The effects of blockchain implementation on Cyber risks mitigating strategies in the financial sector in the United Arab Emirates

الآثار المترتبة على تطبيق تقنية البلوك شين على استراتيجيات تقليل المخاطر الإلكترونية في القطاع المالي في دولة الإمارات العربية المتحدة

by

YASSER MOHAMMED SAADEH

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

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that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.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

The author whose copyright is declared on the title page of the work has granted to the British University in Dubai the right to lend his/her research work to users of its library and to make partial or single copies for educational and research use.

The author has also granted permission to the University to keep or make a digital copy for similar use and for the purpose of preservation of the work digitally.

Multiple copying of this work for scholarly purposes may be granted by either the author, the Registrar or the Dean only.

Copying for financial gain shall only be allowed with the author's express permission.

Any use of this work in whole or in part shall respect the moral rights of the author to be acknowledged and to reflect in good faith and without detriment the meaning of the content, and the original authorship.

Abstract

Blockchain technology will be the base of current and future business in all fields, as it allows information to be transferred and updated by network participants in a trustworthy, secure and efficient way. This feature and other main success factors of blockchain encourage researchers to concentrate on the chances to benefit from blockchain in the efforts to decrease the effects of cyber threats on the business and improve the cyber defense. Also, to shift from reactive to proactive risk resilience.

This study has been devoted to finding out the effects of blockchain implementation on cyber risks mitigating strategies, mainly in the financial sector in the UAE.

The study concentrates on the following factors: governance, insider threats, technology and processes.

The quantitative method was used by creating an online questionnaire to collect data. Besides that, a hard copy was distributed to get more feedback. Ethical issues were anticipated and considered in this research. A total of 149 completed and accepted responses were received. The statistical package for social sciences (SPSS) was used to analyze the responses by using different analysis techniques like Cronbach's alpha, correlation test and regression test.

The findings show that there is an influence of blockchain implementation factors on cyber risks mitigating strategies. Therefore, the blockchain supports these factors on mitigating the cyber threats and executing proactive steps to avoid any future threats.

The paper is limited to evaluate the effect of blockchain implementation on cyber risks mitigating strategies which related to governance, insider threats, technologies and processes. Therefore, further studies are required for better and deeper understanding of the effects of blockchain on insider threats, governance and processes. In addition, it is recommended to extend the study towards the effects of blockchain on other factors of cyber risks. Finally, further studies are required to explore the blockchain implementation in the financial sector.

Keywords: Cyber risk, Cyber security, Cyber threats, Cyber Attacks, Blockchain

الملخص

تعد تقنية بلوك شين من أهمية التقنيات الحديثة التي سوف تلعب دورا حيويا في كافة المجالات لما تتمتع به من مزايا مهمة، حيث أنها تتيح نقل المعلومات وتحديثها من قبل المشاركين في الشبكة بطريقة جديرة بالثقة وآمنة وفعالة.

هذه الميزة وعوامل النجاح الرئيسية الأخرى شجعت الباحثين على التركيز على فرص الاستفادة من تقنية البلوك شين في الجهود المبذولة للحد من آثار التهديدات الالكترونية او ما تسمى بتهديدات الفضاء العيني على الأعمال التجارية وتحسين سبل الحماية، والعمل على التحول لالية توقع المخاطر وتجنبها بدل من العمل فقط على تقليلها عند حدوثها.

تم اعداد هذه الدراسة لاستكشاف آلية الاستفادة من تقنية البلوك شين في دعم الاجراءات المتخذه للحد من المخاطر الالكترونية مع التركيز علي القطاع المالي في دولة الامارات العربية المتحدة.

ركزت هذه الدراسة على العوامل الرئيسية التالية : الحوكمة، التهديدات الداخلية، التقنيات، العمليات.

تم استخدام تقنية التحليل الكمي للبيانات، من خلال اعداد استبيان من خلال الانترنت ونسخة ورقية لجمع البيانات، وتم تعبئة الاستبيان بشكل تام ومقبول من قبل 149 مشارك، حيث تم استخدام برنامج التحليل الاحصائي SPSS لتحليل البيانات من خلال استخدام تقنيات التحليل المختلفة الملائمة لهذا الاستبيان.

تظهر النتائج أن هناك تأثير لتطبيق تقنية البلوك شين على عوامل النجاح الخاصة بالأمن الالكتروني، لذلك فإن تقنية البلوك شين تدعم عوامل الامن الكتروني في التقليل من المخاطر الناجمة عن التهديدات الالكترونية، كما تدعم تنفيذ خطوات استباقية لتجنب أي تهديدات مستقبلية.

تقتصر هذه الدراسة على تقييم تأثر تطبيق تقنية البلوك شين على عوامل النجاح الخاصة بالأمن الالكتروني والتي تتعلق بالحوكمة والتهديدات الداخلية والتقنيات والعمليات. لذلك ، هناك حاجة إلى مزيد من الدراسات من أجل فهم أفضل وأعمق لآثار تطبيق تقنية البلوك شين على التهديدات الداخلية والحوكمة والاجراءات المختلقة. كما توصي الدراسة بتوسيع نطاق البحث نحو تأثيرات تقنية البلوك شين على العوامل الأخرى المتعلقة بالأمن الالكتروني. وأخيرًا ، فإن هناك حاجة لإجراء مزيد من الدراسات لاستكشاف تأثير تنفيذ تقنية البلوك شين على القطاع المالي.

كلمات البحث الرئيسية : المخاطر الالكترونية، الأمن الالكتروني ، التهديدات الالكترونية، الهجمات الالكترونية، تقنية البلوك شين.

Acknowledgement

First and foremost, I would like to thank my God, Allah, for His continuous support, to enable me to accomplish my goals in life.

I want to express my sincere appreciations to my supervisor Dr. Khalid Almarri, for his constant guidance, monitoring and infinite support during my work on the dissertation.

My deepest thanks to the professors in the Faculty of Engineering & IT, for the valuable knowledge they gave me, and the efforts they expended on me to move me forward during my study.

My gratitude is further extended to my family and all colleagues who support me throughout the duration of my studies at the British University in Dubai.

Contents

List of figures

List of tables.

Chapter One: Introduction

1.1. Background and Statement of the Problem

Transferring operations of business from manual to digital, besides using the latest technologies nowadays supports different organizations to minimize the time to perform different operations. Also, helps them to increase the efficiency and customer satisfaction (E&Y 2011; Porter & Heppelmann, 2014). On the other hand, the automation processes increase the cyberattacks by exploiting the vulnerabilities of online business to get the information and using it on illegal processes like transferring money from clients to the attackers or encrypt the databases and asking for money to decrypt it or part of it. Also, selling stolen information or identities on the dark net websites (Aloul, 2012).

The target of attacks can be directed to disrupt, destroy or weaken the main systems for countries by targeting the main sectors like military, health or public sectors, these threats directly effect on the global economy and society. Also,, it may threaten the country's security and its financial safety, besides the effects of attacks on all other sectors (Watkins, 2014).

The reasons for threats differ from one organization to another, so there are important areas that should be targeted by public and private institutes on their effort to reduce cyber threats and reach to robust cyber resilience, such areas can be categorized as governance, insider threats, technology and processes (PwC-3, 2016).

Governance: The organization leaders should lead the process of protecting the different operations of the organization from insider and outsider threats that targeted the critical information, CEO should understand the importance of cyber resilience and the effect of cyber-attacks on the profit and the reputation of his organization (Scully, 2013).

Furthermore, executive members have to change the idea of postponing the cyber security process until the threat becomes true and the systems of their company hacked.

The responsibilities for protecting the information must be distributed correctly among the executive members because most of the organizations consider cyber risks as an IT issue and the responsibility for any threats rest on the CIO. This idea should be changed and process should be done by all the team and the CEO should lead the process and consider the cyber security as the main factor in the organization policy (Scully, T 2013; Ryan, O. 2016; PwC-3, 2016)

Insider threats: human factor plays the main role in the process of protecting an organization, a lot of researchers concentrate on the human factor, as it is the most important factor in the success of efforts to protect information (Pfleeger *et al*. 2009; Munshi *et al*. 2012; Crossler *et al.* 2013; AlKaabi 2014; MeriTalk 2015)

Pfleeger *et al*. (2009) asserted that the processes of monitoring and protecting organizations from external threats always takes priorities while working on building strategies to protect any institute from cyber threats, which causes unexpected insider threats. Therefore, the processes and procedures to avoid insider threats should take more attention and different actions should be implemented, like: building employees' awareness program of cyber-attacks. Also, engaging the staff in building and suggesting the suitable protection systems. Besides that, building appropriate employees' training programs. Moreover, monitoring the flow of information and the volume of outgoing and incoming data. Finally issuance of a system of incentives for cyber resilience ideas to encourage employees to interact positively. (MeriTalk, 2015).

Technology and processes: Cyberattacks take different types, like ransomware, adware, spyware, phishing, backdoor, Trojan horse, worm, viruses, spam and Daniel-of-Service-

attacks (DoS). Also, distributed DoS (DDoS) which uses a technique to send a huge amount of meaningless data to the targeted machines, that hanging the machines and postponing the response. Also, freezing or crashing the servers because of lack of capacity (Putte *et al*., 2013; Holmes 2017).

Mentioned attacks could be organized and executed by individuals, organizations or criminal groups. Moreover, the objectives of cyber-attacks differ from one attacker to another.

As a result of increasing cyber threats many actions are executed and others are suggested to be executed from different levels of the organizations to mitigate the effects of threats on their business. like using latest technologies to prevent networks and hardware, also using different types of software to prevent their systems, starting from using firewall, secured domains antiviruses and not end with transferring their systems to the cloud solutions or using blockchain technology and big data analysis techniques (PwC-3, 2014; Dougherty, 2015).

Different proactive processes can be executed to prevent the organizations from any attacks. Dougherty (2015) suggested integrating cyber resilience strategy with risk management strategy of the organization thru creating cyber resilience standards and policies. Friedman (2016) discussed the cybersecurity technology innovation, and how to exploit the new technologies like cloud solutions, blockchain technology and big data techniques to decrease cyber threats and to enhance cyber risk management.

Blockchain technology: Blockchain will be the base of current and future business in all fields. Iansiti (2017) asserted that the new technology relies on distributed network concept. Also, peer to peer techniques, which means ignoring the idea of depending on mediator to execute the processes between two parties, so one party can send payment directly to another

party without going thru banks. Also, it helps in gathering all services within one online ledger. Therefore, it will reduce the duration, resources and cost required to perform different tasks.

Howard Lee (2016) says "distributed ledger technology (DLT) allows information or records to be transferred and updated by network participants in a trustworthy, secure and efficient way". On the other hand, using blockchain technology to build large, open source systems, besides using new types of digital or smart contracts, requires to study the related legal and regulatory very well and update the rules of the business to protect it from any breaches (Batlin *et al,* 2016).

In October 2016, Dubai announced its blockchain strategy with a main objective to be the first city on the blockchain by 2020.

1.2. Aim

The aim of this study is to establish the effects of blockchain implementation on cyber risks mitigating strategies in the financial sector in the United Arab Emirates.

1.3. Objectives

The objectives are:

- To study the cyber risks and the challenges that face online business.
- To review the current tools used to protect different businesses from the threats of cyber-attacks.
- To evaluate the uses of blockchain technology to reduce the cyber threats and increase the efficiency.

1.4. Scope

The main scope is to study the vulnerabilities of the digital services that increases the cyber threats. Besides that, the current solutions implemented from different sectors to reduce the effects of cyber-attacks. Furthermore, studying the future recommendations to reduce any future threats that are caused by using the latest technologies.

1.5. Research questions

As will be seen in the literature review, this research will try to answer the following questions:

What are the weaknesses of the financial operations that cause increase in cyberattacks?

How are governance, insider threats, technology and executing different processes effects on cyber resilience?

How to benefit from blockchain technology to reduce the digital threats?

Summary

In this study, we will discuss the challenges during executing the financial operations, how to mitigate different types of cyber threats, how to minimize the technical weakness, lastly and not the least what is the effect of using blockchain technology on minimizing the threats and increasing the productivity.

Chapter Two: Literature review

Introduction

Trustwave experts investigated cyberattacks in different fields in 2016; they provided a clear picture of how and where attackers concentrated their attempts. Referring to their global security report, the breaches distributed between different sectors as the following: retail industry affected by 22% of incidents. Then, beverage and food at 20%. After that, insurance and finance by 14%. Followed by hospitality 13%. In addition, the remaining ratio for other sectors. Referring to the results by environment, the corporate and internal network was the most penetrated in 2016 at 43% compared with 40% in 2015. Followed by point of sale at 31% in 2016, which increased 9% than 2015. The third sector was e-commerce, the breaches to e-commerce decreased from 38% in 2015 to 26% in 2016, because of more efforts directed to this sector (Trustwave, 2017).

Symantec (2016) results displayed the total number of mega breaches in 2015, 9 mega breaches registered, each of them included more than 10 million identities, the number of identities hacked has increased 23% in 2015 to reach 429 million records, noting that a lot of companies not declaring the full extent of their data breaches .

In the commercial environment, payment card data was the main targeted for breaches. Most of them came from point of sale at 33%. Besides that, 30% of breaches were directed to card-not-present data, which mainly came from e-commerce. On the other hand, the results of Trustwave study related to the methods of penetration displayed that remote access method caused around 30% of breaches in 2016 compared with 13% in 2015. Followed by, phishing and social engineering at 19% in 2016 which was around 8% in 2015 (Trustwave, 2017).

IBM x-force research reviewed the major attacks and data breaches in 2015. Referring to their research, the facilities offers to the clients in the banks' sector like credit cards, ATM and mobile banking apps attracted the hackers to concentrate on the vulnerabilities of banking systems, besides that many banking clients fell victims to the

Dyre and Dridex Trojans. Moreover, in the financial industry, the number of breaches related to blackmail or theft of currency increased by 80% in 2015, 38% of them related to malicious attachment or links (IBM, 2016).

Gilderdale (2017) studied the dangers of cyber-attacks; he mentioned that malware threats increased by 36% in 2015 compared with the previous year. Also, he discussed that the local infrastructure of banks became an important target for attackers to get more benefits. On the other hand, the cyber-attacks against different banks, like the Bangladesh Central Bank, showed the necessities to coordinate the efforts to face cybercrime, fraud and money laundering. In addition, to integrate the cyber resilience with anti-fraud controls and insider threat management.

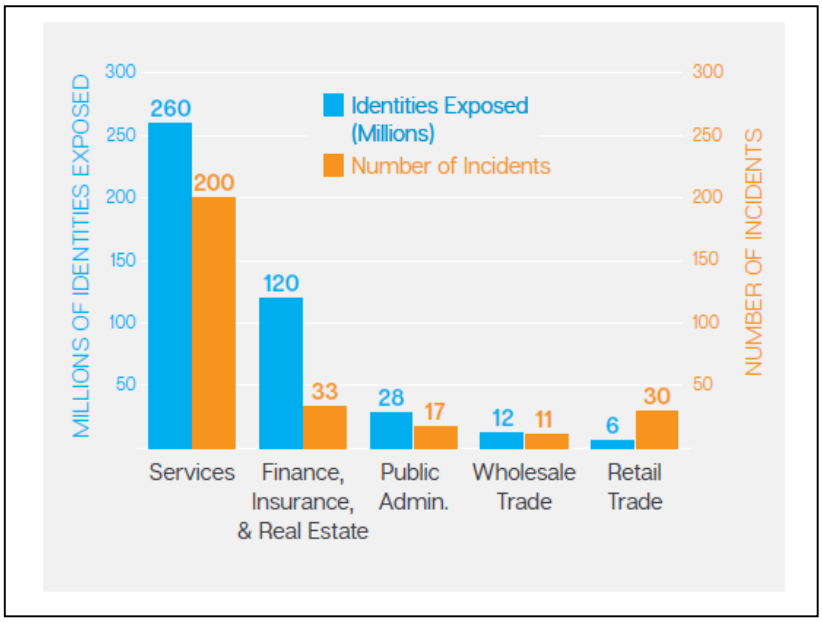

Figure 1: **Top 5 High Level Sectors Breached by Number of Identities Exposed and Incidents** (adopted from Symantec 2016, p.49).

The findings in "risk in review study" regarding the maturity of management in cyber threats are 62% of respondents expected cybercrime to make disruption to their business. On the other hand, only 3% scored very high maturity in cyber risk management, whereas 74% scored low or no maturity. In addition, they found that cyber risk maturity and risk culture maturity differs from one organization to another, financial services scored high ratio for both cyber risk and risk culture maturity, but still a lot of efforts and proactive actions are required from different sectors to face the increasing ratio of cyber-attacks (PwC, 2017).

The 2018 GSIS survey concentrates on the methods to prevent digital environments from different types of cyber-attacks. Referring to their results, 39% of respondents cite the loss or breach of critical data, 44% do not have security strategy for their information. Also, 54% of respondents do not have any idea about response process for incidents.

2.1. Cyber risks factors:

The financial crime study by PwC (2016) recommends financial institutes to measure and monitor the cyber risk, insider threats and anti-fraud to prevent their organizations from different attacks. Also, the study suggests the following actions for the following threats:

Cyber risk: cyber risk measures started with reviewing the current protect, detect and response actions have been done to protect institutes from different threats. Also, monitor the internal and external traffic, besides implementing the latest update to control software. Furthermore, review the response process and validation controls.

Insider threat: insider threat measures in the financial field concentrate on the authority's access given to the employees, vendors, contractors and other users to use the SWIFT and other payment software, besides monitor the traffic trend for all users. Also, review the policies and procedures for payment and fund transfer. Moreover, educate and train different users to minimize the internal threats.

Anti-fraud: anti-fraud measures which related to financial transactions included applying Anti-Money Laundering and Know Your Customer policies. Also, identify indicators to monitor irregular and failed transactions. Moreover, implement big data analytics technique to analyze data and the relationship between all databases related to financial transactions, Also, regularly evaluate fraud prevention, detection and response controls, which could include approval rules for transaction and the approaches for authentication.

PwC (2016) summarize the main factors of mitigating cyber risks as the following:

2.1.1 Governance

2.1.1.1 Involvement of the boards

Involving top management in risk decision making was one of the most important challenges discussed and raised by PwC (2016), their surveyed data showed that only 13% from the front liner lead risk decision making. On the other hand, 46% planning to transfer it during next three years, upon their study, transferring the responsibility will help the organizations to align risk management with the global strategy, besides that it will encourage top management to include the business risk within the execution plan when specifying the priorities. Moreover, it will support managing the risk tolerance level.

The National Association for Corporate Directors (NACD) studied the participation of board members in identifying and driving cybersecurity strategy, referring to their results, 45% boards participate in overall security strategy, the involvement in security budget increased to 46% in 2015 compared with 40% in 2014. Also, it is increased in security technology to reach 37%. NACD recommended the executive members to concentrate on the effects of the financial, legal and strategic impacts of cyber risks on the different operations of their institutes.

Cybersecurity has emerged among the top priorities in the boardroom, as any breach could damage the trust that clients have in their bank, and affect the future profitability of the institute (KPMG, 2018).

2.1.1.2 Cybersecurity strategy

Having a cybersecurity strategy became an essential pillar for any organizations to prevent their investments from any cyberattacks, besides that the cybersecurity strategy should be part of the overall strategy. As an example, Russia adopted its security strategy in 2000, United Kingdom published in 2016 its second cybersecurity strategy to protect online business and attract more investment in this field (ITU, 2017).

Each part of any business requires different levels of protection, therefore executive leaders should priorities their business objectives, implement the proactive security plan, besides that incident, response plan should be ready, and security awareness plan should be created and implemented by all members of the organization (IBM, 2016).

KPMG's UAE banking perspectives 2018 advises that UAE banks reshape their response strategy and should consider investing in cyber security from a consumer-centric point of view.

Dubai Cyber security strategy

The Dubai Electronic Security Center (DESC) was established in 2014 to improve, monitor and execute information security practices, DESC's strategic plan describes the processes required to mitigate the risks and build trusted environment.

In 2016, DESC launched its cyber security strategy that provides rules to protect the digital services from different cyber threats and cyber-attacks. Also, to provide confidence for individual users beside the different sectors, in order to place Dubai one of the most secure cities electronically in the world.

DESC (2017) pointed out that the Dubai cyber security strategy has a set of main domains:

Cyber security: Raising rules in order to protect confidentiality, integrity and availability, for different sectors in Dubai.

Cyber resilience: Avoiding any discontinuity of information technology systems and Ensuring their availability.

Cyber smart society: Performing security awareness, proficiencies and capabilities to control cyber security threats.

Innovation: Encouraging research and development (R&D) activities and creating a secure environment while using new technologies.

National and international collaboration: strengthen the communication and collaboration to mitigate cyber risks and prevent all sectors from cyber threats.

