EBU European Business University Luxembourg

EUROPEAN BUSINESS UNIVERSITY OF LUXEMBOURG

BLOCKCHAIN-BASED AUDITING: A QUALITATIVE RESEARCH INTO THE SUITABILITY OF BLOCKCHAIN-BASED AUDITING TO ELIMINATE WEAKNESSES OF CONTEMPORARY AUDITING, THEIR EFFECTIVENESS ON AUDITING OF ACCOUNTS RECEIVABLE, AND COMPLIANCE TOWARD GAAS STANDARD AU-C 505

By
Markus G. Selg
Master of Science

A dissertation submitted in partial fulfillment of the requirements for the degree of
Doctor of Business Administration

Graduate School of Business Administration

Supervisor: Prof. Shachmurove
Professor of Economics and Business at the City College and the Graduate Center of the City University of New York

2023

DECLARATION

I, Markus Selg, declare that

(i) The research reported in this dissertation, except where otherwise indicated, is my original research.

(ii) This dissertation has not been submitted for any degree or examination at any other university.

(iii) This dissertation does not contain other persons' data, pictures, graphs, or additional information unless specifically acknowledged as being sourced from other persons.

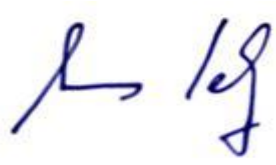
(iv) This dissertation does not contain other persons' writing unless specifically acknowledged as being sourced from other researchers.

(v) Where other written sources have been quoted, then:
a) their words have been re-written, but the general information attributed to them has been referenced;
b) where their exact words have been used, their writing has been placed inside quotation marks and referenced.

(vi) Where I have reproduced a publication of which I am the author, co-author, or editor, I have indicated in detail which part of the publication was actually written by myself alone and have fully referenced such publications.

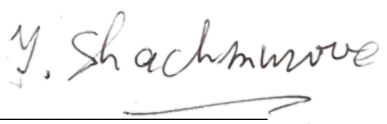
(vii) This dissertation/thesis does not contain text, graphics, or tables copied and pasted from the Internet unless specifically acknowledged, and the source is detailed in the dissertation/thesis and in the references´ sections.

Signed:



_____ 03/31/2023

Signature Markus Selg Date



_____ 03/31/2023

Signature Supervisor Date

ACKNOWLEDGEMENTS

First and foremost, I am extremely grateful to my supervisor Prof. Shachmurove for his valuable advice and continence during my DBA study. Furthermore, I want to thank Dr. Mulli, who motivated me to perform research into blockchain technology. Their immense knowledge has encouraged me in all the time of my academic study and daily life. I also would like to thank Prof. Joo, who advised me on the conception of the research methodology and supported the dissertation project with a professional review. Lastly, I want to thank my family for the inspiration to enter the DBA studies and the support in establishing the staying power to work consistently on the doctoral thesis.

ABSTRACT

As a consequence of advancing digitalization, public accounting firms must adapt and refine their business models by offering digitalized auditing and consulting services. In this context, the doctoral thesis is researching the characteristics of blockchain technology and its suitability for auditing. Further analysis is made on the ability of blockchains to eliminate weaknesses of contemporary auditing. In particular, the balance sheet position accounts receivable is researched, if blockchain-based auditing provides higher efficiency to replace traditional substantive auditing procedures of requesting external confirmations. As audits have to be performed in compliance with a codified audit framework, compliance with blockchain-based auditing by the example of accounts receivable is evaluated if it complies with the requirements of GAAS audit standard AU-C 505. Research of the doctoral thesis was performed by a qualitative approach based on a critical literature review. The results of the literature research were verified with primary data collected through interviews. In conclusion, blockchains are suitable tools for auditing purposes. Due to consensus mechanisms and characteristics, blockchains are highly efficient and effective for audit procedures. They provide a high potential to eliminate traditional auditing weaknesses and to disrupt the audit profession. Auditors must rethink their role in a future blockchain-based audit environment, whereas adequate audit frameworks and standards for blockchain-based auditing must be codified.

Keywords: Accounts receivable, audit weaknesses, blockchain technology, US GAAS

Table of Content

List of Tables

Table

List of Figures

Figure

CHAPTER I: INTRODUCTION

Chapter one introduces the problem, context, background of the research, statement of the problem, purpose statement, rationale for the study, dissertation outline, research questions, and objectives.

1 Introduction to the Problem

The doctoral research aims to analyze the suitability of blockchains for audit purposes, to evaluate the potential of blockchains to eliminate weaknesses of current manual audit procedures, auditing accounts receivable with blockchains, and potential compliance of blockchain-based auditing of accounts receivable toward GAAS audit standard AU-C 505 "External confirmations" (AICPA, 2012b). Traditional risk-oriented substantive audit procedures are based on costly, time-consuming, and work-intensive sampling methods that provide reasonable but not absolute assurance whether financial statements are free of material misstatement (AICPA, 1989). AU-C 505 does not guide blockchains (AICPA, 2012b). Under the current GAAS, no auditing standards for blockchain-based auditing exist (Alarcon & Ng, 2018). Thus, a literature gap exists.

