أثر العقود الذكية القائمة على تكنولوجيا البلوك تشين على تقييم الخطر الملازم مع: دراسة ميدانية

Impact of Blockchain-based Smart Contracts on Inherent Risk Assessment :With A Field Study

Zakaria Elsayed Hasaneen

Teaching assistant -Accounting Department
Faculty of Commerce, Kafrelsheikh University

Email: hasaneen.zakaria@gmail.com

Dr. Ayman Mohaned Sabry
Assistant Prof. of Accounting
Faculty of Commerce, Kafrelsheikh University

Dr.Abdo Ahmed Ettish
Lecturer of Accounting
Faculty of Commerce, Kafrelsheikh University

مجلة الدراسات التجارية المعاصرة

كلية التجارة – جامعة كفر الشيخ
المجلد العاشر - العدد السابع عشر - الجزء الرابع
يناير 2024م
رابط المجلة : https://csj.journals.ekb.eg

1.1 Abstract

This paper examines the potential impact of smart contract risks on auditors' procedures in assessing businesses using blockchain technology. It identifies five key risk considerations related to smart contracts: Business and regulatory risks, contract enforcement risks, legal liability risks, and information security risks. By considering these risks, auditors can assess smart contract effectiveness and reliability and identify potential areas of weakness. The paper aims to help auditors understand the smart contract and blockchain technology challenges and opportunities.

KEYWORDS: Blockchain -Smart contracts -Auditing-Inherent risk

1.1 ملخص البحث

تدرس هذه الورقة البحثية الأثر المحتمل لمخاطر العقود الذكية على الإجراءات التي يقوم بها المراجعين لتقييم الأعمال التي تستخدم تقنية البلوكشين. وتحدد خمس اعتبارات رئيسية للمخاطر المتعلقة بالعقود الذكية: مخاطر الأعمال والمخاطر التنظيمية ومخاطر تنفيذ العقود ومخاطر المسؤولية القانونية ومخاطر امن المعلومات. من خلال النظر في هذه المخاطر، يمكن للمراجعين تقييم فعالية وموثوقية العقود الذكية وتحديد النقاط المحتملة لضعفها. تهدف هذه الورقة البحثية إلى مساعدة المراجعين على فهم التحديات والفرص التي تواجه العقود الذكية وتقنية البلوكشين.

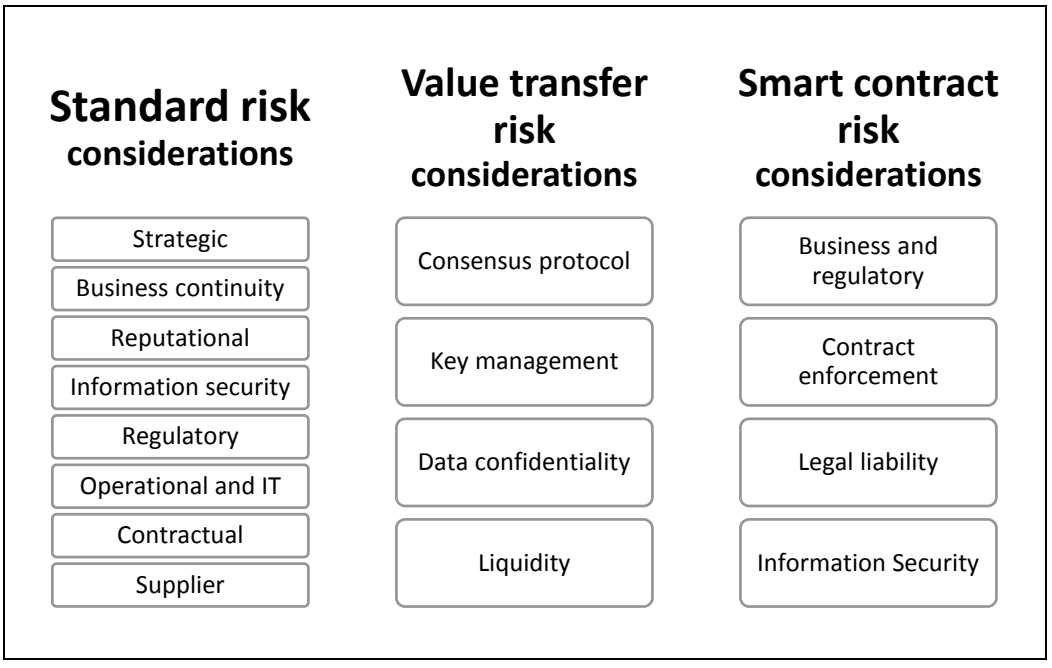
الكلمات الرئيسية: البلوكشين ـ العقود الذكية ـ المراجعة – المخاطر المتأصلة

1.2 Introduction

Due to the rapid evolution of information technology and its many capabilities, global corporations and governments have sought the finest technology available to save time, money, and effort. Blockchain technology is one of the most distributive technologies that may change the face of Business and the working of accountants and auditors.

This technology does not come without risks. There are many risks associated with this technology. Deloitte, 2017, showed that the inherent risks could be classified under three categories: standard, value transfer, and smart contract risks.

Fig 1-1 *"Risk considerations in blockchain"*



Source: *(Deloitte, 2017)*

1.3 Research Problem

Blockchain technology is associated with many risks, as shown in the literature and Big 4 companies' reports. This may lead to many obstacles and challenges auditors face as traditional audit approaches do not work with Blockchain. Especially companies that will convert their current systems to Blockchain or already applied blockchain systems.

So, the traditional role of the auditor should be changed. Moreover, the auditors should not only know how Blockchain works but also an assessment of risk inherent in blockchain technology. (White et al., (2019). Therefore, the researcher chooses the framework for audit risks associated with blockchain technology set by Deloitte because it is more straightforward and comprehensive.

The critical question here is if the terms of the business contract changed. Shall we create a new code, or what we do, as the code cannot be changed after published? Moreover, if anyone executes the order to destruct the code and data with it, what will the Business do in such things.

In this paper, the researcher aims to know the following**:** What is The Impact of Blockchain-based Smart Contracts on the Assessment of Inherent Risks?

1.4 Research Objective

Therefore, the main objective of this research is: -

Investigating the impact of Blockchain-based Smart Contracts on Inherent Risk Assessment

1.5 Research Importance

The research may be significant in several aspects and contributes to the literature both in terms of theory and practice.

Theoretical importance: -

1- It is expanded to the literature by understanding the inherent risks related with Blockchain-based Smart Contracts and how they influence the auditor's job.

2- Assessment of inherent risks in Blockchain-based Smart Contracts, which might be regarded as a new topic of auditing research.

Practical importance:

1- Create awareness among auditors on the types of inherent risks information that they could assess in their auditing of the companies that apply blockchain and. Moreover, it can improve the auditing profession.

2- Help the auditors to make appropriate judgments about blockchain technology and why companies need professional auditors to help them to adopt this technology.

1.6 Research Hypothesis

The main Hypothesis: There is a significant impact of Blockchain-based Smart Contracts on Inherent Risk assessment.

1.7 Literature Review

The impact of blockchain technology on accounting, financial reporting, and taxation has been the subject of several publications. The researcher below summarizes the most current publications on blockchain's influence on auditing. Furthermore, any publication that attempts to determine the risks associated with Blockchain.