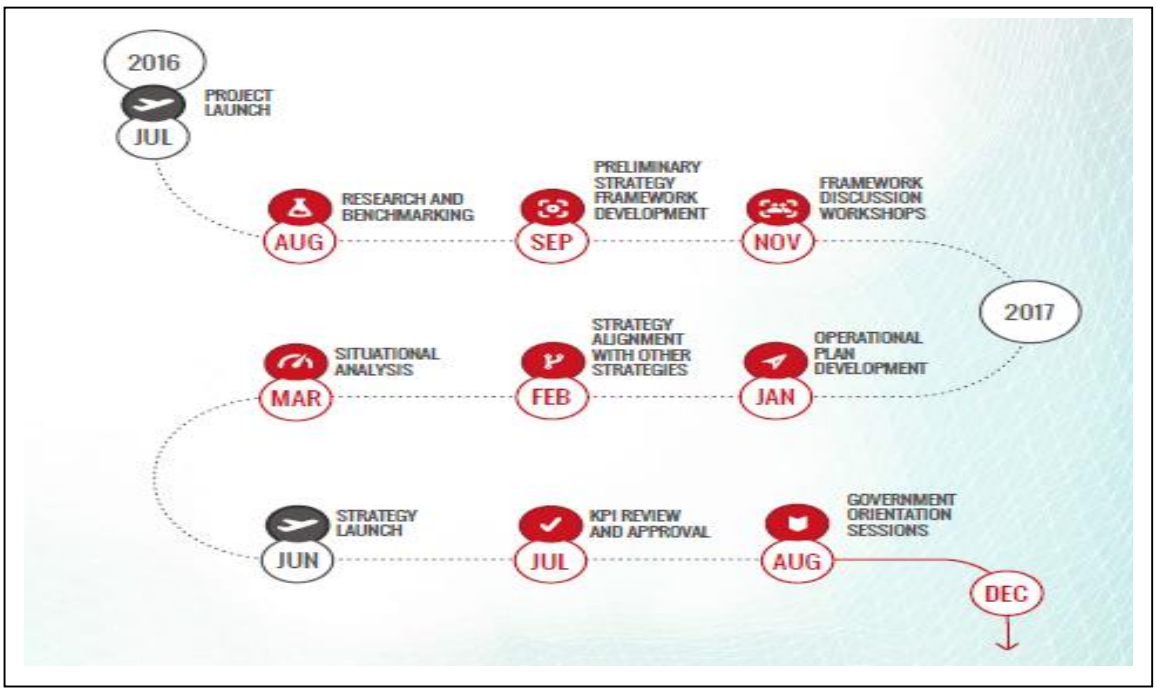

Figure 2: **Launching phases for Dubai cyber security strategy** (Dubai cyber security strategy 2017, p.31).

2.1.1.3 Rules and regulations

Because of negative impact of misusing technology and increasing ratio of cybercrime incidents, many governments start establishing cybersecurity rules and regulations to protect their organizations. In 2009, Colombia published a law dedicated to manipulate illegal uses of information. Also, Georgia in 2011, established legislation related to cybercrime. Oman created the e-Governance framework that includes the rules and procedures that ensure the sustainability of information technology projects and control of IT risks. Moreover, cybersecurity training executed by other governments as a part of their cybersecurity strategy (ITU, 2017).

The UAE issued Cybercrime Law in 2012 to discourage the misuse of internet and social media; the law consisted of 51 articles and covered the majority of cybercrime incidents. The law includes strict punishments that could go up to a life sentence and/or a fine varying between Dh50000 and Dh3 million depending on the seriousness and severity of the cybercrime.

The Dubai Electronic Security Center (DESC) has published the Information Security Regulations (ISR), which is mandatory for Dubai's public and semi-public sectors and recommended for the private sector. DESC also provides an auditing function to ensure that the standard has been executed correctly (DESC, 2017).

2.1.2 The Insider threats

The insider threat is referred to authorized and trusted users who exploit their privileges and perform some activities that can easily cause significant damage or losses even intentionally or unintentionally. The damage that effects from the insider threat has a major impression on the institutes in terms of strategies and plans, finance, reputation and sensitive information sharing (Munshi, 2012).

Even attackers was the main source of hacking as reported by Symantec, but NetDiligence (2015) reported that the insider breach was responsible for one of the most publicized data breaches of the year at Ashley Madison. On the other hand, insider threats compared with 55% in 2014, these threats came from employees, contractors, consultants or any other external clients or vendors who have access to the systems (IBM, 2016) cause 60% of attacks in 2015.

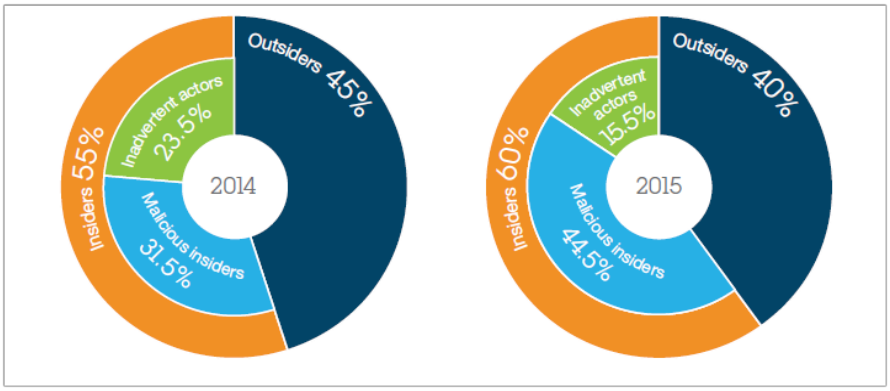

Figure 3: **The responsibilities of attacks: insider, outsider** (adopted from IBM 2016, p.12).

45% of respondents to MeriTalk survey indicated that their institutes were targeted by insider threats. Also, 29% mentioned that they have lost data due to insider incidents. On the other hand, just 39% replied positively to the point related to the security training offered by their institutes. Moreover, 65% asserted that they use their personal emails to receive official emails, besides that they transfer official documents to their personal emails. Regarding sharing data, 45% of respondents cannot recognize if a document has been correctly shared or not. Also, 34% cannot distinguish what data lost (MeriTalk, 2015).

There are various processes that can reduce the insider threat occurrence; these processes can be categorized as the following:

2.1.2.1 Education and Awareness

Many recommendations raised to reduce the effects of insider threats, most of them concentrated on end-user training to make employees, contractors and different stakeholders more involved in the efforts to protect their organizations from cyber-attacks. Also, an incentive scheme has been recommended to reward firms addressing cyber security in their products. Alkaabi (2014) asserted that the institutes need to educate and create awareness among employees, they should understand the value of the information they manipulate, the possible attacks that might happen, the type style such attacks may take, and how and who to notify suspected social engineering attacks too.

2.1.2.2 Security culture

Enhance security culture between all levels of employees and management to be more aware of threats and the rules to avoid any direct or indirect attacks. Crossler (2013) asserted that cultural behavior background is one of the main source of cyber threats.

2.1.2.3 Sensitive information sharing

Employees can share sensitive information with each other and with external customers, this information can be disclosed to third parties and exploited to breach of privacy. To control accessing information, an institute may require different users to use passwords, a personal identification number (PIN), or biometric identifiers to access specific information (Siddiqui & Muntjir, 2013).

2.1.2.4 Tools and Techniques

MeriTalk (2015) suggest the following tools and techniques to protect the insider environment from cyber threats:

Real-time alerts

Activating real-time alerts to notify the security team about any misuse of data, illegal transactions, any penetration to the systems, or any attacks like phishing or DDoS causes data loss or memory overload.

Software development

Developing programs like data loss prevention to protect systems and software from insider threats. Also, all software used should be up-to-date to prevent it from different attacks that could exploit any vulnerabilities to hack the systems.

Authentication

Using two way authentication instead of normal password policy to secure data is an important factor, according to MeriTalk survey results, more than half of respondents are still using only password technique to protect data.

Answer Options	*Used agency-wide*	*Used selectively*	*Plan to implement within the next 2 years*
Data loss prevention	48%	36%	10%
Two-factor authentication	46%	33%	13%
Digital signatures	44%	39%	13%
Email encryption	43%	40%	9%
Endpoint encryption	40%	37%	18%
Access management solution	39%	39%	15%
File/folder encryption	37%	47%	12%
Anomaly detection	36%	45%	10%
Social mapping to track unusual behaviors	25%	30%	22%

Figure 4: **Inside Job: The Federal Insider Threat Report** (adopted from MeriTalk 2015, p.10).

2.1.3 Technology

Referring to data security standard from Payment Card Industry, any organization using sensitive data can implement the following steps to reduce any penetration:

System configuration and change control process, firewall configuration to control inbound and outbound signals, policy of passwords, remote access control by using two ways authentications, using latest updated versions of suitable antivirus and malware removal,

train and educate the employees on best practices of information security and implement policies and procedures to manipulate and process data in secured way.

2.1.3.1 Using mobile with payment

57% of respondents to GSIS survey said they have started using mobile payment systems; the increasing ratio toward using mobile technology encourages hackers to exploit the vulnerabilities of new technologies beside human weaknesses. On the other hand, 57% said malicious and malware programs are the main source to mobile payments risks, whereas 45% recommended protecting the hardware platforms. Also, 45% of respondents raised the necessity of provisioning and verification processes to decrease the threats, 43% recommended to concentrate on the protection of customer's data when using mobile technology for payment purpose and 42% raised the importance to look for end-use vulnerabilities and risks to increase the security when using mobile payment (PwC 2016).

2.1.3.2 The effects of ransomware

Ransomware is a type of malware that targeted devices connected to internet, the main objective for attackers is to get money from the victims.

The main type of malware is locker ransomware, which is designed to lock the computer and prevent the user from using it, the other type is crypto ransomware, which designed to encrypt the data. In 2015, 64% of detected ransomware have been crypto ransomware while the other 36% created by locker ransomware (Savage et al, 2015).

2.1.3.3 Using Internet of Things (IoT) components

The number of devices connected to Internet increased rapidly. It was 13 billion in 2015 and it will increase to 20 billion in 2020 as predicted by IDC research institute (2015). Therefore, the risk related to privacy and security increased 152% between 2014 and 2015 as reported by respondents to GSIS survey, for example attacks to mobile devices increased from 24%

in 2014 to 36% in 2015, whereas penetration to embedded systems increased to 30% compared with 13% in previous year. Also, breaches to consumer technologies increased 3 times and hacking operational systems increased from 10% to 26% (PwC 2016).

2.1.3.4 The effects of using big data analysis techniques

Data is a pillar for any organization; managing and organizing data is the main challenges. The financial organizations have huge daily transactions that should be structured and saved in a secure environment, to protect it from unexpected attacks. Analyzing and monitoring data to understand when it is used, also how it is used and by whom encourages different firms to use big data analysis techniques. The respondents to GSIS survey found that using different techniques to manage data helped to understand the external threats, the internal threats, besides understanding user behavior. Also, giving better view of irregular network activities. Finally, developing the ability to identify and reply to the different security incidents in quick and professional way (PwC 2016).

2.1.3.5 Cloud-based technologies

Transferring different applications to this secured platform helps different organization to reduce the impact of cyber-attacks on their business, besides that it transfers the concentrate to achieve risk resilience. The cloud solution support the organizations of different levels to concentrate on their business and build trust with their customers. Besides that decrease the investment on building robust architecture, which needs to dedicate a huge amount of budget to perform it (Harper, 2017).

2.1.4 Processes:

Referring to 2018 Global State of Information Security Survey (GSISS), less than 50% of respondents execute the key processes for avoiding cyber-attacks in business systems,

including breach tests, information security monitoring and controlling, besides vulnerability and threat assessments

The collaboration and sharing security information with trusted stakeholders and competitors in the same fields is another important factor to reduce the possibilities of future cyber risks, as well as, to decrease the response time for any unexpected attack besides improving the security. Referring to GSISS respondents, only 58% share security information with others (PwC 2017).

Classifying data is one of the most important factor to start protecting it. Categorizing data differs from one organization to another, but in general , data could be classified as sensitive, not sensitive or critical and not critical , Also, it could be categorized depend on its size.

2.1.4.1 **Cybersecurity standards**

Many governments start creating standards to secure and prevent digital services from any breaches. Germany established in 2009 security research and development programs to support the cybersecurity research. Moreover, public awareness campaigns related to cybercrimes was created. Also, security solutions distributed free of charge by Latvia government. Another effort was done to organize cybersecurity professional training courses, besides that many universities start creating new programs related to information security and cybersecurity (ITU, 2017).

2.1.4.2 **Implementing security framework**

The 2016 Global State of Information Security Survey (GSISS) studied the challenges related to cybersecurity and the recommended solutions to mitigate cyber threats, referring to their results, the majority of organizations implanted a security guidelines or framework like NIST, IS27001, COBIT, SAS or COSO to identify the risks, also to priorities it, depends

on its impact on their business. Moreover, to test the maturity of their implementation of cybersecurity practices and to improve the communication internally.

Referring to their results on the benefits of security framework, 49% of organizations using it to identify and priorities the cyber threats. Then, 47% of respondents' their targets was to accelerate the process of detection and mitigation of cyberattacks. Then, 45% looking to make their sensitive data more secure.

NIST framework

The National Institute of Standards and Technology (NIST) framework was created on 2014 to help different organizations shifted from reactive to proactive risk resilience standards, the main functions including identify, protect, detect, respond and recover (Mont 2015).

Identify: understand the organization structure, the core business, also the resources required to support the core functions and the cyber threats which may effects on risk management strategy, so identify function concentrated on data gathering beside analyzing the output data, the results includes risk management strategy and risk assessment.

Protect: implement and execute the suitable solutions to protect the business from different cyber threats, the output will be the data protection procedures and the recommended technologies to protect data.

Detect: monitor and control the cyber resilience events during implement suitable activities, the outcome concentrate on the processes to monitor and detect the cyber-attacks.

Respond: take suitable respond regarding detected cyber-security event that can be done thru executing an urgent action using an appropriate technique.

Recover: take action to recover the hacked data due to cyber-attacks. Also, develop the plan to protect data from any future threats, the output include a recovery planning.

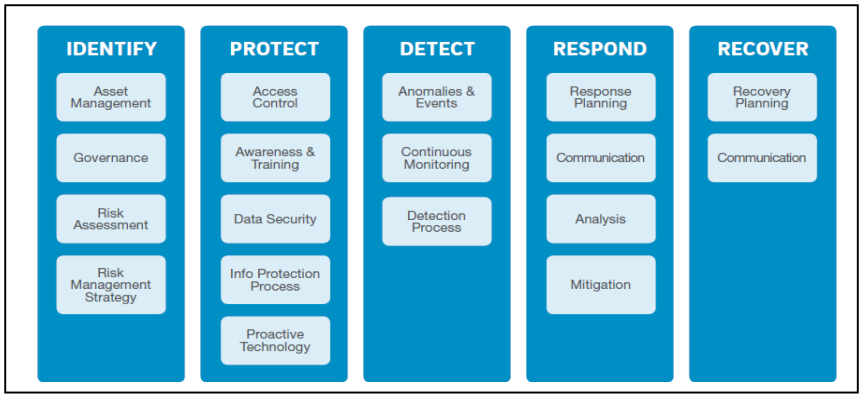

Figure 5: **The five core functions in the NIST Cybersecurity Framework with category examples** (adopted from Trustwave-2 2017, p.07).

NIST suggested the following steps to be executed from top management to mitigate the risks and improve performance:

- Creating cyber security governance thru specifying the operating processes and the workflow of reporting. Also, integrate cyber risk plan with the general plan for whole risks.
- Understanding the areas that affected by cyber-attacks which targeted data or flow of data in the different levels, besides specifying the most important revenue stream, assets and business process and the actions done to protect them.
- Increasing the capabilities of cyber security team to identify and analyze the cyber threats beside execute the suitable solution on the correct time and create the feedback or lessons learned reports.
- Planning and preparing responses to decide who should take the action, their responsibilities and the actions to be done.

2.2 Blockchain technology

2.2.1 Blockchain definition

Iansiti (2017) asserted that blockchain technology is a distributed database, which depends on storing all records in the public data store or all users who have privileges after confirmed

and verified by consensus, saved transactions can access ledger. Furthermore, it allows the users to transfer data in secured and safe manner. Also, any data saved in public leger cannot be deleted.

Siba (2016) pointed out that blockchain can be categorized as public, private and hybrid, in the public blockchain, the database is totally decentralized and accessible by any user-using internet. Also, records can be added by any user after validated and verified by consensus, Bitcoin uses public blockchain technology. On the other hand, a central authority in the private blockchain monitors the transactions, it cannot be added to the ledger before approved by the authority, hybrid blockchain stands in the middle between public and private, the transactions depends on partially decentralized technique (Siba, 2016).

2.2.2 Blockchain success factors

Blockchain is a trusted and secured network, therefore the permissions to read or write are granted to the participants. The privileges are given to each of them depends on the role and responsibility. Moreover, the transactions are created and saved in the blocks which secured by hash algorithm, therefor the created transaction cannot be moved or deleted as it is chained with previous blocks (Siba, 2016).

Batlin *et al.* (2016) asserts that distributed ledger reduces the redundant information by sharing one database, which includes all information required by different organizations instead of saving it separately by each of them. In addition, it reduces the time required to manipulate data and execute different operations on it. Moreover, the cost to maintain and keep one environment secured is less than executing the same process in each database for different organizations, besides that data cleansing process will be easier, so maintaining and keeping one database secured is easier than distributing same data in different databases.

Immediate transfer and near real-time settlement

There is no single party controls the data or flow of information, each party has the same authority to access database and display the historical records.it is also known as distributed database. Collomp and Sok (2016) sum up in the figure (6) below the key differences between centralized databases and decentralized one.

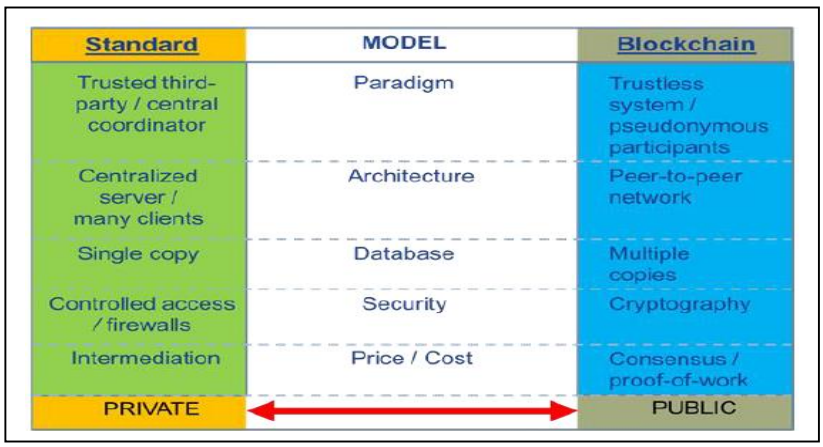

Figure 6: **Standard vs. blockchain-based transactional models (adop**ted from Collomp & Sok. 2016, p.3).

Communications between two parties are done direct by using proof-of-work to record a public history of transactions without the need for a trusted third party, so there is no mediator to verify and transfer transactions between different parties, therefore transactions can be verified in near real-time (Nakamoto, 2008).

Improving managing data through Immutable capabilities

Once the transaction saved to the database, it cannot be deleted or altered because the database is an immutable record and the records stay in the ledger permanently. Moreover, any changes are done in the public blockchain can be viewed by all parties. On the other hand, cryptography allows participants to see only the parts of the ledger that are related to them.

Supporting quality and accuracy of data

A consensus required to allow transactions to be executed between different parties in the network, so no new information can be inserted to the ledger without the approval from the majority of nodes in the network. In addition, the approved information must be stored to all nodes. Because of that, the consensus features supports quality and accuracy of data (Swan, 2015).

Cryptography Techniques

Blockchain uses public-key cryptography to generate a unique cryptographic key for each user, this primary key has two segments: a network identifier, which represents the public key and a private key, which is like a password. Also, the physical assets has a unique identifies in blockchain which can be dealt with or accounted for using blockchain colored coins which represents tokens of things instead of money, a token of an asset can connected only with one account. In addition, dealing with assets is easy with an auditable and traceable record of ownership return back to the first owner (Batlin et al, 2016).

Different encryption techniques could be used to keep transactions secured during transfer process between two parties. For example when a user transfer a bitcoin to another user in the network, the created transaction that signed with private kay and includes the amount of coins and the public key of new owners is published in the network to inform all participants about it. Besides that there is signature attached to each message to confirm the validity and authenticity.

The sequence of records represents the ledger. All participants in the network have the same ledger and any changes happened by adding new blocks can be shown by all users.

Bitcoins uses Hashcash function, which depends on symmetric key cryptography to make sure the security, this function accepts any type of data as input. Then, encrypt it, so any changes to the original data will cause generating new hash differs than previous one.

