages huge database of records including the records of bitcoin transactions. Since the data is stored across a network, the technology of blockchain eliminates the need of central management of the data. Technology of blockchain therefore provides digital trust as the distributed network is committed to the transaction network's recordkeeping and security (Wright and De Filippi 2015). The transactions are secure and authentication is ensured in each transaction. The structured data in the blockchain represents the financial ledger entry that is capable of recording the transactions. Each transaction is needed to be signed digitally in order to ensure that the authenticity of each transaction. In blockchain, the chain of growing records is linked using cryptographic techniques that ensure the security and authenticity of each transaction.

2.3. HISTORY OF BLOCKCHAIN TECHNOLOGY

The most basic and primitive form of blockchain network was hash tree, which is also known as Merkle tree. Ralph Merkle in the year 1979 had patented the data structure. In peer to peer computing network, it is essential to validate data to make sure that nothing is altered or changed during the transfer. The need to ensure that only true data is sent and to maintain the integrity of the data to be shared, it was needed to create a secure chain of blocks. In the year 1991, the Merkle tree was able to create a secured chain of blocks containing a series of data records. In this chain, the newest record contains the history of the entire chain of records. This is how the blockchain was created. Followed by this, in the year 2008, Satoshi Nakamato has conceptualized the technology of distributed blockchain. In this version of blockchain, a secure history of data exchange is maintained. The transactions or data exchange is managed autonomously without making use of any central authority and thus it became the backbone of bitcoin.

In the year 2009, bitcoin was offered up to an open source community. Blockchain was introduced with the invention of bitcoin which was although proposed in 2008, it was implemented in the year 2009. The invention of blockchain for bitcoin solved the problem of double spending without the need of a trusted authority or the central server. The technology of blockchain was designed to make use of nodes agreement for transactions so that frauds in the transactions can prevented. The network of blockchain and bitcoin orders each and every transaction by putting them together in blocks. Each of the blocks of blockchain contains a definite amount of transactions which are link to the previous block. Thus blockchain emerged rapidly as it provided an option of safe and secure transaction in form of blockchain.

2.4. WORKING PRINCIPLE OF BLOCKCHAIN

Blockchain technology is considered to be one of the best inventions since the invention of internet. According to Mougayar(2016), this is particularly because the technology of blockchain allows the exchange of value without the need of a central authority. Blockchain is considered as a distributed ledger as the ledger file is not stored in any central entity or servers (Wright and De Filippi 2015). Blockchain is considered to be secured and most trusted as the blockchain keeps all the records of data exchanges. Furthermore, blockchain make use of a distributed system that verifies each transaction. Only after proper verification of a transaction, a new transaction can be added to a blockchain. The verified transaction in a blockchain is referred to as a block. One a blockchain transaction is signed and verified, it cannot be altered (Atzori 2015). Blockchain keep records of all data exchanges as every time a transaction occurs the transaction is to be signed. Both public and private key is involved in this verification process. Apart from that, each verification includes a timestamp and a unique ID number. The anonymity in each transaction come from the fact that the public key used in the transactions is a randomized sequence of letters and numbers and therefore the real identity of a person is not revealed.

Decentralization in blockchain makes it quite impervious to tampering, corruption and censorship. It is practically indestructible since a bitcoin can possess over 35000 nodes in its P2P network which cannot be destroyed. Blockchain applications works for digital asset transaction exchanged online. There are three major stages of a blockchain transaction which are validating the entries, safeguarding the entries and preserving the historic records. The application of bitcoin makes use of cryptographic proof. Each transaction in a blockchain network is protected with the

help of digital signature. This is the step that is required to verify the entries. In a blockchain transaction, the entity that is receiving a digital signature verifies the proof of ownership of the transaction (Lemieux 2016). In the next step, each transaction is broadcasted to each and every node of bitcoin network, which is then recorded in public ledger for verification. Therefore, the verification node of bitcoin has to ensure two things; one is that the spender actually owns a cryptocurrency, which is verified with the digital signature on transaction. Apart from that, it also ensure that the spender has sufficient cryptocurrency in his account or not (Crosby*et al.* 2016).

There are certain benefits of making use of a distributed network which can be well understood by 'if a tree falls in forest' through experiment. In this experiment, if a tree falls in the forest, with the cameras recording the fall, it can be certain that the tree fell. Similarly in the blockchain technology, there are a number of validators that reach a consensus by witnessing the same thing as at the same time (Wright and De Filippi 2015). Instead of cameras, mathematical verifications are used. Since the size of the network is very large, security of the network can be ensured quite easily.

Blockchain can be configured to work in a number of ways. One of the widely used applications of blockchain is bitcoin. The blockchain transaction is a shared public ledger on which the entire transaction of bitcoin relies on. The transaction in a blockchain technology enables the buying and selling of any goods.

2.5. BENEFITS OF BLOCKCHAIN

Blockchain has a number of benefits. The lack of requirement of central authority makes it an ideal ledger. Furthermore, the computers verify the transactions that settle the need of central authority for management of the transactions associated with blockchain. Furthermore, the

presence of digital signatures for verification make it more secure as in such case, fraud in the system is reduced. The concept of blockchain therefore works well in tracking the movement of assets making it more users effective.

The technology of blockchain offers the benefits of cost effectiveness and traceability. Block chain is generally used to track the movement of goods and their origin. This helps in bringing an altogether new level of transperancy to B2B ecosystem (Mainelli and Smith 2015). Since blockchain helps in detecting the point of origin of a transaction, its application in business enables the businessmen to carry out investigations in execution of certain necessary action.

Apart from this, it offers transactional and accounting benefits. Recording the transactions with the help of blockchain technology helps in eliminating human error thus protecting the data from tempering. This is possible as the blockchain records are verified every time they are passed on from one node of blockchain to other.

Another significant application of blockchain technology is smart contract. The use of smart contracts eliminates the need of time consuming contractual transactions. Transparency is maintained in smart contracts that makes its implementation even more advantageous.

Blockchain technology makes it possible to seamlessly carry out a global transaction. With the enhanced security feature, each and every transaction is encrypted and linked to the previous transactions. The improved traceability it is easier to deal with the products that are traded through a complex supply chain.

The blockchain transaction further increases the speed and efficiency of a transaction. The traditional paper based process is prone to human errors that require third party mediation. Blockchain helps in streamlining and automating the different processes of blockchain,

transactions can be completed faster and more efficient. Furthermore, with the blockchain technology, every member of the transaction has an access to the same information since it becomes easier to trust each other without the need of intermediaries. Since blockchain is a public ledger system, it records and validates every transaction that is made (Lemieux 2016). This makes the technology of blockchain more secure and reliable.

Another important benefit of making use of blockchain technology is reduced cost. For most of the business, reducing the cost of business becomes a priority and therefore, the use of blockchain technology can work for the benefit of an organization. The decentralization technology discard the need for any third party or the central authority of the system.

The industries that have successfully made use of blockchain technology include defense, government, law, energy. Blockchain offer the benefit of secure data exchange by making the process of data transfer easier. This is possible as all the transactions made in blockchain technology is made by authorized miners.

2.6. BLOCKCHAIN ARCHITECTURE

The blockchain is a sequence of blocks that stores a complete list of transactional records like a conventional public ledger. In blockchain architecture, each block is connected with the previous block. The first block is known as genesis and it does not have any parent block. The following picture represents the architecture of blockchain-

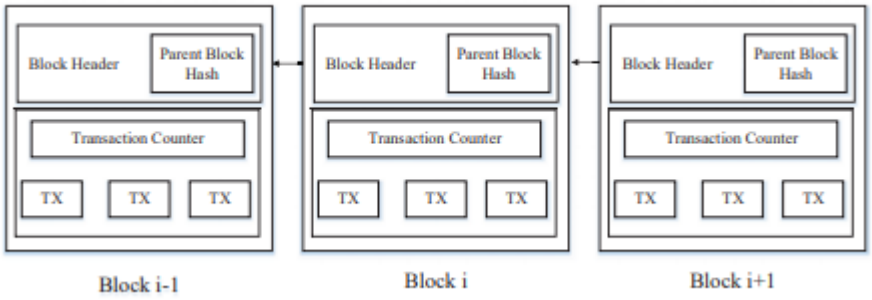

Figure 1: Representing blockchain architecture

(Source: Lemieux 2016)

Blockchain is a sequence of blocks that records and holds a complete transactional lists and records. The main composition of the architecture of blockchain is blocks of records linked together. A block forms the current part of blockchain that record the most recent transactions. The blocks are stored in the database of blockchain permanently. With the completion of each blocks of a blockchain, a new block is generated. All the blocks that are generated in blockchain are linked in a appropriate chronological order linked by the hash of the previous block. Therefore the entire copy of blockchain has a record of each and every bitcoin transaction that has been executed ever.

Each block of a blockchain contains a block header and block body. A particular block can be further divided into ***block version, Merkle tree root hash, timestamp, nBits, Nonce and parent***

hash block. The body of the block is composed of a transaction counter and transactions. The body of the block on the other hand consists of transaction counter. With asymmetric cryptography, the blockchain transaction is secured.

2.7. KEY CHARACTERISTICS OF BLOCKCHAIN

The key characteristics of blockchain are technology is as follows-

1. Decentralization: In a centralized transaction system, each and every transaction is needed to be approved through a central trusted agency. Consensus algorithm in blockchain is used to maintain consistency of a transaction in a distributed network.

2. Persistency: This is one of the key characteristics of blockchain technology. With persistency, the transactions can be validated quickly with the characteristic of persistency. Blocks containing the invalid transaction can be discovered immediately with this characteristic of persistency.

3. Anonymity: With the feature of anonymity, each user can interact with a blockchain with a particular address that is generated, without actually revealing the real identity. However, blockchain cannot guarantee the privacy preservation.

Blockchain has received an increased momentum in a small time mainly because it provides increased capacity, which is an important feature of blockchain technology. One of the most remarkable things about the use of blockchain technology is that it increases the capacity of the entire network. This is possible as a network of computers work together which offers a great computing power which is not possible for fewer devices, Most importantly it provides a better security to than any other technology.

2.8. CHALLENGES WITH BLOCKCHAIN

With the increase in the number of transaction, the entire blockchain becomes bulky. Each blockchain node needs to store all transaction and validate them as well, which makes it bulky. Therefore, a blockchain technology has scalability issues. However, there are a number of efforts that are proposed in addressing the scalability problems of blockchain technology. Storage optimization is an effort that is proposed to address the scalability problem.

Another issue that is associated with blockchain technology is privacy leakage. Although the blockchain can preserve the amount of privacy with the use of public key and private key, there is a risk of privacy. This is mainly because blockchain cannot guarantee the transactional privacy of a system.

Another issue associated with the use of technology of blockchain is that the blockchain is susceptible to the attack of different colluding selfish miners. In the process of selfish mining strategy, the selfish miners keep their mind blocks without broadcasting.

Blockchain relies on encryption to provide the security and to establish a consensus network as well. The users of blockchain have permission to write complex chain of algorithms which requires a lot of computing power which can be costly. This is one of the main reasons behind the value of bitcoin. Improved security is essential to protect blockchain and its application. Furthermore, the transaction costs in the bitcoin network is costly as it is seen that there is some politically charged aspect of making use of bitcoin and blockchain network. This is mainly because protocols of blockchains offer a good opportunity to digitize the governance models. Furthermore, the miners are forming another type of incentivized governance models giving rise to public disagreements among the different community sectors. These public disagreements are considered

to be one of the notable features of blockchain and involve updating the protocol only when the majority of the users have given consent to it. Blockchain indicates non territorial crypto-sessions that often challenge the economic position of government and legacy firms. The entangling political economy is one of the politically charged aspects of making use of blockchain technology.

The issues associated with the use of blockchain and its applications give rise to certain amount of data security risks that are needed to be addressed. The following section of the research paper discusses the risks to which the technology of blockchain or its applications are exposed to. Furthermore, the technology of blockchain is quite complex and therefore making use of the blockchain technology involves certain amount of risks as well. The network size of blockchain is huge and therefore it is not much resistant to the bad actors. A large network of users makes the network of blockchain vulnerable to attacks such as Man in the Middle attack. Blockchain is prone to Man in the Middle attack mainly because the system relies on different key agreement protocols and exchange of any type of secret key is vulnerable to attack.

It has been observed that blockchain network has an unavoidable security flaw in bitcoin. If half of the computers working as nodes in blockchain tell a lie, it will be considered as truth. This is mainly because there is no central control of authority. This type of attack is also known as 51% attack which was highlighted by Satoshi Nakamoto who is the inventor of bitcoin. The occurrence of this security flaw is however very less.

The above discussed challenges and the risks associated with the blockchain and its application gives rise to certain risks which is needed to be addressed.

2.9. MAJOR RISKS WITH BLOCKCHAIN

The issues associated with the use of blockchain technology gives rise to a number of risk that is needed to be addressed. Blockchain has a good potential to revolutionize the process by which a business is executed (Scott 2016). However, implementation of standard blockchain technology requires a significant amount of investment and management of the risks. The risk may arise with the lack of real world testing while the implementing the blockchain technology.

The blockchain transactions are considered to be secured as a consensus approach is followed. The inherent security features although make blockchain resistant to attack, it does not make them immune to attack. The security vulnerabilities associated with the blockchain technology are discussed in the following paragraphs-

End Point Vulnerability: It is one of the most likely vulnerabilities associated with the use of blockchain technology. Endpoint can be described as spaces where blockchain makes connection with human. These endpoints are computers that the users of blockchain make use of. It has been observed that the data of the blockchain is more vulnerable during its access as at that time the data on that chain is most vulnerable. This is possible as in order to access the blockchain network, the shared distributed ledger need to share his credentials. These credentials can be exposed by the present security vulnerabilities of the endpoint thus making it susceptible to attack.

Security of Public and Private Key: The data in block chain is encrypted and therefore, an access to the network of blockchain requires the use of both public and private keys. It is practically impossible to access a data in blockchain network without the correct combination of the public and private keys. This can be both strength and weakness of the technology of blockchain and its application (Wang*et al.* 2017). This is because without the right combination of public and private

keys the data in the blockchain cannot be accessed. However, with the correct knowledge of the keys, a hacker can easily access the data from the system (Byström 2016). There is no possibility of guessing the public and the private keys and therefore the only way to get its access is by stealing them. This can be done by attacking the weakest point of a blockchain network that is the endpoints.

Vendor Risks: There are certain risks associated with the blockchain integration platforms and in payment processing. With the increase in adoption of the blockchain and its application, the security risks in making use of third party blockchain applications and platforms increases (Raval 2016). A threat from a blockchain vendor increases more with the use of blockchain applications like smart contract. The entire operation of an organization can be at a greater security risk as the vulnerability in blockchain network or in its applications like smart contracts can be catastrophic (Morabito 2017). Furthermore, avoiding the vendor related blockchain weakness might require a thorough venting of each and every vendor.

Untested growth: The growth of the blockchain technology poses certain significant security risks. The blockchains are large and it is susceptible to attack. With a drastic growth in blockchain network, there is a risk of it being untested at a full scale. Although the blockchain architectures are inherently scalable, there might be certain significant security issue that might arise from organic expansion of blockchains.

Lack of Standards and Regulations: Lack of standards imposes a huge security risk on the use of blockchain and its applications. The lack of standard protocols means that the developers cannot benefit from the mistake of others. Furthermore, at some point of time, the

chain of blockchain is needed to be integrated as lack of standardization can result in increase of the security risks in the blockchain.

The above discussed point gives an idea of the major security risks associated with the use of blockchain technology (Aste, Tasca and Di Matteo 2017). Apart from this, the technology of blockchain is associated with the privacy concerns. Since the blockchain technology is here to stay it is essential to ensure proper risk management in blockchain.

The blockchain can be divided into two categories, which are permissionless blockchain and permissioned blockchain. The technology of blockchain is further associated with a number of risks in their current business processes. The risks are categorized into external risks and internal risks. These risks are as follows-

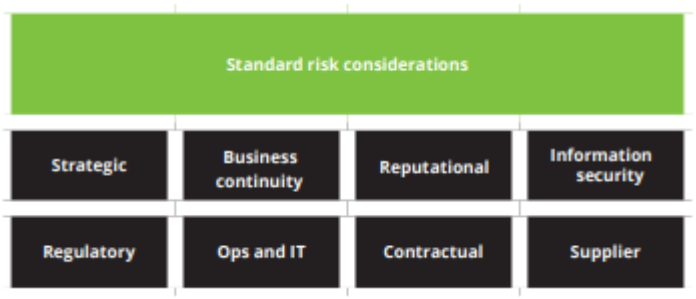

Figure 2: Representing the Risks

(Source: Mainelli and Smith 2015)

External Risk to Business

The external risks associated with blockchain that are needed to be addressed are as follows -

Strategic Risks: There are certain strategic risks associated with the use and application of blockchain. The different business strategies that are followed in the organizations have varied level of risks. The peer reviewed nature of the blockchain application makes it more vulnerable to attacks.

Business Continuity Risk: This is another significant risk associated with the use of blockchain and its application. The business processes that are built on the blockchain network make it more vulnerable to cyber attacks mainly because it is a payment processing system and hacking into the system will be beneficial to the attacks. In order address this risk, it is needed for a firm to have a robust framework of business continuity and a governance framework to mitigate the associated risks (Ølnes 2016). Since the blockchain technology shorten the duration of the many business processes the business continuity plan that is to be proposed should account for a considerably shorter incident response and recovery time.

Reputational Risk: The technology of blockchain involves working on a legacy infrastructure. Any issues with the use of blockchain can result in poor experiences of the client along with certain regulatory issues (deloitte.com. 2018). Blockchain is a part of core infrastructure and it needs to work seamlessly with the legal infrastructure as well if implemented. Failure in doing so might result in poor client experience along with the regulatory issues.