As these issues are worth further exploration, the researcher collected primary data from interviews and secondary data through a detailed and critical literature review. The study adds knowledge to the academic body, standard setting, regulation, and audit practice as it provides guidelines for public accounting firms on implementing and operating blockchain-based auditing in their businesses. The study offers an outlook on future research in auditing with blockchains. It is a blueprint of the potential future blockchain audit standard toward accounts receivable.

2 Background, Context, and Theoretical Framework

2.1 Background

Auditors gather audit evidence by risk-oriented sampling methods covering only a fraction of the accounting data population (Wang et al., 2020). Due to sampling limitations in contrast to auditing whole populations, risks remain with material misstatements and fraud in financial statements remaining undiscovered (Barandi et al., 2020). Misstatements in financial statements can result from either fraud or error (AICPA, 2012a). Key risks are often identified only weeks or months after the balance sheet date (Byrnes et al., 2018). Auditing accounts receivable requires effortful and time-consuming requests for external confirmations from the auditee customers, with relatively low response rates (Byrnes et al., 2018). Thus, contemporary audit procedures entail potential weaknesses (Cheng & Huang, 2019).

Today, blockchain technology is spreading rapidly toward the audit profession, which can impact and disrupt the economy in a way not seen since the early days of the internet (Lombardi et al., 2022). Auditing with blockchains can significantly increase the speed of transactions and audit quality, while fraud risks in financial reporting may decrease (Wang & Kogan, 2018). As data under audit face cybersecurity risks and the complexity and amount of business transactions rise, public accounting firms shall transform their audit approach into automated and tool-based auditing procedures such as smart audit procedures by blockchains (Rozario & Vasarhelyi, 2018). Blockchain-based auditing with smart contracts can solve trust problems and traditional auditing procedures' inefficiencies (Fan et al., 2020).

A prerequisite to efficiently operating blockchains provides an appropriate IT architecture (Vishnia & Peters, 2020). The architecture must encompass the

confidentiality and security of the auditee's data (De Andrés & Lorca, 2021). It must enhance controls among different client processes as supply chains or financial services and improve collaboration among auditees and regulators (Vincent et al., 2020). However, financial statements in a blockchain environment must comply with GAAS standards and GAAP principles (Barandi et al., 2020). No audit standards under GAAS exist for blockchain-based auditing (Elommal & Manita, 2022), whereas AU-C 505 contains manual audit procedures to receive third-party confirmations (AICPA, 2012b) that do not address audit procedures with blockchains.

2.2 Context

The research aims to analyze the suitability of blockchains in auditing and their potential to eliminate weaknesses of risk-oriented manual audit procedures. The study affects public accounting firms, auditees, regulators, standard setters, and the interested public. The study examines the research problem and the literature gaps through primary data from 22 interviews and secondary data from an in-depth and critical literature review from 2017 to 2022.

2.3 Theoretical Framework

The thesis incorporated the two theoretical frameworks. GAAS audit standards constitute the audit framework (AICPA, 2001). GAAS audit standards consist of general standards, fieldwork, and reporting standards (AICPA, 2001). See Appendix C for further details. Blockchains, the second framework, includes infrastructure and libraries (Qasim et al., 2020). Blockchains consist of decentralized infrastructure (Puthal et al., 2018). The network infrastructure consists of nodes and software that run on a peer-to-peer network (Attia et al., 2019).

3. Problem Statement

The audit profession has been shocked by recent and more distant past scandals. In 2001, the huge accounting fraud scandal caused by Enron in collaboration with the large public accounting firm Arthur Andersen and in 2002 by WorldCom undermined public confidence in the accounting rules under the US GAAP and the reliability of the audit work by a large public accounting firm (Carnegie & Napier, 2010). Another gross accounting fraud resulted from the German firm Wirecard in 2020, whereas the public accounting firm EY claimed to have been deceived by the client about fraudulent and invented business activities (Engelen, 2021). Beneath such large scandals, relevant compliance issues concerning, in particular, small public accounting firms regularly identified by yearly PCAOB peer review inspections refer very often to impaired independence of the auditors, lack of due professional care when performing the audits, and inappropriate quality reviews (Guo et al., 2020).

It is yet to be discovered if blockchain technology suits auditing purposes. Traditional audits due to risk-oriented sampling methods, periodic auditing, high costs, heavy workload, large audit teams, and requirements for external confirmations provide several areas for improvement. Based on the researcher's experience, public accounting firms tend to accept material weaknesses of the auditee's internal controls and processes to keep the audit mandate. From the background of these audit weaknesses, the study intends to articulate the superiority of blockchain-based audits. By exploring continuous audits with smart audit procedures, additional periodic audits on blockchains beneath ongoing procedures, and audits of the ICS, the thesis outlines how to eliminate the weaknesses, as mentioned earlier. Finally, an outlook is given on the areas for future research.