2.2.3 The opportunities to implement Blockchain

Blockchain technology can be used in different sectors, which can be financial or nonfinancial.

Digital currency

The operations using digital currency is one of the most important areas to implement this technology, for instance the payment during purchasing process between two parties in e-commerce can be executed directly using digital currency and the verification will be done by all participants, noting that no mediator required. Moreover, using digital currencies will be useful in the operations with different currencies (Siba 2016).

Digital Ledger

It is another area to exploit blockchain; it can be used to keep all records of patients in the healthcare sector, which includes personal information and historical data, and healthcare records. In addition, land and properties sector can benefit from this technology to register property owner info and all transactions related to selling or buying. Another area is education and academic sector; there are many opportunities to use blockchain in the registration, administrative tasks and e learning. Moreover, the blockchain is recommended for supply chain processes to register all transactions generated from different parties in the network (Siba 2016).

Smart Contract

Recording an agreement between two parties, besides monitoring the execution of its conditions requires an intermediator to do it. In the blockchain these tasks can be executed by supporting the ledger with some programming capabilities which giving the users the privileges to add some conditions to transactions, besides supporting them to execute any kind of business logic, these features enables the creation of smart contract.

Smart contracts have unique identifiers to protect it, also it has the capabilities to send and receive information. Smart contracts can be programed to make decisions related to different operations in the different fields like buying and selling things (Batlin et al, 2016).

Smart securities

The process of issuing and managing securities is complex, it needs the services of consultants to organize, price and publishing the securities in the market. In addition, a lot fees needs to be calculated and follow up, which required a system to manage the whole process and avoiding any illegal operations of fraud.

Batlin et al. (2016) asserted that smart securities tool created in the blockchain to reduce the cost of securities issuance and servicing by programming all mentioned process, therefore smart security supports different organizations to benefit from an efficient and cost-effective securities issuing and servicing process live on the chain.

Identity management

The blockchain gives better means of identity, users are known by their pseudonymous public key, so each user can validate his identity and preserve his privacy that reduces the time required to execute different transactions in the financial system or any other field because the process of proving identity is eliminated. Also, participants can manage their identity to determine which personal info to be displayed for each transaction by creating different profiles which can be attached to each related transaction (Birch , 2014).

2.2.4 Blockchain in the financial systems

Using the distributed ledger instead of centralized databases. In addition, utilizing smart contracts to register financial agreements and establishing digital identities in blockchain can help in simplifying the financial processes that lead to reduce the cost and time required to execute different transactions and make the environment more reliable and secure.

Blockchain enables direct transactions between different parties in the network, which leads to little or no waiting, immediate transfer of funds and near real-time settlement. Also, guides to reduce the cost of transactions, simplifies the processes in the banks, ignores the need to follow-up manually, immediately settled in the trades and free up the capital for firms and investors (Batlin et al, 2016).

Blockchain uses complicated methods for cryptographic to ensure the continuity of business and reducing the cyber-attacks probability and the effects of cyber threats on the business.

Smart wallet tool: smart wallet helps the users in the network to connect directly to the blockchain and execute many tasks, like performing different transactions besides managing their accounts and preferences, communicating with other users and selling or buying any time. Smart wallet connects the users with financial system directly, as Batlin (2016, p.27) said: "Having a smart wallet will be a lot like having your own bank in your pocket".

Smart contracts open up different possibilities to automate many financial processes like escrow agents besides self-servicing others like digital securities. In addition, it can be used to automatically transfer value added taxes to the governments, prepare business tax returns and generate financial statements and annual reports, besides transferring created reports to all registered shareholders.

Smart securities tool simplifies securities issuing and servicing process. In addition, it facilitates the processes to automate auditing functions and reduces the risk of accounting faults.

2.2.5 Blockchain Applications

Banking Applications: Tasca et al. (2016) asserted that using blockchain technology to create banking applications could decrease costs by around 20 billion dollars thru increasing the security and efficiency and eliminating intermediaries.

Vault Operation system is one of the first applications developed by ThoughtMachine, based on cloud solution techniques and uses smart contract coding. It provides fast, secure and reliable banking system with excellent capabilities to manage all banking operations and financial products. Corda is another blockchain application, it is distributed ledger platform that is developed by R3 and another world's largest financial organizations, it can be used to manage and execute the financial agreements in perfect synchrony between different parties.

The New York based financial technology firm joined forces with nine of the world's biggest banks including Goldman Sachs and Barclays to establish a framework for using blockchain technology in the financial sector, other banks like UBS, JPMorgan have joined this initiatives (Crosby et al, 2015).

Payments and Money Transfers applications: different blockchain services is created to manage transferring processes, like a mobile application Abra that facilitates peer-to-peer money transfer. In addition, Allign Commerce is payment service provider allows using local currencies to execute payments. Moreover, Bitspark is created as end-to-end remittance platform. Furthermore, another different service is developed to manage money transfer like Rebit, CoinRip and BitPesa.

Securities trading applications: a lot of securities and stock exchanges like the Australian securities exchange, the London stock exchange, and the Tokyo stock exchange start using blockchain technologies to simplify settlement processes and reduce cost and time. Also, banks and financial firms begin exploring the opportunities to implement blockchain applications for security trading. On the other hand, many blockchain based applications like OpenBazaar is published to simplify person-to-person trade (Makridakis et al, 2016).

2.2.6 Implement blockchain technology by governments

Some countries start implementing blockchain in different sectors, Estonia applied blockchain-based services in eGovernment, eSafety, eSecurity and eHealth. Also, Sweden already started transferring its operations to blockchain. Furthermore, Dubai announced its blockchain strategy in 2016, which is built on three pillars of industry creation, government efficiency and international leadership, with main objective to be the first city on the blockchain by 2020. Dubai plan to save around 25 million hours and 1.5 billion dollars from productivity increases in document processing, besides reducing CO2 emission by 114 million tons yearly. On the other hand, the Global Blockchain Council was established in 2016 by the Dubai Future Foundation in cooperation with 42 government entities and private companies to explore the best applications and the different opportunities in blockchain technologies. (Smart Dubai, 2017).

During the launch of the "UAE Blockchain Strategy 2021", His Highness Sheikh Mohammed Bin Rashid Al Maktoum said: "the adoption of blockchain would help the government prepare for future challenges and contribute to saving Dhs11 billion spent annually on document transactions and documents, 77 million hours of work, reduce government documents by 389 million, and save 1.6 billion kilometers spent driving".

Sheikh Mohammed added: "This technology will save time, effort and resources and enable individuals to conduct most of their transactions in a timely manner that suits their lifestyle and work".

2.2.7 Challenges to implement Blockchain technology

Implementing any new technology required time to reach to the stability, blockchain as technology still in the development phase, the main challenges related to utilize it correctly in the different sectors depends on the requirements for each of them.

There are many difficulties stands in the way to use blockchain; technical obstacle is one of them. The speed of manipulation or throughput issues is an important challenge specially in the sectors like finance and insurance, Xu (2016) mentioned that Bitcoin network manipulates 3 to 20 transaction per second, besides that the time needed to process one bitcoin transaction block is about 10 minutes while response time for visa is seconds at most (Swan, 2015). In addition, blockchain is not suitable for keeping big data because of huge redundancy from the different processing nodes (Staples et al, 2017). Moreover, revoking the privileges to delete any transaction is another challenge.

Other different technical challenges are negatively effect during the implementation and processing, like managing network and data storage.

The governance is another challenge, new legal framework required to control all processes and transactions in the blockchain. On the other hand, the direct connections to the financial system using the smart wallet with no central authority add new challenges to the users. It increases the risks to lose different transactions or private key because malicious people will target it. Noting that, no one can restore the private key if it is lost. Moreover, users may lose their money because the transactions cannot be deleted or reversed if it is executed (Batlin et al, 2016).

2.2.8 The quality requirements for blockchain implementations

The success blockchain implementation should produce security, privacy, reliability and data integrity (Swan, 2015).

The strategy to handle the transactions must be applied. In addition, the early involvement of testing team is important before starting the testing process of the blockchain implementation. A guidance on the test strategy is suggested by Sundarraman (2017) and explained in figure (7) below. Testing process of blockchain implementation is started with system appreciation; the system appreciation phase concentrates on studying the impacted

components, which needs to be included in the testing plan and strategy. In the phase of test design assurance, a detailed level test strategy should be created; the main components that need to be checked include building a model of the blocks structure, transactions and contracts. In addition, defining use cases for each part, besides validating end and specifying non-functional requirements.

Testing planning and use cases is the next phase, in this phase the full test strategy is created which includes the testing methodology, testing tools and automation, besides specifying the coverage and estimated number of tests and use cases mapped to tests. The last phase is the test cases execution and result verification, during this phase many processes executed like low-level verification. Also, validation of transactions, blocks and smart contracts. Moreover, third party interface checks, last and not the least user interface and functional flows.

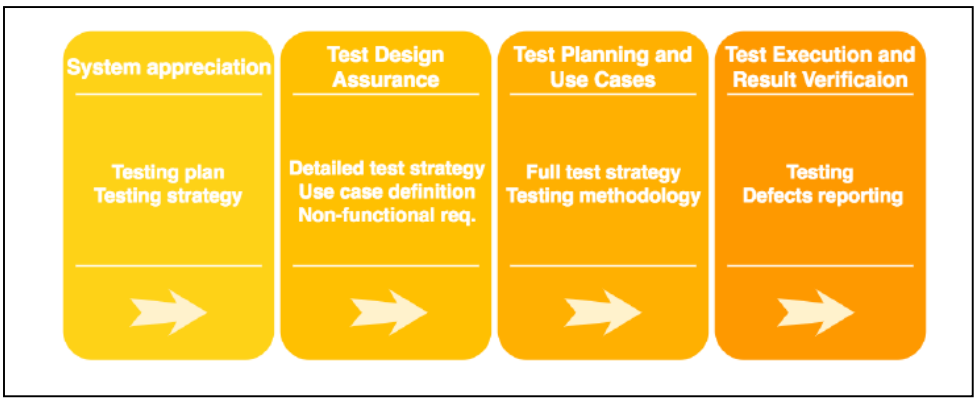

Figure 7: **Testing process of blockchain implementation (adop**ted from Sundarraman. 2017, p.6).

To solve the throughput issue, Yli-Huumo (2016) suggested expanding the size of each block, but the effect on performance should be studied before deciding to increase the size of blocks. On the other hand, Xu (2017) asserted that the capacity limitation can be avoided by specifying the type of data and computation processes that should be placed on-chain and what others should be saved off-chain.

2.2.9 Enabling the blockchain future

There are many opportunities to empower the blockchain; one of the most important task is to create a public underlying layer that could be used by everyone to build their own service. Other important capabilities are required at a system level to increase the benefits of the blockchain:

Identity issue: in the financial industry, their system connects unclear number of entities together; it includes many subsystems, each of them targeting a specific area, which create an issue in identifiers. To solve this issue an efforts should be done thru standardization to provide the credentialing for each parts of the system.

Blockchain and legal tender: blockchain-based financial system uses bitcoin and other digital currencies to transfer the value between two nodes in the network, these currencies need to be exchanged into legal coins to be used in the real world.

Central banks in different countries start studying different opportunities to use legal tender onto the blockchain, which may lead to create cryptodollars and cryptopounds or other crypto coins.

Governance: blockchain-based financial system needs rules to control dataflow between different nodes. At the technical level, different protocols need to be created to manage the creation or update process , also other specialized protocols are required, which will be asset-class based.

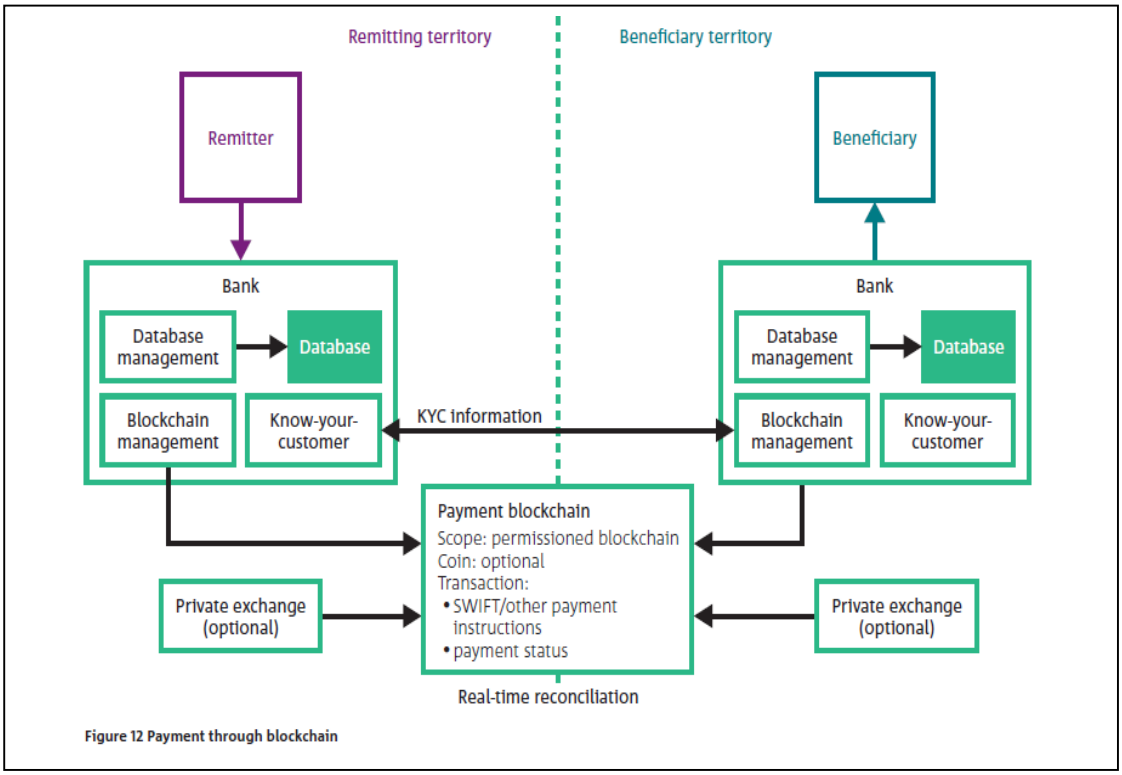

Figure 8: **Payment through blockchain (adop**ted from Staples et al. 2017, p.28).

Batlin et al. (2016) asserts that smart contract still not accepted as binding legal contract, so more efforts are required to create additional legal principles. In theory, smart contract is self-enforceable in order to make it secure, but in practice, no one can guarantee that codes are not included hidden conditions or bugs. Staples et al. (2017) supports the idea that smart contract is not legal contract; it can be considered as an evidence for an agreement.

2.3 Blockchain and cyber risks factors:

Blockchain will affect the way that organizations' interact, also the way that businesses cooperate with one another, the transparency of procedures and data. In addition, the sustainability and productivity of our economy (Deloitte 2016).

According to Piscini(2017, p.4),"Blockchain could potentially help improve cyber defense as the platform can secure, prevent fraudulent activities through consensus mechanisms, and detect data tampering based on its underlying characteristics of immutability, transparency, auditability, data encryption & operational resilience".

2.3.1 Blockchain and Governance

Piazza (2017) asserted that using blockchain technology as a corporate governance tool could result in improved timeliness and corporate information accessibility; he also added that people who have access to the ledger could track any change as it happens and access the shared ledger to submit requests for updating or adding some transactions. Moreover, it helps chief security officer and security team in any organization to monitor transactions and explore the vulnerabilities to avoid any cyber threats. Also, it will support top management to make informed decisions.

On the other hand, one of the challenges of the blockchain approach is that it reduces oversight by avoiding regulation to process inefficiencies in traditional payment networks. Therefore, Distributed networks, particularly in financial services can be much less resilient to shocks than centralized systems, which can affect participants directly. Because of that, there are arguments for blockchain applications to work within existing regulatory structures not outside of them (Deloitte 2016).

2.3.2 Blockchain and insider threats

Automating the Back-Office

Zuberi (2017) asserted that the financial institutes start using blockchain to automate back office transactions; she added that using the new technology would increase the efficiencies for the organizations. Also, it will decrease the cyber threats by exploring the vulnerabilities and minimizing the opportunities to exploit it, according to Williams-Grut (2017) blockchain-based applications could save banks 12 billion dollars yearly in back office cost.

2.3.3 Blockchain and new technology

Blockchain and DDoS

Blockchain depends on consensus from different nodes in the network to confirm transactions before it can be added to the database, therefore, if any node go offline because of DDoS attack, the other nodes continue to operate and the services will continue available. Blockchain can provide necessary techniques of demonstrating and protecting the integrity of databases. Also, blockchain has at its core a fully traceable lineage (Holmes, 2017).

Blockchain and IoT

The blockchain technology could provide the basis for IoT security, Blockchain ledger can be used to store information that generated from IoT devices, so the management of devices will be easier and the traffic will be more organized. On the other hand, automating business process will facilitate the working relationship between different parties.

The uses of blockchain for IoT will help on building trust between parties and reducing the risks of collusion and rigging. Furthermore, it reduces the cost by removing the overhead related to intermediaries and central controls. Additionally, it accelerates transactions by reducing settlement time (IBM, 2017).

The blockchain technology simplifies the implementation of decentralized IoT network such as record keeping as well as secured and trusted data exchange.

Samsung in partnership with IBM have built autonomous decentralized peer to peer telemetry (ADEPT) that uses three protocols- Ethereum for smart contracts, BitTorrent for file sharing and TeleHash for peer-to-peer messaging (Crosby et al, 2015).

Blockchain and Big data

Blockchain technologies can empower the security of big data besides accelerating the speed at which transactional data is implemented (Harper, 2017).

Zheng (2016) mentioned that big data could be well combined with blockchain; he classifies the combination to data management and data analytics. As for data management, the distributed and security properties of blockchain can be exploited to store an important and critical data. On the other hand, the transactions on blockchain can be used for big data analytics, so key performance indicators can be generated and the patterns of data may be used to take decisions.

Blockchain and Cloud solutions

Highlights from Forrester's 2017 Predictions indicate, "The cloud will be trusted and by 2020, it will be where trusted and secured IT lives, enhanced by blockchain-based security." (Harper, 2017).

Storj platform provides a blockchain based distributed cloud file storage application, it is a peer-to-peer cloud storage network that gives users the privileges to share and transfer data, share spare disk space and internet bandwidth without depending on third party or a central control.

Absence of a third party role in the Storj network decreases data failures, as well as significantly increasing security, privacy and data control (Crosby et al, 2015).

2.3.4 Blockchain and Processes

Blockchain uses advances cryptographic techniques to protect data saved in the blocks and the transactions during the processing operations. Moreover, cryptography is used to ensure the viability of the database. Therefore, Blockchain is highly resilient to cyber threats, which decrease the cyber risks mitigating costs (Batlin et al, 2016).

Deshpande (2017) asserted that Standards could perform a significant role in ensuring interoperability between multiple blockchain implementations, which could help in decreasing the risk of a fragmentation and ensuring the integrity of data exchanged.

He also added that the security and integrity of customers' data stored in the ledger should be considered by the organizations, because the distributed access and decentralized nature of blockchain across different nodes could present a serious security risk. Therefore, standardization is required to ensure resilience and security of the platforms and to increase the trust.

Standards could play a role in digital identity management; it could help control risks associated with identity. Especially, authentication of digital identities for financial transactions.

Summary

In this chapter, we examine from the literature review the information about cyber risks, cyber risk factors, blockchain and the effects of blockchain on mitigating cyber risks. Moreover, we extracted from the literature review the relation between blockchain implementation and cyber risk factors like governance, insider threats, technology and processes, which consisted our conceptual framework for this study. In the next chapter, we will present the conceptual framework.

Chapter Three: Conceptual Framework

Introduction

A conceptual framework is an analytical tool that "explains either graphically, or in narrative form, the main things to be studied – the key factors, concepts or variables and the presumed relationship among them" (Miles & Huberman 1994, p18).

The variables of cyber risk factors and blockchain

The following table displays the main factors of blockchain and cyber risk and its variables, besides that, the relation between them.