Risk of information Security: The transactions associated with a blockchain network is quite secure, it does not actually provide the guarantee of information security. Although the presence of cryptographically sealed ledger prevents data corruption, the values stored in the system might be susceptible to attack (deloitte.com. 2018). Therefore, information security is a major risks associated with the use of blockchain technology. The information security risk is not that prominent as of now since the advanced blockchain technology of blockchain provides transactional security. Since the transactions are accessible by the public, there is a risk of account takeover with a planned cyber security attack. The cyber security risks in blockchain still exits and therefore it is needed to mitigate this risk.

Regulatory Risk: The technology of blockchain is associated with the regulatory risk (deloitte.com. 2018). The regulatory risk might be associated with the application use case of blockchain technology associated with domestic and cross border transactions. The regulatory risk arises mainly because there are certain uncertainties associated with the regulatory requirements in blockchain applications.

Operational and IT Risks: With the increase in size of the blockchain, there are certain operational and the IT risks associated with the blockchain technology (Scott 2016). The technology concerns associated with the use of blockchain include speed, scalability and the interface issues.

Contractual Risk: It is common to have different service level agreements between the participating nodes in a blockchain network. This gives rise to the contractual risks associated with the use of blockchain technology. This type of risk is associated with an application of

blockchain that is called smart contract. Smart contract can be described as a computerized transaction protocol that executes the terms of a contract.

Supplier Risk: Firms that are making use of blockchain technologies are exposed to a significant third party risks which are generally sourced from the external vendors. The supplier risks are significant as blockchain enables peer to peer transfer of value without any supervision of a central intermediary.

Apart from these major risks, it is essential to consider the value transfer risks which are needed to be addressed as well. These risks are listed in the following section

Internal Risk to Business

The internal risks associated with blockchain that are needed to be addressed are as follows -

Consensus Protocol Risk: The value transfer in a blockchain network needs the use of cryptographic protocols that arrives at a consensus among the participating nodes. A number of cryptographic protocols are used in order to achieve a consensus among the nodes participating in a blockchain transaction (Zheng*et al.* 2016). There are certain risks associated with these protocols that are needed to be addressed.

Key Management Risks: The use of consensus protocol involves the use of public and private keys. Both these keys are to be maintained and managed in a secure way in order to prevent the accidental loss or left of the private key (deloitte.com. 2018). The key revocation is managed by generating the key revocation certificate as soon as a key pair is created. Key

management is necessary to maintain integrity in blockchain transactions. In key revocation, the public keys are permanently retired.

Data Confidentiality Risk: Although the transactions in the blockchain are secure there is a risk of data confidentiality in blockchain technology. The consensus protocol of blockchain ensures that all the participant of the transaction is able to view the transactions. In a permissioned blockchain, these transactions can be easily stored in a hashed format so that the contents of the network are not revealed (Nofer*et al.* 2017). However, a meta data will always remain available to the network participants. The monitoring of the metadata can easily reveal the information stores in blockchain thus increases the data security risks.

These are the major risks associated with the use of blockchain technology. These risks are associated with the technology of blockchain mainly because it operates in a peer to peer framework (Yermack 2015). An effective risks management framework can help in addressing and mitigating the risks that might be involved with blockchain technology.

2.10. BLOCKCHAIN AND RISK MANAGEMENT

The different risk management theories and practices helps in analyzing the risks associated with the use of blockchain. There are certain risks associated with the use of blockchain environment. Evaluation of the previously published journals and literatures provides an idea of the different techniques, processes and theories that are used for addressing the different risks associated with the technology of blockchain.

A ***contingency theory*** of risk management is found to be effective for managing the risks associated with the blockchain technology (Walch 2017). This is because the contingency approach of risk management primarily focuses on the elimination of the components contributing to the risks. There are a number of risks associated with the use of the technology of blockchain. The technology of blockchain is exposed to a number of risks that are needed to be managed. The strategic risks can be managed by the differences in the issues associated with the use of smart contracts.

The concept of risk management has become a significant consideration in both government and private sector. Risk management is an integral part in application of blockchain technology (Heires 2016). It is needed as well since with the increase in the use of blockchain and its applications, it becomes essential to identify and mitigate any risks associated with it. In the contingency theory of risk management, a senior management of an organization takes the charge of analyzing, identifying and mitigating the identified risks.

2.10.1. RISK MANAGEMENT

Risk Management is a process of identification, evaluation and prioritization of the risks so that the issues associated with the technology and application of blockchain can be evaluated. The aim of this research project is to identify and evaluate the risks associated with the technology of blockchain. The process of risk management is represented in the following picture-

Figure 3: Representing the steps of Risk Management

(Source: Lam 2014)

The first step of risk management is identification of risk. There are a number of risks associated with the technology of blockchain, one of which is the risk of privacy and confidentiality (Zheng*et al.* 2016). There is a considerable risk associated with the public and the private key that is used to encrypt the blocks of a blockchain. Any organization making use of blockchain or its application should identify these risks associated with the use of the technology.

After successful and accurate identification of all the risks associated with the blockchain technology and its application, it is essential to access the risk. Risk assessment is considered to be a significant process of risk management as it helps in prioritizing the risks (Tapscott and

Tapscott 2017). The risk with high priority and severity should be addressed first followed by the risks with low priority. The priority is set on basis of the severity and impact of the risks that are making use of blockchain and its application in the organizations.

The process of risk assessment is followed by the process of controlling the risk. A set of risk mitigation approaches is proposed against the identified risks in order to eliminate the risk. The application of blockchain technology although is considered to be secure, it is essential to address the possible risks that the technology might face. With the increase in size of the blockchain, the risks associated with the technology increases as well (Lindman, Tuunainen and Rossi 2017). This research project will be identifying the different risks associated with a blockchain technology and will enforce adequate control in order to reduce the effect of the risk on use of blockchain and its application (Mainelli and Milne 2016). The risk control stage therefore holds an important place in the risk management process.

After enforcing the control of the project, it is essential to review whether the controls that has been proposed for the project has been effective or not (Zheng*et al.* 2016). The measurement of the risk control and reviewing it therefore becomes a necessary process of risk management.

These are the necessary steps of risk management which will be followed in ensuring that the blockchain technology and the applications of blockchain can be used without any risks.

2.11. RISK MANAGEMENT IN BLOCKCHAIN

The technology of blockchain has a wide array of applications. The major use of blockchain lies in the use of cryptocurrencies. Cryptocurrencies exist in electronic and digital form and therefore it is known as digital currency. Since it exists in digital form, it can be exposed to a number of cyber security risks. Use of cryptocurrencies is convenient, simple and easy quite contrast to centralized economy (Morabito 2017). In centralized economical system, a central authority or central bank controls the monetary base and transaction of money. On the other hand, the decentralized monetary system does not have any central authority to control the monetary base. The peer to peer network of nodes creates the currency and is controlled by algorithms.

The use of most of the blockchain applications require the owning of linked digital currency. The hacking of a blockchain transaction can actually lead to the bankruptcy of an organization (Kakavand, Kost De Sevres and Chilton 2017). This is the reason behind the increasing need and importance of risk management in blockchain. Furthermore, with the increase in demand and use of blockchain and cryptocurrencies, it is possible that more organization will be looking for opportunities for participating in blockchain related activities (Shrier*et al.* 2016). Different financial and technical companies are looking forward to make a use of blockchain technology to verify the trading of gold thus digitizing the gold market. This can possibly increase the transparency and speed of gold trading thereby reducing its costs as well.

However, in order to make a correct use of blockchain technology, the banks or the organization need to understand the different risks associated with the blockchain technology and should manage those risks as well (Yeoh 2017). This is necessary as the blockchain will not only work as an application but will also be a significant component of the infrastructure of the

organization. Although the distributed nature of blockchain reduces the security risks associated, it cannot guarantee the elimination or not introduction of a completely new set of risk. The risks that a blockchain technology can possibly face will be because of certain situations, which are discussed as follows-

1. There are no intermediaries associated with the handling of the risk or dispute resolution, which is a major risks associated with blockchain technology. The absence of any controller might result in accidental loss of the private keys thus causing an irretrievable loss.

2. Secondly, sourcing blockchain technology from the vendors might often result in the third party risk exposure which should be mitigated.

3. Furthermore, in the nascent stage of blockchain, there are uncertainties regarding the regulatory requirements, resulting in regulatory risks.

An appropriate scrutinizing of the cryptocurrencies unveils a number of issues and risks associated with the technology of blockchain (Zhao, Fan and Yan 2016). One of such significant issues is tax status. However, certain countries have already worked on this issue. Switzerland has categorized Bitcoin as a foreign currency (Imbault*et al.* 2017). On the other hand, Italy has a policy of zero taxation on the use of cryptocurrencies. Russia is trying to develop a framework for regulation and taxation of cryptocurrencies (Raval 2016). However, countries like China have already banned the exchange of cryptocurrency in domestic market. Apart from the taxation issues, there are a number of other issues associated with the blockchain technology that makes the process of risks management mandatory.

There are certain challenges of risk management in blockchain. With the presence of risks such as uncertain regulatory status along with the issue in control, security and privacy, there exists a huge need of managing such risks in an effective manner.

The risk management processes that should be followed in the organizations that are making use of blockchain technology are as follows-

The use of blockchain technology indicates the requirement of significant changes to the existing tools and system. In order to participate in this transition and to avoid any possible risks it is essential for the companies to strategize the transition as a part of the risk management process (Kosba*et al.* 2016). The technology of blockchain involves a complete shift to a decentralized network and therefore development of the strategies is essential for mitigation of any risks associated with the blockchain technology and its adoption. The adoption of blockchain technology is most likely to increase since it has an ability to shape the financial sector as it is a cost effective alternative.

Apart from the risk of adoption, there are certain other risks associated with the use of blockchain and its technology. There are certain legal risks associated with the use of cryptocurrencies (Malinova and Park 2017). This is a major risk that is needed to be managed. The technology of blockchain has an ability to cross the jurisdictional boundaries as the nodes of blockchain can be located from anywhere in the world. This in turn gives rise to complex jurisdictional issues related to contractual relationships that needs careful consideration (Lindman, Tuunainen and Rossi 2017). Even in the simplest level, each blockchain transaction can fall under the jurisdiction of the location of its nodes, resulting in the need of blockchain to be compliant with an unwieldy number of regulatory regimes and legal issues. The legal issue can therefore be

termed as a major issue associated with the use and adoption of blockchain technology and thus becomes an essential part of risk management process.

There are certain performance challenges associated with the use and adoption of blockchain. The database of blockchain is growing rapidly in size with the addition of new transactions every second (Davidson, De Filippi and Potts 2016). This gives rise to certain performance challenges which is needed to be addressed. The willingness of vendors to offer performance assurance depends on three major criteria. These criteria include their risk and reward profile, the delivery model of the services provided by them and the factor of accepting the liability of a number of customers.

There are a number of different risks associated with blockchain technology mainly because of its complexity and manner of operation (Zheng*et al.* 2016). One of the major issues associated with the use of a public blockchain is its inability to be controlled or stop its functioning (Hull*et al.* 2016). Therefore, lack of control is a major issue associated with the use of public blockchain. However, this issue is not associated with private blockchain. There must be an attribution of risk and liability associated with the technology of blockchain.

As a risk management approach is it essential to evaluate whether an organization is prepared for the new risks that is posed by a blockchain framework (Frantz and Nowostawski 2016). The successful adoption of the technology of blockchain is dependent of the appropriate risk management process (Porru*et al.* 2017). Blockchain will enable business to make the transfer of data more quickly and securely. However, there is no greater risk than the global economy in coming years.

The risks management activities that is recommended to an organization that will be making use of blockchain technology are as follows-

It is essential to access the firm's activity to date in order to understand the technology department of the institution (Yli-Huumo*et al.* 2016). This will help in identifying the different risks associated with the use and adoption of blockchain technology.

It is furthermore essential to stay plugged in. The regular updates will help in easier identification of the risks and management of those risks. Apart from that it is essential to monitor the insurance market's response in order to develop appropriate strategies of risks management (Lam 2014). With the possibility of data security and privacy risk, it is essential to ensure network security for the internal network of the organization.

There are certain steps that can help in mitigation of the risks associated with the project. For example, in order to mitigate the end point vulnerability, encryption method can be enforced. Similarly the contractual risks can be mitigating by making the digital signature compulsory in each transaction (Zheng*et al.* 2016).. Cryptography is another chosen method for addressing the IT and operational risks. Resource sharing is an approach that can be used for mitigation of the risk of untested growth.

Therefore it can be said that risk management in blockchain is essential since the adoption and use of blockchain technology is likely to increase in the recent years. In order to manage the risks associated with the technology of blockchain, it is essential for the organizations to establish a robust risk management strategy and governance framework in order to eliminate the associated risk (Wright and De Filippi 2015). The technology of blockchain is considered to be secured with a lesser number of risks in consideration to a centralized authority. Therefore, it is considered to

be secure for adoption. The most important risk management strategies associated with the use and adoption of blockchain is securing the blockchain transaction on basis of cryptography, encryption, digital signature and efficient key management (Zheng*et al.* 2016). However, it is essential to develop certain strategies of risk management that will help in easy identification of the causes of the risks. Certain strategies of risk management is needed to be set so that the organization can easily identify and manage the risks associated with the technology of blockchain and issues associated with the use and adoption of blockchain technology. These strategies might relate to the use of in house designing of the blockchain network, if an organization plans to implement the same in their business processes. However, the effectiveness of each of the risk mitigation approaches is needed to be evaluated.

2.12. CHAPTER SUMMARY

Literature review is an important section of the research papers as it evaluates the previous research papers. The previously published literatures have provided a good idea of the technology of blockchain and the risks associated with the blockchain technology. The contents of this section relate to the research objectives and provide an idea of the research which will be conducted in the topic. The section of the research paper provides a brief idea of the technology of blockchain and the need for managing the risks associated with the technology of blockchain. This is because the successful adoption and operation of blockchain technology is often associated with the appropriate risk management. Since the adoption of blockchain technology will add to the core infrastructure of an organization, the identification and the management of the risks associated with is it is essential. This section of the research paper gives a clear idea of the technology behind blockchain and the benefits of making use of blockchain technology. Along with the number of

benefits there are certain issues associated with the use of blockchain technology. This section of the research paper identifies the issues and the risks that the technology of blockchain might face.

The technology of blockchain is considered to be one of the most secure forms of transaction. This is mainly because it follows a consensus protocol of self checking each transaction. The adoption and use of technology of blockchain is likely to increase as the services provided by blockchain are quite efficient. Along with this, the absence of any intermediary and its decentralization nature adds in to the benefits of blockchain.

As the technology of blockchain continues to mature, the risk practitioners across the sectors are quite excited about its promise to offer maximum services to the organizations making use of blockchain technology. Although blockchain technology is secure, there are certain issues associated with it which this chapter identifies. In order to mitigate the risks associated with the blockchain technology, it is essential for the firms to understand the business processes of blockchain in order to mitigate the risks associated with blockchain. Blockchain fall under two types, the permissionless and permissioned blockchain chain. Regardless of the type of blockchain, it is essential to identify and mitigate the risks associated with the technology of blockchain. A number of risks have been identified in context to blockchain which include strategic risk, business continuity risk, reputational risk, information security risk and so on. The risk management approach that has been proposed for management of the risks associated with blockchain is development of certain risk mitigation strategies that will help in managing and mitigating the risk.

CHAPTER 3: METHODOLOGY

3.1. INTRODUCTION

The section of the research study will help in identifying the different tools and techniques that will be used for collection and analysis of the collected data. A specific research method should be undertaken by a researcher so that the identified objectives of the research study are fulfilled. This is necessary as a particular research essentially includes a process of information accumulation and analysis of the accumulated information. Research methodology therefore refers to a collection of different tools, techniques and processes that are needed for gathering the information necessary for conducting a particular research. The research methodology will not only be evaluating the different techniques of data collection but will also provide a complete understanding of the methods being adopted. Identifying the research methods is essential for understanding the approach of the research. This chapter of the research study will provide a detailed insight of the theories and the methods that will be used for conducting the research study. The chapter will be discussing the research onion that was developed by Saunders in 2007. It provides an effective progression or idea through which a research methodology can be designed. Research methodology finds its use in a variety of context and a research study is undertaken with an aim of evaluating the risks associated with blockchain. The techniques, methods and the philosophy along with the data collection techniques are discussed in following section.

3.2. RESEARCH ONION

The different stages or phases of a research are illustrated in research onion. Research onion is used both for academic and scientific (Al 2013). Similar to the peeling of onion, a researcher go from the outer layer to the inner layer of a research onion to identify the tools, techniques and the

methods that will be used in the research study. The following picture represents the structure of research onion.