1.7.1 First group: Blockchain and its relationship with the future of Auditing and Accounting

1. Appelbaum & Nehmer, (2017)

This paper theoretically discusses transactions, contracts, and workflows for classes of viable accounting systems in this context, how auditors will assure systems with these characteristics. How distributed ledger technologies pertain to the evidence standards of both internal and external auditors. How would such systems affect confirmations? Also, provide a proof of concept using a cloud computing environment. The author used Design science research (DSR) in this paper. The main findings suggested that draw attention to the fact that current business IT and data collection/storage systems are complex and may be cloud-based. The

potential for DLT and its audit should be considered in these circumstances. The audit profession will need to adjust itself to the phenomenon of Blockchain. There may be a conflict between the basic philosophies of blockchain and auditing. Blockchain is a decentralized technique with minimal regulation, structure, and authority, where all participants have an equal vote.

2. Dai & Vasarhelyi, (2017)

This paper gives us a fundamental theoretical discussion on how Blockchain could enable a real-time, verifiable, and transparent accounting ecosystem. And how blockchain transforms current auditing practices, resulting in a more accurate and timely automatic assurance system. The main findings suggested that Blockchain technology is emerging and rapidly developing. As new algorithms and approaches are introduced, their accounting and assurance applications may need to be expanded and reconsidered. This paper only provides a general discussion of blockchain technology's role in the accounting and assurance environment. Blockchain's applications and challenges in specific areas, such as government auditing, need further thought. Concepts like triple-entry accounting may be just an adaptation to the extant world, which may not be advanced enough to use going forward in a rapidly changing world.

3. Rozario & Vasarhelyi, (2018)

This paper theoretically examines if blockchain-enabled smart contracts can help auditors deliver enhanced audits. Through improved audit data analytics (ADA) and real-time auditing. This paper studies if a permissioned blockchain is implemented. The main findings suggested that a new type of audit data analytics (ADA) that will help change the way auditors do financial auditing of companies.It is necessary for auditing standards and academics to know to disrupt business ecosystems and the audit ecosystem, such as blockchain.Auditing client blockchain and smart contracts introduce new risks to its auditing that the auditors should be aware of. This may lead to a new type of IT auditing.This paper introduced many future research questions regarding blockchain's security, privacy, scalability, and flexibility—also the impact of blockchain on auditor judgment.

4.Liu et al., (2019)

This theoretical paper aims to introduce two types of blockchain (i.e., Permissionless and Permissioned) and their technological features, in addition to the challenges and opportunities that auditors face with them. The main findings suggested that The auditors should consider the following initial steps to adapt to the new environment: Acquire competency in blockchain technology and governance of blockchain. (Auditors should be able to assess the costs and benefits of adopting specific blockchains). Actively participate in blockchain development with an emphasis on risk control (Audit firms should shift their focus to evaluate the effectiveness of risk management and advise on solutions and assurance for internal control).Move to continuous auditing. Grow the advisory function.

5- Fuller & Markelevich, (2020)

The possible impact of blockchain technology on the accounting profession is investigated in this theoretical article. This article examines data security and privacy, technology, adoption, and implementation issues, as well as some accounting and auditing-specific challenges. The main findings suggested that the ability of blockchain to offer wide-scale two-party verification of a significant chunk of a company's transactions provides enormous potential for accounting data reliability. Furthermore, blockchain integration can transform auditing by providing auditors with more efficient and effective ways to verify accounting data through two-party transaction verification and smart contract innovations, allowing auditors to conduct audits more autonomously and continuously. Although these are clear advantages, widespread blockchain adoption in the accounting and auditing fields faces several substantial obstacles. Scalability concerns and the costs involved with blockchain integration are two of the most significant barriers. Each potential blockchain member must address its concerns about costs, data privacy, security, and willingness to adopt common standards.

1.7.2 Second group: Risks associated with Blockchain.

1. Li et al., (2017)

This paper conducts a systematic theoretical study on the security threats to blockchain and surveys the corresponding actual attacks by examining popular blockchain systems. (e.g., Ethereum, Bitcoin, Monero, etc.), Also,

review the security enhancement solutions for blockchain, which could be used in developing various blockchain systems, and suggest future directions to research efforts in this area. This study used Survey the real attacks on the blockchain systems as methodology. The main findings suggested that the researchers divide the common blockchain risks into nine categories as follows:

Risks exist in blockchain 1.0 and 2.0, and their causes are mostly related to the blockchain operation mechanism. By contrast, other risks are unique to blockchain 2.0 and usually result from the development, deployment, and execution of smart contracts. For each risk or vulnerability, the researchers analyze its causes and possible consequences.

2. Zamani et al., (2018)

This paper examines the associated risks and concerns of blockchain. And explore relevant standards and regulations related to blockchain. This Study uses the case study method as methodology. The sample consists of an examination of 38 existing cases of security breaches based on a root cause analysis approach. The main findings suggested that the blockchain is designed to be secure, and the technology has great potential benefits. However, through interactions with software systems, web-based systems, clouds, and other platforms, security risks can be introduced to blockchain systems. The incidents reviewed highlight key points that should be included in a blockchain-specific framework, including regulatory compliance, blockchain provider selection, the need for thorough, smart contract code reviews and both internal and external audits, the automation of IR methods and checks, appropriate use of cold storage techniques where possible and end-to-end product life cycle reviews and automated checks.

3- Morganti et al., (2018)

In this paper, the researcher theoretically outlines the blockchain's key risks and examines their effect. Then, a qualitative risk assessment is carried out using a NIST-compliant approach. The researcher outlines a list of the most important risks by surveying the literature and gathering information from sources covering news regarding bugs and incidents with blockchains that have recently been identified as methodology. The main findings suggested that the number of blockchain risks that may lead to a significant risk of adverse effect (i.e., moderate or higher) is 76.47%. There are already potential mitigations for some of the attacks. Nevertheless, it is necessary to always explore new forms of mitigation and, where possible, prevention for

all the risks, particularly for the remaining 23.53%. The area of threats surrounding smart contracts and blockchain 2.0 is the one that is more exposed to risk, and the researcher expects to explore countermeasures for those vulnerabilities in a future job. Future research includes enriching the evaluation with further attackers (e.g., insiders), contrasting the findings with real case studies, and considering different blockchain forms based on threats specific to them.

4. White et al., (2019)

This paper theoretically discussed the associated risks related to blockchain and the auditor's role in dealing with it. The main findings suggested that. Blockchain has many benefits, including improved efficiencies, lower costs, enhanced transparency, and immutable audit history of all transactions, however, with benefits come associated risks. The associated risks include technological, data security, interoperability, and third-party vendor risks.

5.Prewett et al., (2019)

In this paper, the researchers highlight theoretically some of the significant obstacles and risks associated with this Blockchain technology. The main findings suggested that the full impact of blockchain and other distributed ledger technologies is unknown. However, blockchain adoption is inevitable for enterprises, and careful consideration of risks and challenges before, during, and after implementation will result in long-term success.

6.Vincent & Barkhi, (2020)

This article theoretically gives practitioners an overview of smart contracts and discusses the risks of participating in a blockchain consortium. It also lists relevant internal control considerations while joining a consortium or executing a smart contract. Then evaluate whether current frameworks, notably the COSO integrated and COSO Enterprise Risk Management (ERM) frameworks, adequately address a collaborative supply chain ecosystem. The main findings suggested that internal controls assessment for a firm can be complex because the company may be merely a participant with no influence over how the technology and smart contracts are applied.Most businesses will have to accept the single source of truth without knowing whether or not there are any preventative, detective, or

corrective controls in place for transaction creation, updating, and processing. As a result, a crucial point that needs to be investigated further is whether existing frameworks meant to approach risk and controls from the perspective of a single firm are appropriate in a blockchain and smart contract ecosystem that spans numerous organizations.