4. Purpose of the Study

The purpose of the study is to answer the research questions by exploring blockchain principles toward their suitability for audit purposes, to evaluate how blockchains contribute to eliminating weaknesses of traditional auditing in general and on accounts receivable, and to analyze potential compliance toward GAAS standard AU-C 505 when auditing accounts receivable with blockchains. A combined GAAS and a blockchain framework provide guidelines to answer the research questions. They support the analysis and interpretation of the results of blockchain-based auditing.

The methodology follows Saunders's research onion model (Saunders et al., 2019). The qualitative study adheres to the theory of positivism, as it enables the researcher to operate in an observable social reality to generate law-like generalizations and produce detailed and accurate knowledge (Saunders et al., 2019). The approach to theory development considers inductive research logic (Mayan, 2016). The methodological choice includes primary data from interviews and a literature review to obtain secondary data (Morse & Richards, 2013).

The research strategy observes ethnography, a form of field research that seeks to learn the culture of a particular setting or environment (Saunders et al., 2019). At the same time, it relies on the researcher's observation through fieldwork as semi-structured interviews (Saunders et al., 2019). The target population for the interviews shall consist of experienced auditors focusing on IT-related auditing and experience with blockchains. The geographic location of the panelists will be Europe and the USA.

5. Research Questions

Based on the identified problems and purpose of the study, the research raised three research questions that scrutinize the suitability of blockchains for auditing, the ability of

blockchains to eliminate weaknesses of contemporary auditing towards auditing accounts receivable, and compliance of blockchain-based auditing on AU-C 505.

The following research questions guide this qualitative study:

Research Question 1

How must blockchain technology be designed to serve as a suitable digital tool for auditing?

Research Question 2

How do blockchain-based audit procedures eliminate weaknesses of manual and semi-manual auditing and requirements for external confirmations?

Research Question 3

How is blockchain-based auditing toward accounts receivable compliant with GAAS standard AU-C 505?

6. Rationale and Significance of the Study

6.1 Rationale for the Study

Traditional audit procedures focus on risk-oriented manual and semi-manual sampling methods to examine audit clients' transactions, assess the risk of material misstatements or fraud in the financial statement, and express an audit opinion thereon (AICPA, 2016; Soonawalla & Stroehle, 2022). Several authors, such as Lombardi et al. (2021), stressed these audit weaknesses (Lombardi et al., 2022). According to the standards setters AICPA and CPA Canada, blockchain technology will highly impact the performing of financial audits and other processes that require review and confirmation services (AICPA & CPA Canada, 2017). The researcher is aware of these weaknesses and understands what new audit technologies and procedures may contribute to eliminating these weaknesses by improving audit quality and efficiency. Further considerations of the

researcher concerned the issue of auditing with blockchains will comply with existing GAAS.

6.2 Significance of the Study

Blockchains support digital audit procedures on financial statement data (He & Chen, 2021). Blockchain-based auditing of the balance sheet position accounts receivable is not compliant with GAAS audit standard AU-C 505. This audit standard contains manual procedures to request the auditee's customers to confirm by verifying balances of accounts receivable (Flood, 2021). Audit standard AU-C 505 does not regulate continuous audit procedures with smart audit tools in blockchains (Lombardi et al., 2022). Thus, a research gap exists in this matter. The identified research gap is of special interest to standard setters. They become aware of the need to codify new audit standards or revise existing standards to enable regular audits with blockchains. Referring to the gap on AU-C 505, the thesis research adds knowledge on academia by analyzing this gap, as only a little information in the literature is available thereon. The audit profession capitalizes on the study as the thesis outlines the suitability of blockchains for auditing and provides guidance on the superiority of blockchain-based auditing. Thus, new business opportunities for public accounting firms based on digitalized audit procedures emerge.

7. Nature of the Study

The research sample of the thesis consists of 22 panelists. Each of the participants possesses many years of experience in auditing. In addition, most recipients are familiar with audits of IT systems. During their audit work, they came into contact with blockchain technology. The research was performed through individual interviews to answer the research question. The audit profession capitalizes on the study as the thesis outlines the suitability of blockchains for auditing and provides guidance on the superiority of

blockchain-based auditing. Thus, new business opportunities for public accounting firms based on digitalized audit procedures emerge.

8. Definition of Terms

The following terms were used operationally in this doctoral study.

Auditing: Audit means testing activities relating to transactions of firms, whereas the core concept of audit refers to independent third-party reviews of the authenticity and correctness of an entity's economic activities and compliance with laws and procedures (Cheng & Huang, 2019) while auditors express their opinion on the compliance of financial statements with IFRS, e.g. (Ånerud, 2007 as cited in Pamungkas et al., 2020).