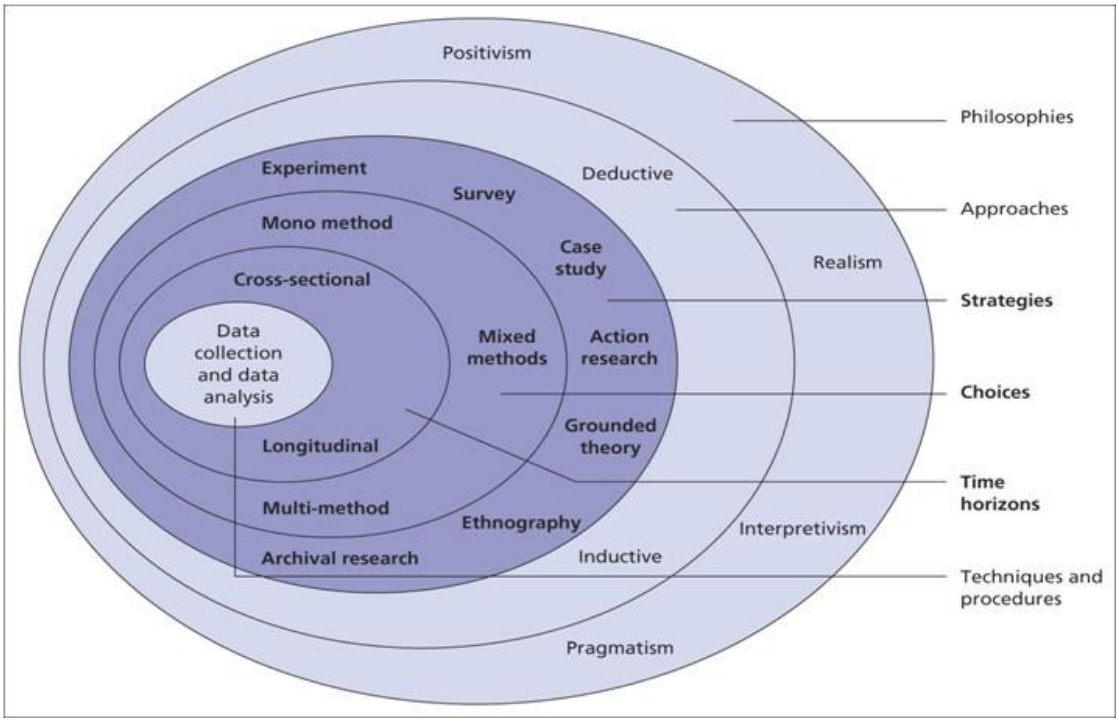

Figure 4: Representing the structure of a research onion

(Source: Sahay 2016)

Academic or scientific researchers are generally designed in order to find an answer to a specific question. Most of the researchers design a research in order to answer a specific question and therefore it is essential for the researchers to identify the type of data that will be required in order to find an answer to the specific problem (Saunders, Lewis and Thornhill, 2009). The research onion further helps indentifying the tools and the techniques that should be undertaken in order to address a specific problem.

The outermost layer of the research study talks about the philosophy of the research. Choosing an effective research philosophy is essential to route the research in a specific direction.

The next layer gives an idea of the different research approaches that is essential for a research. The next layer of research onion gives an idea of the different research strategy. Choosing a particular and appropriate research strategy is essential as it ascertains the process and the techniques that will be used for the research study. Following the research strategy, the other layers of the research onion provides an idea of the techniques and the procedure of research study. Each phase of the onion will be evaluated in the following sections.

3.2.1. FIRST LAYER OF RESEARCH ONION

The first layer of research onion gives an idea of the philosophical stances associated with a research. Research philosophy gives a structure and guidance for performing the research study. With research philosophy, it is possible for a researcher to get aware of the different processes of gathering and analyzing research information which is an essential need of a finite research. This layer gives an idea of six philosophical instances which include objectivism, constructivism, positivism, realism, interpretivism and pragmatism. The objectivism research philosophy gives an idea of the different social phenomenon which might be useful for a research. It helps in learning the different meanings of social phenomenon that may have on the social workers (Alvesson and Sandberg 2013). The constructivism is just the opposite of objectivism and it establishes that the social actors are responsible for creating a social phenomenon and that the social phenomenon may not have any impact on the social actors. The research philosophy of positivism is completely different from objectivism and constructivism. The positivism research approach helps in developing such research questions and hypothesis that can be easily tested. In the positivism research approach the researchers might find same outcome and it gives importance to quantitative results. The realism research philosophy on the other hand indicates that every theory can be revised. It establishes the fact that one cannot find reality without any continuous research

(Saunders, Lewis and Thornhill, 2009). The realism philosophy promotes the fact that a researcher should not hesitate on using the new research methods. The realism research philosophy however, enables a researcher to work with a number of research methods. The interpretivism research approach helps in interpreting the possible ways through which people generally participate in social and cultural life (Brown and Stowers 2013). The interpretivism research methods helps in interpreting the different ways through which people mainly participate in the social and cultural life. The pragmatism research philosophy on the other hand establishes the fact that constructivism and objectivism research philosophy are the ideal ways of conducting a research. For this research, positivism research philosophy has been chosen.

3.2.2. SECOND LAYER OF RESEARCH ONION

The second layer of research onion includes the different research approaches that a researcher might choose to work on a research project. There are mainly two types of research approaches, which are deductive and Inductive. In a deductive research approach the aim of the researcher is to find answer to the questions associated with the research (Saunders, Lewis and Thornhill, 2009). The objective of a deductive research approach is to come up with an option of yes or no in response to the research question. Apart from that, in the deductive research methodology, the theories of the research question are scanned to gather the data that will in finding an answer to the research question.

The inductive research approach on the other hand helps in creation of own theory and thus when the inductive research approach is undertaken for a research, the research onion works in a complete opposite way in comparison to the deductive research methods (Sahay 2016). In inductive research approach, the hierarchy of the research runs from research question to research

observation. The inductive research method works on the observation, description and analysis of the problem which in turn helps in developing a new theory at the end of the research. The inductive research methodology is therefore used in the researches that have no big requirements. In this particular research, the deductive research approach is used.

3.2.3. THIRD LAYER OF RESEARCH ONION

The third layer of research onion discusses the different strategies that can be used in a research study. The different strategies of the research study that can be followed involves experiment, survey, case study and so on. In academic research, survey and experiments and interviews are mainly used for primary research while that for secondary research the strategy of case study might be used as well.

3.2.4. FOURTH LAYER OF RESEARCH ONION

The fourth layer of research onion sheds light to the different ways of performing a qualitative and a quantitative research. This section of research onion ensures whether the qualitative and the quantitative research methods are to be used in the research or whether any one method of the research will be fine. This section of research onion further gives an idea about the frequency of making use of qualitative and quantitative research method in case a mixed research method is chosen for the research study. This layer gives an idea of the different methods of research study, which are mono method, mixed method and multi-method. In the mono method of research study the researcher mainly gathers only one type of information from the qualitative and quantitative research method. This can be determined in relation to the identified research strategy and philosophy of the research.

The mixed method of research involves both qualitative and quantitative methods for the study purpose (Sahay 2016). This method can be used for gathering as well as for analyzing the collected data. It is possible to combine both the research methods if the research objectives have a requirement for it.

The multi method of research makes use of both qualitative and quantitative data in the research but the focus mainly stays on one source only. This helps in analyzing the data in a particular point of view.

3.2.5. FIFTH LAYER OF RESEARCH ONION

This layer of research mainly deals with two time horizon methods. One of the methods is cross sectional while the other method is longitudinal (Saunders, Lewis and Thornhill, 2009). The cross sectional time horizon method can be used for conducting a short time study while that of longitudinal time horizon is used for doing a long term study.

In cross sectional research, both qualitative and quantitative research method is used. In Longitudinal research method, both qualitative and quantitative research methods are used.

3.2.6. SIXTH LAYER OF RESEARCH ONION

This layer of research onion provides an idea of the different methods of data collection and analysis. This particular section of the research onion helps in deciding the questionnaire content and the sample groups. It helps in identifying the different questions in the interviews or in online surveys (Sahay 2016). However, the philosophical stances, strategies choices and time horizons determine the data collection and analysis methods.

According to the phases of research onion the techniques, methods and the research philosophy that will be used in this particular research study is evaluated in the following sections.

3.3. RESEARCH PHILOSOPHY

Research philosophy is essential in a research study as it helps in identification and building of data and information that can be used for directing an examination. The research philosophy furthermore evaluates the appropriateness in choosing a particular process and procedure that is required for undertaking a research (Chandra and Sharma 2013). The different types of research philosophies are discussed in the research onion section of the research study.

The use of pragmatism research philosophy includes the use of logical techniques for assessing the different information that will be used for the research. The use of this philosophy therefore permits an examiner in breaking down the theme of the examination (Eaton 2013). The use of positivism research philosophy permits a researcher in making use of rationale in a logical way for evaluating the different fundamental information that has been collected for the research. Interpretivism research philosophy helps in interpreting the activities of the people and the participants of the research (Saunders, Lewis and Thornhill, 2009). The realism research philosophy on the other hand establishes the fact that one cannot find the realty of the research without continuous research. These four are the main research philosophies that are used in an academic research. For this particular research the researcher has chosen a positivism philosophy for conducting the research study.

3.3.1. DEFENSE OF SELECTING POSITIVISM PHILOSOPHY

A positivism research philosophy is chosen for the research study. The researcher has chosen this approach as utilization of the positivism approach permits a researcher in uncovering

shrouded data. Furthermore, the positivism philosophy permits the researchers to test different research questions and research hypothesis. The use of positivism research philosophy is therefore appropriate for the research study. The researcher did not consider the interpretivism and the pragmatism approach of the research as the research has a restricted time. Furthermore, the use of positivism research approach limits the research study only in the investigation and the information translation phase.

3.4. RESEARCH APPROACH

As discussed in the research onion section, the research approach can be mainly of two types, the inductive approach and the deductive approach. Deductive research approach is mainly used in the research studies that deal with the dissection of past hypothesis set by previous researchers. The use of inductive research approach on the other hand involves search of the data or searching the answers to the research question following a particular pattern or observation thus resulting in development of a new theory (Leedy and Ormrod 2013). The significant difference between the two research approaches is that the inductive approach is mainly concerned with the generation of a new theory from the available and analyzed data while that of the deductive approach encourages a researcher to make use of past theories for conducting a research (Mitchell and Jolley 2013). The use of deductive research methodology enables a researcher in conducting a research study is a legitimate way. While the use of inductive approach of research generally gives rise to new speculations and new theories associated with the research problem. The researcher has chosen to make use of deductive research approach in this research study.

3.4.1. DEFENSE FOR SELECTING DEDUCTIVE RESEARCH APPROACH

A deductive research approach is identifed for this research as it makes use of the available theories to scan a particular research question. The deductive research approach helps in gathering the data that is required for answering the identified research question. The deductive research approach further helps in collection of the data that is essential for performing a research project. The researcher has mainly chosen the deductive approach for directing the research study towards the recognizable key factors that effects the change in the research process. The use of the deductive research approach is justified since it helps in analyzing the different factors that contributes to the issues and the risks associated with the use of blockchain and its applications. The use of the deductive research approach will further enable the researcher in making use of the past idea and the speculations associated with this particular research. Therefore the choice of deductive research approach for this particular research study is justified.

3.5. RESEARCH DESIGN

For ensuring successful collection of data, it is essential to formulate a particular research design that will enable a researcher in investigating the information that is gathered from the different project source. The research design therefore enables a researcher in performing a research in a correct manner (Novikov and Novikov 2013). A particular research design ensures that the research is conducted in a particular fashion with the help of the available research information. The different types of research design are descriptive, exploratory and explanatory research design technique (Salaberry and Comajoan 2013). The aim of exploratory research design is to study the different aspects and the contexts of the area under research. On the other hand, the exploratory research design assures that the conclusive research solutions are addressed in the end

of the research. The exploratory research therefore explores the different research questions with a view of understanding the existing research problem. This type of research design is mainly chosen for the research studies where the research problem is not clearly defined (Thomas 2013). The exploratory research design therefore does not im in providing a conclusive evidence of the research problem.

The use of descriptive research design on the other hand describes the different characteristics of a subject of the research (Uprichard 2013.). In the descriptive research design, the participants are depicted and analyzed in an accurate manner and thus the researcher has chosen the descriptive research design for the research study.

3.5.1. DEFENSE FOR SELECTING DESCRIPTIVE RESEARCH DESIGN

The Researcher has developed a clear research plan for conducting a primary research and analysis of the collected data. The descriptive research design helped the researcher in making use of logical approach in analyzing and deducing the collected information. The descriptive research design is considered to be an innovative tool that the researcher makes use of for performing the qualitative and the quantitative research. Along with the appropriate research plan, the choice of the descriptive research design has helped the researcher in proper analysis of the collected data.

3.6. DATA COLLECTION METHODOLOGY

Data is a term that is specific to an information set. A set of information is necessary to understand the problems identified in a research and it further helps in analyzing the significant aspects of a particular research work (Bryman and Bell 2015). The data collection strategy of any research study is mainly classified into two types, which are primary data collection method and secondary data collection method (Brannen 2017).

Primary Data Collection: The primary data collection methodology incorporates a collection of information from the sources having a firsthand knowledge about the identified problem or the topic being researched (Ritchie*et al.* 2013). Primary data is mainly gathered by a number of approaches that include interviews, observation and surveys. Interviewing the operational personnel and the experts can be effectively used for conducting a research. Interviews are generally conducted through a telephonic process and by meeting direct respondents. However, the most widely used method for collection of the data includes survey. Online surveys are mostly used for gathering and collecting the primary data that will be used for the research.

Secondary Data Collection: The secondary data collection method mainly refers to the process of collection of data from the secondary sources (Mayer 2015). This includes the information that has been published in books, scholarly articles and in the research papers. One of the advantages of making use of secondary research method is that a huge amount of information is already available on the field of research.

The researcher has chosen a primary data collection methodology for the research study. For collection of primary data, a questionnaire has been designed with close ended questions. The questions were based on the mitigation approaches of the risks that have been identified in the literature review section of the research study. The data analysis method for the research is discussed in the following section.

3.7. DATA ANALYSIS METHODOLOGY

There are mainly two types of data analysis methodologies that are followed in an academic research. These are qualitative data analysis and quantitative data analysis.

The qualitative data analysis is associated with a range of processes and procedures that evaluates the non numeric information of the data collected (Smith 2015). There are mainly five categories into which the qualitative data can be analyzed (Jensen 2013). These include content analysis, narrative analysis, discourse analysis, framework analysis and grounded theory (Eriksson and Kovalainen 2015).

Quantitative data analysis on the other hand involves mathematical calculation of the collected data (Edson, Henning and Sankaran 2016). Excel spreadsheets and SPSS are two of the most commonly used tools of quantitative data analysis.

In order to evaluate the risks associated with the use of blockchain and its application, an online survey will be conducted. The collected data will undergo quantitative data analysis as it will enable the researcher to collect and analyze an accurate data that can be used in the research.

3.8. POPULATION AND SAMPLE

The research will be considering the use of online survey based on a set questionnaire to collect the information associated with the research and the risk mitigation approaches of the research. For this, more than 80 respondents were approached to attend the survey so that data about the mitigation process of the identified risks can be obtained. The respondents of the survey mainly include Blockchain Developer, Network Security Officer, Blockchain Architect, Information Security Officer and others.

3.9. ETHICAL CONSIDERATIONS

Since the research will be considering a primary data collection technique, certain research considerations should be enforced. There are several fundamental guidelines associated with a

research which are needed to be followed while performing the research. These are discussed as follows (Cacciattolo 2015)-

1. Respect and safety of the respondents will be first and foremost priority for the researcher.

2. It is essential to obtain the permission of the participants before proceeding with the process of data collection (Connelly 2014).

3. The anonymity of the respondents participating in the survey should be maintained.

4. The transparency in the collected data should be maintained and misquoting the collected data should be prohibited in the research.

3.10. CONCEPTUAL FRAMEWORK

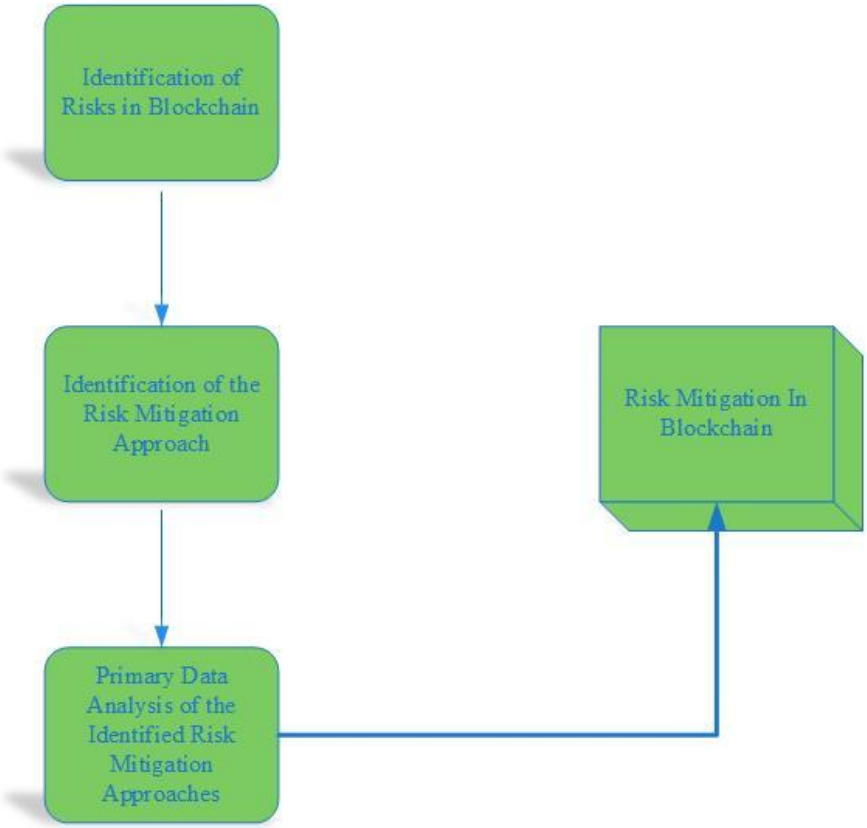

Figure 5: Representing the conceptual framework

(Source: created by author)

3.11. RESEARCH HYPOTHESIS

On basis of the research question, the following research hypothesis is established.

Null Hypothesis (H0): There are no such mitigation approaches that can completely mitigate the risk in blockchain

Alternative Hypothesis (H1): The Identified mitigation approach can possibly mitigate the identified risks in blockchain.

3.12. CHAPTER SUMMARY

This chapter of the research study provides an idea of the different tools and techniques that will be used in the research. This chapter of the research paper gives an idea of research onion and explains its use in conducting the research. The research about the risks associated with a blockchain will involve the use of positivism research philosophy along with a descriptive research design. A deductive approach is chosen for the research in order to find the answers to the set research questions. Choice of appropriate tools and techniques ensure accurate analysis of data. The researcher will be collecting a primary data for the research and will embark on a quantitative data analysis. The chapter furthermore gives an idea of the ethical considerations associated with a research study.