1.7.3 Comments on the Literature

1- Some papers addressed the impact of using blockchain technology on accounting and auditing in general.
2- Other papers study the types of risks associated with blockchain technology.
3- Most studies focus on the effect of blockchain technology in general; however, the issue of how an auditor might assess the inherent risks connected with blockchain technology is not addressed in depth.
4- The papers showed blockchain's many benefits, especially related to financial institutions and companies.
5- Some papers showed the general risks of blockchain but did not address how they affect the future of auditing after applying the blockchain around the world.
6- Traditional audit approaches do not work with blockchain.
7- Most papers published that address the relationship between blockchain and auditing are theoretical; therefore, there is a need for more research based on empirical studies.

1.7.4 Research Gap

The existing literature on blockchain technology and its impact on accounting and auditing is quite general. However, a noticeable research gap exists regarding the specific assessment of inherent risks connected with blockchain technology and smart contracts from an auditor's perspective. While the benefits of blockchain technology, particularly in financial institutions and companies, have been highlighted in several studies, there is limited exploration of how these risks might shape the future of auditing on a global scale. Furthermore, the traditional audit approaches are found to be inadequate when dealing with blockchain. Therefore, there is a need for more studies to complement the current literature to address how the risks of blockchain are assessed by auditors. Therefore, further research is required to delve deeply into the assessment of risks, the impact on auditing

practices, and to bridge the gap between theory and practical application in this domain, especially smart contracts.

1.8 Smart Contracts

Computer scientist, lawyer, and cryptographer Nick Szabo invented the concept of smart contracts in the early 1990s. Szabo has written numerous articles and papers over the years concerning smart contracts. (Schulpen, 2018). A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. (Zapotochnyi, 2016)

According to (Maesa & Mori, 2020), carrying out a smart contract in the Blockchain offers a collection of new properties, such as:

- Atomicity**:** the process runs entirely or fails without affecting the state.
- Synchronicity: Code execution is sequential
- Provenance**:** Code can be executed only by traceable external calls
- Availability**:** Code is always available, and associated data
- Immutability**:** Unable to update or alter the code after deployment
- Immortality**:** The only way to delete or remove the code and data is to conduct an auto-destruct procedure.

1.9 Smart contract risk considerations

1.9.1 Business and regulatory risks

Regulatory risk is defined as "the risk that a change in laws and regulations will materially impact a security, business, sector, or market"**.**(investopedia. com, 2020)

There are different Smart contracts legal and regulatory challenges **(**McMillan, 2017**),** such as Interpretation and uncertainty, Inflexibility of the code**,** Reliance on external sources of information**,** Bugs and errors, Liability and risk allocation**,** Ability to unwind, Confidentiality, security, and privacy, Jurisdictional issues, Evidentiary matters**,** Regulated contracts and regulatory and policy settings:

Also, there are risks associated with smart contracts from a regulatory perspective, according to **(**World Economic Forum, 2020**)** as follows:

- Due to a lack of smart contract auditing, company or legal arrangements are implemented incorrectly.
- Governance of smart contracts: For regulated organizations, the organization's governing body and responsible senior managers must properly control the smart contracts and obtain daily management reports on their performance.
- Risk of product design flaws leading to non-compliance with data-related regulations. For example, Do the regulations allow data to be stored on-chain or must it be stored off-chain?
- The risk of non-compliance with industry cybersecurity regulations and requirements, which Blockchain solutions must meet.

*From all the above, the researcher concludes that***:** There are numerous legal and regulatory challenges that smart contracts face, which necessitate internal auditors working with the company's legal team or technical team to determine the potential impact on security, industry, sector, or market.

1.9.2 Contract enforcement

Although a smart contract has a legally binding contractual effect, the technology used to execute it can sometimes trigger legal enforceability issues. If a conflict arises, there may be no central administering authority to settle it. Dispute settlement mechanisms are currently one of the options for addressing jurisdictional differences and enforceability problems. (Shah, 2019)

One of the essential features of smart contracts is their ability to conduct transactions without the need for human interference automatically. However, this automation and the fact that smart contracts cannot be easily amended or terminated unless the parties have specific capabilities during the smart contract's creation are two of the most significant barriers to widespread smart contract adoption. (Vasile & Neal, 2021)

In January 2020, Illinois approved a law explicitly targeting blockchain technology and smart contract enforcement called the Blockchain Technology Act ("BTA"). According to BTA, "a smart contract, record, or

signature may not be denied legal effect or enforceability solely because it was created, stored, or verified on a blockchain." (Vasile & Neal, 2021)

Also, there are vital aspects that should be given more importance than usual to ensure that the smart contract is a legally binding and enforceable contract, according to(World Economic Forum, 2020), such as Legal formalities, Transparency, Auditability, Retrospective resolution and Marginal judgement:

From all the above, the researcher concludes that the auditor may review the preceding factors to determine if the smart contract is legally binding and enforceable. There are problems with enforcement because, even though they obtain an order from a judge, the court does not have authority over people who are part of this public Blockchain and are decentralized worldwide.

1.9.3 Legal liability

Under BTA, "a smart contract, record or signature may not be denied legal effect or enforceability solely because a blockchain was used to create, store, or verify.

Many parties to a smart contract will lack the technical capability to create a smart contract and instead hire a third party to do so or rely on a smart contract "template" offered by a third party. In such cases, it is possible that the developer made a mistake or that the parties did not accurately communicate their intentions to the developer. Parties must consider the implications of these situations and the appropriate risk and liability allocation. Smart contract developers may also need to be aware of their liability if the smart contract code they created is used for illegal purposes. (Vasile & Neal, 2021)

Where will anyone seek relief if anything goes wrong with the contract's execution and they lose money? We will need a technologically advanced court system. The courts have begun to accept Blockchain as a method for strengthening the administration of justice. Courts would need to be able to deal with blockchain evidence as they dealt with e-discovery. (Shah, 2019)

When using smart contracts on a blockchain in the private law domain, there are also plenty of legal issues to consider. For example, if the contract

has been miscoded and does not achieve the parties' purpose, or if the oracle makes a mistake or intentional error, the question of liability must be addressed. The parties must also agree on the relevant legislation, jurisdiction, general governance standards, dispute resolution, protection, and digital identity methods. Is the contract available in written and code form so that both parties understand what they agree to? Can the parties' identities be determined with reasonable certainty to make the contract valid? If these issues are not resolved ahead of time, despite the parties' best efforts, they will discover that they do not have a contract and that if problems occur, they will have no agreed-upon method of resolving them(Deloitte, 2018b)

From a public-law standpoint, there are explicit risks that permissionless blockchains could be used for criminal purposes such as money laundering or to manipulate completely anonymous participation to circumvent competition-law issues. Participants may be exposed to "miners" who build new blocks behaving recklessly or not in good faith. There are currently no clear legal solutions available to combat dishonest miners. Since smart contracts run on a blockchain, they cannot be changed after the fact, and because they are self-executing, they cannot be stopped. The transaction is immediately carried out if the precondition is met, even if the parties have reasonable reason to believe otherwise. (Deloitte, 2018b)

From all the above, the researcher concludes that A smart contract must have all elements of the original paper contract regardless of originating in an electronic format. Many challenge face auditors regarding if things go wrong, what court are going to sue in what country because it could be the situation where when something goes wrong, every single place there is a node is a point of liability, so suddenly you could be subject to conflicting laws across different nations.