Factor	*Variable*	*Source*
Governance	• Involvement of the boards. • Having a cybersecurity strategy. • Establishing cyber security rules and regulations.	Scully (2013) PwC (2014) KPMG (2018) ITU (2017) IBM (2016) DESC (2017) Ryan (2016) PwC-3 (2016)
Insider Threats	• Educating and creating awareness among end-users. • Enhancing security culture. • Avoiding sharing sensitive information. • Activating real-time alerts. • Developing programs to protect systems. • Using two way authentication	Munshi (2012) NetDiligence (2015) IBM (2016) MeriTalk (2015) Alkaabi (2014) Crossler (2013) Siddiqui & Muntjir (2013) Pfleeger et al. (2009) Munshi et al. (2012)
Technology	• Using suitable tools to protect mobile payment systems.	PwC (2016) Savage et al. (2015)

	• Finding the suitable mitigation techniques to decrease the effects of ransomware. • Using Internet of Things (IoT) components • Using big data analysis techniques. • Using cloud-based technologies.	Harper (2017) Zheng (2016) Putte et al., (2013) Holmes (2017) PwC-3, (2014) Dougherty, (2015) Friedman (2016)
Processes	• Creating cybersecurity standards • Implementing security framework	PwC (2017) ITU(2017) Mont (2015) Deshpande (2017)
Blockchain	• Immediate transfer and near real-time settlement. • Improving managing data through Immutable capabilities. • Supporting quality and accuracy of data. • Getting traceable and auditable transactions by using cryptography techniques. • Automating the operations using digital currencies. • Registering and saving all transactions (Digital ledger). • Making decisions related to different operations by using the smart contract. • Managing the process of issuing and servicing securities (Smart securities tool). • Giving better means of identity (Identity management).	Howard Lee (2016) Siba (2016) Batlin et al. (2016) Collomp and Sok (2016) Nakamoto (2008) Swan (2015) Batlin et al. (2016) Birch (2014) Tasca et al. (2016) Crosby et al. (2015) Makridakis et al. (2016) Smart Dubai (2017) Xu (2016) Staples et al. (2017) Sundarraman (2017) Yli-Huumo (2016) Deloitte (2016) Piscini (2017) Piazza (2017) Zuberi (2017)

	• Connecting the users with financial system directly by using Smart wallet tool.	Williams-Grut (2017) Holmes (2017) IBM (2017) Harper (2017) Zheng (2016) Deshpande (2017) Iansiti (2017)

Table (1): The main factors of blockchain and cyber risks and its variables.

The Conceptual framework

From the above literature review and the main factors analysis table, we can conclude a general conceptual framework representing the effects of blockchain implementation on cyber risks mitigating factors: -

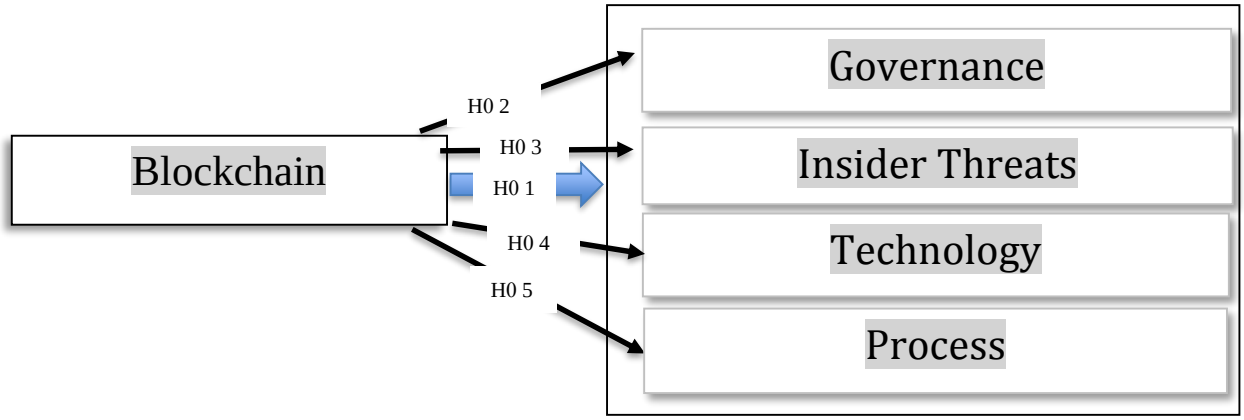

Figure 9: Conceptual Framework hypothesis (The effects of blockchain implementation on Cyber risks mitigating factors)

The hypothesis

PwC (2016) summarized the main factors of mitigating cyber risks as the following governance, insider threats, technology and processes. Based on the literature review, the relations between blockchain implementation and different factors are studied and the following hypothesis is proposed:

H0 1: There is no significant influences of blockchain on mitigating cyber risks.

Based on the literature review, the involvement of the boards, having a cybersecurity strategy and establishing cybersecurity rules and regulations became an essential pillars for any organizations to prevent their investments from any cyberattacks. On the other hand, the distributed and immutable attributes of blockchain could play an essential role to suppot the variables of governance on mitigating the cyber threats.The relation between blockchain implementation and governanc factor is studied and the following hypothesis is proposed:

H0 2: There is no significant influences of blockchain implementation on mitigating governance cyber risks.

The damage that effects from the insider threat has a major impression on the organizations (Munshi, 2012). There are various processes that can reduce the insider threat occurrence, these processes can be categorized as the following: Education and awareness, security culture and sensitive information sharing. In addition, MeriTalk (2015) suggest the following tools and techniques to protect the insider environment: real-time alerts, software development and authentication. On the other hand, the immutable attribute and the cryptography techniques used by blockchain could play an essential role on mitigating the cyber threats. The relation between blockchain implementation and governance factor is studied and the following hypothesis is proposed:

H0 3: There is no significant influences of blockchain implementation on mitigating cyber risks related to the insider threats.

As a result of increasing cyber threats from using different technologies. Many actions are executed to mitigate the effects of cyber threats. Like using latest technologies to prevent networks and hardware, also using different types of software to prevent the systems, starting from using firewall, secured domains antiviruses and not end with transferring their systems to the cloud solutions and big data analysis techniques (PwC-3, 2014; Dougherty, 2015). On the other hand, the different attributes of blockchain technology could play an essential role on mitigating the cyber threats. The relation between blockchain implementation and technology factor is studied and the following hypothesis is proposed:

H0 4: There is no significant influences of blockchain on mitigating technologies cyber risks.

Many governments start creating standards to secure and prevent digital services from cyber risks. In addition, the majority of organizations are implanting a security guidelines or framework to identify the risks, also to priorities it and to test the maturity of their implementation of cybersecurity practices. On the other hand, the different attributes of blockchain technology could play an essential role on mitigating the cyber threats. The relation between blockchain implementation and process factor is studied and the following hypothesis is proposed:

H0 5: There is no significant influences of blockchain on mitigating processes cyber risks.

Summary

In this chapter, the main variables of each factor are defined, after that, the conceptual framework is created based on the literature review, and then five null hypothesis are proposed. In the next chapter, the research methodology we will be presented.

Chapter Four: Research Methodology

Introduction

Research refers to the systematic method including the case or problem, writing a hypothesis, gathering and analyzing the facts, and reaching specific inference either in the form of solution or in certain generalization (Kothari 2004).

Research type can be classified as descriptive or analytical, descriptive research includes fact-finding enquiries and surveys. Whereas, analytical research, includes using and analyzing information or facts already exist. On the other hand, research type can be categorized as qualitative or quantitative. Qualitative research is of specific related to the study of social relations, due to the fact of the pluralization of life worlds. It is generally deals in words, images and the subjective (Flick, 2009). In addition, it is exploratory in nature and interested in subjective assessment of behavior, opinions and attitudes (Kothari 2004). Whereas, quantitative research indicates to systematic experiential investigation of phenomenon using computational, mathematical or statistical techniques (Flick, 2009). Also, Saunders et al. (2009) asserted that quantitative analysis techniques helping researchers to explore, describe and test relationships and trends within their data. He also argues that it is used to confirm the hypothesis and to generalize it from the sample of population to the entire population. Last and not the least, the qualitative method is associated with ‘why’ questions. Whereas, the quantitative technique is useful for questions of ‘what’ (Barnham, 2016). Kothari (2004) summarized the basic types of research, as follows:

Type of research	
Descriptive vs. Analytical	**Descriptive research** includes surveys and fact-finding enquiries of different kinds to describe the state of affairs, as it exists at present. **Analytical research:** the researcher has to use facts or information already available, and analyze these to make a critical evaluation of the material.
Applied vs. Fundamental	**Applied research** aims at finding a solution for an immediate problem facing a society or an industrial/business organization. **Fundamental research** is mainly concerned with generalizations and with the formulation of a theory.
Quantitative vs. Qualitative	**Quantitative research** is based on the measurement of quantity or amount. **Qualitative research** is concerned with qualitative phenomenon, it is especially important in the behavioral sciences.
Conceptual vs. Empirical	**Conceptual research** is that related to some abstract idea(s) or theory. **Empirical research** relies on experience or observation alone; it is data-based research.

Table (2): Basic types of research, adopted from Kothari, 2004, p. 15-17.

Bryman (2011) summarized the differences between quantitative and qualitative research, as follows:

	Quantitative	Qualitative
Principal orientation to the role of theory in relation to research	Deductive; testing theory	Inductive; generation of theory
Epistemological orientation	Natural science model, in particular positivism	Interpretivism
0ntological orientation	Objectivism	Constructivism

Table (3): Differences between quantitative and qualitative research, adopted from Bryman and Bell, 2011, p. 27.

4.1 Research strategy

The flow of the research methodology for this study is graphically illustrated in Figure (10) below:

1- Defining aims, objectives, scope, research questions, with main objective related to study the cyber risks and the effects of implementing blockchain on it.

2- Writing literature review: where we have an introduction about the cyber risks and the results of the researches related to it, then identifying the cyber risk factors that related to governance, insider threats, technology and processes, after that discussing the

blockchain as technology, finally discussing the effects of blockchain implementation on cyber risks mitigating strategies.

3- Defining hypothesis and creating the conceptual framework based on the literature review.

4- Creating questionnaire in order to gather the feedback.

5- Analyzing data using SPSS program as statistical technique.

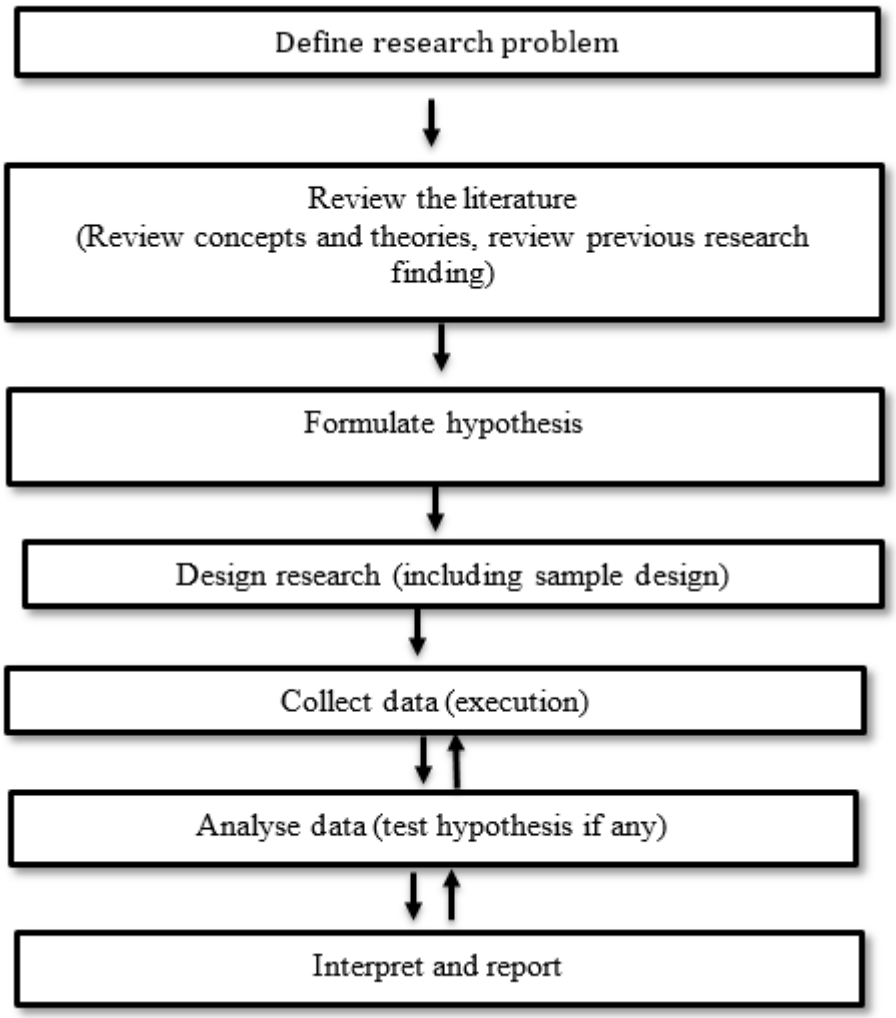

Figure (10): Research strategy, adopted from Kothari, 2004, p. 24.

4.2 Research Approach

In this research, the researcher investigates the relationship between the blockchain implementation and cyber risks mitigating strategies. The quantitative research method is used to analyze the collected data, ensure data validity and allows for popularizing the results. Quantitative method is used because the researcher aims to cover a large number of respondents for this study. Tsang (2014) asserted that the quantitative method reflects large samples and uses statistical procedures to examine relationships among the variables concerned.

The questionnaire is chosen to collect feedback, as it is one of the best methods of quantitative techniques. Besides that, it can be carried out easily by e-mail, web-based-survey, face-to-face and telephone (Park & Park 2016). In addition, it is more practical to collect data with respect to time, distance, and number of approached participants.

The collected data from the questionnaire is treated as representative of a sample population and it is used to test the relationship between the different factors (Malhotra & Grover 1998; Saunders et al, 2009).

The surveyMonkey program is used to create a web-based questionnaire to facilitate the process of gathering the results and analyzing it. Fricker & Schonlau (2002) asserted that web-based surveys are conducted more quickly, easily and effectively than surveys conducted via conventional modes. Moreover, it reduces missing values due to some data entry mistakes; also, it offers higher levels of accuracy (Boyer et al, 2002).

In addition, a hard copy of the questionnaire is created to collect the results from the respondents who prefer not to use web-based one.

4.3 Questionnaire design and structure

The questionnaire is designed to find out the effect of blockchain implementation on cyber risks mitigating strategies, which will provide the required feedback for data analysis. The

questionnaire consist of a cover letter with an introduction including the purpose of it and ethical acknowledgment, and then an introduction to the subjects of the three sections. General ethical issues are taken into consideration while formatting questionnaire such as informed consent, confidentiality of data and anonymity of participants' identities and researchers affecting the responses of participants (Saunders et al, 2012).

The questionnaire is divided into 3 sections with 32 items, first section examines the demographic data like position level, education level, age, organization type, years of experience and the primary role. The second and third sections consist of questions derived from the literature review and conceptual framework.

The demographic questions gave an idea about the type of respondents with reference to their experiences and roles on their organizations, which can help the researcher to compare the responses from each sector and from the different levels on each sector.

The second section study the items of dependent variables which is related to the cyber risks mitigating strategies (16 items), the third section concentrates on the main factors of Blockchain (10 items).

Saunders et al (2009) asserted that the rating method is usually associated if the opinion data is conducted and always reduces the required time to answer each question. Therefore, five point Likert scale is used to scale responses in survey research, (5 choices for each question starting from: 5, strongly agree to: 1, strongly disagree). Five-point Likert-type scale is used to increase response quality and response rate along with reducing respondents' "frustration level" (Babakus et al., 1992). Research confirms that data from Likert items becomes significantly less accurate when the number of scale points drops below five or above seven. Johns (2010).

4.4 Sampling and Population

4.4.1 Pilot Sample

A random sample selection method was adopted. In addition, a pilot sample of 5 respondents were chosen to fill the questionnaire before starting the process of data collection. The pilot sample was chosen to test the validity and reliability of questions, also to know the margin of errors and level of confidence, and to avoid any problem when answering the questionnaire by the respondents (Saunders et al, 2009).

The feedback from the pilot sample improved the overall questionnaire experience.

The link of online survey was sent via email to the respondents from public and private sector.

4.4.2 Research Sampling

It took a round one month to reach to the target of accepted responses. The collected sample amounted to 160 respondents. Part of the collected sample was eliminated because it was not completed. A total of 149 completed and accepted questionnaires have been received, 9 out of 149 were filled manually using hard copy and the other copies were received online. The statistical package for social sciences (SPSS) was used to define variables, add data, test it, and analyze the results, in addition to test the relationship between blockchain and cyber risks mitigating strategies using Cronbach's alpha, correlation test and regression test.

4.5 Analyses

Different analyses are used to describe data and check relationships using statistics. The choice of statistics are affected by the research questions and the objectives of research. The following statistics are used during this study:

4.5.1 Descriptive statistics

The descriptive statistic is used in this study to check the frequency scores of the items of each factor. In addition, the mean and median are calculated to describe the central tendency; also, the value of standard deviation is calculated to describe the dispersion (Saunders et al, 2009).

4.5.2 Reliability Test

Reliability bases on the idea that individual items should produce results consistent with the overall questionnaire (Field, 2012). Cronbach's alpha provides researchers with an overall reliability coefficient for a set of items.

In this study, the reliability test is executed to check the internal consistency for each factor also overall test is done for all factors

4.5.3 Correlation Test

A correlation coefficient enables the researcher to assess the strength of the linear relationship between two variables. This coefficient can take on any value between (+1) and (-1), A value of (+1) represents a perfect positive correlation. This means that the value of one variable will be increased, if the other value is increased. Whereas, a value of (-1) represents a perfect negative correlation. On the other hand, a value of (0) meaning the variables are perfectly independent (Saunders et al, 2009).

A correlation test discusses the relationship between two variable, it says nothing about which variable is the independent and which the dependent one is. It does not study the cause and effect between the variables. It only establishes that there is a connection, with a specified closeness of fit between the variables (Denscombe, 2010).

The regression test is executed in this study to examine the strength of the linear relationship between different factors.

4.5.4 Regression Test

A regression test enables the researcher to assess the strength of relationship between a numerical dependent variable and one or more numerical independent variables; also, to predict the value of a dependent variable from one or more independent variables. Moreover, researchers can use regression analysis to study the connections in terms of cause and effect.

The regression coefficient is represented by (r square) and it can take on any value between (0) and (+1). The value (+1) means that the regression equation is a perfect predictor. On the other hand, F-test is used to discover the overall probability of the relationship between the dependent variable and all the independent variables occurring by chance (Saunders et al, 2009).

In this study, the regression test is conducted to test the relationship between blockchain as independent factor and each dependent factor.

Summary

The quantitative method technique has been employed and found to be suitable and appropriate for this study. In addition, a questionnaire was created to collect data, and a pilot test was executed to check the validity and reliability of the questionnaire.

A random sampling was selected to gather responses by creating an online questionnaire and distribute it by email or as web-based one. Besides that, a hard copy was distributed to get more feedback. The ethical issues were taken into consideration during the research. A total of 149 completed and accepted responses were received.

The statistical package for social sciences (SPSS) was used to analyze the responses by using different analysis techniques like cronbach's alpha, correlation test and regression test.

Chapter Five: Main Findings and Interpretation

Introduction

In this chapter, different test and investigation are executed like demographic and employment data test, descriptive statistics, reliability test and correlation and regression tests. Cronbach's alpha used to describe the internal consistency and measure the reliability of the items. Pearson correlation test used to measure the significance, strength and direction of any relationship between the variables, in order to accept or reject the null hypotheses. Regression test used to predict the value of variable depends on the value of another variable.

5.1 Demographic and employment Data

The total number of responders is 149, and they are divided based on position level as the following: 24 of them from top management, which came as (16.1%), while 53 of them from middle management, which came as (35.6%). 41 with (27.5%) are executive staff, and 31 with (20.8%) are support staff.

Position Level

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Top Management	24	16.1	16.1	16.1
	Middle Management	53	35.6	35.6	51.7
	Executive staff	41	27.5	27.5	79.2
	Support staff	31	20.8	20.8	100.0
	Total	149	100.0	100.0	

Table (4): Position levels frequency distribution table: frequency, percent and valid percent of respondents.

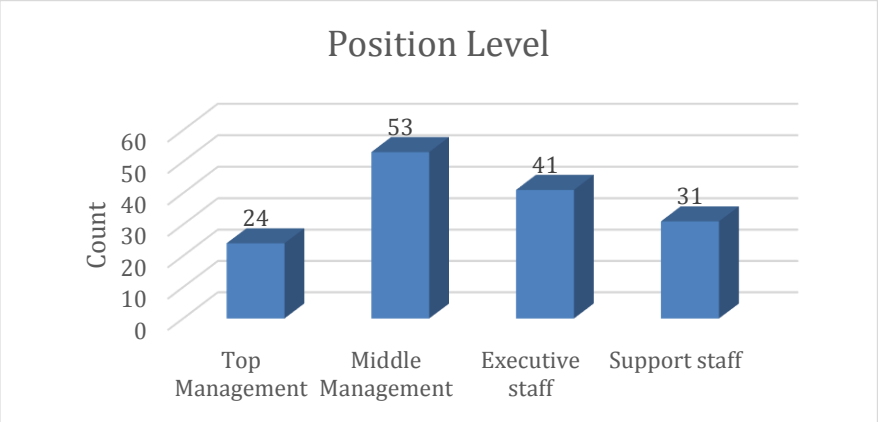

Figure (11): Position levels

Table (5) shows the results for the education level, the holders of master degree or above represent (29.5%) of respondents, while bachelor degree comprise (47%) then (20.1%) for college degree and (3.4%) for high school or less.