CHAPTER 4: DATA ANALYSIS

4.1. INTRODUCTION

The different risks that are associated with blockchain are identified in the literature review section. Based on the risk mitigation approaches that are identified, a survey has been done with 80 respondents to check whether the identified risk mitigation approaches for the risks in the blockchain are viable or not. The different risk mitigation approaches that have been proposed for mitigation of the risks associated with blockchain include encryption, use of digital signature, choosing a trusted vendor, cryptography, shorter incident response plan and by enforcement of standardized control, management of public and private keys and so on. Certain strategies are proposed as well in order to reduce the data vulnerabilities associated with blockchain. These are certain basic steps that can be taken for mitigation of the risks. In this section of research project the collected data will undergo quantitative analysis in order to assess the viability of the proposed solution and to identify the mitigation approach that will be best suited for accessing the problem. With the help of graphs and charts in the collected data will be analyzed to determine the viability of the option. The use of Blockchain has seen an exponential increase and therefore the risks in blockchain increases as well. This is one important section of the research report as it will analyze the collected data and will help finding an answer to the problem identified. The survey has acquired mixed reaction on the mitigation approaches that have been chosen for mitigation of the risks associated with the technology of blockchain.

4.2. ANALYSIS OF THE COLLECTED DATA

The literature review section of the research project has identified different risk mitigation approaches for the identified risk. Based on certain major mitigation approaches a questionnaire

had been prepared to collect data about the opinion of the respondents regarding the viability of the mitigation approaches that has been identified against the major identified risks associated with the project. The respondents are chosen from a group of people who have an experience in working with blockchain and security. The opinions of these members are collected to assess the risk management process in blockchain.

4.2.1. DEMOGRAPHIC DATA

A total of 80 respondents are chosen for the analysis and data about their field of work has been collected. The table below represents the detailed field of work of the respondents of the survey. The table below represents the details of the respondents in the survey.

Row Labels	Count of What is your Field of Work?
Blockchain Architect	16
Blockchain Developer	9
Risk Manager	15
Network Security Officer	29
Testing Engineer	11
Grand Total	**80**

Table 1: Demographic Data of Field of Work of the Respondents

From the above table, it is clear that the majority of the respondents of the survey have a work experience in the field of Network security officer. The responses have been collected from the individuals having a firsthand knowledge about the risks and the issues in blockchain. . The Chart below represents the percentage of the respondents in each category.

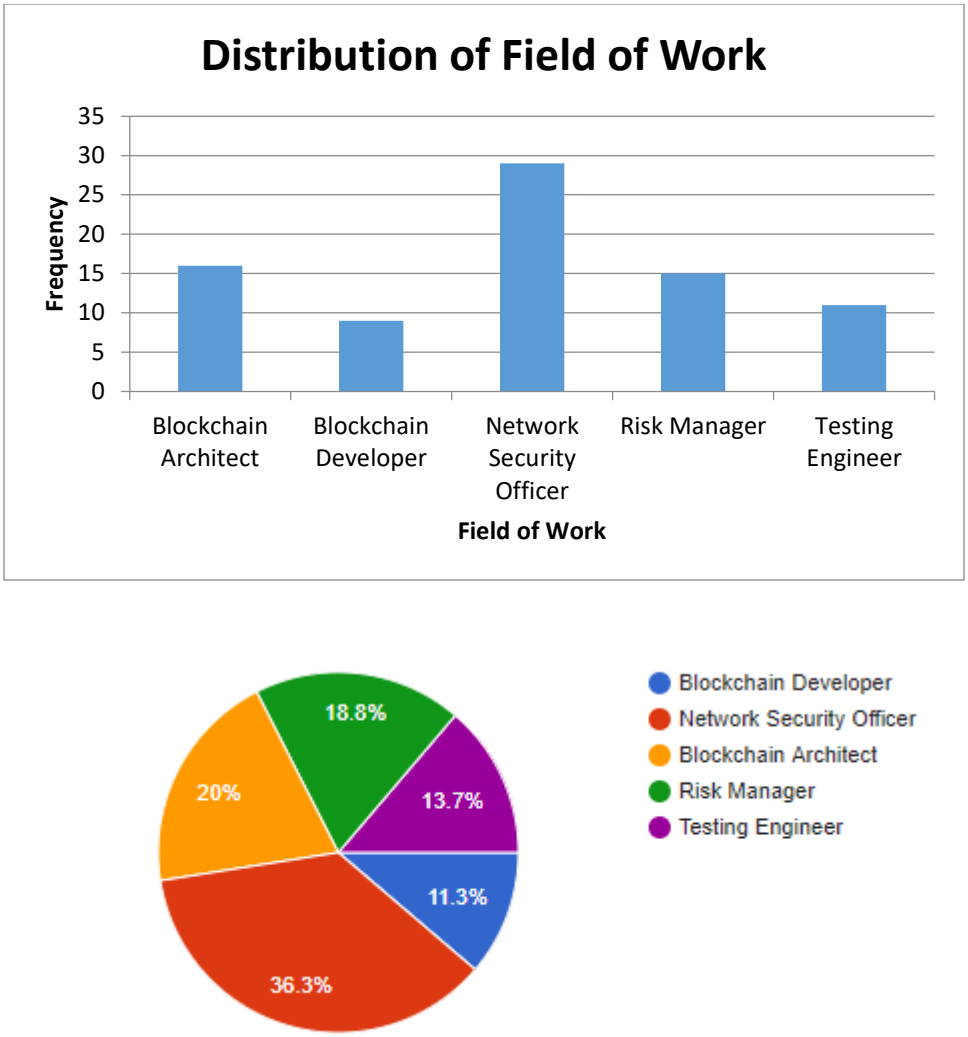

Figure 6: Demographic Data of Field of Work of the Respondents

(Source: Data Based)

As a part of the demographic data that has been collected during the survey, the experience of each of the respondents in their field of work is identified. The table below represents the field of work of each respondent of the survey.

Row Labels	Count of What is your Work Experience in this Field?
0-2 Years	7
3-5 Years	58
More than 5 Years	15
Grand Total	**80**

Table 2: Demographic Data about the experience of the respondents in their field of work

From the above table it can be concluded that all the respondents have a significant experience in the field of blockchain and therefore these respondents are suitable to access the risk mitigation approaches that has been identified against the different risks associated with the project. The chart below represents the distribution of the work experiences of the respondents.

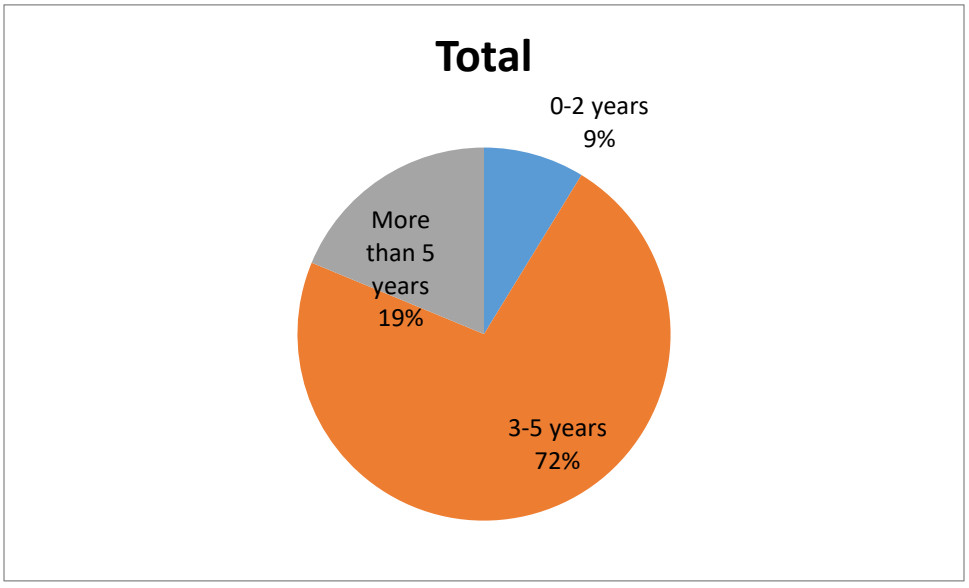

Figure 7: Demographic Data about the experience of the respondents in their field of work

(Source: Data Based)

From the above chart, it can be seen that almost 72 percent of the respondents of the survey has at least 3 years of experience. The following section of the research report analyses the collected data to evaluate whether the proposed risk mitigation approaches are viable or not.

4.2.2. DATA ANALYSIS OF THE DATA COLLECTED FROM SURVEY

The respondents were asked to opine about the use of encryption in mitigation of the end point vulnerability risk in blockchain. Majority of the respondents have agreed that encryption is indeed a good approach for mitigation of the ***end point vulnerability*** in blockchain.

	Frequency	Percentage
Strongly Disagree	5	6.3 %
Disagree	5	6.3%
Neutral	12	15.00%
Agree	56	70
Strongly Agree	2	2.5%

Table 3: Representing the opinion about encryption being a risk mitigation approach

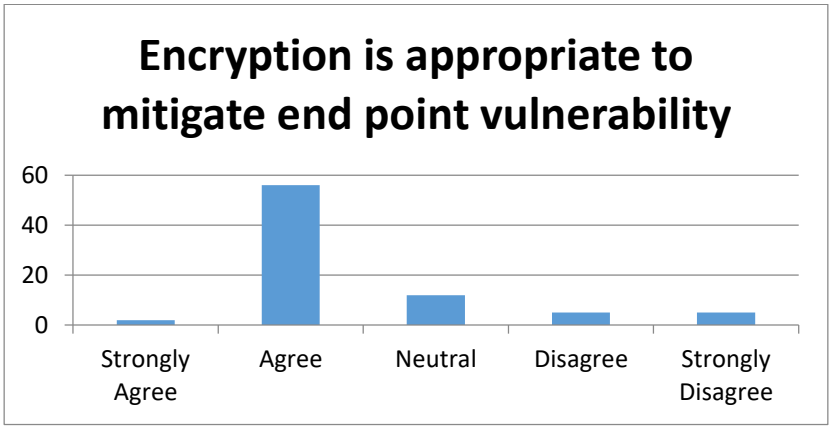

Figure 8: Representing the opinion about encryption being a risk mitigation

(Source: Data Based)

From the above data it can be deciphered that the majority of the respondents have agreed with the fact that encryption can be used for addressing the end point vulnerability risk associated with blockchain. Encryption is one of the important characteristic of blockchain technology. The security method of blockchain makes use of encryption. The use of public key and private key is common for encryption and decryption in a blockchain transaction. This might be the reason behind the denial of this mitigation approach for the end point vulnerability risk in blockchain. Since about 70 % of the respondents have agreed to the fact that encryption is a good risk mitigation approach, it is clear that this strategy is here to stay. Blockchain have been making use of encryption as an integral risk mitigation approach and therefore this approach is appropriate for mitigation of the end point vulnerability risk.

The respondents were further asked to opine about the use of digital signature as a mitigation approach for mitigation of the **contractual *risks*** associated with blockchain. For example, in one of the applications of blockchain, which is smart contract, a significant transactional risk arises mainly because the transactions in smart contracts cannot be reversed.

	Frequency	Percentage
Strongly Disagree	2	2.5%
Disagree	5	6.3%
Neutral	15	18.8%
Agree	55	68.8%
Strongly Agree	3	3.8%

Table 4: Representing the opinion about enforcing digital signature a Risk mitigation approach

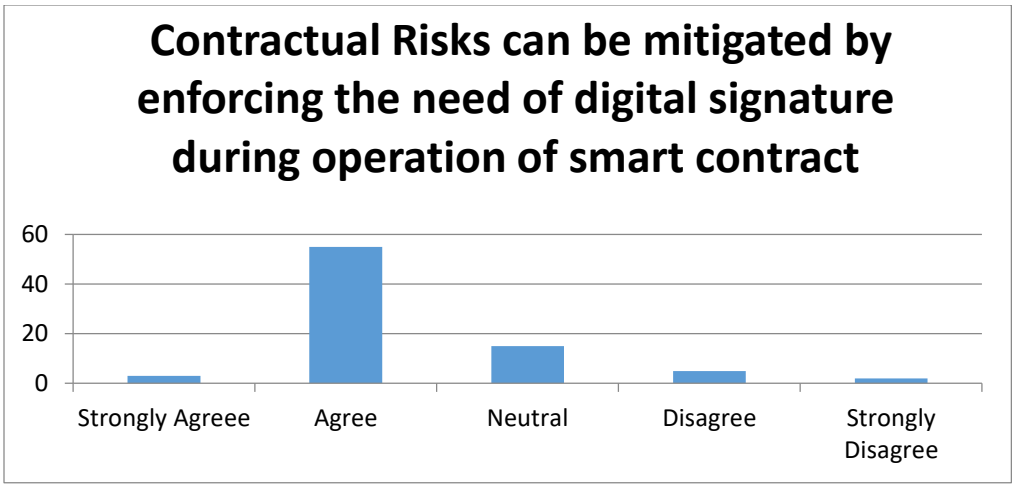

Figure 9: Representing the opinion about enforcing digital signature a Risk mitigation approach

(Source: Data Based)

If it can be enforced that every transaction in a smart contract should incorporate the use of digital signature, the risks of illegal transactions can be mitigated. However, it is seen that almost 19% of the respondents chose to remain neutral in this topic. This gives rise to the dilemma that whether the use of digital signature alone can mitigate the serious contractual risks that are associated with blockchain. Digital signatures are used in majority of the digital transactions and therefore certain other risk mitigation approaches are needed to be identified for mitigating the risks associated with transactions in different application of blockchain, mainly smart contract.

The respondents are asked if the ***supplier risks*** can be mitigated by choosing a trusted cloud vendor. The table below discusses the responses obtained from the respondents.

	Frequency	Percentage
Strongly Disagree	3	3.7%
Disagree	5	6.3%
Neutral	15	18.8%
Agree	54	65.7%
Strongly Agree	3	3.7%

Table 5: Representing the response about the choice of a trusted vendor

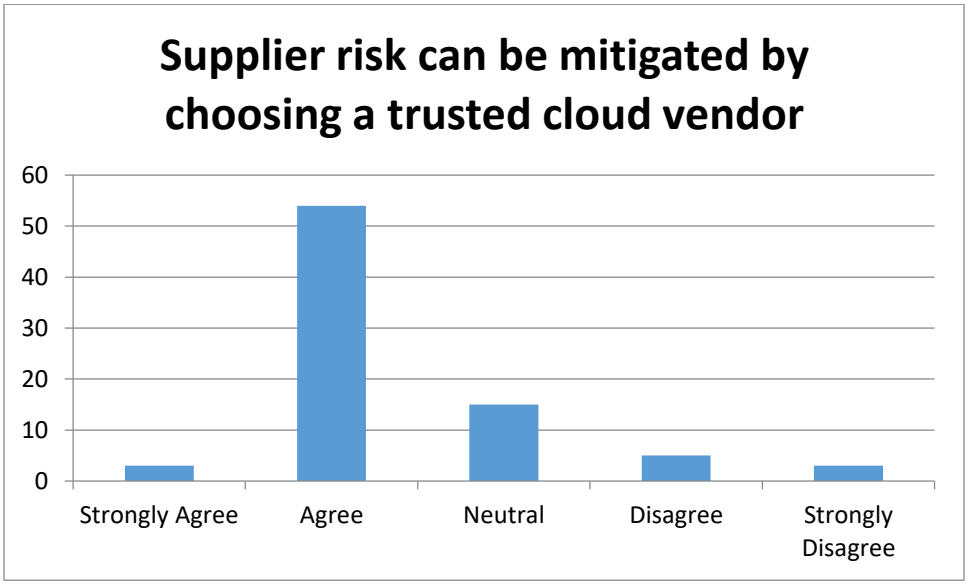

Figure 10: Representing the response about the choice of a trusted vendor

(Source: Data Based)

The respondents were asked to opine about cryptography being one of the significant mitigation approach for the ***operational and the IT risks***. The data obtained are represented in the following table-

	Frequency	Percentage
Strongly Disagree	4	5%
Disagree	6	7.5%
Neutral	12	15%
Agree	53	66.3%
Strongly Agree	5	6.3%

Table 6: Representing the opinion about Cryptography being useful to mitigate the operational and IT Risks

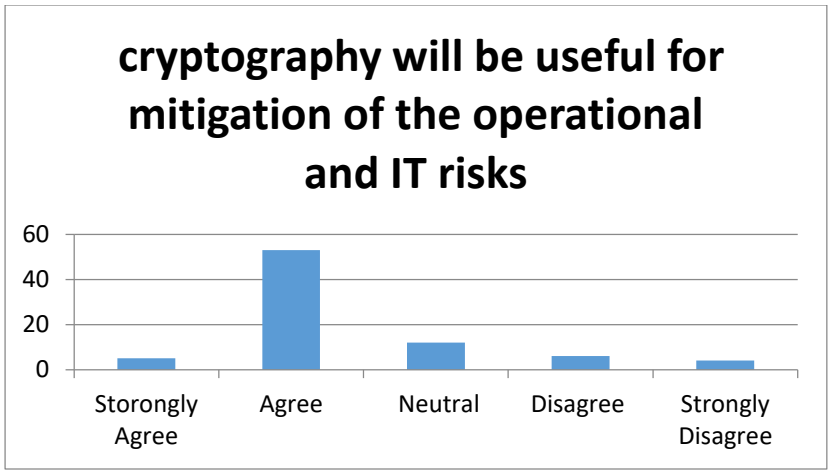

Figure 11: Representing the opinion about Cryptography being useful to mitigate the operational and IT Risk

(Source: Data Based)

It can be seen that majority of the respondents have agreed on the fact that cryptography can be used to mitigate the operational and IT risks associated with the use of Blockchain. Few of the respondents also disagreed with the same but the count of it is negligible. Cryptography can mitigate a number of risks associated with blockchain and therefore it can be considered as a significant risk mitigation approach

Cryptographic keys can be used for mitigation of certain other risks associated with blockchain which include the ***transactional privacy leakage risk***. The respondents were asked to opine about the same. The table and the chart below gives an idea of the responses obtained from the survey.