1.9.4 Information Security risks

The steady acceptance of smart contracts has led to tens of thousands of contracts containing millions of dollars in digital currencies, and minor errors may result in significant losses and entail dangers for future accidents.(Mense & Flatscher, 2018)

An information security risk may arise due to the uncertainties and weaknesses of the operation and use of information systems and the

environments in which those systems work. It has consequences for an organization and its stakeholders.(Gantz & Philpott, 2013)

Although the Blockchain is safely built and backed by widely studied and tested cryptographic algorithms, smart contracts such as software are likely to contain security vulnerabilities in their code, which, combined with their irreversible existence and potential to run in sensible environments such as financial or health issues, presents a serious security danger.(López Vivar et al., 2020)

According to ISACA, (2019), The Auditor may be checking the following procedures in the light of the following control objectives and controls when assessing Information security risks related to smart contracts in Blockchain.

Testing Step for First Control item Figure (1-2):

• For permissionless repositories (e.g., GitHub), ensure that security is reasonable. Consider the following:

a. Reputation of repository (including known security incidents)

b. process for approving source-code changes (including input from core developer group, community feedback, approval of changes)

c. Activities of the repository and degree of community engagement (e.g., number of active contributors, number of commits, pull requests, active issues, etc.)

• For permissioned repositories (e.g., private or consortium), ensure adequate security controls exist. Verify that:

a. Appropriate security controls are in place for code repositories (e.g., segregation of duties, approval process for changes, access controls).

b. Policies and procedures are documented and understood by all parties, where code repositories are shared by the enterprise via consortium.

Testing Step for Second Control item Figure (1-2):

• Ensure that adequate code reviews take place. Verify the following:

a. For permissionless blockchains, source code is vetted at least quarterly through manual code review, penetration tests and/or automated scans.

b. For permissioned blockchains, source code is reviewed in accordance with relevant policies and procedures.

c. Source code is independently reviewed by qualified security professionals with experience in the enterprise's specific blockchain platform(s).

• Determine whether appropriate stakeholders participate in the code review process (e.g., information security and information technology stakeholders).

Testing Step for Third Control item Figure (1-2):

• Verify that an adequate remediation process is in place for identified source-code vulnerabilities. Determine whether:

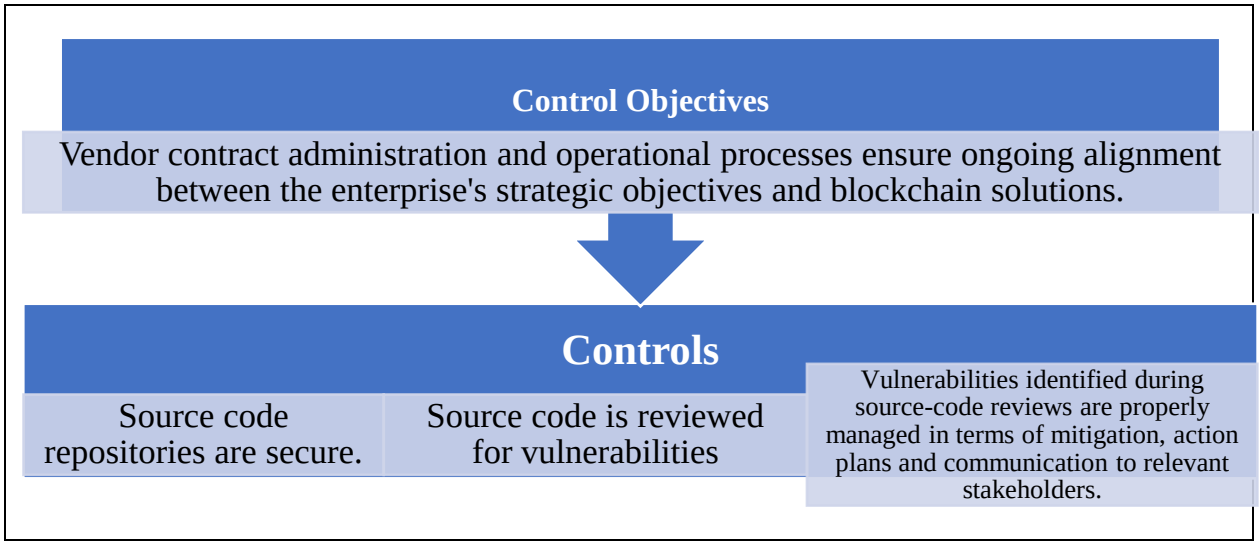
a. For permissionless blockchains, the enterprise has considered appropriate actions (e.g., forking to a different blockchain, limiting certain transactions).

b. For permissioned blockchains, the enterprise has considered actions consistent with relevant policies and procedures.

• Verify that the process for remediating blockchain source-code vulnerabilities has been approved by relevant stakeholders.

• Select a sample of identified blockchain source-code vulnerabilities and verify adherence to the blockchain source-code remediation process.

Figure (1-2): *Information security risks Control considerations in Blockchain(Smart contracts) by Internal Auditor*



Source: *The Researcher*

*From all the above, the researcher concludes that***:** Errors are an inescapable part of software development. When creating a smart contract on Blockchain, it has bugs as well. A smart contract's bugs result in a loss of assets. As a result, if the auditors do not engage in smart contract code analysis before its implementation on the blockchain network, the organization could be exposed to greater risk.

1.10 Field Study

In this section, the focus shifts towards the field study, which aims to measure Impact of Blockchain-based Smart Contracts on Inherent Risk Assessment

1.10.1 Analysis of Demographic Variables: Population and Sample

A population refers to an entire set of elements from which a sample is drawn, as collecting data from the entire population may not be practical due to various factors such as time, money, and accuracy. Thus, the researcher attempted to obtain a representative sample of the study population.

In this study, the main purpose is to investigate impact of Blockchain-based Smart Contracts on Inherent Risk Assessment; and thus, the population includes five categories, which are outlined below:

1. **Accountants**
2. **External auditors**
3. **Internal auditors**
4. **Academics in auditing and accounting**
5. **Professional workers in a blockchain-related field**

For the selection of the study sample, the researcher employed judgmental sampling. The sample comprises Accountants, External auditors, Internal auditors, Academics in auditing and accounting, and Professionals working in the blockchain-related field from various countries. The questionnaire was distributed using electronic means, and Google Forms was utilized to design it. A total of 211 valid and usable questionnaires were obtained for statistical analysis.

1.10.2 Sample Categories

The sample consists of five categories, as per the study population. The table below illustrates these categories along with the number of questionnaires received and subjected to statistical analysis:

Table (1. 1)

Sample Categories

Sample categories	Number of Qs. sent	Number of Qs. received	Excluded Qs.	Correct Qs to statistical analysis.	Percentage
Accountant	55	50	3	47	22.3%
External auditor	30	25	5	20	9.5%
Internal auditor	40	35	5	30	14.2%
Academic in auditing and accounting	114	110	7	103	48.8%
work in a blockchain-related field	16	15	4	11	5.2%
Total	255	235	24	211	100.0%

Source: Results of the statistical analysis

1.10.3 Scientific Qualification of Sample Members

The following Table (1-2) displays the characteristics of the study sample according to their scientific qualifications. The collected data reveals that out of the respondents, 45 (21.3%) hold a bachelor's degree (BSc), 8 (3.8%) hold a diploma, 63 (29.9%) hold a master's degree (MSc), 85 (40.3%) hold a PhD, and 10 (4.7%) hold a professional certificate such as CPA, CIA, CMA, CFA, etc. These results indicate that the respondents possess diverse scientific qualifications.