Audit quality: Compliance with audit standards, professional principles and ethical code of conduct, auditing standards, and rules and procedures established by regulators to regulate the audit profession and to safeguard the independence and integrity of auditors (Montenegro & Brás, 2018).

Accounts Receivable: "Many companies sell goods or services to customers on account, which means the customer promises to pay in the future. When this happens, the amount of unpaid customer invoices goes into an account called accounts receivable." (Loughran, 2020, p. 15).

Blockchains: Gupta (2017) defines blockchain technology as a "shared, distributed ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible - a house, a car, cash, land - or intellectual property, such as patents, copyrights, or branding." (Gupta, 2017, p. 3). Bonyuet defined blockchains as a "(…) digital ledger that allows to capture transactions conducted among several parties on real-time and serves as a decentralized database where each participant keeps an identical copy of the ledger." (Bonyuet, 2020, p. 31).

Public Blockchains: "No one controls these completely decentralized blockchains. Anyone can join as a new node and perform operations, such as reading historical data and submitting transactions." (Zhong et al., 2020, p.8).

Private Blockchains: "In contrast with the public blockchain, the write rights of private blockchains are entirely in the hands of an organization, so all the nodes involved in the chain are strictly controlled. A private blockchain is also called a "permissioned blockchain," emphasizing data privacy, which is limited to user access within an enterprise" (Zhong et al., 2020, p.8).

Consortium Blockchains: "(…) a consortium blockchain operates under the leadership of a group of entities, thus enabling collaborative business transformation among organizations and innovative business models." (Dib et l., 2018).

9. Assumptions, Limitations, Delimitations

9.1 Assumptions

Auditors from Germany, Austria, Switzerland, the Czech Republic, the UK, and the USA provide answers to enable broad thematic coverage of the research topics. The researcher assumes that the panelists do not deceive the researcher with their answers. The participants answer all questions honestly and to the best of their ability, as the interviewees do not talk about ethical issues or disclose business secrets. The researcher can evaluate this assumption based on his knowledge of the facts and professional experience.

9.2 Limitations

The research limitations encompass the number of interview partners available, their geographic location, and the research method. The study is conducted as a qualitative method because of the novelty of the subject matter. The researcher did not identify

sufficient data sets for quantitative analysis. Thus, data collection by interviews provides the most appropriate method. The population is limited to up to 25 participants (Mason, 2010). However, the number of participants is appropriate to reveal valid answers. Auditing with blockchains is a very complex topic new to most auditors and their firms. The interviewees were selected as they were very experienced auditors in IT-related audits. Auditors from the 20 largest UK and USA public accounting firms declined interview requests.

9.3 Delimitations

Delimitations of the research refer to the omission of GAAS in general, the sample of interviewees, and the time frame of research data. The analysis of blockchain-based auditing toward GAAS is limited to the audit standard AU-C 505, showing that audits with blockchains do not comply with this particular GAAS audit standard. The participants of the interviews consist of experienced auditors acquainted by professional contacts with the researcher or persons affiliated, limiting the population. Because of the timeliness requirements of the research, most of the secondary data that formed the basis for the literature review was collected from 2017 to 2022, when the most relevant literature on blockchain-based auditing was published.

10. Summary and Organization of the Study

The research problem deals with the suitability of blockchains for auditing and eliminating weaknesses from traditional auditing due to sole periodical audit procedures, risk-oriented audit sampling, and high costs and low efficiency from manual audit procedures (Cheng & Huang, 2019). Blockchains can eliminate these weaknesses by continuously auditing entire populations in real-time (Tiran-Tudor et al., 2021), especially toward accounts receivable (Wang & Kogan, 2018). The study's theoretical framework

relies on GAAS as an audit framework (AICPA, 2001) and blockchain framework (Qasim et al., 2020). As a problem, it is unknown if and when blockchains will replace traditional auditing (Schmitz & Leonie, 2019). Three research questions answer the problem statement. The study's methodology is qualitative (Poucher et al., 2020). The study's limitations concern the geographical restriction mostly on European participants. Delimitations refer to the number of interviewees and the period to perform the literature review.

The following chapter presents the theoretical and conceptual framework, an in-depth and critical literature review on basic features of blockchain technology, blockchain-based auditing procedures, their advantages in contrast to traditional manual audit procedures, auditing of accounts receivable with blockchains to render external confirmations obsolete, and potential compliance of auditing accounts receivable with blockchains towards GAAs audit standard AU-C 505. Chapter 3 describes the study's research methodology, design, and data analysis procedures. Chapter 4 describes the results from the interviews, the data analysis performed, and a written summary of the research results. Finally, Chapter 5 will contain discussions and conclusions on the results of the interviews by facing them with the findings from the literature review and motivates future research and a potential continuation of the study.

CHAPTER II: LITERATURE REVIEW

Chapter two includes a critical literature review to collect secondary data from the existing literature that provides the basis to gain a comprehensive understanding of a specific topic.