	Frequency	Percentage
Strongly Disagree	6	7.5%
Disagree	7	8.8%
Neutral	14	17.5%
Agree	51	63.7%
Strongly Agree	2	2.5%

Table 7:Representing the opinion about Cryptography being useful to mitigate the transactional privacy Risk

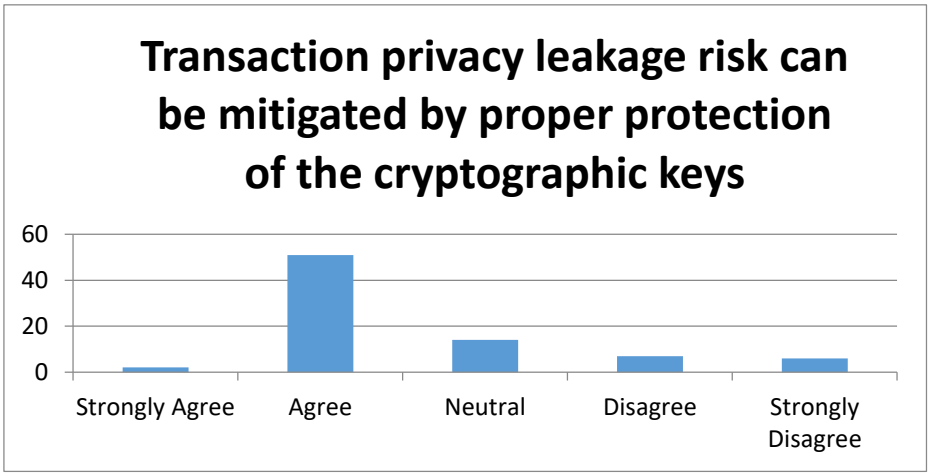

Figure 12: Representing the opinion about Cryptography being useful to mitigate the transactional privacy Risk

(Source: Data Based)

From the obtained data, it can be concluded that the use of cryptographic keys is a valid risk mitigation approach that can be used for mitigation of the transactional privacy leakage risk.

The respondents were asked to opine about the use of incident response plan that can act in a quick manner to mitigate the ***business continuity risks*** associated with blockchain at the time of a disaster. The data obtained are represented as follows-

	Frequency	Percentage
Strongly Disagree	5	6.30%
Disagree	9	11.30%
Neutral	14	17.50%
Agree	48	60.00%
Strongly Agree	4	5.00%

Table 8: Representing the opinion about incident response plan being useful to mitigate business continuity Risk

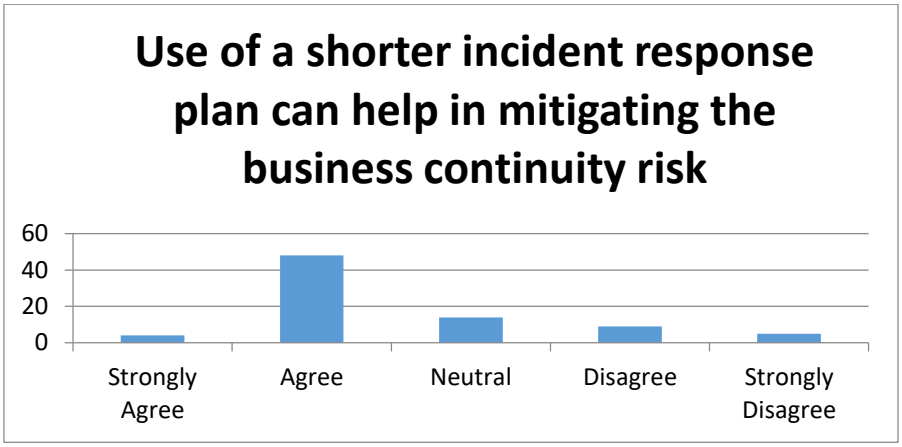

Figure 13:Representing the opinion about incident response plan being useful to mitigate business continuity Risk

(Source: Data Based)

From the data statistics, it can be observed that majority of the respondents can agree to the fact that this plan can help in mitigation of the ***business continuity risk***. However, it is seen that 14 respondents out of 80 respondents have chosen not to comment about the mitigation approach. However, as it is seen that majority of the respondents are agreeing to the fact that shorter incident response plan can help in mitigation of the business continuity risk.

It is seen that untested growth is a major risk associated with the blockchain as it can give rise to a number of other issues. The respondents of the survey are therefore asked to opine about the use of resource sharing as a mitigation approach for the risk of ***untested growth*** in blockchain. Their responses are as follows-

	Frequency	Percentage
Strongly Disagree	5	6.30%
Disagree	8	10.00%
Neutral	19	23.75%
Agree	48	60.00%
Strongly Agree	3	3.80%

Table 9: Representing the opinion about resource sharing plan being useful to mitigate the risk of untested growth

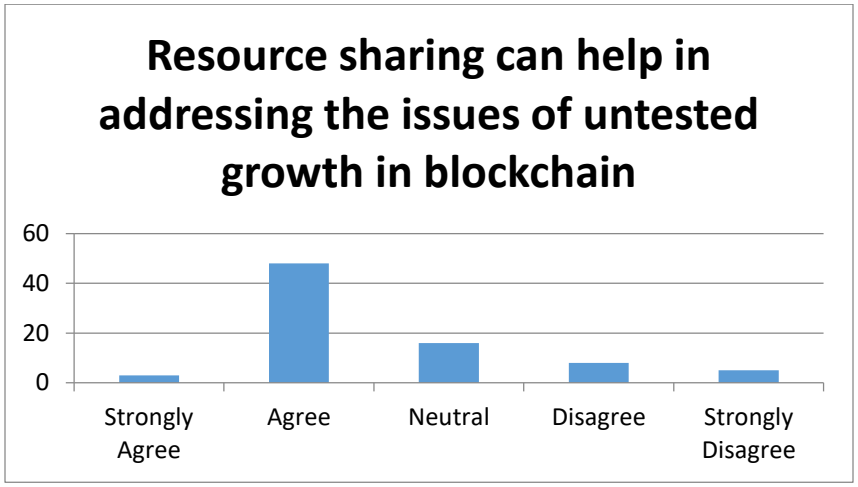

Figure 14: Representing the opinion about resource sharing plan being useful to mitigate the risk of untested growth

(Source: Data Based)

From the above chart, it can be seen that resource sharing can be used for addressing the different issues associated with the untested growth of blockchain. Resource sharing is a concept that enables multiple users to make use of a particular resource. The feasibility of the use of resource sharing to deal with the problem of untested growth in blockchain should be tested. In this survey, majority of the respondents found this approach to be a possible mitigation approach of the risk. However, a large percentage of the respondents have been seen to stay neutral about the topic and therefore the feasibility about making use of resource sharing should be checked.

The respondents were asked to opine about making use of standardized control in mitigation of the ***risk of decentralization*** and their responses are as follows-

	Frequency	Percentage
Strongly Disagree	3	3.70%
Disagree	5	6.30%
Neutral	16	20.00%
Agree	53	66.30%
Strongly Agree	3	3.8%

Table 10: Representing the opinion about standard control being useful to mitigate the risk of decentralization

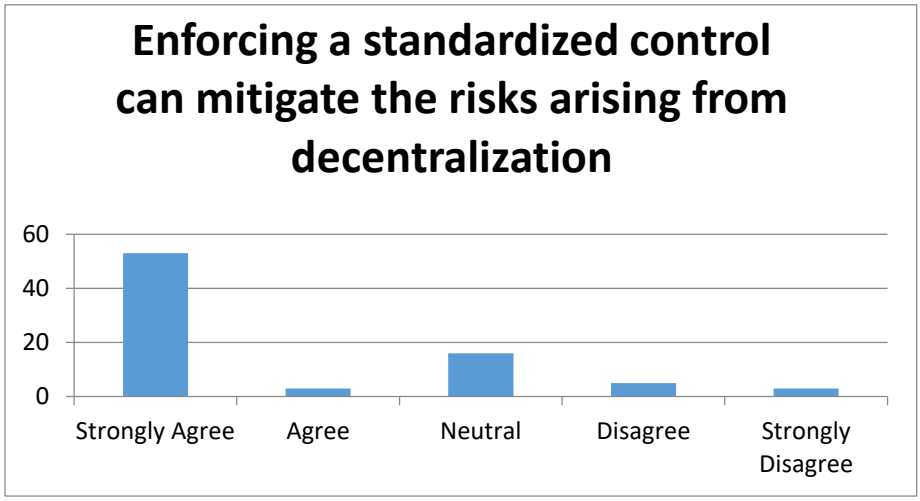

Figure 15:Representing the opinion about standard control being useful to mitigate the risk of decentralization

(Source: Data Based)

From the above data it can be seen that majority of the respondents have agreed to the fact that standardized control can be enforced in mitigating the risks associated with the decentralized nature of blockchain. A standardized control can be used as a mitigation approach for the risk and should be enforced as well.

The respondents were asked to opine about the use of data governance policies in ***access control***. The responses of the survey are as follows-

	Frequency	Percentage
Strongly Disagree	5	6.30%
Disagree	6	7.50%
Neutral	13	16.20%
Agree	51	63.70%
Strongly Agree	5	6.30%

Table 11: Representing the opinion about data governance being useful in access control

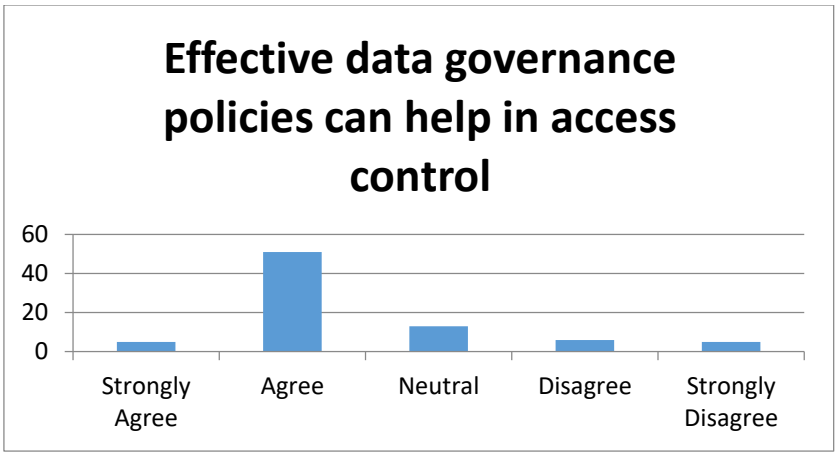

Figure 16:Representing the opinion about data governance being useful in access control

(Source: Data Based)

From the above data it can be concluded that the use of effective data governance policies that help in access control, which is one of the significant risk mitigation approach in blockchain.

The respondents were asked to opine about the use of efficient key management in mitigation of the ***security risks*** associated with the use of blockchain. The responses that has been obtained are as follows-

	Frequency	Percentage
Strongly Disagree	3	3.7%
Disagree	6	7.5%

Neutral	13	16.25%
Agree	55	68.8%
Strongly Agree	3	3.8%

Table 12: Representing the opinion about efficient key management being useful in mitigating security Risk

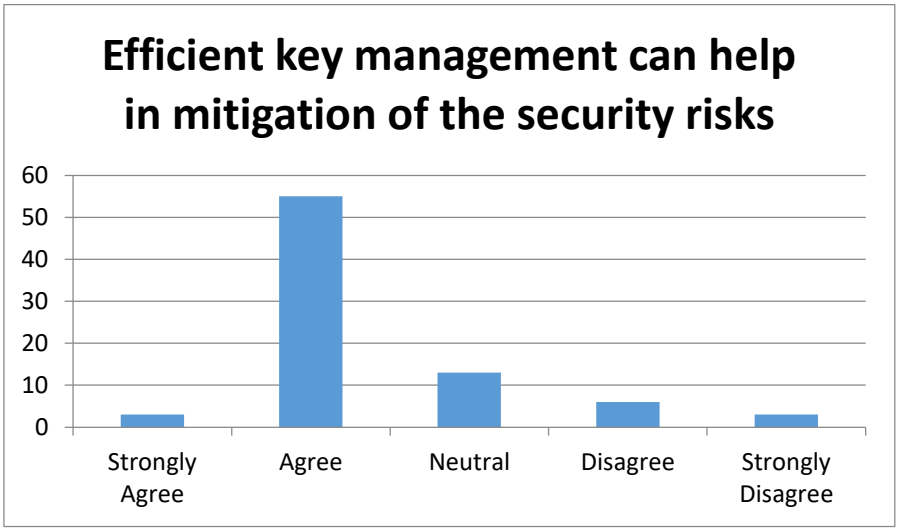

Figure 17:Representing the opinion about efficient key management being useful in mitigating security Risk

(Source: Data Based)

The data about the use of efficient key management as a mitigation approach of certain security risks associated with blockchain clearly depicts that majority of the respondents have agreed on the fact that efficient key management can be considered as a mitigation approach for certain security risks. There are very less percentage of the respondents who disagreed to the fact

that efficient key management can be used for mitigation of the security risks associated with the use of blockchain and blockchain applications.

On evaluating the use of public and private cryptographic keys, it has been observed that the use of good anti-virus can help in mitigation of the risks associated with blockchain and risk management.

	Frequency	Percentage
Strongly Disagree	2	2.5%
Disagree	4	5%
Neutral	11	13.8%
Agree	58	72.5%
Strongly Agree	5	6.3%

Table 13: Representing the response about the use of antivirus

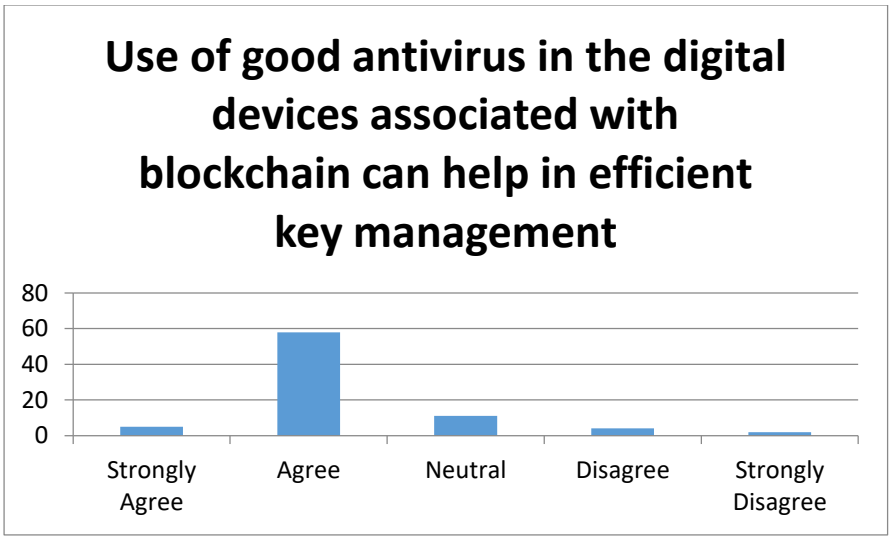

Figure 18:Representing the response about the use of antivirus

(Source: Data Based)

The respondents were asked to provide their opinion about the use of trusted vendor for mitigation of the ***supplier risks*** and their responses are represented below-

	Frequency	Percentage
Strongly Disagree	2	2.5%
Disagree	6	7.5%
Neutral	16	20%
Agree	52	65%
Strongly Agree	4	5%

Table 14: Representing the opinion about trusted vendor being useful in mitigating supplier risk

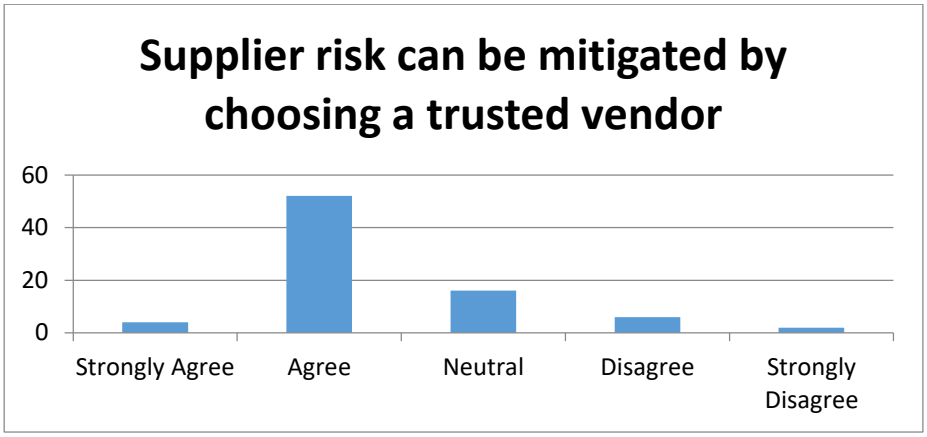

Figure 19:Representing the opinion about trusted vendor being useful in mitigating supplier risk

(Source: Data Based)

From the data above it can be observed that more than 60% of the respondents have agreed on the fact that the choice of a trusted vendor can help in mitigation of the supplier risks associated with blockchain. This is however subjective and a further more research is necessary in this field to understand how this mitigation approach can be used for mitigation of the supplier risks.