Table (1. 2)

Scientific Qualifications

Scientific Qualifications	Number of Respondents	Percentage
Bachelor	45	21.3
Diploma	8	3.8
Master	63	29.9
PHD	85	40.3
Professional certificate	10	4.7
Total	211	100.0

Source: Results of the statistical analysis

1.10.4 Job Experience of Sample Members

The following Table (1.3) outlines the characteristics of the study sample based on their years of experience. The table exhibits that the sample has been categorized into four groups based on job experience, as follows:

Table (1. 3)

Job Experience

Job Experience	Number of Respondents	Percentage
less than one year	21	10.0%
from 1 year to less than 5 years	4	1.9%
from 5 years to less than 10 years	55	26.1%
from 10 years and more	131	62.1%
Total	211	100.0%

Source: Results of the statistical analysis

1.10.5 Country of Sample Members

The following Table (1.4) showcases the characteristics of the study sample according to their country. The table indicates that the questionnaire was distributed to participants from 15 countries, as listed below:

Table (1. 4)

Country

Country	Frequency	Percent
Egypt	157	74.4
Saudi Arabia	9	4.3
Palestine	4	1.9

Country	Frequency	Percent
Kuwait	1	.5
Iraq	23	10.9
Yemen	3	1.4
Jordan	4	1.9
Syria	2	.9
Algeria	2	.9
The UAE	1	.5
Qatar	1	.5
Tunis	1	.5
Germany	1	.5
Spain	1	.5
USA	1	.5
Total	211	100.0

Source: Results of the statistical analysis

According to Figure (1-4), the majority of the sample consists of participants from Egypt (74.4%), followed by Iraq (10.9%), then Saudi Arabia (4.3%), and Palestine and Jordan (1.9%) respectively. Yemen accounts for 1.4% of the sample, while Syria and Algeria each represent 0.9%. Additionally, the USA, Spain, Germany, Tunis, Qatar, The UAE, and

Kuwait each represent 0.5% of the sample. These findings suggest that the sample includes a diverse range of participants from different countries.

1.10.6 Research Tool

To attain the primary goal of the study, the researcher employed a questionnaire as the data collection tool. The researcher made every effort to ensure the accuracy of the questionnaire by considering the following factors:

- Providing clear definitions of key terms relevant to the research topic.
- Designing the questionnaire using a five-point Likert scale to capture the respondents' opinions on the questionnaire's contents.

Table (1. 5)
Classification according to Likert scale

Category	Completely Agree	Agree	Neutral	disagree	Totally disagree
Degree	5	4	3	2	1

Source: Results of the statistical analysis

- The questionnaire included some general questions that aimed to gather information about the sample members' job positions, scientific qualifications, and years of experience.

- The researcher utilized certain phrases extracted from the National Academic Reference Standards (NARS) while formulating the questionnaire's questions.

1.10.7 Data Encoding

The questions of the questionnaire were coded by the following symbols to facilitate statistical analysis process:

$X3_1$ ……. $X3_6$: are codes for questions of the hypothesis.

1.10.8 Reliability and Validity Questionnaire Testing

A- Reliability Questionnaire Testing

Reliability refers to the degree to which a scale provides consistent measurements when applied to the same individuals under the same conditions. The researcher used Cronbach's alpha coefficient to assess the degree of reliability in the study's measures. Cronbach's alpha coefficient ranges from zero to one, and when it is close to one, it indicates high reliability of the survey. A ratio of 60% can be considered acceptable for judging the reliability of the survey, while any variable that obtains an item-total correlation coefficient of less than 30% with the other variables in the same scale is excluded. The degree of reliability of the measures used in the study is measured as follows:

The following Table (1.6) presents the reliability results for the Hypothesis, which are as follows:

Table (1. 6)

Cronbach's Alpha Test Results for the third dimension

	Corrected Item-Total Correlation	**Cronbach's Alpha**
X31	.622	.836
X32	.601	
X33	.615	
X34	.708	
X35	.575	
X36	.544	

Source: Results of the statistical analysis

Based on Table (1.6), it is evident that all items in the scale possess a total correlation coefficient greater than 30%. Moreover, the alpha coefficient for the scale is 0.836, indicating a high degree of internal consistency. Consequently, it can be concluded that the scale exhibits a high level of reliability.

B- Validity Questionnaire Testing

Validity pertains to the degree to which a measurement tool can effectively accomplish its intended purpose by measuring what it was designed to measure. To ensure the questionnaire's validity, the researcher employed three types of validity: content validity, subjective validity, and internal consistency validity, as follows:

i. Content Validity

Content validity is based on the logical content of the test and its correlation with the measured phenomenon. It primarily relies on the test's ability to accurately and consistently represent the contents of the measured trait with high significance to achieve the intended objective. Typically, to assess content validity, the researcher presents the tool to experts in the field and asks them to evaluate the validity of its vocabulary and paragraphs in measuring the intended trait. Then, they determine the level of agreement among the experts and retain the paragraphs that achieve a high level of agreement. The researcher presented the study tool to a number of referees and specialists in the study area to ensure that the questionnaire effectively measures the intended trait.

ii. Subjective Validity

The Subjective validity of the questionnaire was calculated for the dimension by finding the square root of the reliability coefficient as follows:

Table (1. 7)

the subjective validity results of the questionnaire

Dimension	Cronbach's Alpha	Subjective Validity
The impact of Blockchain on the assessment of Smart contract risks.	0.836	0.914

Source: Results of the statistical analysis

Based on Table (1.7), it can be observed that all dimensions exhibit a high level of validity, indicating that the survey possesses a high degree of validity.

iii. Internal Consistency Validity

The validity of the employed tool can be assessed by measuring the degree of correlation between the scores of each domain and the scores of the overall scale questions, as demonstrated in Table (1.8) below:

Table (1.8)

Average Variance of Variables

		The impact of Smart contracts risk considerations of blockchain on the auditor's assessment of inherent risk
The impact of standard risk considerations of blockchain on the auditor's assessment of inherent risk.	Pearson Correlation	.614**
	Sig. (2-tailed)	.000
	N	211
The impact of value transfer risk considerations of blockchain on the auditor's assessment of inherent risk.	Pearson Correlation	.673**
	Sig. (2-tailed)	.000
	N	211
The impact of Smart contracts risk considerations of blockchain on the auditor's assessment of inherent risk	Pearson Correlation	1
	Sig. (2-tailed)	
	N	211
The overall mean of the survey	Pearson Correlation	.880**
	Sig. (2-tailed)	.000
	N	211

Source: Results of the statistical analysis

As depicted in Table (1.8), the previous correlation coefficients are deemed acceptable and statistically significant. Therefore, the researcher has verified the questionnaire's reliability and validity, rendering it valid for implementation on the study sample.

1.10.9 Normality Distribution Questionnaire Testing

Normality distribution tests are employed to ascertain whether a dataset is normally distributed or not. Based on the results of this test, the type of statistical methods to be employed is determined. If the data is normally distributed, parametric tests are utilized for statistical analysis, whereas nonparametric tests are used for statistical analysis if the data is not normally distributed. In this study, normality tests were conducted using the Kolmogorov-Smirnov (K-S) test. The following Table (1.9) shows the Kolmogorov-Smirnov test outcomes, indicating that if the significance level is above 0.05, the data is considered normally distributed. However, if the significance level is below 0.05, the data is deemed not normally distributed.

Table (1. 9)

Kolmogorov–Smirnov (K-S) test

One-Sample Kolmogorov-Smirnov Test				
			The impact of Smart contracts risk considerations of blockchain on the auditor's assessment of inherent risk	
Kolmogorov-Smirnov Z			1.700	
Asymp. Sig. (2-tailed)			.006	
Normality distribution decision			UNNORMAL	

Source: Results of the statistical analysis

Based on Table (1.9), it can be observed that the level of statistical significance (Sig) for the first, second, and third dimensions is less than the significance level (α = 0.05). Therefore, the null hypothesis was rejected, and the alternative hypothesis was accepted, indicating that the data for these dimensions are derived from a population that does not adhere to a normal distribution. Hence, non-parametric tests are utilized for statistical analysis. Conversely, it is observed that the level of statistical significance (Sig) for the "Impact of Blockchain Technology on Inherent Risk Assessment" dimension is greater than the significance level (α = 0.05). Therefore, the null hypothesis is accepted, indicating that the data for this dimension is derived from a population that adheres to a normal distribution. Hence, parametric tests are utilized for statistical analysis.