Education Level

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	High school or less	5	3.4	3.4	3.4
	College degree	30	20.1	20.1	23.5
	Bachelor degree	70	47.0	47.0	70.5
	Master degree or above	44	29.5	29.5	100.0
	Total	149	100.0	100.0	

Table (5): Education levels frequency distribution table: frequency, percent and valid percent of respondents.

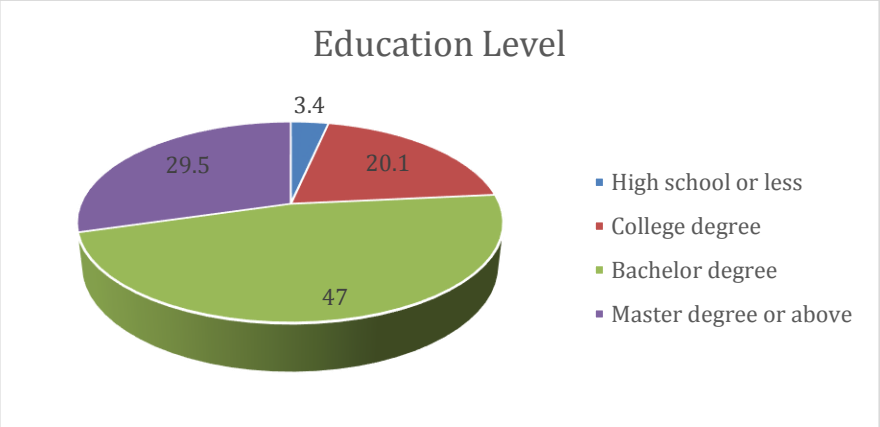

Figure (12): Education levels

For the age categories of respondents, table (6) shows that 7 with (4.7%) of respondents are less than 25 years old, 58 with (38.9%) are between 25 - 34, while 51 with (34.2%) are between 35 - 44 .16 with (10.7%) are greater than 44 and less than 55, and 17 with (11.4%) are 55 or above.

Age category

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 25	7	4.7	4.7	4.7
	25 - 34	58	38.9	38.9	43.6
	35 - 44	51	34.2	34.2	77.9
	45 - 54	16	10.7	10.7	88.6
	55 or Above	17	11.4	11.4	100.0
	Total	149	100.0	100.0	

Table (6): Age categories frequency distribution table: frequency, percent and valid percent of respondents.

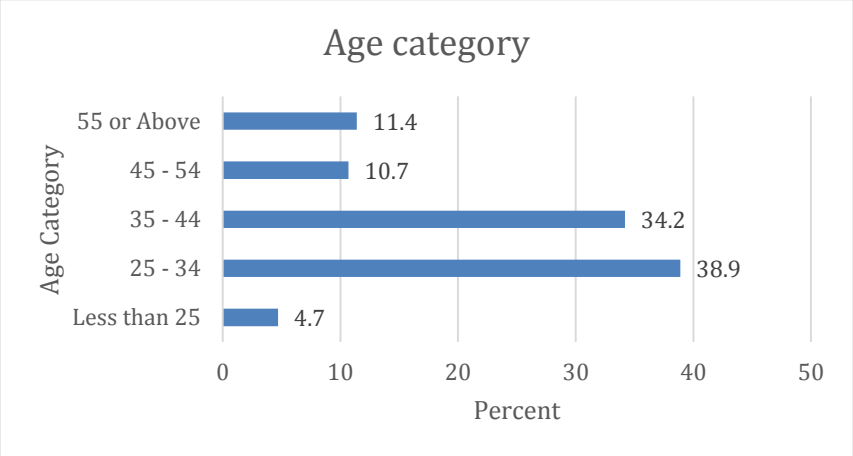

Figure (13): Age categories

The frequencies of organization type in table (7) below shows that the majority of respondents are working in the private sector (a percentage of 51%). The low percentage of government-sector respondents gives indicators that the blockchain-led transformation of business and government, is still many years away (Iansiti, 2017).

Organization Type

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Federal Government	19	12.8	12.8	12.8
	Local Government	35	23.5	23.5	36.2
	Private sector	76	51.0	51.0	87.2
	Other	19	12.8	12.8	100.0
	Total	149	100.0	100.0	

Table (7): Organization types frequency distribution table: frequency, percent and valid percent of respondents.

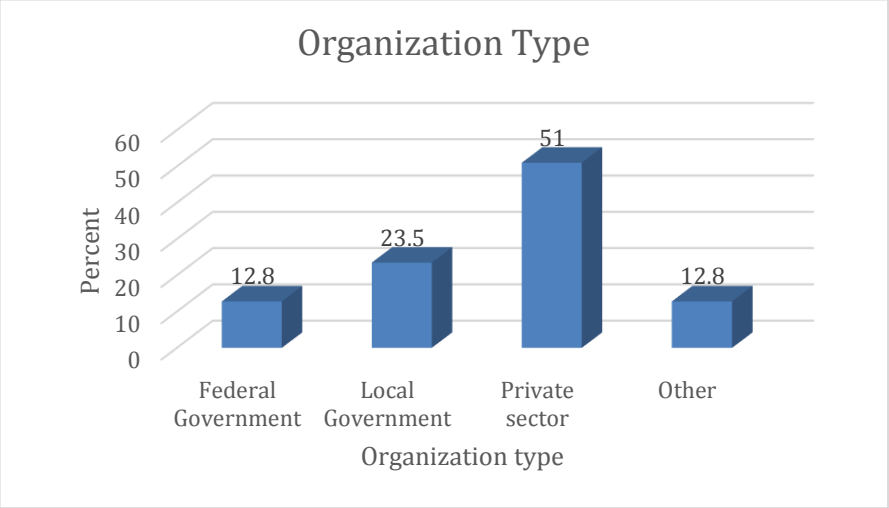

Figure (14): Organization types

The experience of respondents shows 33 with 22.1% have 5 years or below experience, while 44 with 29.5% have experience from 6 to 9 years. On the other hand, 39 with 26.2% have 10 to 13 years of experience. 33 with 22.1% have more than 13 years of experience.

Years of experience

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	One year or less	3	2.0	2.0	2.0
	2 - 5	30	20.1	20.1	22.1
	6 - 9	44	29.5	29.5	51.7
	10 - 13	39	26.2	26.2	77.9
	14 years or above	33	22.1	22.1	100.0
	Total	149	100.0	100.0	

Table (8): Years of experience frequency distribution table: frequency, percent and valid percent of respondents.

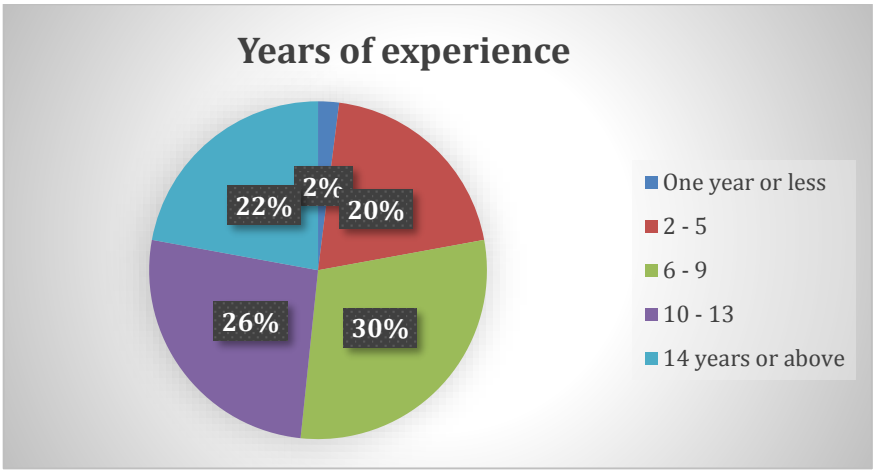

Figure (15): Years of experience

The frequencies of primary role in table (9) below shows that more than half of participants are working in the IT and engineering fields and about a quarter have a management role. On the hand, 10 respondents with (6.7%) are working in the financial sector. The high percentage of technical participants, besides the low percentage of financial respondents gives indication that a huge effort are required to convince top management in the financial institutes to start implementing blockchain technology in their institutes.

Primary role

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Financial	10	6.7	6.7	6.7
	Supply Chain	16	10.7	10.7	17.4
	IT & Engineering	75	50.3	50.3	67.8
	Management	22	14.8	14.8	82.6
	Legal	1	.7	.7	83.2
	Quality & Excellence	5	3.4	3.4	86.6
	Others	20	13.4	13.4	100.0
	Total	149	100.0	100.0	

Table (9): Primary role frequency distribution table: frequency, percent and valid percent of respondents.

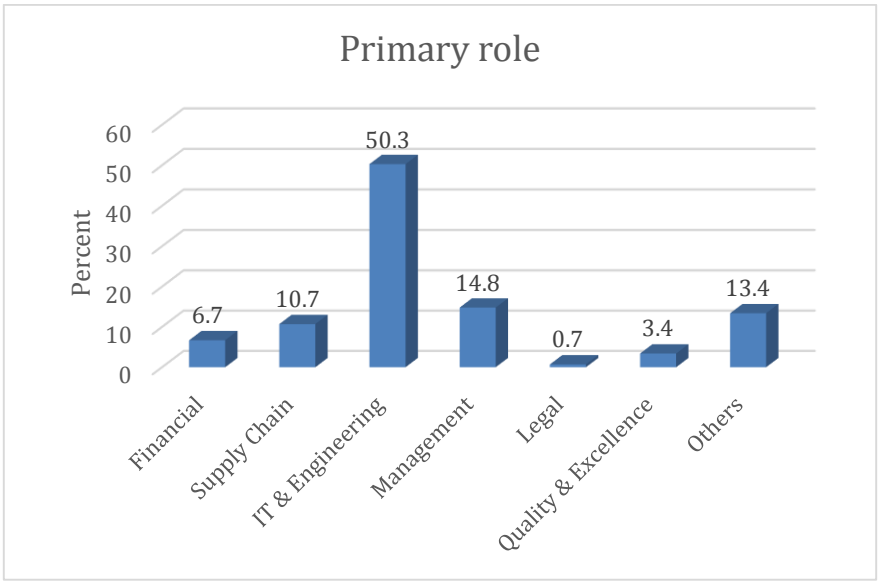

Figure (16): Primary role

5.2 Descriptive statistics

5.2.1 Governance descriptive statistics

The bar chart shown in Figure (17) demonstrates the frequency scores of each item of the governance. It is observed that most of the items have scored either strongly agree or agree. In addition, the results of mean (4, 4.4, 4.3) and median (4, 5, 4) in table (10) below supports our observation. Moreover, the value of standard deviation which is a round (1) provides an indication that all values are a round the mean. Therefore, all of these items are important to mitigate cyber risks related to governance risk category.

	Item1	Item2	Item3
Valid	149	149	149
Missing	0	0	0
Mean	4.00	4.40	4.30
Median	4.00	5.00	4.00
Std. Deviation	1.059	.914	.866
Variance	1.122	.835	.750

Table (10): Governance descriptive statistics

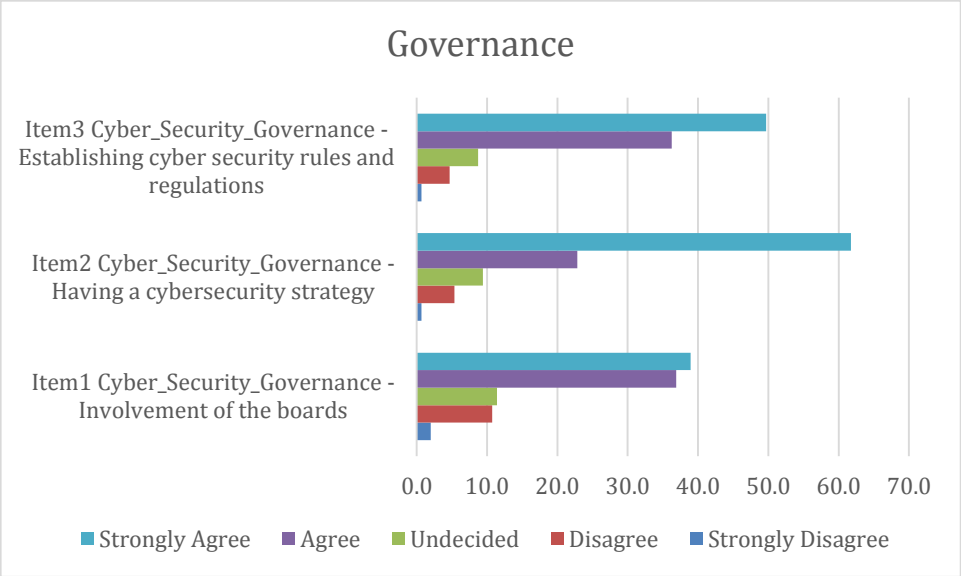

Figure (17): Frequencies for Governance

5.2.2 Insider threats descriptive statistics

The frequency scores of each item of the insider threats in figure (18) below shows that most of the items have scored: either strongly agree or agree. In addition, the results of mean (4.28, 4.38, 4.45, 4.32, 4.36, 4.34) and median (4, 5, 5, 5, 5, 5) in table (11) below supports our observation. Therefore, all of these items are important to mitigate cyber risks related to insider threats risk category.

	Item1	Item2	Item3	Item4	Item5	Item6
Valid	149	149	149	149	149	149
Missing	0	0	0	0	0	0
Mean	4.28	4.38	4.45	4.32	4.36	4.34
Median	4.00	5.00	5.00	5.00	5.00	5.00
Std. Deviation	.869	.926	.896	.856	.814	.914
Variance	.755	.858	.803	.733	.663	.835

Table (11): Insider threats descriptive statistics

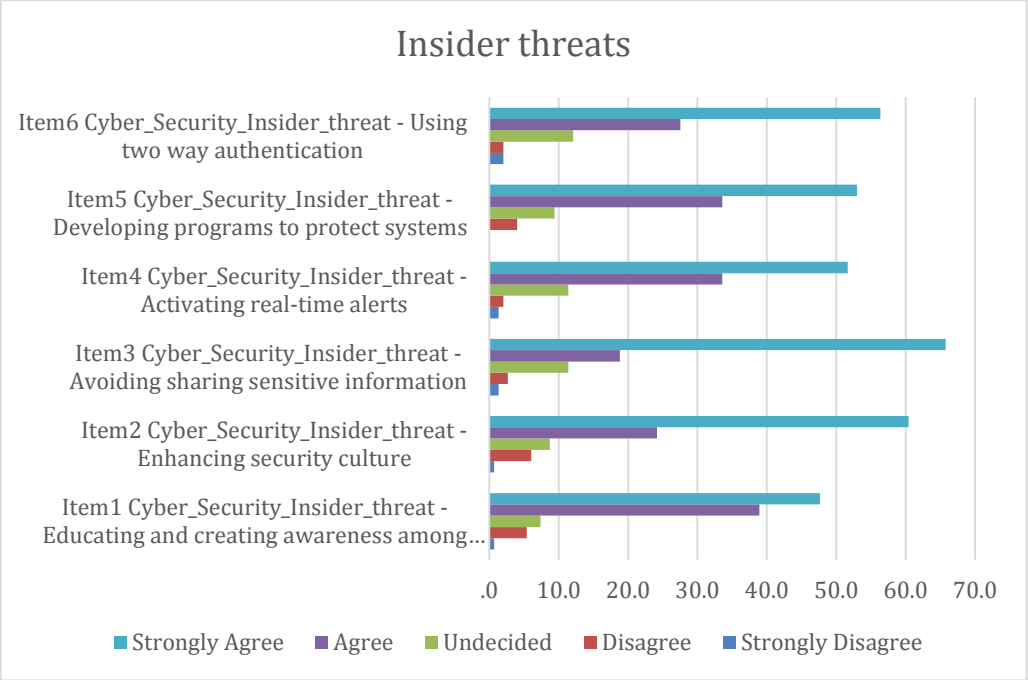

Figure (18): Frequencies for Insider threats

5.2.3 Technology descriptive statistics

The bar chart shown in Figure (19) demonstrates the frequency scores of each item of the technology risk category. It is observed that most of the items have scored either strongly agree or agree. In addition, the results of mean (4.5, 4.3, 4.06, 4.02, 3.58) and median (5, 5, 4, 4, 4) in table (12) below supports our observation. Therefore, all of these items are important to mitigate cyber risks related to technology risk category.

	Item1	Item2	Item3	Item4	Item5
Valid	149	149	149	149	149
Missing	0	0	0	0	0
Mean	4.50	4.30	4.06	4.02	3.58
Median	5.00	5.00	4.00	4.00	4.00
Std. Deviation	.802	.897	1.008	1.010	1.140
Variance	.644	.804	1.017	1.020	1.300

Table (12): Technology descriptive statistics

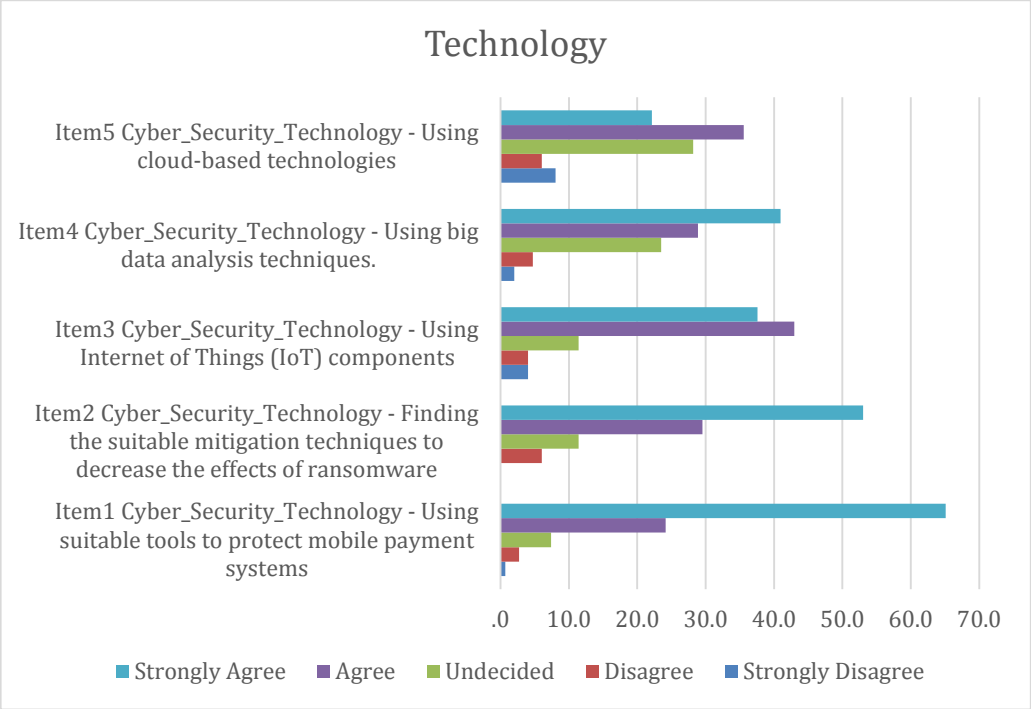

Figure (19): Frequencies for Technology

5.2.4 Processes descriptive statistics

The frequency scores of each item of the process in figure (20) below shows that most of the items have scored: either strongly agree or agree. In addition, the results of mean (4.49, 4.38) and median (5, 5) in table (13) below supports our observation. Therefore, all of these items are important to mitigate cyber risks related to process risk category.