The respondents were asked to opine about the use of cryptographic protocols to address the ***consensus protocol risks***. The reposes are as follows-

	Frequency	Percentage
Strongly Disagree	5	6.3%

Disagree	6	7.5%
Neutral	17	21.3%
Agree	49	61.3%
Strongly Agree	3	3.8%

Table 15:Representing the opinion about cryptographic protocols being useful in mitigating consensus protocol risk

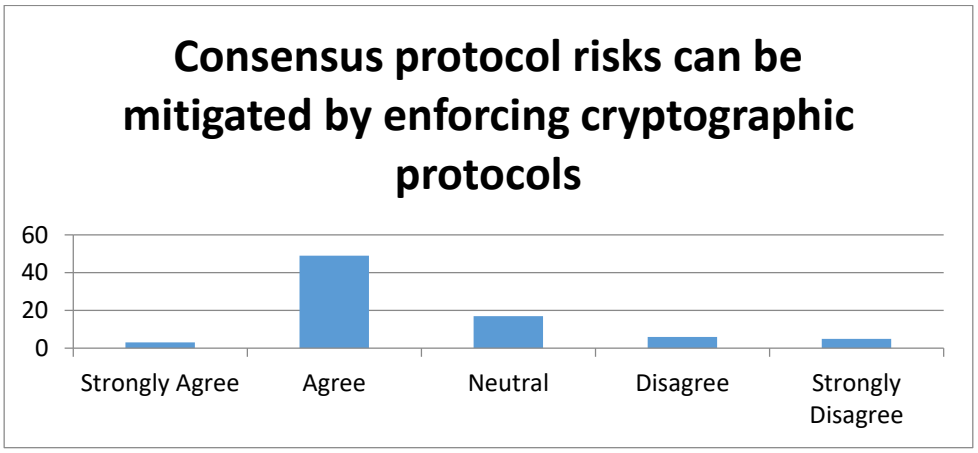

Figure 20:Representing the opinion about cryptographic protocols being useful in mitigating consensus protocol risk

(Source: Data Based)

As majority of the respondents have agreed to the fact that the consensus protocol risks can be mitigated by the use of cryptographic protocols, this can be considered as a valid risk mitigation approach. However, since a large portion of the respondents have chose to remain neutral about the topic, it can be said that further researches in this field is necessary to ensure that cryptographic methods can be used for addressing the consensus protocol risks.

As discussed in the literature review section of the research report, there are a number of vulnerabilities associated with the use of blockchain. The respondents were asked to opine about different risk mitigation strategies that can considerably reduce vulnerabilities in blockchain. These mitigation approaches include validation of data quality, careful network design, security of the private key of the user and use of permissioned blockchain. On an average, it is found out that almost 65% of the respondents have agreed to the fact these approaches can considerably reduce the vulnerabilities associated with blockchain. The data below represents the response of the respondents on the question about the use of data quality validation as a risk mitigation approach in blockchain.

	Frequency	Percentage
Strongly Disagree	4	5%
Disagree	4	5%
Neutral	17	21.3%
Agree	53	66.3%
Strongly Agree	4	5%

Table 16: Representing the rsponse about data quality validation

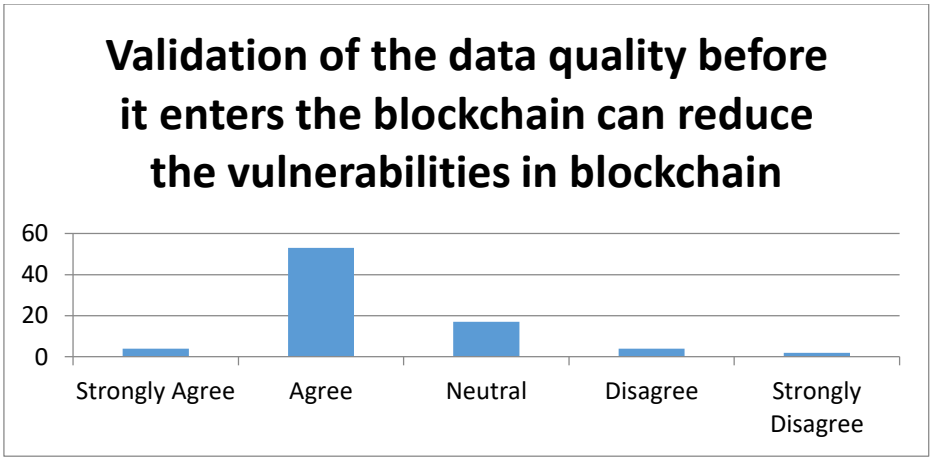

Figure 21:Representing the response about data quality validation

(Source: Data Based)

From the above chart it can be concluded that validation of the data quality can mitigate the risks associated with blockchain.

The use of private blockchain network is effective another sector as well. The use of private blockchain considerably reduces the vulnerabilities in blockchain and therefore the use of private

blockchain network can reduce the reputational risks as well. The respondents were asked to opine about the use of private blockchain in mitigation of the reputational risks associated with blockchain. The table below represents the response as obtained from the respondents of the survey.

	Frequency	Percentage
Strongly Disagree	4	5%
Disagree	3	3.7%
Neutral	16	20%
Agree	53	66.3%
Strongly Agree	4	5%

Table 17: Response about the use of Private blockchain

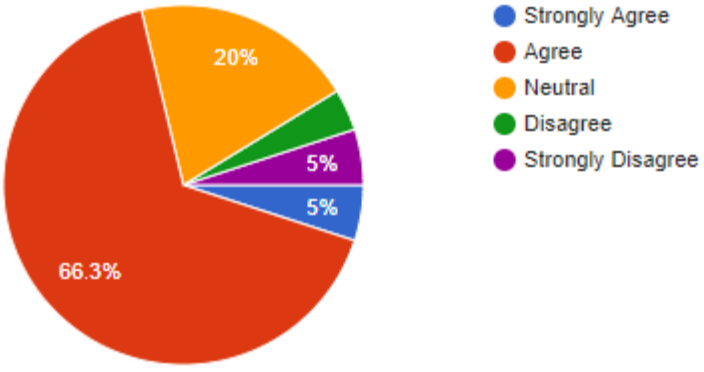

Figure 22: Response about the use of Private Blockchain

(Source: Data Based)

From the above data it is seen that majority of the respondents have agreed on the fact that use of private blockchain can eliminate the chances of reputational risk in blockchain. However, there can be a number of reason behind the reputational risk and therefore, further researches in this field is necessary to ensure that the reputational risks can be managed by making use of private blockchain network.

Apart from this, the respondents of the survey were asked about risk control in the initial stages of deployment. It can be a major risk management approach associated with blockchain. It is seen that majority of the respondents have agreed to the fact that secure deployment, reduction in use of open-source blockchain and in house designing of blockchain can mitigate several risks associated with blockchain. The viability of each of these approaches is discussed in the following section.

These are the major risk mitigation approaches that have been identified and the analysis is based on some major approaches. However, an elaborate research is necessary in each of these fields to understand the viability of the risk mitigation approach. As of now, it can be said that the use of strong cryptographic protocols can help in mitigation of a number of risks.

4.3. TEST OF RESEARCH HYPOTHESIS

From the analysis of the collected data, it has been observed that majority of the respondents have agreed to the fact that the chosen mitigation approaches can possibly mitigate the identified risks in blockchain. From the analysis of the collected data from the survey, it is seen that only a smaller portion of the population has disagreed to the appropriateness and effectiveness of the mitigation approaches that has been chosen for the research study. Thus it is being observed that the research study follows the alternative hypothesis of the research.

The Figure below represents the response of the respondents about the one of the risk mitigation approach of blockchain.

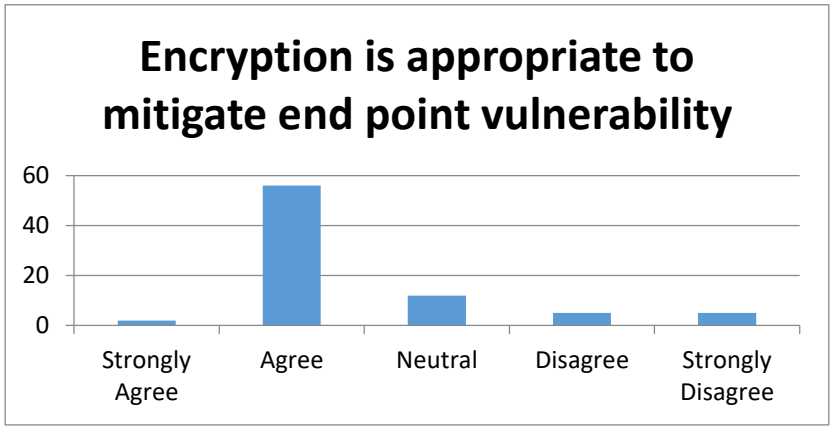

Figure 23: Response of the respondents

(Source: Data Based)

As seen in the picture above, the percentage of the respondents who have disagreed to the chosen mitigation approach is quite less. The responses have been quite similar for the other mitigation approaches that have been chosen for the research. Thus it is observed that the research is following the alternative hypothesis.

4.4. CHAPTER SUMMARY

This is one of the most important sections of the research report as it analyses the chosen approaches of risks mitigation and assess the risk management process in blockchain. The blockchain transactions are generally quite secure and therefore the number of risks associated with blockchain is quite less in comparison to a centralized structure. Certain risks that are associated with blockchain have been identified in the literature review section and the mitigation approach for some of the major risks associated with the blockchain is analyzed. It is seen that the

mitigation approaches that have been proposed are quite viable; however, further research in this field in necessary in order to understand the process of enforcing the identified mitigation approaches and to mitigate any such risk that might endanger a transaction or the owner of blockchain. In short, this chapter analyses the viability of the identified risk mitigation approaches.

CHAPTER 5: DISCUSSION

5.1. INTRODUCTION

The primary data that is being collected has undergone a quantitative analysis to determine whether the risk mitigation approaches that have been identified in the extensive literature review section holds true. Data has been collected from varied sources by the method of survey and the data is analyzed based on the responses of the individuals. The previous chapter of the research study illustrated the responses of respondents of the survey to identify whether the chosen approach will help in mitigation of the identified risks associated with blockchain. A mixed response has been obtained from the respondents and the primary reason behind that might be the fact that the respondents might not have faced those risks in operation of blockchain. This is possible as blockchain is considered to be one the most secure method of transactions. This chapter of the research project aims in discussing the effectiveness of each of identified approaches of risk mitigation in blockchain. The risks that are identified in the literature review section of research study are obtained from an extensive search of the findings from previously published journals. The mitigation approaches that have been identified are obtained from the previously published journals as well. The online survey that has been performed aimed in checking whether the proposed mitigation approaches will actually help in mitigation of a particular risk if that case arises. The discussion about the effectiveness of some of the most important risk mitigation approaches such as encryption, cryptography, digital signature and key management is illustrated in the following sections.

5.2. EFFECTIVENESS OF ENCRYPTION

The effectiveness of encryption as a risk management or mitigation approach in blockchain is true since blockchain make use of encryption as a major protocol (Zyskind and Nathan 2015). There is no denying the fact that the security method in blockchain makes use of the encryption technology in order to secure each block of the blockchain. Encryption in blockchain prevents misuse of sensitive information that is being shared via blockchain transaction (Cachin 2016). The use of encryption as a security method further ensures that the information that is being stored or shared in a blockchain is not forged.

The ledger of blockchain records each and every transaction taking place in the blockchain and each transaction needs to be get verified (Wright and De Filippi 2015). The transactions can be verified by anyone who is present in that particular blockchain network. Thus every blockchain transaction and encryption securely works on basis of mathematics aligned with a mining network (Kishigami*et al.*, 2015). The encryption method associated with the use and verification of a blockchain transaction is considered to be secure since a particular transaction in blockchain is verified by solving an algorithm. Another characteristic of blockchain that makes it a secure transaction system is that once a transaction is added in a blockchain network, it cannot be changed.

The high level mathematical algorithms used in securing the transactions in a blockchain makes the use of encryption as one of the most secure and the easiest way of safeguarding the sensitive and the confidential information associated with the use of blockchain (Li*et al.* 2017). Encryption of the transactions and the information stored in blockchain ensures that a particular information can be accessed by an authorized person only and will not be misused. However, the

effectiveness of encryption is mitigation of end point vulnerability in blockchain should be reviewed.

The end points of the blockchain can be described as the point where a human and the blockchain meet. The end point vulnerability risk in blockchain indicates that the point during which a human makes a contact with blockchain. At this point, the risk of the confidential information of blockchain being forged or misused is the highest and therefore end point vulnerability is considered to be one of the most significant risks associated with blockchain. As a mitigation approach to the end point vulnerability of the risk, encryption is proposed to be the only solution. The use of public key and private key is definitely capable of mitigation of this risks as it will limit the use and access of the data only to authorized individual that is, the individual who have an access to the private key required for decryption of a particular encrypted data in a blockchain network. From the response that has been obtained from the online survey it is seen that majority of the respondent has chosen encryption to be one of the most secure approaches of managing the risks associated with end point vulnerability in blockchain (Kosba*et al.* 2016). The picture below represents the responses in a chart form-

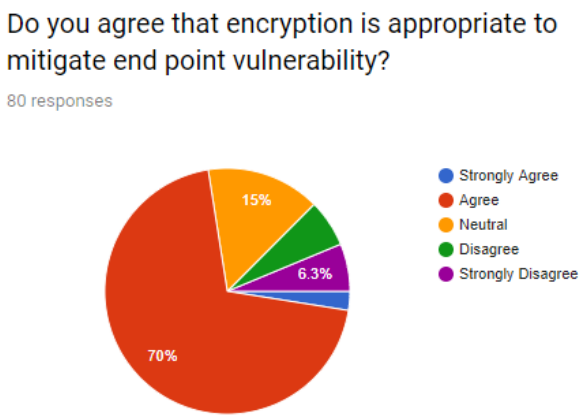

Figure 24: Responses of the Respondents

(Source: Data based)

However, it is also seen a group of people have disagreed to this risk management approach. While researching further about the reason behind such disagreement, it is found out that the disagreement might be a cause of the issues associated with the use of encryption keys. In a blockchain transaction, an encrypted data can only be decrypted with the use of a private key and in any case if the private key is lost, the user will never be able to get an access to the transaction which is one disadvantage of making use of private key in a transaction. This might be one primary reason behind the disagreement of a group of respondents regarding the use of encryption in mitigation of the end point vulnerability in blockchain (Watanabe*et al.* 2015). However, since encryption is used as one of the standard methods in mitigation of the risks in blockchain and is one of the most essential characteristics of blockchain, the recommendation of making use of encryption in mitigation of the end point vulnerability risk in blockchain is justified.

5.3. EFFECTIVENESS OF DIGITAL SIGNATURE

Digital signature can be described as a digital code that is generally attached to a electronically transmitted document to verify the authenticity of the document. It would be interesting to evaluate whether the use of digital signature can actually mitigate the presence of contractual risk in a blockchain transaction (Zyskind and Nathan 2015). An extensive literature search pin points the fact that each and every transaction in blockchain has to be verified by the electronic signature of the sender. The existence of blockchain is null without the use of hashing or digital signature. Therefore the recommendation of making use of digital signature in mitigation of the contractual risks associated with the use of blockchain is justified. The use of digital signature allows non repudiation which confirms that the individual having an access to the private key of the encryption will only be allowed to access particular information. The use of digital signature in a blockchain transaction ensures that the transactions are conducted by the rightful owners only (Back*et al.* 2014). Thus it can be said that every transactions in a blockchain can greatly be benefitted by the use of digital signature. With the increasing use of digital signatures in electronic transaction, the digital signature has become considerably more secure by adding different cryptographic functionalities in digital signatures (Zheng*et al*. 2016). The use of advanced electronic signatures in contractual transaction of blockchain is therefore considered to be one justified recommendation (Aitzhan and Svetinovic 2018). The respondents of the survey were asked about the effectiveness of making use of digital signatures in the management of the contractual risks associated with blockchain. The responses that has been obtained is represented in the following chart-

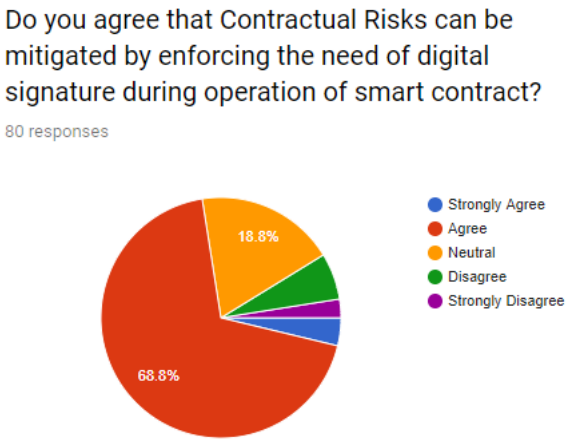

Figure 25: Responses of the Respondents

(Source: Data based)

From the above chart, it is observed that majority of the respondents have agreed to the fact that use of digital signatures can actually help in mitigation of the mentioned risk. The disagreement of some of the respondents comes from the fact that blockchain needs high level of security as mostly; the confidential information is generally stored in a blockchain (Lin*et al.* 2018). However, although blockchain might be seemingly complex or complication, the architecture of blockchain is quite simple (Aitzhan and Svetinovic 2018). In order to create a fresh transaction in blockchain, a hash of the previous transaction is recorded where the public key of the recipient of the transaction is used in the process of encryption along with the private key of the signer of the digital signature. Thus the signer needs to have an access to the private key in order to participate in a transaction (Lin*et al.* 2018). One of the advantages of making use of blockchain is that once a data is entered, it cannot be edited. The use of digital technology in blockchain works on a number of properties, which are log replication, provable value chain, public key cryptography and decentralized transaction ledger. Thus digital signatures and blockchain can easily work together as the use of digital signature has become the key control in a number of organizations (Kiktenko*et*

al. 2018). The advanced digital signature furthermore relies on the use of complex mathematical algorithms in providing the much needed authenticity and protection of data against forgery. Thus the recommendation of making use of digital signature as a risk mitigation approach for mitigation of the contractual risks associated with the use of blockchain.