1.10.10 Statistical Analysis and Testing Hypotheses

The collected data were analyzed by using Statistical Package for Social Science (SPSS) version 21. The researcher tested the hypotheses by using three methods of statistical analysis as follow:

1. Data Descriptive Analysis

This step involves determining the frequencies, percentages, arithmetic mean, and standard deviation to identify the overall trend of responses for each statement. It should be noted that the interpretation of the means based on the Likert scale is as follows:

Table (1. 6)

Interpretation of averages according to a Likert scale

Weighted average	Level
1.8 _1	Completely disagree
2.6 _1.8	Disagree
3.4_2.6	Neutral
4.2_3.4	Agree
5_4.2	Totally Agree

2. Sign Test

The Sign Test is a nonparametric test utilized as an alternative to the T-TEST, and it is employed to test hypotheses concerning the mean of a single population.

3. Chi-Square Test

The Chi-Square Test is a non-parametric test aimed at determining if there are statistically significant differences between the expected frequency and the observed frequency of all survey statements represented by the sample's responses. This is accomplished by comparing the level of statistical significance (sig) with the level of significance (α) for each paragraph or response. If the significance level (sig) value is less than the significance level (α), this indicates that there are statistically significant differences between the expected and observed repetition, signifying the significance of that particular paragraph or response if it carries a higher repetition.

4. Kruskal Wallis Test

The Kruskal Wallis Test is a non-parametric test utilized to contrast more than two independent groups. This test is employed to compare the viewpoints of study sample groups and identify significant differences among them. The test is based on comparing the level of statistical significance (Sig) with the level of significance (α) value. If the significance level (Sig) value is less than the significance level (α), this indicates that there are significant differences among the sample groups' perspectives.

1.10.10.1 Testing the Hypothesis

The hypothesis is formulated in the null and alternative forms as follow:

H0: There is no significant impact of Blockchain on the assessment of Smart contract risks.

H1: There is a significant impact of Blockchain on the assessment of Smart contract risks.

1.10.10.2 Descriptive Analysis of Data

The following Table (1-11) shows the frequencies, percentages, means, and standard deviations for questions (1 to 6) in the questionnaire related to The Third Sub-Hypothesis.

Table (1. 11)

Frequencies, Percentages, Means, and Standard Deviations for Third Sub-Hypothesis

Item	Completely agree	Agree	Neutral	Disagree	Totally disagree	Mean	Std. Deviation	General Trend
X31	94	92	19	6	-	4.2986	.75020	Completely agree
	44.5%	43.6%	9.0%	2.8%	-			
X32	108	77	22	4	-	4.3697	.74695	Completely agree
	51.2%	36.5%	10.4%	1.9%	-			
X33	103	80	20	8	-	4.3175	.79799	Completely agree
	48.8%	37.9%	9.5%	3.8%	-			
X34	91	92	21	5	2	4.2559	.80528	Agree
	43.1%	43.6%	10.0%	2.4%	.9%			
X35	107	82	18	4	-	4.3839	.72343	Completely agree
	50.7%	38.9%	8.5%	1.9%	-			

Item	Completely agree	Agree	Neutral	Disagree	Totally disagree	Mean	Std. Deviation	General Trend
X36	98	79	26	7	1	4.2607	.83570	Completely agree
	46.4%	37.4%	12.3%	3.3%	.5%			
Total	601	502	126	34	3	4.3143	0.7765	Completely agree
	47.4%	39.6%	9.9%	2.6%	0.2%			

Source: Results of the statistical analysis

Based on Table (1.11), it can be observed that the preliminary analysis of the means reveals a general inclination among the study sample to concur with the statements examining the third sub- hypothesis pertaining to impact of Blockchain on the assessment of Smart contract risks. The average mean of the statements reached (4.3143), which is considerably higher than the weighted average of the Likert scale. This indicates that, initially, the study sample leans towards agreeing with the statements that:

- The Audit team should check that Governance of smart contract.
- The Audit team should check that smart contracts are legally binding and enforceable.
- The Audit team should check that A smart contract must have all elements of the original paper contact regardless of originating in electronic format.
- The audit team should verify that the oracles associated with the contract are working properly.
- The audit team should verify that the implementation of the smart contract is actually implemented in a reality.
- The audit team should work together with the smart contract programmers from the start to ensure that there are no errors from the beginning.

1.10.10.4 Sign Test

In order to measure the impact of Smart contracts risk considerations of blockchain on the auditor's assessment of inherent risk, the sign test is employed due to the data for testing the third sub-hypothesis not conforming to a normal distribution. The test was conducted, and the results are presented in Table (5.28).

Table (1. 12)

Sign Test for Third Sub-Hypothesis

Binomial Test						
		Category	N	Observed Prop.	Test Prop.	Asymp. Sig. (2-tailed)
The impact of Smart contracts risk considerations of blockchain on the auditor's assessment of inherent risk	Group 1	<= 3.4	14	.07	.50	.000[a]
	Group 2	> 3.4	197	.93		
	Total		211	1.00		
a. Based on Z Approximation.						

Source: Results of the statistical analysis

Based on the information presented in Table (1.12), the researcher has determined that the level of statistical significance is (Sig =0.000), which is lower than the significance level of ($\alpha = 0.05$). This indicates that the null hypothesis, which states that there is no statistically significant impact of Blockchain on the assessment of Smart contracts risks, must be rejected. Instead, the alternative hypothesis is accepted, which states that there is a

statistically significant impact of Blockchain on the assessment of Smart contracts risks, with a confidence level of 95%.

1.10.10.5 Chi-Square Test

The following table (1.13) shows the results of the Chi-Square test, which was conducted to determine the sub-variables Smart contracts risk considerations of blockchain that hold the greatest impact on the auditor's assessment of inherent risk.

Table (1. 13)

Chi-Square Test Results for Third Sub-Hypothesis

Item	Chi - Square	Asymp. Sig.
1- The Audit team should check that Governance of smart contract.	124.5	.000
2- The Audit team should check that smart contracts are legally binding and enforceable.	132.0	.000
3- The Audit team should check that A smart contract must have all elements of the original paper contact regardless of originating in electronic format.	120.2	.000
4- The audit team should verify that the oracles associated with the contract are working properly.	196.9	.000
5- The audit team should verify that the implementation of the smart contract is actually implemented in a reality.	140.0	.000
6- The audit team should work together with the smart contract programmers from the start to ensure that there are no errors from the beginning.	181.7	.000

Source: Results of the statistical analysis

From the previous Table (1.13) the researcher finds that:

The level of statistical significance for all sub-variables (Sig = 0.000), which is less than the level of significance (α = 0.05)) and this means that:

- The Audit team should check that Governance of smart contract.
- The Audit team should check that smart contracts are legally binding and enforceable.
- The Audit team should check that A smart contract must have all elements of the original paper contact regardless of originating in electronic format.
- The audit team should verify that the oracles associated with the contract are working properly.
- The audit team should verify that the implementation of the smart contract is actually implemented in a reality.
- The audit team should work together with the smart contract programmers from the start to ensure that there are no errors from the beginning.