	Item1	Item2
Valid	149	149
Missing	0	0
Mean	4.49	4.38
Median	5.00	5.00
Std. Deviation	.722	.827
Variance	.522	.684

Table (13): Processes descriptive statistics

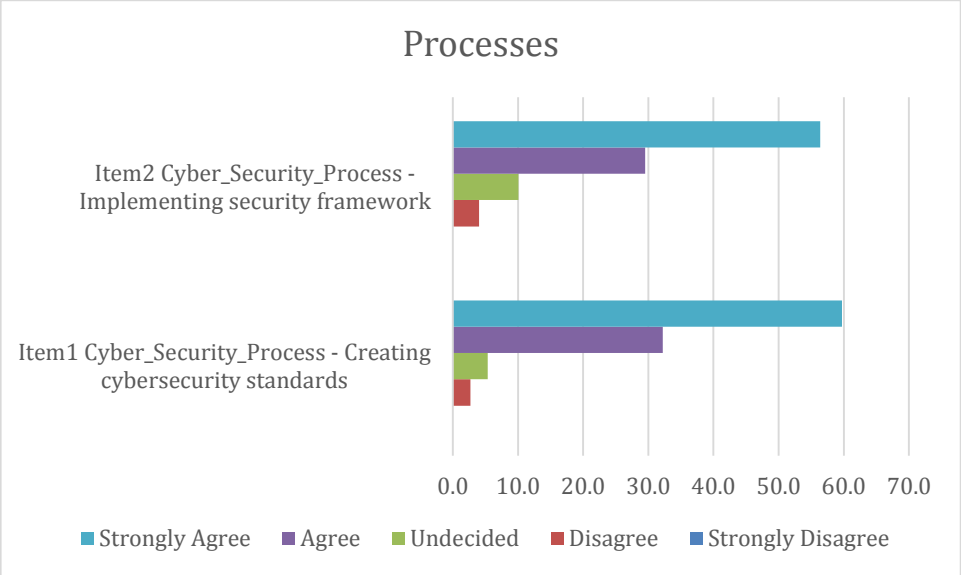

Figure (20): Frequencies for Processes

5.2.5 Blockchain descriptive statistics

The bar chart shown in Figure (21) demonstrates the frequency scores of each item of the blockchain. It is observed that most of the items have scored either strongly agree or agree. In addition, the results of mean and median in table (14) below supports our observation. Moreover, the value of standard deviation which is a round (1) provides an indication that all values are a round the mean. Therefore, all of these items are important.

	Item1	Item2	Item3	Item4	Item5	Item6	Item7	Item8	Item9	Item10
Valid	149	149	149	149	149	149	149	149	149	149
Missing	0	0	0	0	0	0	0	0	0	0
Mean	4.09	4.15	4.38	4.21	3.81	4.21	3.93	4.15	4.50	3.91
Median	4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00	5.00	4.00
Std. Deviation	.735	.644	.730	.882	1.076	.827	.901	.748	.684	.783
Variance	.540	.415	.533	.778	1.158	.683	.812	.559	.468	.613

Table (14): Blockchain descriptive statistics

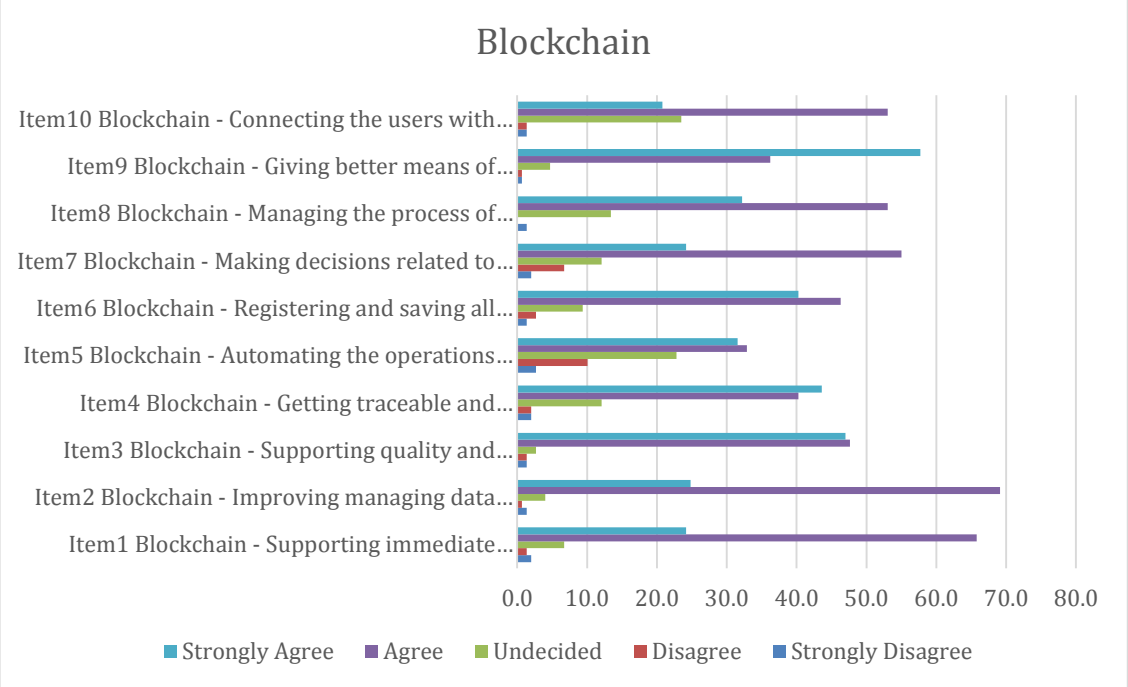

Figure (21): Frequencies for Blockchain

5.3 Reliability Test

Reliability means that a questionnaire should consistently reflect the construct that it is measuring (Field, 2012). Cronbach's alpha measures the interrelatedness of a set of items, it is simply provides researchers with an overall reliability coefficient for a set of items. Value of Cronbach's alpha 0.7 or above is considered as reliable and acceptable in research, noting that the higher the value, the more reliable the generated scale is.

In order to examine the reliability of blockchain implementation and cyber risks mitigating factors, the reliability test is conducted to test the internal consistency for each factor also overall test is done for all factors as displayed in the appendices also the summary results is displayed below.

5.3.1 Governance reliability statistics

As shown in table 15, Cronbach's Alpha is 0.825, which indicates a high level of internal consistency for our scale with this study, and there is no need to delete any item to improve Cronbach's alpha.

Governance Reliability Statistics

Cronbach's Alpha	N of Items
.825	3

Table (15): Governance factor reliability statistics

5.3.2 Insider threat reliability statistics

As shown in table 16, Cronbach's Alpha is 0.886, which indicates a high level of internal consistency for our scale with this study, and there is no need to delete any item to improve Cronbach's alpha.

Cronbach's Alpha	N of Items
.886	6

Table (16): Insider threats factor reliability statistics

5.3.3 Technology reliability statistics

As shown in table 17, Cronbach's Alpha is 0.758, which indicates a high level of internal consistency for our scale with this study, and there is no need to delete any item to improve Cronbach's alpha.

Cronbach's Alpha	N of Items
.758	5

Table (17): Technology factor reliability statistics

5.3.4 Process reliability statistics

As shown in table 18, Cronbach's Alpha is 0.728, which indicates a high level of internal consistency for our scale with this study, and there is no need to delete any item to improve Cronbach's alpha.

Cronbach's Alpha	N of Items
.728	2

Table (18): Process factor reliability statistics

5.3.5 Blockchain reliability statistics

As shown in table 19, Cronbach's Alpha is 0.878, which indicates a good level of internal consistency for our scale with this study, and there is no need to delete any item to improve Cronbach's alpha.

Cronbach's Alpha	N of Items
.878	10

Table (19): Blockchain factors reliability statistics

There was inter-consistency among each scale and its remaining elements. In conclusion, all scales and their remaining values are reliable.

5.4 Correlation and Regression Tests

In this research, both correlation and regression tests have been conducted to test the relationship between dependent and independent factors to take a decision about accepting or rejecting the null hypotheses.

5.3.1 Correlation Tests

Pearson correlation coefficients is a test to measure the strength, direction and the significance of any relationship between the variables, in order to accept or reject the null hypotheses. The determined criteria for the strength of the correlations is as follows: if the correlation results of the test is 0.3, it is considered as being weak, 0.7 considered as strong, and 1 considered as a perfect relation (Saunders et al, 2009).

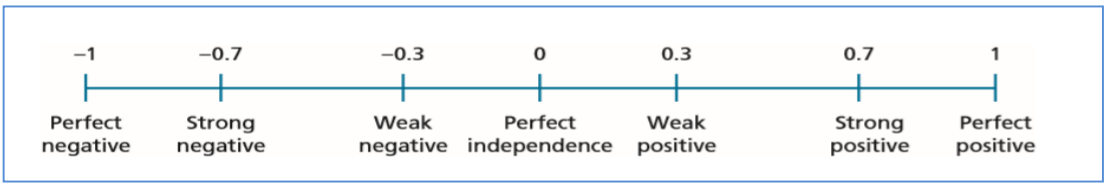

Figure 22: **Values of the correlation coefficient** (adopted from Saunders et al. 2009, p.459).

The first correlation coefficient test is conducted between Cyber risk global variables, and blockchain global variables, the results are shown in table (20) below:

Correlations

		Cyber_risks_Summary	Blockchain_summary
Cyber_risks_Summary	Pearson Correlation	1	.522**
	Sig. (2-tailed)		.000
	N	149	149
Blockchain_summary	Pearson Correlation	.522**	1
	Sig. (2-tailed)	.000	
	N	149	149

**. Correlation is significant at the 0.01 level (2-tailed).

Table (20): Correlation test between Cyber risk global variables, and blockchain global variables

There was a significant positive relationship between implementing blockchain and cyber risks mitigating factors (r = 0.522, p = .001), correlation is significant at the 0.01 level (2-

tailed). Therefore, the null hypothesis H0 1 is rejected as the result shows significant influences of blockchain on cyber risks factors.

The second correlation coefficient test is executed between governance variable, and blockchain global variables, the results are shown in table (21) below:

Correlations

		Governance_Summary	Blockchain_summary
Governance_Summary	Pearson Correlation	1	.429**
	Sig. (2-tailed)		.000
	N	149	149
Blockchain_summary	Pearson Correlation	.429**	1
	Sig. (2-tailed)	.000	
	N	149	149

**. Correlation is significant at the 0.01 level (2-tailed).

Table (21): Correlation test between governance, and blockchain global variables

There was a positive relationship between implementing blockchain and governance factors (r = 0.429, p = .001), correlation is significant at the 0.01 level (2-tailed).), Therefore, the null hypothesis H0 2 is rejected as the result shows significant relationship between blockchain and governance.

The third correlation coefficient test is conducted between insider threats variable, and blockchain global variables, the results are shown in table (22) below:

Correlations

		Insider_Threat_Summary	Blockchain_summary
Insider_Threat_Summary	Pearson Correlation	1	.395**
	Sig. (2-tailed)		.000
	N	149	149
Blockchain_summary	Pearson Correlation	.395**	1
	Sig. (2-tailed)	.000	
	N	149	149

**. Correlation is significant at the 0.01 level (2-tailed).

Table (22): Correlation test between insider threats, and blockchain global variables

There was a positive relationship between implementing blockchain and insider threat mitigating factors (r = 0.395, p = .001), correlation is significant at the 0.01 level (2-tailed). Therefore, the null hypothesis H0 3 is rejected as the result shows influences of blockchain on insider threats.

The fourth correlation coefficient test is executed between technology variable, and blockchain global variables, the results are shown in table (23) below:

Correlations

		Technology_Summary	Blockchain_summary
Technology_Summary	Pearson Correlation	1	.547**
	Sig. (2-tailed)		.000
	N	149	149
Blockchain_summary	Pearson Correlation	.547**	1
	Sig. (2-tailed)	.000	
	N	149	149

**. Correlation is significant at the 0.01 level (2-tailed).

Table (23): Correlation test between technology, and blockchain global variables

There was a significant positive relationship between implementing blockchain and technology factor (r = 0.547, p = .001), correlation is significant at the 0.01 level (2-tailed), Therefore, the null hypothesis H0 2 is rejected as the result shows significant relationship between blockchain and the other technologies.

.

The fifth correlation coefficient test is done between process variable, and blockchain global variables, the results are shown in table (24) below:

Correlations

		Processes_Summary	Blockchain_summary
Processes_Summary	Pearson Correlation	1	.479**
	Sig. (2-tailed)		.000
	N	149	149
Blockchain_summary	Pearson Correlation	.479**	1
	Sig. (2-tailed)	.000	
	N	149	149

**. Correlation is significant at the 0.01 level (2-tailed).

Table (24): Correlation test between process, and blockchain global variables

There was a positive relationship between implementing blockchain and processes factors (r = 0.479, p = .001), correlation is significant at the 0.01 level (2-tailed). Therefore, the null hypothesis H0 2 is rejected as the result shows significant relationship between blockchain and the processes

5.3.2 Regression Test

To find the prediction of using blockchain technology on cyber risks mitigating factors, the regression analysis using enter method then stepwise method has been conducted for each of them.

	R Square	VIF	F	B	Sig.
Insider Threat Summary	.156	1.18	27.194	.298	.000
Governance Summary	.184	1.23	33.108	.188	.000
Technology Summary	.300	1.43	62.895	.341	.000
Processes Summary	.230	1.30	43.847	.118	.000

Table (25): Regression test Summary

As displayed in table (26-a), the values of R^2 and adjusted R^2 for global cyber risks variables are 0.273 and 0.268 respectively using enter method. The values indicate that there is a high degree of goodness of fit of the regression model also indicate that over 27% of variance in cyber risks factors could be explained by implementing blockchain.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.522[a]	.273	.268	8.658

Table (26-a): Regression test - Model summary of cyber risks factors

a. Predictors: (Constant), Blockchain_summary
- Dependent Variable: Cyber_risks_Summary

The F-ratio, which is 55.167 and significant at $p < 0.01$, indicates that using blockchain technology predicts cyber risks factors well.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	4135.217	1	4135.217	55.167	.000[b]
	Residual	11018.823	147	74.958		
	Total	15154.040	148			

Table (26-b): Regression test – ANOVA (F value) of cyber risks factors

a. Dependent Variable: Cyber_risks _Summary
- Predictors: (Constant), Blockchain_summary

The beta value of 0.945 indicates that using blockchain supports the mitigating strategies of cyber risks, which reiterates the results of the correlation test conducted previously.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	29.078	5.307		5.479	.000
	Blockchain_summary	.945	.127	.522	7.427	.000

Table (26-c): Regression test – Coefficients (Beta value) of cyber risks factors

a. Dependent Variable: Cyber_risks _Summary

As displayed in table(27-a),the values of R^2 and adjusted R^2 for Insider threats cyber risks factors are 0.156 and 0.150 respectively using enter method. The values indicate that there is a moderate degree of goodness of fit of the regression model, also indicate that over 15% of variance in insider threats factors could be explained by using blockchain.

The value of variance inflation factor (VIF) is 1.18, which indicates that collinearity does not exist.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.395[a]	.156	.150	3.887

Table (27-a): Regression test - Model summary of Insider threats mitigating factors

a. Predictors: (Constant), Blockchain_summary

- Dependent Variable: Insider_Threat_Summary

The F-ratio, which is 27.194 and significant at $p < 0.01$, indicates that using blockchain technology predicts insider threats well.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	410.868	1	410.868	27.194	.000[b]
	Residual	2220.957	147	15.109		
	Total	2631.826	148			

Table (27-b): Regression test – ANOVA (F value) of Insider threats mitigating factors

a. Dependent Variable: Insider_Threat_Summary

- b. Predictors: (Constant), Blockchain_summary

The beta value of 0.298 indicates that using blockchain supports the success factors of insider threats, which reiterates the results of the correlation test implemented previously.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	13.808	2.383		5.795	.000
	Blockchain_summary	.298	.057	.395	5.215	.000

Table (27-c): Regression test – Coefficients (Beta value) of Insider threats mitigating factors

a. Dependent Variable: Insider_Threat_Summary

As displayed in table (28-a), the values of R^2 and adjusted R^2 for governance cyber risks factors are 0.184 and 0.178 respectively using enter method. The values indicate that there is a high degree of goodness of fit of the regression model, also indicate that over 18% of variance in governance factors could be explained by using blockchain.

The value of variance inflation factor (VIF) is 1.23, which indicates that collinearity does not exist.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.429[a]	.184	.178	2.223

Table (28-a): Regression test - Model summary of governance factors

a. Predictors: (Constant), Blockchain_summary

Dependent Variable: Governance Summary

The F-ratio, which is 33.108 and significant at $p < 0.01$, indicates that using blockchain technology can predicts the governance.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	163.565	1	163.565	33.108	.000[b]
	Residual	726.234	147	4.940		
	Total	889.799	148			

Table (28-b): Regression test – ANOVA (F value) of governance factors

a. Dependent Variable: Governance Summary

b. Predictors: (Constant), Blockchain_summary

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	4.922	1.362		3.613	.000
	Blockchain_summary	.188	.033	.429	5.754	.000

Table (28-c): Regression test – Coefficients (Beta value) of governance factors

a. Dependent Variable: Governance Summary

The beta value of 0.188 indicates that using blockchain supports the success factors of governance, which reiterates the results of the correlation test executed previously.

As shown in table(29-a),the values of R^2 and adjusted R^2 for technologies cyber risks factors are 0.3 and 0.295 respectively using enter method , the values indicate that there is a high

degree of goodness of fit of the regression model, also indicate that 30% of variance in technologies factors could be explained by using blockchain.

The value of variance inflation factor (VIF) is 1.43, which indicates that collinearity does not exist.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.547[a]	.300	.295	2.928

Table (29-a): Regression test - Model summary of technologies factors

a. Predictors: (Constant), Blockchain_summary

- Dependent Variable: Technology_Summary

The F-ratio, which is 62.895 and significant at $p < 0.01$, indicates that using blockchain technology predicts the technology variables well.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	539.062	1	539.062	62.895	.000[b]
	Residual	1259.905	147	8.571		
	Total	1798.966	148			

Table (29-b): Regression test – ANOVA (F value) of technologies factors

a. Dependent Variable: Technology_Summary

- Predictors: (Constant), Blockchain_summary

The beta value of 0.341 indicates that using blockchain supports the success factors of technologies, which reiterates the results of the correlation test executed previously.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	6.353	1.794		3.540	.001
	Blockchain_summary	.341	.043	.547	7.931	.000

Table (29-c): Regression test – Coefficients (Beta value) of technologies factors

a. Dependent Variable: Technology_Summary

As displayed in table (30-a), the values of R^2 and adjusted R^2 for processes cyber risks factors are 0.230 and 0.225 respectively using enter method. The values indicate that there is a degree of goodness of fit of the regression model, also indicate that over 23% of variance in insider threats factors could be explained by using blockchain.

The value of variance inflation factor (VIF) is 1.30, which indicates that collinearity does not exist.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.479[a]	.230	.225	1.213

Table (30-a): Regression test - Model summary of processes factors

a. Predictors: (Constant), Blockchain_summary

Dependent Variable: Processes Summary

The F-ratio, which is 43.847 and significant at $p < 0.01$, indicates that using blockchain technology can predicts the process variables.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	64.462	1	64.462	43.847	.000[b]
	Residual	216.115	147	1.470		
	Total	280.577	148			

Table (30-b): Regression test – ANOVA (F value) of processes factors

a. Dependent Variable: Processes Summary

b. Predictors: (Constant), Blockchain_summary

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.995	.743		5.376	.000
	Blockchain_summary	.118	.018	.479	6.622	.000

Table (30-c): Regression test – Coefficients (Beta value) of processes factors

a. Dependent Variable: Processes Summary

The beta value of 0.118 indicates that using blockchain supports the success factors of processes, which reiterates the results of the correlation test executed previously.

The value of variance inflation factor (VIF) is below 10, which indicates that collinearity does not exist.

Summary

As shown in the analysis, cronbach's alpha analysis is used to test the reliability, most of the results indicate a high level of internal consistency, and there is no need to delete any item to improve Cronbach's alpha.

The results of correlation tests show that there was a significant positive relationship between implementing blockchain and cyber risks mitigating factors, therefore, the null hypotheses are rejected as the result shows significant influences of blockchain on cyber risks factors.

The results of regression test indicate that there is a high degree of goodness of fit of the regression model also show that the variance in cyber risks factors could be explained by implementing blockchain.

In next chapter, the hypotheses presented in this study will be discussed.

Chapter Six: Discussion

Introduction

This chapter will discuss all of the hypotheses presented in this study, based on literature review and data analysis, and in general, the relationship between blockchain implementation and cyber risks mitigating strategies. The results are in line with previous studies published. Also, it supports the literature review and conceptual framework and show that there is relationship between the implement of blockchain and cyber risks mitigating methods.

6.1 Relationship between blockchain implementation and Technology

The results from both the Pearson correlation coefficients test and the regression test of this study revealed that there is a significant positive relationship between blockchain implementation and cyber risks factors related to technology, the strong positive relationship indicates that using blockchain supports the efforts to mitigate cyber-attacks, as the following:

6.1.1 Blockchain and ransomware: blockchain supports the efforts to protect databases and machines from the effects of DDoS and other ransomware, by utilizing the consensus mechanism to confirm transactions before it can be added to the database. Also, blockchain supports the business continuity, so if any node go offline; the other nodes continue working and the services will continue available. In addition, blockchain has at its core a traceable lineage. This results are in line with previous study done by Holmes (2017) who found that the techniques uses by blockchain to protect the integrity of database, and the fully traceable feature of it, effects positively on cyber risks factors by supporting the efforts to prevent the loss of sensitive information.