5.4. EFFECTIVENESS OF CRYPTOGRAPHY

Cryptography is a process that enables storage and transmission of data in a certain form so that only the authorized individuals are able to read the data. It is synonymous to encryption. The use of cryptography blockchain transactions is not a new concept as the original protocol of Bitcoin Blockchain had introduced the concept of crytoeconomics in creation of a robust and fault tolerant blockchain network (Singh and Singh 2016). Cryptography can be used for preserving the privacy as well as transparency in a blockchain transaction. The use of cryptography is mainly seen in permisionless blockchain such as Bitcoin, Ethereum and similar other protocols and applications of blockchain. The aim of making use of cryptography in mitigation of the Information technology risks associated with the use of blockchain is to make sure that a network of actors even if they do not trust each other reach over a particular consensus protocol. When the respondents in the survey that has been undertaken were asked about the use of cryptography as a risk mitigation approach, a majorly positive response has been obtained. The response is illustrated in the following chart.

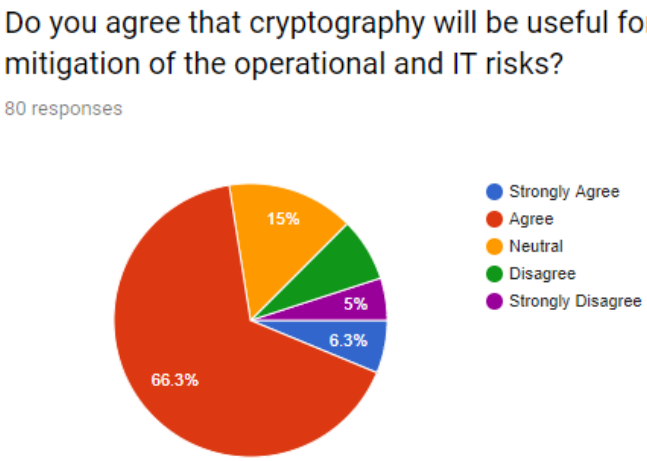

Figure 26: Response of the Respondents

(Source: Data Based)

As seen in the above chart, majority of the respondents have provided a positive view on the use of cryptography as the major risk mitigation approach for different operational and the IT risks associated with the use of blockchain. Bitcoin, one of the most widely used applications of blockchain make use of public key cryptography for a secure transaction. In public key cryptography, both the public key and the private key are used in a transaction. Although cryptography is quite similar to encryption, cryptography does not simply incorporate the encryption and decryption of the messages (Hari and Lakshman 2016). The different cryptographic algorithms that are used in a blockchain or more precisely, in a bitcoin transaction are designed around a wide range of computational hardness assumption. In this case, even if it is theoretically possible to break such cryptographic protocol, it is practically impossible to actually break it.

However, it must be kept in mind that the excessive use and growth of different cryptographic protocols have given rise to a number of legal issues (Halpin and Piekarska 2017). This is particularly because cryptography has a potential to be used for espionage and sedition. Nevertheless, the use of cryptography in blockchain and its applications provides a much needed

security and therefore it can be considered as one of the efficient ways of securing a blockchain transaction. The use of public key encryption is considerably better for securing a blockchain transaction.

5.5. EFFECTIVENESS OF EFFICIENT KEY MANAGEMENT

Since encryption is an inseparable part of blockchain, there are certain issues associated with the inefficient management of the keys in blockchain. These issues give rise to certain risks that are needed to be mitigated (Halpin and Piekarska 2017). Therefore efficient key management is considered to be one of the most important risk management approaches associated with the use of blockchain. The respondents of the survey were asked to give their views on considering efficient key management as one of the risk mitigation approaches in blockchain. The response of the respondents is represented in the following chart.

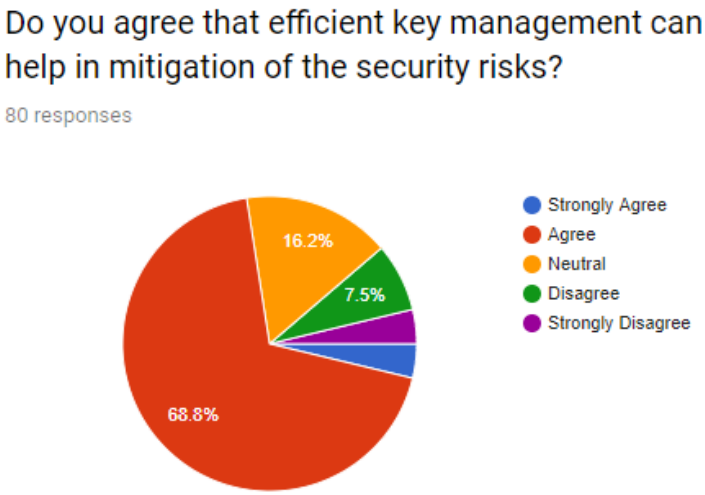

Figure 27: Responses of the Respondents

(Source: Data based)

From the above chart, it can be deduced that majority of the respondents have agreed to the fact that efficient key management can rightly help in management of the security risks in blockchain. Mostly, the blockchain transactions and encrypted and decrypted with the public and private key respectively. The need for management of the key is considerably huge in blockchain as any issue with either of the public or the private key can make an entire transaction void and therefore it is utmost necessary to consider the need of key management in a blockchain transaction.

The term key management can be defined as the use of cryptographic keys that are used in a cryptosystem. The term key management is an umbrella term that encompasses the generation, exchange and the storage of the keys that are used in a cryptographic transaction, precisely, the public key and the private key (Halpin and Piekarska 2017). Key management is an essential aspect of the encryption that is taking place in a blockchain transaction. It can surely mitigate a number of security risks associated with the use of blockchain and therefore the recommendation of the researcher to make use of efficient key management as a risk management approach in blockchain is justified. However, from the chart in figure 18, it is also seen that a group of the respondents have disagreed to the fact that efficient key management can be used as a risk management approach in blockchain (Halpin and Piekarska 2017). This can be possibly because the term “key management” is quite broad in its aspect and does not precisely mentions what sort of key management techniques should be employed in management of the various security risks in blockchain and the fact that there are a large number of security risks in blockchain as well which may not be mitigated by simple management of the keys associated with a blockchain transaction. Therefore, in this context, a proper definition of the security risks was necessary.

5.6. MITIGATING THE DATA VULNERABILITY RISKS

There is a number of data vulnerability Risks associated with the use of blockchain which is needed to be mitigated. A number of risks mitigation approaches has been proposed that can eliminate the data vulnerability risks. It is seen that in a blockchain network it is needed to check the data quality before the data can be used in blockchain. A survey has been conducted where the respondents were asked to opine about the restriction of data upload in public blockchain for reduction of the security risks associated with a blockchain network. The respondents agreed to the fact that it is indeed beneficial to enforce proper quality checks before data upload in blockchain in order to reduce the data vulnerability risk.

With the increase in the use of blockchain, it is essential to implement an effective network design in order to eliminate certain vulnerabilities sin the blockchain network. When the respondents were asked to opine about the effectiveness of careful network design in elimination of the vulnerabilities in blockchain, majority of them have agreed to the fact that it is indeed a good option. The picture below represents the responses of the respondents when asked about the same.

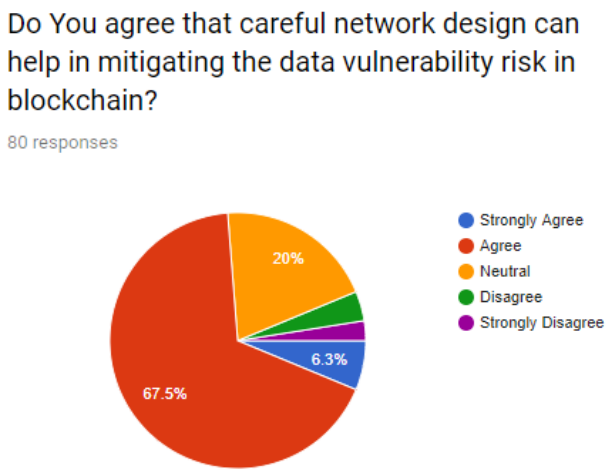

Figure 28: Responses of the Respondents

(Source: Data based)

Along with the careful network design, it is necessary to ensure that the private key of the user is properly secured. Thus it can be said that a combination of a number of risk mitigation approaches can help in addressing the vulnerabilities in a blockchain network. The secure implementation of a blockchain network in an organization can eliminate the data security risks associated with blockchain. The organizations are therefore recommended to design the blockchain network in-house in order to mitigate the data security risks in blockchain.

5.7. CHAPTER SUMMARY

This chapter proves to one of the most vital chapters of research study. This is particularly because it discusses three primary risk management techniques of blockchain that have been identified on the literature review section. The researcher analyzes the information collected in the literature review section and the information obtained from the collection of primary data to evaluate whether the proposed methodology will actually work in management of the different

risks associated with blockchain. It has been observed that all the three methods, encryption, cryptography and key management are capable of mitigation of certain risks associated with blockchain. End point vulnerability is one of the most significant risks in blockchain and the primary risks mitigation approach that has been proposed for managing this risk is the use of encryption. Similarly the use of cryptography coupled with an efficient key management process can help in mitigation of a number of security risks associated with the use of blockchain and its applications. The use of digital signature and encryption is quite common in a blockchain and its associated transactions. The chapter further discusses about the effectiveness of the mitigation approaches that have been proposed by the researcher to mitigate the vulnerabilities associated with the blockchain. It has been observed that if the organizations that plan to make use of blockchain in their daily business can opt of in house designing of the same, it might help in mitigation of a number of risks associated with the blockchain network. However, it is recommended that before implementation of the blockchain, appropriate risk management is necessary to identify the risks that might affect the implementation process.

CHAPTER 6: CONCLUSION AND RECOMMENDATION FOR FURTHER RESEARCH

Blockchain is one of the evolving or emerging concepts. A research has been undertaken in order to evaluate the blockchain concept, its risks and the mitigation techniques of the risks associated with the use of blockchain. The research has mainly highlighted the system and application risk management process associated with blockchain technology so that the implementation and use of blockchain technology becomes easier. The entire research has been divided into a number of subsections for better understanding of the each stages of research. The research in the field of blockchain is necessary as it is an emerging technology. The researcher has embarked on an extensive literature search in identification of the different issues associated with the blockchain. Since blockchain is a new technology, the successful adoption and operation of this new technology mainly depends on the management of the different risks associated with the technology of blockchain. The research mainly focused on the system risk management process that helped in identifying and accessing the risks associated with the blockchain technology. In future majority of the business organizations will be making use of blockchain in their transactions as it is considered to be one of the most secure options of information delivery. Therefore, it is essential to research about the different risks in blockchain and the mitigation techniques of the technology of blockchain. The successful adoption and the operation of blockchain mostly depend on the appropriate management of the risks and the issues. The researcher has done an extensive literature review to understand the structure and concepts of blockchain and to identify the different issues and the challenges that the users of blockchain might face. The risk practitioners across the different business sectors are working on the identification of the issues and the risks associated with the use of blockchain. Along with the secondary data collection through an extensive

literature review, the researcher has involved in collection of primary data and that data is analyzed to understand the effectiveness of the risk mitigation approaches. The different risks associated with the use of blockchain include end point vulnerability risks, contractual risks, supplier risks, information security risks as so on. The survey that has been conducted takes the opinion of the respondents about the effectiveness of the identified risk mitigation approaches in mitigation of the vulnerabilities associate with network design and implementation. From the results of the survey, it has been found out that majority of respondents have agreed to the fact that in house designing and careful network design can possibly mitigate the vulnerabilities associated with the implementation of blockchain in different organizations.

6.1. LINKING WITH THE OBJECTIVE

The objectives of the project were to understand the technology of blockchain along with the identification of the different risks and issues associated with blockchain technology. The research further aimed in assessing the risks associated with the blockchain technology and to recommend certain risks mitigation approach that will help in mitigation of the identified risks.

While understanding the different concepts of blockchain, the researcher has embarked on an extensive literature search. The literature review section of the research study is one of the most important chapters of this research study. Identification and understanding of all the concepts and the characteristics of blockchain technology considerably helped the researcher in understanding and identifying different risks and issues associated with the use of blockchain technology. The researcher further identified the different issues and the risks associated with the blockchain technology thus fulfilling two of the most important objectives of the project. Another objective of the project was to access the different risk mitigation approaches to eliminate the risks and the

issues associated with blockchain. Thus is can be said that apart from identification of the different risks and issues associated with the blockchain technology, the researcher have also identified the different approaches by which the identified risks can be mitigated. The risk mitigation approaches are identified from an extensive literature search.

The researcher, in order to recommend the strategies or the risk mitigation approaches to mitigate the identified risks, has embarked on a primary data collection and quantitative analysis of the data to identify the most appropriate approach of risk mitigation. The primary data collection was done by surveying 80 respondents who are associated with blockchain and has an experience in the field of blockchain. With the increasing use of blockchain in the different business processes, it becomes essential to identify the risks associated with the use of blockchain. Blockchain is the backbone of many different applications that is based on blockchain and hence it is necessary to identify the risks and the issues in blockchain. The different nature of the blockchain transactions has a number of risks that has been identified in the literature review section of the research study. The primary data is collected with an aim of identifying the most appropriate risk mitigation approach. The researcher has been successful in the research and the identified objectives of the research are addressed as well. The research aim that was set by the researcher were fulfilled as the researcher was able to identify the risks, assess the process of risk management and mitigation in blockchain and was able to identify the most significant risks mitigation approaches for mitigation of the most common risks and the issues associated with blockchain. The four most important risks mitigation approaches that is identified for the project include the use of encryption, cryptography, digital signature and efficient key management. The data analysis along with the discussion chapter of the research study is important as it helps in analyzing the identified approaches of risks mitigation in blockchain. The discussion chapter is important as it

recommended the most important risks mitigation strategies of blockchain. The four recommended approaches will theoretically help in elimination of the different risks that is associated with the use of blockchain and with the use of different applications of blockchain including bitcoin and smart contracts.

Objective 1:To understand the technology of blockchain

The research project aimed in understanding the technology of blockchain. With an extensive literature search and review of the literature, this objective of the research was fulfilled. In the literature review section of the research report, the concept, history and the technology of blockchain has been discussed in detail to understand the technology of blockchain.

Objective 2:To identify the risks associated with the blockchain technology

The research project aimed in identification of the different risks associated with the technology of blockchain. The literature review chapter of the research report identifies the different risks associated with blockchain and its application. Identification of the risks associated with the blockchain technology was essential to identify the mitigation approaches to be used in primary data collection and analysis.

Objective 3:To assess the risk management process in blockchain

The research project aimed in identification of the different risk mitigation approaches associated with the risk mitigation in blockchain. In the literature review section, the mitigation approaches of the risks in blockchain are identified. The identified risks are mainly the system risks, elimination of which is essential for improved use and implementation of blockchain technology.

The effectiveness of the risk mitigation approaches is further discussed in the data analysis chapter.

Objective 4:To recommend certain strategies to eliminate the risks associated with blockchain technology

The project aimed in identification risk mitigation approaches which will be appropriate for mitigation of the risks associated with the blockchain technology. The data analysis and the discussion chapter evaluate the risk mitigation approaches that are appropriate in mitigation of the identified risk in blockchain. The discussion chapter recommends the most effective risk mitigation approaches for blockchain.

6.2. RESEARCH LIMITATION

The research aimed in analyzing the characteristics and the features of blockchain. The architecture and the working principle of the blockchain is discussed in the research. The objective of this research project was to identify the different risks and the issues associated with use of blockchain and its application. The researcher was able to identify the risks and the different risk mitigation approaches in blockchain. A primary data collection and analysis of the collected data was carried out by the researcher to assess the effectiveness of the identified risk mitigation approaches. However, there are certain limitations associated with the research project which are discussed in the following paragraphs-

The researcher has mainly focused on the most significant risks associated with blockchain and their mitigation approaches. However, there are certain other risks associated with the use of blockchain that were needed to be identified as well. Similarly there was a limitation with the risk mitigation approaches that has been identified and evaluated in this research study.

Another limitation with this research project is that it was executed in a limited timeframe and with a limited number of respondents. A wider approach would have helped in collection and analysis of a more appropriate data. Therefore apart from the time constraint, constrain in the risks mitigation approaches identified in the research study is another major limitation of the project.

The research was implemented with an aim of identification of the different issues associated with blockchain and management of the risks associated with a blockchain technology.

6.3. RECOMMENDATIONS

Certain recommendations for the research study are as follows-

1. A wider audience base should have been used inform the research project
2. For mitigation of the different risks associated with blockchain, the organization making use of the blockchain and its application should ensure that the risks and the issues associated with the use of blockchain are correctly identified and mitigated.
3. Blockchain is considered to be a secure technology; however this should not be misinterpreted as there are certain issues associated with the use of blockchain and its application. The research identified few of such issues and recommended the mitigation approaches of the research as well.
4. The supplier risks associated with the blockchain is although hard to mitigate, the need for management of such risk in high. Therefore, it is needed to understand the risk mitigation approach for mitigation of the supplier risks associated with the use and adoption of blockchain.
5. Further researches in the field of blockchain are necessary for identification of the various other risks and issues associated with the use of blockchain. The mitigation approaches that

have been identified in the project should be more appropriate. Further researchers in this field are necessary as the current research has a number of limitations. There is scope of further researchers in this field and therefore it is necessary.

6.4. FUTURE RESEARCH

The researcher has performed a research on the topic of blockchain and risk management. However, blockchain is a broad concept and a significant research in the field of blockchain is further necessary. Further researches can be conducted in order increase the effectiveness of the other approaches of risk mitigation in this field. The effectiveness of the four chosen risks mitigation approaches have been highlighted in the research project and therefore, there is a scope for future research in this filed in assessing the risk mitigation process.