1 Introduction to the Literature Review

1.1 Purpose of the Literature Review

The literature review aims to explore critically and in-depth if blockchain technology is a suitable tool to eliminate the weaknesses of traditional audits if blockchain-based auditing with smart audit tools in general and in particular by the example of accounts receivable is superior to traditional manual and semi-manual audit procedures, and if blockchain-based auditing on accounts receivable is compliant within the audit standard of AU-C 505. The literature review adds knowledge to academia, standard setters, and the audit profession. It is performed by researching articles in renowned journals covering blockchain-based audits, publications from audit standard setters, audit standards, conference papers, and large accounting firms.

1.2 Organization of Chapter Two

Paragraph 1.3 describes the procedures for performing the literature review. Paragraph 2.1 discusses the theoretical framework, while paragraph 2.2 includes the conceptual framework. The structure of the literature review and presenting the results under paragraph 3 follow the research questions. Characteristics and the functionality of blockchains are the content of paragraph 3.1, whereas paragraph 3.2 discusses the potential of blockchain-based auditing to eliminate weaknesses of traditional auditing. Paragraph 3.3 analyzes the potential compliance of blockchain-based auditing through

the accounts receivable example toward GAAS audit standard AU-C 505. Paragraph 3.4 presents a summary of key points revealed by the literature review.

1.3 Performing the Literature Review

The literature review presents an essential component of the research process and assists in establishing a theoretical framework (Snyder, 2019). The literature review covers the period from 2017 to 2022. Google Scholar was the source for most journal articles as it contains a broad range of scholarly reviewed articles from various journals. The systematic literature review uses keywords (Park & Jeong, 2019). The literature reviewed focuses on articles from renowned journals on blockchain-based auditing to investigate potential compliance gaps for blockchain-based audits of accounts receivable towards AU-C 505 publications from standard setters, and related GAAS audit standards were analyzed. Sampling the literature research to answer the three research questions is done by specific search terms such as "accounts receivable, AICPA, AU-C 505, audit weaknesses, blockchain architecture, blockchain audit standards, blockchain-based auditing, blockchain characteristics, compliance of blockchain-based auditing, continuous auditing, encryption, external confirmations, GAAS, hashing, Merkle tree, smart contracts, smart audit procedures". The software ATLAS.ti performs the analysis of results from the systematic literature review in the form of content analysis (Kalpokas & Radivojevic, 2021). A content analysis evaluates data from the literature review to classify the data by searching for texts where the relevant topic appears (Zakaria et al., 2015).

The literature review provides the basis to gain a comprehensive understanding of a specific topic. The research follows O'Leary's approach that divides the literature research into four steps:

- Find it: Identify the relevant literature types by using the relevant resources (journals, articles, books),
- Manage it: To work efficiently on the available literature by skilled reading techniques and the making of marks and notations,
- Use it: Choosing the research topic, designing a research method, and developing suitable research questions,
- Review it: Ensure sufficient coverage of the relevant literature and understanding of the review's purpose (O'Leary, Z. 2004).

2. Theoretical Framework and Conceptual Framework

2.1 Theoretical Frameworks for Auditing and Blockchains

Theoretical frameworks that emerge from the literature review provide the structure that supports a research approach (Kivunja, 2018). The dissertation's theoretical framework comprises blockchains as technical infrastructure and basis (Ølnes & Jansen, 2018) and AU Section 150 that provides the GAAS (AICPA, 2001). The adequacy of theoretical frameworks is tested during the research approach (Saunders et al., 2019) by a review of the auditing and blockchain-related literature and the GAAS standards.

2.1.1 Theoretical Framework of Auditing

The theoretical audit framework provided by GAAS is codified in the AU Section 150 by AICPA (AICPA, 2001). GAAS is a set of systematic principles and guidelines that have to be followed principally by auditors when performing audits of financial

statements (AICPA, 2019). GAAS consists of ten audit standards that comprise three General Standards, three Standards of Fieldwork, and four Standards of Reporting (AICPA, 2001). General Standards require auditors to obtain adequate training, proficiency, an independent attitude toward the audit, and due professional care (AICPA, 2001).

Standards of fieldwork guide the conduct of the audit at the client's premises (AICPA, 2001). They contain rules for planning and supervising the audits, understanding internal controls, and obtaining appropriate evidential matters (AICPA, 2001). To adequately design auditing procedures' nature, extent, and timing, each auditor must understand audit clients' businesses. This includes the business' internal control systems and the clients' environments to estimate the potential risks for material misstatements in financial statements (AICPA, 2001). To express an audit opinion, auditors must collect sufficient and appropriate audit evidence (AICPA, 2001). Standards of Reporting require auditors to declare in the audit report if financial statements under audit are prepared according to the GAAS standards and principles (AICPA, 2001).