6.1.2 Blockchain and IoT: the positive relationship between blockchain and IoT supports the previous research of IBM (2017), who found that blockchain helps on building trust between parties and reducing the risks of collusion and rigging by using it for IoT. Also,

Crosby et al. (2015) who discussed the roles of blockchain on built autonomous decentralized peer to peer telemetry.

The blockchain technology could provide the basis for IoT security; in addition, Blockchain ledger can be used to store information that generated from IoT devices, so the data flow will be more organized, and the management of devices that connected to each other will be easier. In addition, the blockchain technology simplifies the executing of decentralized IoT network such as trusted and secured data exchange as well as record keeping.

6.1.3 Blockchain and Big data: the positive relationship between blockchain and big data technique supports the previous research of Harper (2017), who found that blockchain technologies can accelerate the speed at which transactional data is implemented. In addition, blockchain can empower the security of big data. On the other hand, Zheng (2016) found that big data can be combined with blockchain on the level of data management and data analytics, so the distributed and security features of blockchain can be exploited to save an important and critical data. Besides that, the transactions on blockchain can be used for big data analytics, which supports the efforts to generate KPI's and to take correct decisions.

6.1.4 Blockchain and Cloud solutions: blockchain based distributed cloud file storage applications can be used to decrease data failures, beside that it increases security, privacy and data control. Using peer-to-peer relationships gives the users the advantages to control the process of transferring and sharing data and sharing the storage and bandwidth of internet without depending on intermediators to perform mentioned processes. These results are congruent with previous studies done by Crosby et al. (2015) who found that absence of a third party role in the blockchain network decreases data failures, as well as significantly

increasing security, privacy and data control, Also, Harper (2017) who discussed the benefits of blockchain security-based on securing the cloud platform and building the trust.

6.2 Relationship between blockchain implementation and Insider threats

The results disclosed that there is a positive relationship between blockchain implementation and cyber risks mitigating factors related to insider threats, like decreasing sensitive information sharing (Siddiqui & Muntjir, 2013) Activating real time alerts and using authetication to protect data (MeriTalk, 2015). Therefore, a lot of organizations start using private blockchain to automate back office activities. This processes help them to increase the efficiencies and decrease the cyber threats by minimizing the opportunities to exploit the vulnerabilities. In addition, the transactions which created and saved in the blocks are secured by hash algorithm, therefor it cannot be moved or deleted. Moreover, cyber-attacks probability to the insider environment can be reduced by the cryptographic methods used by blockchain. This results are congruent with previous studies done by Zuberi (2017) who found that using blockchain to automate back office activities in the financial institutes will increase the efficiencies and decrease the cyber threats, and Williams-Grut (2017) who found that blockchain-based applications could save banks 12 billion dollars yearly in back office cost. and Batlin et al. (2016) who found that blockchain enables direct transactions between different parties in the network, which leads to little or no waiting, immediate transfer of funds and near real-time settlement.

6.3 Relationship between blockchain implementation and governance

The results from both the Pearson correlation coefficients test and the regression test of this study revealed that, there is a positive relationship between blockchain implementation and

cyber risks mitigating factors related to governance, like involvement of the board (PwC, 2016), cybersecurity strategy (IBM, 2016) and rules and regulations (ITU, 2017).

Piazza (2017) found that blockchain technology can be used as corporate governance tool to improve corporate information accessibility, therefore any changes done in the database can be tracked as it happens, which helps chief security officer and security team in any organization to explore the vulnerabilities and avoid any cyber threats.

Blockchain also can be exploited to support cyber security strategy for any organization, as example, blockchain can support Dubai governemt to execute their cyber security strategy, as the main domain of Dubai cyber security strategy concentrates on protecting confidentiality, integrity, availability and avoiding any discontinuity of information technology systems, besides that ensuring their availability. On the other hand, one of the challenges of the blockchain approach is that it reduces monitoring and controling by avoiding regulation to avoid inefficiencies in traditional payment networks.Therefore, distributed networks can be much less resilient to shocks than centralized systems, this challenge studied in details by Deloitte (2016).

6.4 Relationship between blockchain implementation and processes

The results disclosed that there is a positive relationship between blockchain implementation and cyber risks mitigating factors related to processes, like cybersecurity standards (ITU, 2017) and implementing security framework (GSISS, 2016 ; Mont, 2015).

The standards related blockchain should be established to create trust between the end users and technology, Standards could help control risks associated with identity. Especially, authentication of digital identities for financial transactions. In addition, standards could execute an important role in ensuring integrity between multiple blockchain

implementations, which could help ensure the integrity of data exchanged and to reduce the risk of a fragmentation. This results are congruent with previous studies done by Deshpande (2017) who study the importance of creating standards to get the benefits of blockchain features in reducing the cyber risks.

Summary

This chapter discussed the findings and related discussions for the dissertation's hypotheses. In addition the acceptance of relative importance of blockchain implementation on cyber risks mitigating factors. From this discussion, it can be concluded that the blockchain implementation effects positively on cyber risks factors, and supports this factors to mitigate the cyber threats and executing proactive steps to reduce any future threats. A summary of the main findings and recommendations, which have been discussed in this chapter, will be described in the next chapter.

Chapter Seven: Conclusions and recommendations

Introduction

The main objective to this research is to study the impacts of cyber risks on the business and the role of cyber risks mitigating factors to reduce the effects of cyber-attacks. In addition, the study concentrates on the effects of blockchain implementation on cyber risks mitigating factors, mainly in the financial sector in the UAE. The research questions have been studied and discussed in details during literature review.

In order to achieve the objectives of this research and to answer the research questions, the relevant literature was reviewed and the conceptual framework was developed. In addition, a quantitative research methodology was used to collect and analyze data using relevant tools and techniques, by using the surveyMonkey software to create web-based questionnaire and SPSS program to analyze data. The result is based on data collected from a web based questionnaire from a random sample.

7.1 Conclusions

The findings show that blockchain implementation factors have a strong positive relationship on cyber risks mitigating factors.

The study discuss the factors related to the following areas: governance, insider threats, technology and processes. Therefore, it came to cover and answer the research questions related to the effects of blockchain implementation on cyber risks mitigating factors, and this all came as null hypotheses. The first null hypothesis: “There is no significant influences of blockchain on cyber risks mitigating factors”. The null hypothesis was rejected, as data analysis shows a strong positive relationship between blockchain implementation and cyber risks factors, and this is also supported by the literature review and discussions.

The study shows that the uses of blockchain features plays an important role in different areas like supporting immediate transfer of data and near real-time settlement, also

improving managing data through immutable capabilities. In addition, supporting quality and accuracy of data. Moreover, getting traceable and auditable transactions. Furthermore, connecting the users with financial system directly by using Smart wallet tool. Besides that, managing the process of issuing and servicing securities by using smart securities tools. Also, giving better means of identity through improving identity management processes. Last and not the least using the smart contract to make decisions and to execute transactions related to different operations.

The second null hypothesis: "There is no significant relationship between blockchain and the governance". This null hypothesis was rejected by both the literature review and statistical analysis. The result shows that there is a positive relationship between blockchain implementation and cyber risks mitigating factors related to the governance.

Blockchain can be used as a corporate governance tool to improve corporate information accessibility; also, blockchain technology can be exploited to support cyber security strategy for any organization.

The third null hypothesis: "There is no significant influences of blockchain on insider threats". This null hypothesis was rejected as the result shows that there is a moderate positive relationship between blockchain implementation and cyber risks mitigating factors related to the insider threats, the study concentrates on the effects of automating back office activities by using blockchain on increasing the efficiencies of employees and processing. In addition, the effects of blockchain on securing the transactions by saving it into blocks protected by hash algorithms and different cryptographic techniques.

The fourth null hypothesis: "There is no significant relationship between blockchain and the other technologies". This null hypothesis was rejected by both the literature review and statistical analysis. The result shows that there is a strong and positive relationship between blockchain implementation and cyber risks mitigating factors related to the technologies

like IoT, big data techniques and cloud solutions, illustrated by utilizing and integrating the benefits of blockchain and other technologies to mitigate the cyber threats and to execute more proactive and innovative cyber security strategies.

The fifth null hypothesis: "There is no significant relationship between blockchain and the processes". This null hypothesis was rejected by both the literature review and statistical analysis. The result shows that there is a moderate positive relationship between blockchain implementation and cyber risks mitigating factors related to the processes. The standards related blockchain can create a trust between the end users and technology, and help control risks associated with identity. On the other hand, this relationship is still not clear, because it is not discussed in details in the previous studies.

The policies to mitigate cyber risks were implemented in the UAE by issuing the UAE cybercrime law in 2012, and the cyber security strategy in 2016. In addition, Dubai announced its blockchain strategy in 2016 to be the first city on the blockchain by 2020. Also, the UAE government launch the UAE blockchain strategy 2021.

Many Federal departments in the UAE and local departments in Dubai start exploring the opportunities to implement blockchain in their organizations, but still the actual implementation is limited. Besides that, most of the implementations are related to benefit from the features related to smart contracts and identity management by using permissioned blockchain. On the other hand, none of the financial organizations in the UAE, actually start implementing blockchain in their institutes, except for some attempts.

Such as, The National Bank of Dubai, has reportedly become the first bank in the region to successfully implement blockchain technology in a check-issuance system. In addition, In November 2017, RAK Bank launched remittance services using blockchain start-up Ripple. Also, Abu Dhabi Global Markets recently announced key initiatives using blockchain to facilitate the regulatory requirements of know your-customer (KYC) processes. More

recently, the Central Bank of the UAE announced a joint project with the Saudi Arabian Monetary Authority to use blockchain to issue a digital currency for cross-border transactions between the two countries (Syed, 2018).

Iansiti et al. (2017) asserted that blockchain-led transformation of business and government is still many years away, he also added that blockchain is a foundational technology, therefore the process of adoption will be gradual and steady, not sudden.

Even data analysis shows a strong positive relationship between blockchain implementation and cyber risks mitigating factors, but the effects of blockchain on mitigating cyber risks still needs more study and analysis. The researchers publish a lot of studies related to blockchain as technology, and the positive effect of it on business. On the other hand, the relation between blockchain and cyber risks is still needs a lot of efforts to be discovered. We attempt on our study to concentrate on this side, based on the available studies in this field and the results of data analysis.

7.2 Implications:

7.2.1 Implications to research

The aim of this study is to establish the effects of blockchain implementation on cyber risks mitigating factors. In addition, the results of this study have implications for positive relationship between the effects of blockchain implementation and cyber risks mitigating methods.

The positive effects can be exploited by the researchers to explore the effects of blockchain on the other cyber risks factors or categories, which is not discussed in our study. Moreover, to study the different opportunities to implement blockchain in the financial field.

7.2.2 Implications to practice

Based on the literature review and data analysis, we found that blockchain supports the efforts to protect databases and machines from the effects of DDoS and other ransomware; also, it supports the business continuity. In addition, blockchain helps on building trust between parties and reducing the risks of collusion and rigging by using it for IoT. Moreover, blockchain can empower the security of big data and cloud solutions. Furthermore, blockchain can be used to automate back office activities. Blockchain also can be exploited to support cyber security strategy for any organization. Last but not least, blockchain technology can be used as a corporate governance tool to improve corporate information accessibility.

All of mentioned features needs to be examined practically in order to analyze the applicability, effectiveness, and empirical results of this study.

7.3 Research Limitations

This study has the following limitations:

1- The scope of the study is limited to examining the effects of blockchain implementation on cyber risks mitigating factors related to governance, insider threats, technology and processes.

2- The null hypothesis discussed the relation between blockchain and governance, insider threats, technologies and processes factors.

3- More than half of respondents to the questionnaire are from the IT and engineering fields, which gives an indicator that blockchain concept is still not clear for many organizations.

7.4 Recommendations for Further Research

This study focuses on the effect of blockchain implementation on cyber risks mitigating factors that related to governance, insider threats, technologies and processes.

From our study, we notice that there is positive relation between blockchain and these factors. On the other hand, we notice that further studies are required to overcome the above-mentioned limitations. Also, further studies are required for better and deeper understanding of the effects of blockchain on insider threats, governance and processes. In addition, to extend the study towards the effects of blockchain on other factors of cyber risks. Furthermore, to analyze practically the impact of blockchain on mitigating cyber risks for real case studies. Last and not least, further studies are required to explore the blockchain implementation in the financial sector, and the effects of this implementation on mitigating cyber risks.

Summary

The results and findings of this study show that there is a positive relationship between blockchain implementation and cyber risk mitigating factors, and this is supported by the literature review and discussions. On the other hand, further studies are required to overcome the limitations and to explore the opportunities to expand implementing blockchain in different sectors to enhance the performance and reduce the cyber risk.

References

Alkaabi, A. (2014). Strategic framework to minimize information security risks in the UAE. *Doctoral dissertation, University of Bedfordshire*.

Aloul, F. (2012). The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology*, vol. 3(3), p.176-183.

Babakus, E. & Mangold, G. (1992). Adapting the SERVQUAL scale to hospital services: an empirical investigation. *Health Service Research, vol. 26, p.767-780.*

Barnham, C. (2016). Quantitative and qualitative research: perceptual foundations. *International Journal of Market Research*, vol. 57(6), p. 837.

Batlin, A., Jaffrey, H., Murphy, C., Przewloka, A., Williams, S. (2016). *Building the trust engine - how the blockchain could transform finance (and the world) - A UBS group technology white paper* [online]. [Accessed 19 January 2018]. Available at: https://www.blockchaindailynews.com/attachment/728741/

Beyman, A. & Bell, E. (2011) *Business Research Methods*. 3rd ed. Oxford et al.: Oxford University Press.

Birch, D. (2014). *Identity is the New Money:* London Publishing Partnership.

Boyer, K.K., Olson, J.R., Calantone, R.J. & Jackson, E.C. (2002). Print versus electronic surveys: a comparison of two data collection methodologies. *Journal of Operations Management*, Vol. 20(4), pp. 357-373.

Collomp, A. & Sok, K. (2016). Blockchain / Distributed Ledger Technology (DLT): What Impact on the Financial Sector? *Digiworld Economic Journal Vol. 103(3), pp. 93-103.*

Crosby, M., Nachiappan., Pattanayak, P., Verma, S. & Kalyanaraman, V. (2015). Blockchain technology beyond bitcoin. *Sutardja Center for Entrepreneurship & Technology Technical Report – The University of California Berkeley.*

Crossler, R., Johnston, A., Lowry, P., Hu, Q., Warkentin, M. & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers* & security, Vol.32, p90-101.

Deshpande, A., Stewart, K., Lepitit, L., Gunashekar, L. (2017). *Understanding the landscape of distributed ledger technologies /blockchain challenges, opportunities, and the prospects for standards.* RAND Corporation, UK [online]. [Accessed 15 April 2018]. Available at: https://www.rand.org/content/dam/rand/pubs/research_ reports/RR2200/RR2223/ RAND_ RR2223.pdf

Deloitte (2016). *Blockchain: enigma, paradox, opportunity.* London: Deloitte [online]. [Accessed 15 April 2018]. Available at: https://www2.deloitte.com/content/ dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf

Denscombe, M. (2010). *Research guide for small-scale social research projects, Fourth Edition* McGraw-Hill Education, Englangd.

DESC (2017). *Dubai cyber security strategy – Government of Dubai* [online]. [Accessed 23 February 2018]. Available at: http://csc.dubai.ae/res/wp-content/uploads/DCSS-EN.pdf

Dougherty, S. (2015). Front Lines of Cyber Risk: What's a company's best defense? *Claims Magazine* p.21-23 [online]. [Accessed 23 December 2017]. Available at: PropertyCasualty360.com,

E&Y (2011). *The digitization of everything. How organizations must adapt to changing consumer behavior.* Ernst & Young LLP [online]. [Accessed 15 Dec 2017]. Available at: www.ey.com/Publication/vwLUAssets

Field, A. (2009). *Discovering statistics using SPSS*: London, SAGE.

Flick, U. (2009). *An Introduction to Qualitative Research*. 4th ed. London: Sage Publications.

Fricker, R. and Schonlau, M. (2002). Advantages and Disadvantages of Internet Research Surveys: Evidence from the Literature. *Field Methods*, 14(4), pp.347-367.

Friedman, S. (2016). Taking cyber risk management to the next level: Lessons learned from the front lines at financial institutions. *Deloitte university press, Deloitte Center for Financial Services* [online]. [Accessed 15 December 2017]. Available at: *http://dupress.com/articles/cyber-risk-management-financial-services-industry/*

Gilderdale, S. (2017). SWIFT's customer security programme: preventing, detecting and responding to the growing cyber threat. *Journal of Securities Operations & Custody Vol. 9(3), pp. 198.*

Harper, J. (2017). The new face of big data: AI, IoT and blockchain. KM world, Vol.26, p16-18. Retrieved from https://search-proquest-com.ezproxy.buid.ac.ae/ docview/ 1861823245? accountid=178112

Holmes, S. (2017). *The future of DDoS attacks looks scary. Blockchain will protect us* [online]. [Accessed 6 March 2018]. Available at: https://www.americanbanker.com/opinion/the-future-of-ddos-attacks-looks-scary-blockchain-will-protect-us

Iansiti, M. & Stewart, Lakhani, L. (2017). *The truth about blockchain.* Harvard Business Review, UK [online]. [Accessed 15 May 2018]. Available at: https://enterprisersproject.com/sites/default/files/the_truth_about_blockchain.pdf

IBM (2016). *Reviewing a year of serious data breaches, major attacks and new vulnerabilities - IBM x-force research* [online]. [Accessed 06 January 2018]. Available at: https://www.autoindustrylawblog.com/wp-content/uploads/sites/8/2016/05/IBM_2016-cyber-security-intelligence-index.pdf

IBM (2017). *Watson IoT and blockchain - disruptor and game changer* [online]. [Accessed 09 March 2018]. Available at: https://public.dhe.ibm.com/common/ssi/ecm/ww/en/ ww912350usen/watson-iot-cognitive-solutions-ww-infographic-general-ww912350usen-20180306.pdf

ITU (2017). *Global cybersecurity index 2017* [online]. [Accessed 06 January 2018]. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Johns, R. (2010). Likert items and scales. Survey question bank: methods fact sheet1 [online]. [Accessed 06 June 2018]. Available at: https://www.ukdataservice.ac.uk/media/262829/discover_likertfactsheet.pdf

Kothari, C. (2004). *Research methodology: methods and techniques*: New Age International.

KPMG (2018). *The KPMG UAE banking perspectives 2018 report* [online]. [Accessed 03 June 2018]. Available at:http://www.intelligenttechchannels.com/uae-banking-to-consider-artificial-intelligence-blockchain-fintech-in-2018/

Makridakis, S., Polemitis1, A., Giaglis, G. & Louca, S. (2016) Blockchain: current achievements, future prospects/Challenges and its combination with AI. *10.13140/RG.2.2.16255.92321.*

Malhotra, M.K. & Grover, V. (1998). An assessment of survey research in POM: from constructs to theory. *Journal of operations management*, Vol. 16(4), pp. 407-425.

MeriTalk (2015). *Inside Job: The Federal Insider Threat Report* [online]. [Accessed 25 December 2017]. Available at: https://www.meritalk.com/study/inside-job/

Miles, M. B., & Huberman, M. A. (1994): Qualitative Data Analysis: An Expanded Sourcebook (2nd edition). Beverley Hills, Sage.

Munshi, A., Dell, P., and Armstrong, H. (2012). Insider threat behavior factors: A comparison of theory with reported incidents. *In System Science (HICSS), 2012 45th Hawaii International Conference*, p. 2402-2411.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System* [online]. [Accessed 12 February 2018]. Available at: https://bitcoin.org/bitcoin.pdf

NetDiligence (2015). *2015 Cyber claims study* [online]. [Accessed 28 December 2017]. Available at: https://netdiligence.com/wp-content/uploads/2016/05/NetDiligence_2015_Cyber_Claims_Study_093015.pdf

Park, J, & Park, M (2016). Qualitative versus Quantitative Research Methods: Discovery or Justification? *Journal Of Marketing Thought*, Vol3(1), pp. 1-7.

Pfleeger, S., Stolfo, S. (2009). Addressing the insider threat. *Security & Privacy, IEEE*, Vol. 7(6), p.10-13.

Piazza, F (2017). Bitcoin and the blockchain as possible corporate governance tools: strengths and weaknesses. *Penn State Journal of Law & International Affairs Vol. 5(2), pp. 264-298.*

Piscini, E., Dalton, D. & Kehoe, L. (2017). *Blockchain and cyber security - Deloitte* [online]. [Accessed 27 February 2018]. Available at: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf

Porter M.E. & Heppelmann J.E. (2014).How smart, connected products are transforming competition. *Harvard Business Review, Vol.*92 (11), pp. 64-88.