1.10.10.6 Kruskal Wallis Test

Fourth: determine the extent to which there are statistically significant differences in the average responses of the sample members for the impact of smart contracts risk considerations of blockchain on the auditor's assessment of inherent risk due to country, educational level, job, and years of work experience.

A-The results of Kruskal Wallis test according to Country

The significance of the difference between the opinions of the study sample is measured in terms of Country, as shown in the following table:

Table (1. 7)

Kruskal Wallis test according to Country for Third Sub-Hypothesis

	Country	N	Mean Rank	Chi-Square	Asymp. Sig.
The impact of Smart contracts risk considerations of blockchain on the auditor's assessment of inherent risk	Egypt	157	107.44	17.039	.254
	Saudi Arabia	9	116.94		
	Palestine	4	51.00		
	Kuwait	1	38.50		
	Iraq	23	108.28		
	Yemen	3	172.00		
	Jordan	4	86.75		
	Syria	2	54.00		
	Algeria	2	110.00		
	The UAE	1	2.00		
	Qatar	1	63.50		
	Tunis	1	63.50		
	Germany	1	187.50		
	Spain	1	63.50		
	USA	1	141.00		
	Total	211			

Source: Results of the statistical analysis

From the previous Table (1. 14): The researcher finds that the level of statistical significance is (Sig=0.254), which is greater than the level of significance (α =0.05), and therefore there are no statistically significant differences between the opinions of the study sample according to Country about the impact of Smart contracts risk considerations of blockchain on the auditor's assessment of inherent risk.

B-The results of Kruskal Wallis test according to Educational Level

The significance of the difference between the opinions of the study sample is measured in terms of Educational Level, as shown in the following table:

Table (1. 15)

Kruskal Wallis test according to Educational Level for Third Sub-Hypothesis

	Educational level	N	Mean Rank	Chi-Square	Asymp. Sig.
The impact of Smart contracts risk considerations of blockchain on the auditor's assessment of inherent risk	Bachelor	45	87.56	5.754	.218
	Diploma	8	124.62		
	master	63	110.21		
	PHD	85	110.27		
	Professional certificate	10	111.30		
	Total	211			

Source: Results of the statistical analysis

From the previous Table (1. 15): The researcher finds that the level of statistical significance is (Sig=0.218), which is greater than the level of significance (α =0.05), and therefore there are no statistically significant differences between the opinions of the study sample according to Educational Level about the impact of Smart contracts risk considerations of blockchain on the auditor's assessment of inherent risk.

C-The results of Kruskal Wallis test according to Job.

The significance of the difference between the opinions of the study sample is measured in terms of Job, as shown in the following table:

Table (1. 16)

Kruskal Wallis test according to Job for Third Sub-Hypothesis

	Job	N	Mean Rank	Chi-Square	Asymp. Sig.
The impact of Smart contracts risk considerations of blockchain on the auditor's assessment of inherent risk	Accountant	47	96.38	7.947	.094
	External auditor	20	138.88		
	Internal auditor	30	96.18		
	Academic in auditing and accounting	103	106.44		
	work in a blockchain-related field	11	109.95		
	Total	211			

Source: Results of the statistical analysis

From the previous Table (1. 16): The researcher finds that the level of statistical significance is (Sig=0.094), which is greater than the level of significance (α =0.05), and therefore there are no statistically significant differences between the opinions of the study sample according to Job about the impact of Smart contracts risk considerations of blockchain on the auditor's assessment of inherent risk.

D-The results of Kruskal Wallis test according to Work Experience

The significance of the difference between the opinions of the study sample is measured in terms of Work Experience, as shown in the following table:

Table (1. 17)

Kruskal Wallis test according to Work Experience for Third Sub-Hypothesis

	Years of work experience	N	Mean Rank	Chi-Square	Asymp. Sig.
The impact of Smart contracts risk considerations of blockchain on the auditor's assessment of inherent risk	less than one year	21	106.14	.209	.976
	from 1 year to less than 5 years	4	105.00		
	from 5 years to less than 10 years	55	109.13		
	from 10 years and more	131	104.69		
	Total	211			

Source: Results of the statistical analysis

From the previous Table (1. 17): The researcher finds that the level of statistical significance is (Sig=0.976), which is greater than the level of significance (α =0.05), and therefore there are no statistically significant differences between the opinions of the study sample according to Work Experience about the impact of Smart contracts risk considerations of blockchain on the auditor's assessment of inherent risk.

Based on the aforementioned findings, the researcher concludes that the null hypothesis, which suggests that there is no statistically significant

positive impact of Blockchain on the assessment of Smart contract risks, is rejected. On the other hand, the alternative hypothesis, which suggests that there is a significant impact of Blockchain on the assessment of Smart contract risks, is accepted with a confidence level of 95%.

1.11 Conclusion

In conclusion, this research study aimed to investigate the impact of smart contracts based on Blockchain on inherent risk assessment. The findings of the study, based on the analysis of 211 individuals using statistical methods, revealed a positive significant impact of Blockchain on the assessment of Smart contract risks. In light of these results, the researcher recommends emphasizing the teaching of blockchain technology and smart contracts in accounting and auditing courses, as well as developing auditing standards that provide clarification on how to audit systems based on blockchain technology. Furthermore, it is essential for auditors to be qualified in blockchain technology and smart contracts to meet the demands of the future. Finally, the study suggests several topics for future research, including smart contracts and audit evidence audit procedures.

References

AICPA. (2017). Blockchain Technology and the Future of Audit. Retrieved from.https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf. Access Date :09/04/2020

Beck, R. (2018). Beyond Bitcoin: The Rise of Blockchain World. *Computer, 51*(2), 54-58. doi:10.1109/MC.2018.1451660

Bizarro, P. A., & CISA, A. G. (2019). Blockchain Explained and Implications for Accountancy. *ISACA JOURNAL, Volume 1*. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/blockchain-explained-and-implications-for-accountancy

Dai, J., & Vasarhelyi, M. A. (2017). Toward Blockchain-Based Accounting and Assurance. *Journal of Information Systems, 31*(3), 5-21. doi:10.2308/isys-51804

Deloitte Development LLC. (2017).Blockchain risk management – Risk functions need to play an active role in shaping blockchain strategy. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-blockchain-risk-management.pdf.Access Date:10/02/2020

Deloitte. (2018b). Blockchain Legal implications,questions,opportunities and risks. Access Date:15/03/2020 Retrieved from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Tax/dttl-tax-global-blockchain-wp-march-2018.pdf

Deloitte. (2019b). An internal auditor's guide to Blockchain: Blurring the line between physical and digital. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-blockchain-for-internal-auditors.pdf.7 .Access date :07 /04/2020

Fuller, S. H., & Markelevich, A. (2020). Should accountants care about Blockchain? *Journal of Corporate Accounting & Finance, 31*(2), 34-46. doi:https://doi.org/10.1002/jcaf.22424

Gantz, S. D., & Philpott, D. R. (2013). Chapter 3 - Thinking About Risk. In S. D. Gantz & D. R. Philpott (Eds.), FISMA and the Risk Management Framework (pp. 53-78): Syngress.

Gupta, M. (2020). Blockchain for dummies: NJ: John Wiley & Sons. Investopedia.com. Blockchain explained. Retrieved from https://www.investopedia.com/terms/b/blockchain.asp. Access Date:20/02/2020

ISACA. (2019). Blockchain Preparation Audit Program.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. Future Generation Computer Systems, 107, 841-853. doi:10.1016/j.future.2017.08.020

Liu, M., Wu, K., & Xu, J. J. (2019). How Will Blockchain Technology Impact Auditing and Accounting: Permissionless versus Permissioned Blockchain. Current Issues in Auditing, 13(2), A19-A29. doi:10.2308/ciia-52540

López Vivar, A., Castedo, A. T., Sandoval Orozco, A. L., & García Villalba, L. J. (2020). An Analysis of Smart Contracts Security Threats Alongside Existing Solutions. *Entropy, 22*(2).