While performing an audit under the GAAS principles, auditors must exercise professional judgment by respecting risks and materiality aspects (AICPA, 2001). The following GAAS principles ensure that auditors perform accurate, consistent, and verifiable audits and generate audit reports of good quality (AICPA, 2019). According to AU-C Section 200, auditors must obtain reasonable assurance that financial statements are free from material misstatements and fairly presented in an applicable accounting framework such as US GAAP or IFRS (Flood, 2021).

Any deviation from the GAAS principles has to be examined and reported by the auditors, and how the departure fulfills GAAS principles (AICPA, 2001). Furthermore,

according to findings from audit procedures, auditors have to express an unmodified, qualified, or adverse opinion on the financial statements under audit (AICPA, 2001). If an audit opinion cannot be expressed, the auditor must provide a disclaimer stating the reasons for the declination of an opinion (AICPA, 2001). For further details of the ten audit standards that form GAAS, see Table A1.

2.1.2 Theoretical Framework for Blockchains

Blockchain frameworks consist of decentralized infrastructures (Puthal et al., 2018). The framework includes infrastructure and libraries to develop the relevant application (Qasim et al., 2020). The network infrastructure consists of nodes and software that runs on them in a peer-to-peer structure (Attia et al., 2019). The software provides functions and capabilities such as user identity, transaction details, consensus protocol, and controls for blockchain identity management (Raikwar et al., 2018). The client application interacts with the infrastructure, serves as an interface outside, and consists of the code (Qasim et al., 2020) that runs smart contracts (Attia et al., 2019).

2.2 Conceptual Framework

The conceptual framework defines the organization of research ideas to achieve the purpose of a research project (Shields et al., 2019).

2.2.1 Characteristics of the Conceptual Framework

The conceptual framework defines the organization of research ideas to achieve the purpose of a research project (Shields et al., 2019). It creates a frame for presenting the three research questions of the thesis that underlie the study, which is reported based on the research problem (McGaghie et al., 2001). It is developed during data collection by the literature review as it represents the findings from the literature and is refined during data analysis (Saunders et al., 2019). In contrast to the more abstract concept of

theoretical frameworks, the conceptual framework provides an operationalization of underlying theories and literature by examination of relationships among different research objects to provide a methodological research approach toward the dissertation topic (Baloch, 2011).

2.2.2 Research Topic

Blockchains provide suitable tools for audit procedures. Current manual and semi-manual audit procedures based on a risk-oriented audit approach with sampling methods show areas for improvement as audits cover only some populations of accounting-related data. Blockchains provide the potential to eliminate such weaknesses through a continuous audit approach with smart audit tools that inspect all performed transactions and related data on the blockchain almost in real-time. Investigating may reveal if blockchain-based auditing of accounts receivable, e.g., comply with current GAAS.

2.2.3 Thesis Statement

Applying blockchain technology in auditing leads to higher audit quality and significantly reduces the risk of overlooking material misstatements and fraud in financial statements. Smart audit tools will reduce high costs for work-intensive manual substantive audit procedures and the need for large audit teams. Blockchain-based auditing requires new or revised audit standards.

2.2.4 Synthesis of Literature Review

The findings from the literature review support the thesis statement. Traditional manual audit procedures are less efficient than automated blockchain-based auditing, as they cover all blockchain data and transactions. Auditing with blockchains on accounts receivable is not compliant with the current GAAS standard AU-C 505. Lombardi et al. (2021) summarized the existing literature on auditing with blockchains and found that the

disruption of blockchains toward the audit profession is in the initial stage (Lombardi et al., 2022). The application of smart contracts enabled automated auditing; thus, blockchains improve the audit quality of business information systems, transparency, and efficiency by saving time and preventing fraud (Lombardi et al., 2022).

2.2.5 Identified Variables from Literature Review

The independent variables identified from the literature review represent the blockchain principles of distributed database, transparency with pseudonymity, irreversibility of records, peer-to-peer transmission, and computational logic (Barandi et al., 2020). The dependent variable represents continuous auditing procedures, while reduced audit costs are a mediation variable (Barandi et al., 2020).

3. Review of the Literature

The purpose of the literature review is to comprehensively and critically explore the characteristics of blockchain technology toward their suitability for auditing, the ability of blockchain-based auditing in general and specific towards auditing of accounts receivable to eliminate weaknesses of current manual or semi-manual audit procedures, and potential compliance of blockchain-based auditing of accounts receivable with GAAS standard AU-C 505 critically. The scope comprises scholarly literature about blockchain-based auditing, mainly from 2017 to 2022. The literature review aims to reveal trends, concerns, and literature gaps.

3.1 Characteristics and Functionality of Blockchains

The chapter discusses the characteristics of blockchains, blockchain principles, blockchain architecture, security issues, different types of blockchains, blockchain user access management, alternative views on blockchains, and the relevance of the research for auditing purposes.

3.1.1 Introduction to Blockchains

The following chapters provide definitions of blockchains and an overview of basic concepts.