Putty, D. & Verheist M. (2013). Cyber crime: Can a standard risk analysis help in the challenges facing business continuity managers. *Journal of business continuity and emergency planning Vol. 7(2), pp. 126-137.*

PwC-1 (2016). *Financial crime in funds transfer systems - actions to counter an emerging international threat* [online]. [Accessed 02 December 2017]. Available at: https://www.pwc.com/financialcrime

PwC-2 (2016). *Turnaround and transformation in cybersecurity - Key findings from the global state of information security® survey 2016* [online]. [Accessed 22 December 2017]. Available at: https://www.pwc.com/gsiss

PwC-3 (2016). *A false sense of security? Cyber security in the Middle East. The Global State of Information Security Survey 2016* [online]. [Accessed 01 December 2017]. Available at: www.pwc.com/cybersecurity

PwC (2017). *Risk in review study - managing risk from the front line* [online]. [Accessed 02 December 2017]. Available at: https://www.pwc.com/riskinreview

PwC (2018). *Strengthening digital society against cyber shocks - Key findings from the global state of information security® survey 2018* [online]. [Accessed 05 January 2018]. Available at: https://www.pwc.com/gsiss

Ryan, O. (2016). Assessing cyber risk critical questions for the board and the C-suite, *Deloitte Touche Tohmatsu Limited*. Available at: http://www2.deloitte.com/global/en/pages/risk/articles/assessing-cyber-risk.html#

Saunders, M., Lewis, P. & Thornhill, A. (2009). *Research methods for business students*. 5th edn. Pearson Education India.

Saunders, M., Lewis, P. & Thornhill, A. (2012). *Research methods for business students*, New York, Pearson.

Savage, K., Coogan, P., & Lou, H. (2015). *The evolution of ransomware, Symantec Corporation* [online]. [Accessed 06 January 2018]. Available at: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

Scully, T (2013). The cyber security threat stops in the boardroom. *Journal of Business Continuity & Emergency Planning Vol. 7(2), pp. 138-148.*

Siba, K., Touran and Prakash, A. (2016). Blockchain: an evolving technology. *Global Journal of Enterprise Information System*, vol.8(4), p.29-35.

Siddiqui, A., Muntijir, M. (2013). A study of possible biometric solution to curb frauds in ATM transaction. *International Journal of advanced studies in Computer Science and Engineering (IJASCSE)*, vol.2(2), p.1-6.

Smart Dubai (2016). *Dubai blockchain strategy* [online]. [Accessed 1 February 2018]. Available at*:* http://www.smartdubai.ae/dubai_blockchain.php

Staples, M., Chen, S., Falamaki, S., Ponomarev, A., Rimba, P., Tran, A. B., Weber, I., Xu, X., Zhu, J., (2017). *Risks and opportunities for systems using blockchain and smart contracts.* Data61 (CSIRO), Sydney.

Sundarraman, A. (2017). *Assuring success in blockchain implementations by engineering quality in validation* [online]. [Accessed 4 March 2018]. Available at: https://www.infosys.com/IT-services/validation-solutions/white-papers/Documents/blockchain-implementations-quality-validation.pdf

Syed, F. (2018). *Blockchain: waiting is not an option. The KPMG UAE banking perspectives 2018 report [*online]. [Accessed 3 June 2018]. Available at: https://home.kpmg.com/content/dam/kpmg/ae/pdf/Blockchain.pdf

Symantec (2016). *Internet security threat report* [online]. [Accessed 22 December 2017]. Available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Swan, M. (2015). *Blockchain – blueprint for new economy:* O'Reilly Media, Inc.

Tasca, P., Aste, T., Pelizzon, L. & Perony, N. (Eds.) (2016). *Banking Beyond Banks and Money.* : Springer International Publishing

Trustwave-1 (2017). *2017 Trustwave global security report* [online]. [Accessed 25 November 2017]. Available at: https://www2.trustwave.com/rs/815-RFM-693/images/2017%20Trustwave%20Global%20Security%20Report-FINAL-6-20-2017.pdf

Trustwave-2 (2017). *Beyond PCI compliance: evaluating your IT risks* [online]. [Accessed 6 January 2018]. Available at: https://www2.trustwave.com/rs/815-RFM-693/images/Beyond%20PCI%20Compliance%20--%20Evaluating%20Your%20IT%20Risk%2020170505.pdf

Tsang, E. (2014). Generalizing from research findings: the merits of case studies. *International Journal of Management Reviews, vol.16 (4), p.369-383.*

Watkins, B. (2016). *The Impact of Cyber Attacks on the Private Sector*. : The Association for International Affairs - http://www.amo.cz/

Williams-Grut, O. (2017). *Blockchain tech could save top investment banks $8 billion a year* [online]. [Accessed 6 February 2018]. Available at: http://www.businessinsider.com /accentureblockchain-could-save-top-10-investment-banks-up-to-8bn-ayear-2017-1

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev A., Tran, A. & Chen S. (2016). The blockchain as a software connector. In Software Architecture (WICSA), *13th Working IEEE/IFIP conference on. IEEE, p.182–191.*

Xu, X., IngoWeber, Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C. & Rimba, P. (2017). A Taxonomy of blockchain-based systems for architecture design. In software architecture (ICSA), *IEEE international conference on. IEEE, p.243–252.*

Yli-Huumo, J., Ko, D., Choi, S., Park, S. & Smolander. K. (2016). *Where is current research on blockchain technology? - a systematic review* [online]. [Accessed 4 March 2018]. Available at: https://doi.org/10.1371/journal.pone.0163477

Zheng, Z., Xie, S., Dai, H.N. & Wang, H. (2016). *Blockchain challenges and opportunities: A survey*. Work Pap.–2016, Inderscience Enterprises Ltd.[online]. [Accessed 16 March 2018]. Available at: https://www.researchgate.net/profile/Hong-Ning_Dai/publication/319058582_Blockchain_Challenges_and_Opportunities_A_Survey/links/59d86d50a6fdcc2aad0a2f2a/Blockchain-Challenges-and-Opportunities-A-Survey.pdf

Zuberi, M. (2017). A Silver chain lining: can blockchain technology succeed in disrupting the banking industry. *Banking & Financial Services Policy Report*, vol.36 (3), p.1-4.

Appendices

Questionnaire

Questionnaire	**Part One: General information** ***Please tick one box for each question:***
Dear Sir/ Madam, This questionnaire gives you the opportunity to express your views on **the effects of blockchain implementation on Cyber risks mitigating methods**. Please note that there is no right or wrong answer. The questionnaire will be used to collect the primary data needed for a research study. Therefore, we seek your assistance to be as open, fair, and honest as possible in your responses. The researchers assure you that no individuals will be identified from their responses and there are no requests for confidential information included in the questionnaire. The results of the analysis will be strictly used by the researchers for study purposes ***only.*** The questionnaire comprises three parts: 1. General Information 2. Cyber risks mitigating factors. 3. The main factors of Blockchain Thank you **Researcher**	**A. Position level:** (1) Top management ( ) (2) Middle management ( ) (3) Executive staff ( ) (4) Support Staff ( ) **B. Education level:** (1) High school or less ( ) (2) College degree ( ) (3) Bachelor degree ( ) (4) Master degree or above ( ) ( ) **C. Age:** (1) Less than 25 ( ) (2) 25 - 34 ( ) (3) 35 - 44 ( ) (4) 45 - 54 ( ) (5) 55 or above ( ) **D. Organization Type:** (1) Federal Government ( ) (2) Local Government ( ) (3) Private sector ( ) **E. How many years of experience do you have?** (1) One year or less ( ) (2) 2 - 5 ( ) (3) 6 - 9 ( ) (4) 10 - 13 ( ) (5) 14 years or above ( ) **F. Please select your primary role below:** (1) Financial ( ) (2) Supply Chain ( ) (3) IT & Engineering ( ) (4) Management ( ) (5) Legal ( ) (6) Quality & Excellence ( ) (7) Others ( )

Part Two: Cyber risks mitigating factors

The second part addresses **the mitigation factors of cyber risks**. Please rate the importance of the following from 1 to 5, **1** being strongly disagree, and **5**: strongly agree.					
	1	**2**	**3**	**4**	**5**
1. Involvement of the boards.	( )	( )	( )	( )	( )
2. Having a cybersecurity strategy.	( )	( )	( )	( )	( )
3. Establishing cyber security rules and regulations.	( )	( )	( )	( )	( )
4. Educating and creating awareness among end-users.	( )	( )	( )	( )	( )
5. Enhancing security culture.	( )	( )	( )	( )	( )
6. Avoiding sharing sensitive information.	( )	( )	( )	( )	( )
7. Activating real-time alerts.	( )	( )	( )	( )	( )
8. Developing programs to protect systems.	( )	( )	( )	( )	( )
9. Using two way authentication.	( )	( )	( )	( )	( )
10. Using suitable tools to protect mobile payment systems.	( )	( )	( )	( )	( )
11. Finding the suitable mitigation techniques to decrease the effects of ransomware.	( )	( )	( )	( )	( )
12. Using Internet of Things (IoT) components.	( )	( )	( )	( )	( )
13. Using big data analysis techniques.	( )	( )	( )	( )	( )
14. Using cloud-based technologies.	( )	( )	( )	( )	( )
15. Creating cybersecurity standards.	( )	( )	( )	( )	( )
16. Implementing security framework.	( )	( )	( )	( )	( )

Part Three: Blockchain

This part is about **blockchain success factors and the opportunities to implement it**.
Please tick one box for each question which best describes your opinion. Please rate the importance of the following about blockchain success factors from 1 to 5, 1 being strongly disagree, and **5**: strongly agree.

	1	**2**	**3**	**4**	**5**
1. Supporting immediate transfer and near real-time settlement.	( )	( )	( )	( )	( )
2. Improving managing data through Immutable capabilities.	( )	( )	( )	( )	( )
3. Supporting quality and accuracy of data.	( )	( )	( )	( )	( )
4. Getting traceable and auditable transactions by using cryptography techniques.	( )	( )	( )	( )	( )
5. Automating the operations using digital currencies.	( )	( )	( )	( )	( )
6. Registering and saving all transactions (Digital ledger).	( )	( )	( )	( )	( )
7. Making decisions related to different operations by using the smart contract.	( )	( )	( )	( )	( )
8. Managing the process of issuing and servicing securities (Smart securities tool).	( )	( )	( )	( )	( )
9. Giving better means of identity (Identity management).	( )	( )	( )	( )	( )
10. Connecting the users with financial system directly by using Smart wallet tool.	( )	( )	( )	( )	( )

Analysis Using SPSS:

Reliability

Scale: Reliability Test Results: Governance factor

Reliability Statistics

Cronbach's Alpha	N of Items
.825	3

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Item1 Cyber_Security_Governance - Involvement of the boards	8.69	2.850	.571	.887
Item2 Cyber_Security_Governance - Having a cybersecurity strategy	8.30	2.804	.775	.665
Item3 Cyber_Security_Governance - Establishing cyber security rules and regulations	8.40	3.065	.724	.723

Scale: Reliability Test Results: Insider threats factor

Reliability Statistics

Cronbach's Alpha	N of Items
.886	6

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Item1 Cyber_Security_Insider_threat - Educating and creating awareness among end-users	21.85	12.442	.748	.859
Item2 Cyber_Security_Insider_threat - Enhancing security culture	21.74	11.786	.808	.848
Item3 Cyber_Security_Insider_threat - Avoiding sharing sensitive information	21.67	12.492	.708	.865
Item4 Cyber_Security_Insider_threat - Activating real-time alerts	21.80	13.297	.601	.882
Item5 Cyber_Security_Insider_threat - Developing programs to protect systems	21.77	13.262	.650	.874
Item6 Cyber_Security_Insider_threat - Using two way authentication	21.78	12.498	.689	.869

Scale: Reliability Test Results: Technology factor

Reliability Statistics

Cronbach's Alpha	N of Items
.758	5

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Item1 Cyber_Security_Technology - Using suitable tools to protect mobile payment systems	15.95	9.356	.439	.743
Item2 Cyber_Security_Technology - Finding the suitable mitigation techniques to decrease the effects of ransomware	16.16	8.541	.536	.712
Item3 Cyber_Security_Technology - Using Internet of Things (IoT) components	16.40	7.376	.687	.652
Item4 Cyber_Security_Technology - Using big data analysis techniques.	16.44	7.923	.565	.700
Item5 Cyber_Security_Technology - Using cloud-based technologies	16.88	8.053	.433	.756

Scale: Reliability Test Results: Process factor

Reliability Statistics

Cronbach's Alpha	N of Items
.728	2

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Item1 Cyber_Security_Process - Creating cybersecurity standards	4.38	.684	.578	.
Item2 Cyber_Security_Process - Implementing security framework	4.49	.522	.578	.

Scale: Reliability Test Results: Blockchain

Reliability Statistics

Cronbach's Alpha	N of Items
.878	10

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Item1 Blockchain - Supporting immediate transfer and near real-time settlement	37.24	25.671	.681	.861
Item2 Blockchain - Improving managing data through Immutable capabilities	37.17	26.199	.707	.861
Item3 Blockchain - Supporting quality and accuracy of data	36.95	26.032	.632	.865
Item4 Blockchain - Getting traceable and auditable transactions by using cryptography techniques.	37.11	25.602	.549	.871

Item5 Blockchain - Automating the operations using digital currencies.	37.52	23.711	.611	.869
Item6 Blockchain - Registering and saving all transactions (Digital ledger).	37.11	25.250	.643	.863
Item7 Blockchain - Making decisions related to different operations by using the smart contract	37.40	24.594	.657	.862
Item8 Blockchain - Managing the process of issuing and servicing securities (Smart securities tool).	37.18	25.568	.681	.861
Item9 Blockchain - Giving better means of identity (Identity management).	36.83	27.776	.421	.878
Item10 Blockchain - Connecting the users with financial system directly by using Smart wallet tool.	37.42	26.367	.534	.871

Scale: Reliability Test Results: Mitigating Cyber Risk Factors

Reliability Statistics

Cronbach's Alpha	N of Items
.928	16

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Item1 Cyber_Security_Governance - Involvement of the boards	64.14	89.973	.562	.926

Item2 Cyber_Security_Governance - Having a cybersecurity strategy	63.74	88.664	.749	.920
Item3 Cyber_Security_Governance - Establishing cyber security rules and regulations	63.85	89.104	.767	.920
Item1 Cyber_Security_Insider_threat - Educating and creating awareness among end-users	63.87	89.914	.711	.921
Item2 Cyber_Security_Insider_threat - Enhancing security culture	63.77	88.627	.740	.920
Item3 Cyber_Security_Insider_threat - Avoiding sharing sensitive information	63.69	90.566	.646	.923
Item4 Cyber_Security_Insider_threat - Activating real-time alerts	63.82	91.852	.597	.924
Item5 Cyber_Security_Insider_threat - Developing programs to protect systems	63.79	90.210	.745	.921
Item6 Cyber_Security_Insider_threat - Using two way authentication	63.80	88.662	.749	.920
Item1 Cyber_Security_Technology - Using suitable tools to protect mobile payment systems	63.64	91.962	.636	.923

Item2 Cyber_Security_Technology - Finding the suitable mitigation techniques to decrease the effects of ransomware	63.85	89.496	.713	.921
Item3 Cyber_Security_Technology - Using Internet of Things (IoT) components	64.08	89.750	.609	.924
Item4 Cyber_Security_Technology - Using big data analysis techniques.	64.12	90.931	.542	.926
Item5 Cyber_Security_Technology - Using cloud-based technologies	64.56	93.531	.343	.933
Item1 Cyber_Security_Process - Creating cybersecurity standards	63.65	92.256	.693	.923
Item2 Cyber_Security_Process - Implementing security framework	63.76	91.333	.656	.923

Scale: Reliability Test Results: All Items

Reliability Statistics

Cronbach's Alpha	N of Items
.943	26

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted

Item1 Cyber_Security_Governance - Involvement of the boards	142.98	285.641	.530	.942
Item2 Cyber_Security_Governance - Having a cybersecurity strategy	142.58	285.055	.643	.940
Item3 Cyber_Security_Governance - Establishing cyber security rules and regulations	142.68	286.461	.632	.941
Item1 Cyber_Security_Insider_threat - Educating and creating awareness among end-users	142.70	286.561	.627	.941
Item2 Cyber_Security_Insider_threat - Enhancing security culture	142.60	287.498	.554	.941
Item3 Cyber_Security_Insider_threat - Avoiding sharing sensitive information	142.53	290.048	.488	.942
Item4 Cyber_Security_Insider_threat - Activating real-time alerts	142.66	290.010	.514	.942
Item5 Cyber_Security_Insider_threat - Developing programs to protect systems	142.62	286.912	.659	.940
Item6 Cyber_Security_Insider_threat - Using two way authentication	142.64	285.233	.638	.940
Item1 Cyber_Security_Technology - Using suitable tools to protect mobile payment systems	142.48	289.535	.570	.941

Item2 Cyber_Security_Technology - Finding the suitable mitigation techniques to decrease the effects of ransomware	142.68	285.920	.627	.941
Item3 Cyber_Security_Technology - Using Internet of Things (IoT) components	142.92	285.007	.579	.941
Item4 Cyber_Security_Technology - Using big data analysis techniques.	142.96	284.201	.603	.941
Item5 Cyber_Security_Technology - Using cloud-based technologies	143.40	287.904	.428	.943
Item1 Cyber_Security_Process - Creating cybersecurity standards	142.49	289.941	.621	.941
Item2 Cyber_Security_Process - Implementing security framework	142.60	287.242	.636	.941

Regression – Process Summary - Stepwise method

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	Blockchain_summary	.	Stepwise (Criteria: Probability-of-F-to-enter <= .050, Probability-of-F-to-remove >= .100).

a. Dependent Variable: Processes_Summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.479[a]	.230	.225	1.213

a. Predictors: (Constant), Blockchain_summary

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	64.462	1	64.462	43.847	.000[b]
	Residual	216.115	147	1.470		
	Total	280.577	148			

a. Dependent Variable: Processes_Summary

b. Predictors: (Constant), Blockchain_summary

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.995	.743		5.376	.000
	Blockchain_summary	.118	.018	.479	6.622	.000

a. Dependent Variable: Processes_Summary

Regression – Insider Threats - Stepwise method

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method

1	Blockchain_summary	.	Stepwise (Criteria: Probability-of-F-to-enter <= .050, Probability-of-F-to-remove >= .100).

a. Dependent Variable: Insider_Threat_Summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.395[a]	.156	.150	3.887

a. Predictors: (Constant), Blockchain_summary

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	410.868	1	410.868	27.194	.000[b]
	Residual	2220.957	147	15.109		
	Total	2631.826	148			

a. Dependent Variable: Insider_Threat_Summary

b. Predictors: (Constant), Blockchain_summary

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	13.808	2.383		5.795	.000
	Blockchain_summary	.298	.057	.395	5.215	.000

a. Dependent Variable: Insider_Threat_Summary

Regression – Governance - Stepwise method

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	Blockchain_summary	.	Stepwise (Criteria: Probability-of-F-to-enter <= .050, Probability-of-F-to-remove >= .100).

a. Dependent Variable: Governance_Summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.429[a]	.184	.178	2.223

a. Predictors: (Constant), Blockchain_summary

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	163.565	1	163.565	33.108	.000[b]
	Residual	726.234	147	4.940		
	Total	889.799	148			

a. Dependent Variable: Governance_Summary

b. Predictors: (Constant), Blockchain_summary

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	4.922	1.362		3.613	.000
	Blockchain_summary	.188	.033	.429	5.754	.000

a. Dependent Variable: Governance_Summary

Regression – Technology - Stepwise method

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	Blockchain_summary	.	Stepwise (Criteria: Probability-of-F-to-enter <= .050, Probability-of-F-to-remove >= .100).

a. Dependent Variable: Technology_Summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.547[a]	.300	.295	2.928

a. Predictors: (Constant), Blockchain_summary

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	539.062	1	539.062	62.895	.000[b]
	Residual	1259.905	147	8.571		
	Total	1798.966	148			

a. Dependent Variable: Technology_Summary

b. Predictors: (Constant), Blockchain_summary

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	6.353	1.794		3.540	.001
	Blockchain_summary	.341	.043	.547	7.931	.000

a. Dependent Variable: Technology_Summary

Regression – Processes - Stepwise method

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	Blockchain_summary	.	Stepwise (Criteria: Probability-of-F-to-enter <= .050, Probability-of-F-to-remove >= .100).

a. Dependent Variable: Processes_Summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.479[a]	.230	.225	1.213

a. Predictors: (Constant), Blockchain_summary

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	64.462	1	64.462	43.847	.000[b]

	Residual	216.115	147	1.470		
	Total	280.577	148			

a. Dependent Variable: Processes_Summary

b. Predictors: (Constant), Blockchain_summary

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.995	.743		5.376	.000
	Blockchain_summary	.118	.018	.479	6.622	.000

a. Dependent Variable: Processes_Summary