McMillan, M. (2017). Smart contracts: Legal and regulatory challenges of smart contracts. Access Date:24/03/2021 Retrieved from https://www.linkedin.com/pulse/smart-contracts-legal-regulatory-challenges-matthew-mcmillan/

Mense, A., & Flatscher, M. (2018). Security vulnerabilities in ethereum smart contracts. Paper presented at the Proceedings of the 20th International Conference on Information Integration and Web-based Applications & Services.

Morganti, G., Schiavone, E., & Bondavalli, A. (2018). Risk Assessment of Blockchain Technology. Paper presented at the 2018 Eighth Latin-American Symposium on Dependable Computing (LADC).

Prewett, K. W., Prescott, G. L., & Phillips, K. (2019). Blockchain adoption is inevitable—Barriers and risks remain. Journal of Corporate Accounting Finance.

Rozario, A. M., & Vasarhelyi, M. A. (2018). Auditing with Smart Contracts. *the international journal of digital accounting research*, 1-27. doi:10.4192/1577-8517-v18_1

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences, 9*(9), 1788.

Schulpen, R. R. W. H. G. (2018). *Smart contracts in the Netherlands - . Retrieved 26 October 2019*. University of Tilburg. Retrieved from http://arno.uvt.nl/show.cgi?fid=146860

Shah, P. (2019). Part I: Smart Contracts: Evolution, Benefits, Risks and Challenges. Access Date:16/03/2021 Retrieved from https://www.entrepreneur.com/article/332405

Vasile, S. L. C., & Neal, M. (2021). Blockchain & Cryptocurrency Regulation 2021. 12 Legal issues surrounding the use of smart contracts Retrieved from https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/12-legal-issues-surrounding-the-use-of-smart-contracts

Vincent, N. E., & Barkhi, R. (2020). Evaluating Blockchain Using COSO. *Current Issues in Auditing, 15*(1), A57-A71. doi:10.2308/ciia-2019-509

Wang, H., Zheng, Z., Xie, S., Dai, H. N., & Chen, X. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services, 14*(4). doi:10.1504/ijwgs.2018.10016848

White, B. S., King, C. G., & Holladay, J. (2019). Blockchain security risk assessment and the auditor. *Journal of Corporate Accounting & Finance*. doi:10.1002/jcaf.22433

White, B., & King, C. (2019). Blockchain Risk Assessment Implications Access Date:16/5/2020 Retrieved from https://acua.org/College-

and-University-Auditor-Journal/Summer/Blockchain-Risk-Assessment-Implications?

World Economic Forum. (2020). Legal and Regulatory Compliance. Access Date:19/03/2020 Retrieved from https://widgets.weforum.org/blockchain-toolkit/pdf/legal-and-regulatory-compliance.pdf

Zamani, E., He, Y., & Phillips, M. (2018). On the Security Risks of the Blockchain. Journal of Computer Information Systems, 1-12. doi:10.1080/08874417.2018.1538709

Zapotochnyi, A. (2016). What Are Smart Contracts? [Ultimate Beginner's Guide to Smart Contracts]. Blockgeeks; blockgeeks.com. https://blockgeeks.com/guides/smart-contracts/

Appendix:

Kafrelsheikh University

Faculty of Commerce

Accounting Department

Questionnaire Form

Dear sir,……

Impact of Blockchain-based Smart Contracts on Inherent Risk Assessment :With A Field Study

:With A field study

The Research aims to identify Impact of Blockchain-based Smart Contracts on Inherent Risk Assessment

That is, by identifying the risks associated with this technology that companies that use Blockchain in their electronic systems face, as well as the extent of its impact on auditors' procedures for assessing those risks.

In light of the challenges facing the auditing profession in light of the Fourth Industrial Revolution, the most crucial of which is Blockchain technology, your active participation in this survey is required and vital.

The researcher thanks you for your cooperation, and at the same time that he asks you to answer the questions on the list, he confirms that your responses will be kept completely confidential and used solely for scientific research purposes, and that the results of this study will be made available to you after completion if you request it.

Yours sincerely,

The Researcher

First: Some terms used in the questionnaire:

PricewaterhouseCoopers (PWC) in their report "Making sense of bitcoin, cryptocurrency, and blockchain "described blockchain as a decentralized ledger of all transactions across a peer-to-peer network. Using this technology, participants can confirm transactions without a need for a central clearing authority.

According to Deloitte the inherent risks related to blockchain technology can be classified under three categories as follows:

A-Standard risk considerations are risks that are considered common to all the blockchain projects. It includes:

1. **Strategic risk**
2. **Business continuity risk**
3. **Reputational risk**
4. **Information security risk**
5. **Regulatory risk**
6. **Operational and IT risks**
7. **Contractual risk**
8. **Supplier risks**

B- Value transfer risk considerations

With decentralization, peers can now transfer information without the need of any central authority. This new approach has the ability to change how businesses operate, but not without risks. It includes:

1. **Consensus protocol risk:** Several such cryptographic protocols are used to achieve consensus among participant nodes for updating the blockchain ledger. Each such protocol will have to be evaluated.
2. **Key management risk:** Digital assets could become irretrievable in the case of accidental loss or private key theft, especially given the lack of a single controller or a potential escalation point within the framework.
3. **Data confidentiality risk**
4. **Liquidity risk**

C-Smart contract risk considerations

Smart contracts are at the core of any enterprise blockchain. It helps businesses automate or transform business logic into reality. They can be used to do financial and legal agreements within the network. Their complexity and importance bring in blockchain business risks with it. After all, it is all about mapping the business logic digitally. It includes:

1. **Business and regulatory risks**
2. **Legal liability**
3. **Information security risks**

Audit teams usually comprise the audit partner, senior manager/manager, audit senior, audit staff, and specialists.it helps management achieve its objectives by evaluating the risk and control environment.

First: Demographic data

1-Name (optional):…….
2-Country:……..

3-Educational Level:……

Bachelor	Diploma	Master	PHD	Professional certificate

4-In case of obtaining a professional certificate (please specify the name of the certificate)

CPA	CIA	CMA	CFA	CISA	ACCA	Other

5-Job

accountant	External Auditor	Internal auditor	Academic in Auditing and Accounting	work in a blockchain-related field

6-If you work in accounting and auditing firm, previously or currently, is it considered a

Big Four	Non-Big Four

7-In the case of working <u>in a field related to blockchain</u>, please mention the name of the job?

8-How many years of work experience do you have

Less than 1 year	Between 1-5 years	Between 5-10 years	More than 10 years

Second: Questionnaire

You should determine the extent to which you agree with the following:

Topic:

The impact of Smart contracts risk considerations of blockchain on the auditor's assessment of inherent risk.

#	Statement	Completely agree	Agree	Neutral	Disagree	Totally disagree
1	The Audit team should check that Governance of smart contract.					
2	The Audit team should check that smart contracts are legally binding and enforceable.					
3	The Audit team should check that A smart contract must have all elements of the original paper contact regardless of originating in electronic format.					
4	The audit team should verify that the oracles associated with the contract are working properly.					

#	Statement	Completely agree	Agree	Neutral	Disagree	Totally disagree
5	**The audit team should verify that the implementation of the smart contract is actually implemented in a reality.**					
6	**The audit team should work together with the smart contract programmers from the start to ensure that there are no errors from the beginning.**					

Do you want to add any suggestions or other points?