3.1.1.1 Blockchain Definitions

Alarcon and Ng (2018) define Blockchains as a chronologically linked series of secure data blocks forming a chain of hashed data blocks in a highly secure distributed database system (Alarcon & Ng, 2018). In blockchains, each block consists of a block header, the previous block's hash, timestamp, nonce, Merkle root, and the current block's hash (Peng et al., 2021). Thus, no block in a blockchain is independent, as new blocks depend on the previous blocks of the chain (Inghirami, 2019), while linking with the previous block's hash with encryption of the actual block prevents tampering (Alarcon & Ng, 2018; Puthal et al., 2018). Each server on the blockchain network holds an identic copy of the blockchain ledger containing all historical data (Inghirami, 2019). Nodes of blockchains are combined based on peer-to-peer networks, where participants can read information and initiate transactions (Khalaf & Abdulsahib, 2021).

3.1.1.2 Blockchain Characteristics

Adding a new block to an existing blockchain starts with the authorization and verification of transactions through the nodes of the blockchain that perform several predefined checks (Peng et al., 2020). No central authority is required to perform transactions between blockchain parties (Nair et al., 2020). Consensus protocols consist of a set of agreed-upon policies implemented by all nodes to authorize and verify new transactions and add new blocks to the blockchain (Ghiro et al., 2021). When nodes reach a consensus that transactions are valid, they are grouped with other transactions to form

a block registered in the distributed ledgers (Pahlajani et al., 2021), while new blocks receive a timestamp (Barenji, 2021).

Blocks are hashed and paired with another hash, re-hashed, re-paired, and hashed again to form a single hash called the Merkle Root (Peng et al., 2020). Data entered into the SHA-256 hash function also consists of a message digest of the previous block (Lu et al., 2020) to assure correctness (Bansal et al., 2021). Each block is linked to a predefined number of previous blocks and is authorized and verified before it is added to the blockchain, whereas no outside third party controls this process (Appelbaum & Smith, 2018). By including the block's output hash in the new block's hash encryption, blocks can be attached and locked to the blockchain (Lu et al., 2020).

Adding new blocks occurs in one direction (Woodside et al., 2017). Then a copy of the complete blockchain is automatically created and replicated to all nodes (Lu et al., 2020). After adding new blocks, they are rendered immutable, so it is almost impossible to alter or remove them from the blockchain (Lu et al., 2020). The immutability principle concerns blockchain data and the distributed ledger code (Lashkari & Musilek, 2021). Unless a majority of the users of the blockchain collude, performed transactions are immutable (Wang & Kogan, 2018).

Except for one participant who owns more than 51 percent of the blockchain, a 51 percent attack makes it possible to make changes to the blockchain without being detected (Aggarwal & Kumar, 2021). Changing data from previous blocks would cause a change in input data by creating a different message digest that breaks the cryptographic link to the previous blocks, and the blockchain participants would be alerted that the data has been altered (Mijoska & Ristevski, 2021). Blockchain transactions are always traceable by an audit trail and a complete history of all trades (Bonyuet, 2020), while all

approved transactions receive an ID number (Peng et al., 2020). Permanent cryptographic integrity checks help to ensure that a blockchain is not tampered with (Varma, 2019). All blockchain participants monitor the last block in a blockchain for integrity, which guards the entire blockchain (Jamil et al., 2020).

Due to the blockchain mechanisms and the distributed network structure of blockchain architectures, blockchain data remains accurate in case of attacks on some nodes (Da Xu et al., 2021). Potential intruders face complex consensus mechanisms, encryption, and hashing algorithms with highly complex security mechanisms, whereby cryptographic hashes and consensus protocols assure the consistency and immutability of the blockchain data (Alarcon & Ng, 2018). Thus, blockchains form a highly secure environment for auditing and accounting (Puthal et al., 2018).

3.1.2 Blockchain Principles

The five blockchain principles of distributed database, peer-to-peer transmission, transparency with pseudonymity, irreversibility of records, and computational logic constitute blockchain technology (Barandi et al., 2020).

3.1.2.1 Distributed Database

Distributed ledgers consist of consensus algorithms representing protocol agreements on single data values of distributed ledgers (dos Santos, 2019). They provide identically distributed blockchain data storage for all blockchain participants (Zeng et al., 2019), enabling only one authoritative copy of blockchain data (Howell & Potgieter, 2021). Blockchain data are stored and synchronized in such decentralized databases managed by a peer-to-peer network in which all users own identical copies of the data (Adam & Fazekas, 2021), whereby all data are arranged in chronological order (and stored in a chain structure with time stamps (Cheng & Huang, 2019). Recorded data in

distributed ledgers are stored immutably and permanently (Cao et al., 2018) and replicated among all blockchain participants almost in real-time on all network servers (Alarcon & Ng, 2018).