The process, tools and the techniques that have been utilized in this research project could be further improved. The primary research could have been more accurate. In future research in this field, along with the online survey that has been conducted for the research, an interview with a group of the experts can be also performed to have a more accurate data set. This is mainly because there are certain legal obligations associated with the collection of data from the survey and there are certain limitations as well, which can be eliminated in interview. Along with interview and survey, observation of the trends in blockchain can help in easier identification of the risks and the issues associated with blockchain. The future research will further help in accurate identification of the different risk mitigation approaches associated with the risks in blockchain. The need for management of the different issues associated with the blockchain is huge since different business organization is making use of the blockchain in transactions. The use of

blockchain applications will be increasing in no time and thus this research study will provide an idea about the technology of blockchain and the risks associated with blockchain.

REFERENCES

Aitzhan, N.Z. and Svetinovic, D., 2018. 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.

Al, S. 2013. Interpretive research design: concepts and processes. *International Journal of Social Research Methodology*, 16(4), pp.351-352.

Alvesson, M. and Sandberg, J. 2013. *Constructing Research Questions*. London: SAGE Publications.

Aste, T., Tasca, P. and Di Matteo, T., 2017. Blockchain technologies: The foreseeable impact on society and industry. *computer*, *50*(9), pp.18-28.

Atzori, M., 2015. Blockchain technology and decentralized governance: Is the state still necessary?.

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J. and Wuille, P., 2014. Enabling blockchain innovations with pegged sidechains. *URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains*.

Brannen, J., 2017. *Mixing methods: Qualitative and quantitative research*. Routledge.

Brown, J. and Stowers, E. 2013. Use of Data in Collections Work: An Exploratory Survey. *Collection Management*, 38(2), pp.143-162.

Bryman, A. and Bell, E., 2015. *Business research methods*. Oxford University Press, USA.

Byström, H., 2016. Blockchains, real-time accounting and the future of credit risk modeling. *Lund University, Department of Economics*.

Cacciattolo, M., 2015. Ethical considerations in research. In *The Praxis of English Language Teaching and Learning (PELT)* (pp. 61-79). SensePublishers, Rotterdam.

Cachin, C., 2016, July. Architecture of the hyperledger blockchain fabric. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers* (Vol. 310).

Chandra, S. and Sharma, M. 2013. *Research methodology*. Oxford: Alpha Science International Ltd.

Connelly, L.M., 2014. Ethical considerations in research studies. *Medsurg Nursing*, *23*(1), p.54.

Crosby, M., Pattanayak, P., Verma, S. and Kalyanaraman, V., 2016. Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*, pp.6-10.

Davidson, S., De Filippi, P. and Potts, J., 2016. Economics of blockchain.

Eaton, S. 2013. The Oxford handbook of empirical legal research. *International Journal of Social Research Methodology*, 16(6), pp.548-550.

Edson, M.C., Henning, P.B. and Sankaran, S. eds., 2016. *A guide to systems research: Philosophy, processes and practice* (Vol. 10). Springer.

Eriksson, P. and Kovalainen, A., 2015. *Qualitative methods in business research: A practical guide to social research*. Sage.

Frantz, C.K. and Nowostawski, M., 2016, September. From institutions to code: Towards automated generation of smart contracts. In *Foundations and Applications of Self* Systems, IEEE International Workshops on* (pp. 210-215). IEEE.

Halpin, H. and Piekarska, M., 2017, April. Introduction to Security and Privacy on the Blockchain. In *Security and Privacy Workshops (EuroS&PW), 2017 IEEE European Symposium on* (pp. 1-3). IEEE.

Hari, A. and Lakshman, T.V., 2016, November. The internet blockchain: A distributed, tamper-resistant transaction framework for the internet. In *Proceedings of the 15th ACM Workshop on Hot Topics in Networks* (pp. 204-210). ACM.

Heires, K., 2016. The risks and rewards of blockchain technology. *Risk Management*, *1*.

Hull, R., Batra, V.S., Chen, Y.M., Deutsch, A., Heath III, F.F.T. and Vianu, V., 2016, October. Towards a shared ledger business collaboration language based on data-aware processes. In *International Conference on Service-Oriented Computing* (pp. 18-36). Springer, Cham.

Iansiti, M. and Lakhani, K.R., 2017. The truth about blockchain. *Harvard Business Review*, *95*(1), pp.118-127.

Imbault, F., Swiatek, M., De Beaufort, R. and Plana, R., 2017, June. The green blockchain: Managing decentralized energy production and consumption. In *Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), 2017 IEEE International Conference on* (pp. 1-5). IEEE.

Jensen, K.B. ed., 2013. *A handbook of media and communication research: Qualitative and quantitative methodologies*. Routledge.

Kakavand, H., Kost De Sevres, N. and Chilton, B., 2017. The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies.

Kiktenko, E.O., Pozhar, N.O., Anufriev, M.N., Trushechkin, A.S., Yunusov, R.R., Kurochkin, Y.V., Lvovsky, A.I. and Fedorov, A.K., 2018. Quantum-secured blockchain. *Quantum Science and Technology*, *3*(3), p.035004.

Kishigami, J., Fujimura, S., Watanabe, H., Nakadaira, A. and Akutsu, A., 2015, August. The blockchain-based digital content distribution system. In *Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conference on* (pp. 187-190). IEEE.

Kosba, A., Miller, A., Shi, E., Wen, Z. and Papamanthou, C., 2016, May. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE symposium on security and privacy (SP)* (pp. 839-858). IEEE.

Lam, J., 2014. *Enterprise risk management: from incentives to controls*. John Wiley & Sons.

Leedy, P. and Ormrod, J. 2013. *Practical research*. Boston: Pearson.

Lemieux, V.L., 2016. Trusting records: is Blockchain technology the answer?. *Records Management Journal*, *26*(2), pp.110-139.

Li, S., Liu, M. and Wei, S., 2017, December. A distributed authentication protocol using identity-based encryption and blockchain for LEO network. In *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage* (pp. 446-460). Springer, Cham.

Lin, Q., Yan, H., Huang, Z., Chen, W., Shen, J. and Tang, Y., 2018. An ID-based linearly homomorphic signature scheme and its application in blockchain. *IEEE Access*, *6*, pp.20632-20640.

Lindman, J., Tuunainen, V.K. and Rossi, M., 2017. Opportunities and risks of Blockchain Technologies–a research agenda.

Mainelli, M. and Milne, A., 2016. The impact and potential of blockchain on the securities transaction lifecycle.

Mainelli, M. and Smith, M., 2015. Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology).

Malinova, K. and Park, A., 2017. Market Design with Blockchain Technology.

Mayer, I., 2015. Qualitative research with a focus on qualitative data analysis. *International Journal of Sales, Retailing & Marketing*, *4*(9), pp.53-67.

Mitchell, M. and Jolley, J. 2013. *Research design explained*. Australia: Wadsworth Cengage Learning.

Morabito, V., 2017. Business Innovation Through Blockchain. *Cham: Springer International Publishing*.

Mougayar, W., 2016. *The business blockchain: promise, practice, and application of the next Internet technology*. John Wiley & Sons.

Nofer, M., Gomber, P., Hinz, O. and Schiereck, D., 2017. Blockchain. *Business & Information Systems Engineering*, *59*(3), pp.183-187.

Novikov, A. and Novikov, D. 2013. *Research methodology*. Leiden, Netherlands: CRC Press/Balkema.

Ølnes, S., 2016, September. Beyond bitcoin enabling smart government using blockchain technology. In *International Conference on Electronic Government and the Information Systems Perspective* (pp. 253-264). Springer, Cham.

Peters, G.W. and Panayi, E., 2016. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In *Banking Beyond Banks and Money* (pp. 239-278). Springer, Cham.

Pilkington, M., 2016. 11 Blockchain technology: principles and applications. *Research handbook on digital transformations*, p.225.

Porru, S., Pinna, A., Marchesi, M. and Tonelli, R., 2017, May. Blockchain-oriented software engineering: challenges and new directions. In *Proceedings of the 39th International Conference on Software Engineering Companion* (pp. 169-171). IEEE Press.

Raval, S., 2016. *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology*. " O'Reilly Media, Inc.".

Ritchie, J., Lewis, J., Nicholls, C.M. and Ormston, R. eds., 2013. *Qualitative research practice: A guide for social science students and researchers*. sage.

Sahay, A., 2016. Peeling Saunder's Research Onion.

Salaberry, M. and Comajoan, L. 2013. *Research Design and Methodology in Studies on L2 Tense and Aspect*. Boston: De Gruyter.

Saunders, M., Lewis, P. and Thornhill, A., 2009. Research Onion. *Research methods for business students*, pp.136-162.

Scott, B., 2016. *How can cryptocurrency and blockchain technology play a role in building social and solidarity finance?*(No. 2016-1). UNRISD Working Paper.

Scott, B., 2016. *How can cryptocurrency and blockchain technology play a role in building social and solidarity finance?*(No. 2016-1). UNRISD Working Paper.

Shrier, D., Larossi, J., Sharma, D. and Pentland, A., 2016. Blockchain & Transactions, Markets and Marketplaces.

Singh, S. and Singh, N., 2016, December. Blockchain: Future of financial and cyber security. In *Contemporary Computing and Informatics (IC3I), 2016 2nd International Conference on*(pp. 463-467). IEEE.

Smith, J.A. ed., 2015. *Qualitative psychology: A practical guide to research methods*. Sage.

Swan, M., 2015. *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.".

Tapscott, A. and Tapscott, D., 2017. How blockchain is changing finance. *Harvard Business Review*, *1*.

Thomas, J. 2013. Empathic design: Research strategies. *Australasian Medical Journal*, 6(1), pp.1-6.

Underwood, S., 2016. Blockchain beyond bitcoin. *Communications of the ACM*, *59*(11), pp.15-17.

Uprichard, E. 2013. Sampling: bridging probability and non-probability designs. *International Journal of Social Research Methodology*, 16(1), pp.1-11.

Walch, A., 2015. The bitcoin blockchain as financial market infrastructure: A consideration of operational risk. *NYUJ Legis. & Pub. Pol'y*, *18*, p.837.

Walch, A., 2017. The path of the blockchain lexicon (and the law).

Wang, X., Feng, L., Zhang, H., Lyu, C., Wang, L. and You, Y., 2017, April. Human resource information management model based on blockchain technology. In *Service-Oriented System Engineering (SOSE), 2017 IEEE Symposium on* (pp. 168-173). IEEE.

Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A. and Kishigami, J.J., 2015, October. Blockchain contract: A complete consensus using blockchain. In *Consumer Electronics (GCCE), 2015 IEEE 4th Global Conference on* (pp. 577-578). IEEE.

Wright, A. and De Filippi, P., 2015. Decentralized blockchain technology and the rise of lex cryptographia.

Www2.deloitte.com. (2018). [online] Available at: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu-blockchain-risk-management-27092017.pdf [Accessed 9 Oct. 2018].

Yeoh, P., 2017. Regulatory issues in blockchain technology. *Journal of Financial Regulation and Compliance*, *25*(2), pp.196-208.

Yermack, D., 2015. Is Bitcoin a real currency? An economic appraisal. In *Handbook of digital currency* (pp. 31-43).

Yli-Huumo, J., Ko, D., Choi, S., Park, S. and Smolander, K., 2016. Where is current research on blockchain technology?—a systematic review. *PloS one*, *11*(10), p.e0163477.

Zhao, J.L., Fan, S. and Yan, J., 2016. Overview of business innovations and research opportunities in blockchain and introduction to the special issue.

Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H., 2017, June. An overview of blockchain technology: Architecture, consensus, and future trends. In *Big Data (BigData Congress), 2017 IEEE International Congress on* (pp. 557-564). IEEE.

Zheng, Z., Xie, S., Dai, H.N. and Wang, H., 2016. Blockchain challenges and opportunities: A survey. *Work Pap.–2016*.

Zyskind, G. and Nathan, O., 2015, May. Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE* (pp. 180-184). IEEE.

APPENDIX

Blockchain and Risk Management Survey

The following questions have been made as a part of British University in Dubai (BUiD) requirements to achieve MSc degree in Project Management. Filling this survey will not hold any obligation for the filler or its organization and the results of will be used for the scientific researches purposes only.

This study aim to identify the different concepts of blockchain, which helps in identification of the different risks and the risk mitigation approaches, associated with blockchain technology.

Section A

Questions	Demographic Questions
1. Field of Work	□ **Blockchain Developer** □ **Network Security Officer** □ **Blockchain Architect** □ **Risk Manager** □ **others**
1. Number of years' experience	□ **0-2 years** □ **3-5 years** □ **more than 5 years**

Section B

Questions	Please rate the Risk mitigation Approaches in Blockchain				
1. Do you agree that encryption is appropriate to mitigate end point vulnerability?	(1) Strongly Agree	(2) Agree	(3) Neither	(4) Disagree	(5) Strongly Disagree
2. Do you agree that Contractual Risks can be mitigated by enforcing the need of digital signature during operation of smart contract?	(1) Strongly Agree	(2) Agree	(3) Neither	(4) Disagree	(5) Strongly Disagree
3. Do you agree that the supplier risk can be mitigated by choosing a trusted cloud vendor?	(1) Strongly Agree	(2) Agree	(3) Neither	(4) Disagree	(5) Strongly Disagree
4. Do you agree that cryptography will be useful for mitigation of the operational and IT risks?	(1) Strongly Agree	(2) Agree	(3) Neither	(4) Disagree	(5) Strongly Disagree
5. Do You agree that the transaction privacy leakage risk can be mitigated by proper protection of the cryptographic keys?	(1) Strongly Agree	(2) Agree	(3) Neither	(4) Disagree	(5) Strongly Disagree

Questions	Please rate the Risk mitigation Approaches in Blockchain				
6. Do you agree that the use of a shorter incident response plan can help in mitigating the business continuity risk?	1 Strongly Agree	2 Agree	3 Neither	4 Disagree	5 Strongly Disagree
7. Do you agree that resource sharing can help in addressing the issues of untested growth in blockchain?	1 Strongly Agree	2 Agree	3 Neither	4 Disagree	5 Strongly Disagree
8. Do you agree that enforcing a standardized control can mitigate the risks arising from decentralization?	1 Strongly Agree	2 Agree	3 Neither	4 Disagree	5 Strongly Disagree
9. Do You agree that effective data governance policies can help in access control?	1 Strongly Agree	2 Agree	3 Neither	4 Disagree	5 Strongly Disagree

10. Do you agree that efficient key management can help in mitigation of the security risks?	(1) Strongly Agree	(2) Agree	(3) Neither	(4) Disagree	(5) Strongly Disagree

Questions	Please rate the Risk mitigation Approaches in Blockchain				
11. Do you agree that the use of good antivirus in the digital devices associated with blockchain can help in efficient key management?	(1) Strongly Agree	(2) Agree	(3) Neither	(4) Disagree	(5) Strongly Disagree
12. Do you agree that the supplier risk can be mitigated by choosing a trusted vendor?	(1) Strongly Agree	(2) Agree	(3) Neither	(4) Disagree	(5) Strongly Disagree
13. Do you agree that the consensus protocol risks can be mitigated by enforcing cryptographic protocols?	(1) Strongly Agree	(2) Agree	(3) Neither	(4) Disagree	(5) Strongly Disagree
14. Do you agree that the restriction of data upload to public blockchain can reduce the risks associated with blockchain?	(1) Strongly Agree	(2) Agree	(3) Neither	(4) Disagree	(5) Strongly Disagree

15. Do you agree that the validation of the data quality before it enters the blockchain can reduce the vulnerabilities in blockchain?	**1 Strongly Agree**	**2 Agree**	**3 Neither**	**4 Disagree**	**5 Strongly Disagree**

Questions	Please rate the Risk mitigation Approaches in Blockchain				
16. Do You agree that careful network design can help in mitigating the data vulnerability risk in blockchain?	**1 Strongly Agree**	**2 Agree**	**3 Neither**	**4 Disagree**	**5 Strongly Disagree**
17. Do you agree that the private key of the user is needed to be protected to mitigate the vulnerability risks in blockchain?	**1 Strongly Agree**	**2 Agree**	**3 Neither**	**4 Disagree**	**5 Strongly Disagree**
18. Do you agree that the framework of permissioned blockchain is suitable for mitigation of the vulnerability risk in blockchain?	**1 Strongly Agree**	**2 Agree**	**3 Neither**	**4 Disagree**	**5 Strongly Disagree**
19. DO You agree that the organizations can manage the reputational risks by using private blockchain network?	**1 Strongly Agree**	**2 Agree**	**3 Neither**	**4 Disagree**	**5 Strongly Disagree**

20. Do You agree that the information security risk can be reduced if blockchain can be integrated with wallet security?	(1) Strongly Agree	(2) Agree	(3) Neither	(4) Disagree	(5) Strongly Disagree

Questions	Please rate the Risk mitigation Approaches in Blockchain				
21. Do you agree that one of the risk mitigation techniques of blockchain is secure implementation of the same?	(1) Strongly Agree	(2) Agree	(3) Neither	(4) Disagree	(5) Strongly Disagree
22. DO You agree that appropriate risk management is necessary before implementation of blockchain as a risk mitigation strategy?	(1) Strongly Agree	(2) Agree	(3) Neither	(4) Disagree	(5) Strongly Disagree
23. Do you agree that the risks in blockchain should be identified in the initial stages of its deployment for effective mitigation?	(1) Strongly Agree	(2) Agree	(3) Neither	(4) Disagree	(5) Strongly Disagree

24. Do You agree that the reduction in use open-source Blockchain technology by the organizations can reduce the risks in blockchain?	**1 Strongly Agree**	**2 Agree**	**3 Neither**	**4 Disagree**	**5 Strongly Disagree**
25. Do you agree that in house designing of blockchain can mitigate the data security risks in blockchain?	**1 Strongly Agree**	**2 Agree**	**3 Neither**	**4 Disagree**	**5 Strongly Disagree**