DLT enables the chronological recording of asymmetrically encrypted transactions in public or private ledgers by applying progressive algorithms and massive computational resources (Lashkari & Musilek, 2021). Asymmetric cryptography consists of two complementary encryption keys: a private key and a public key (Abreu et al., 2018), to decrypt data (Cheng & Huang, 2019). Public keys are publicly accessible, whereas private keys are only known to recipients of the message that can decrypt the data (Cheng & Huang, 2019). Private encryption keys protect blockchain data by cipher text, which transforms or encrypts data into a series of numbers of fixed-length respective hashes (Abreu et al., 2018). A public key is applied to turn the cyphered text back into readable data respectively to decipher it (DA Xu et al., 2021). Blockchains use the asymmetric cryptography system to check if user accounts correspond to the public cryptographic key and to authorize the transactions (Huang et al., 2019).

In summary, distributed databases contain all recorded transactions that are accessible to any blockchain participants (Lombardi et al., 2022). The appearance of smart contracts substantially changes potential applications of distributed ledgers, as integrating smart contracts into distributed ledgers significantly improves reliability, accountability, and transparency through automated transactions (Lashkari & Musilek, 2021). Distributed ledgers are suitable for auditing and may significantly impact the auditing industry (Schmitz & Leonie, 2019).

3.1.2.2 Peer-to-Peer Transmissions

Peer-to-peer networks provide the potential to support continuous auditing procedures (Barandi et al., 2020). Blockchain action is initiated by starting transactions, while nodes are notified on the peer-to-peer network and conceived by verifier nodes (Ghiro et al., 2021). Data is sent to the peer-to-peer network nodes, while nodes validate the transaction and the user's status by implemented consensus mechanisms (Carrara et al., 2020). If most nodes reach a consensus regarding the legality and appropriateness of transactions (Inghirami, 2019), a new block is added to the blockchain (Liu et al., 2019). Large nodes make blockchains tamper-proof when peer-to-peer networks expand (Lashkari & Musilek, 2021), but validation becomes time-consuming and expensive (Appelbaum & Smith, 2018).

3.1.2.3 Transparency with Pseudonymity

This feature is characteristic of permissionless blockchains (Alston et al., 2022). Distributed databases keep the identity of the participants anonymous by applying digital signatures (Andoni et al., 2019). The disadvantages of transparency with pseudonymity result in the auditee's refusal to store the firm's data in publicly accessible blockchain databases (Müller et al., 2022).

3.1.2.4 Irreversibility of Records

Blockchain data is protected by hashes (Zheng et al., 2019). A special reference links all blocks to the previous block (Homoliak et al., 2019). Hashing in blockchains is implemented as Merkle tree, a key encryption method to structure data to quickly and efficiently verify large amounts of data and information by transforming large numbers of transaction IDs into a code consisting of 64 characters (Bonsón & Bednárová, 2019). The Merkle root of a blockchain system is a derivative of hashes from the current block

and a preselected number of previous blocks or a preselected time frame (Appelbaum & Smith, 2018). Merkle trees contain the table of data origin hashes, while the root node of the Merkle tree links to the related blockchain transaction (Stetsenko & Khalimov, (2020). It is easy to verify if registered transactions have not been altered after recording (Ghiro et al., 2021). If data secured by hashes were modified, the hash value would be changed accordingly (Ortman, 2018). At the same time, it is almost impossible to decrypt the digest of data output by their ability to encrypt a large amount of data by generating a compressed set (Ortman, 2018). As long as the hash value is unchanged, related data is not altered or irreversible (Zheng et al., 2019). Blockchain ledgers are also immutable and resilient to tampering attacks as a proof of work mechanism validates the blockchain, whereas nodes that identify valid nonces provide it to all other nodes in the peer-to-peer network (Bhushan et al., 2021).

3.1.2.5 Computational Logic

Buterin (2014) defines smart contracts as "systems which automatically move digital assets according to arbitrary pre-specified rules." (Buterin (2014) as cited in Bonsón & Bednárová, (2019), p. 727). They comprise computational logic to perform transactions that fulfill pre-defined conditions (Hammoudeh et al., 2021). Smart contracts contain contractual terms and conditions about the ordered goods' quality, price, and location as business logic (Barenji & Montreuil, 2022). If transactions comply with terms and conditions, smart contracts execute transactions automatically (Zheng et al., 2020). Transactions and respective invoices are recorded and stored in accounts receivable ledgers at supplier firms (Farcane & Deliu, 2020). In case one of the rules in the smart contract does not comply, transactions are not authorized and completed (Mahindrakar & Joshi, 2020).

As an advantage of smart contracts, revenue recognition requires fewer corrections, and the automatization of documentation of accounting transactions reduces the verification of assets significantly, whereby accounting staff gets more time for performing analyses and reporting on the accounting items (Appelbaum & Smith, 2018). Trust, reliability, and data quality will increase due to the security mechanism of the blockchain (Alarcon & Ng, 2018). Costs for transactions and verification will decrease, and their application will reduce human error and fraud (Alarcon & Ng, 2018). No central authorities are required as trusted third parties to monitor and execute the rules of smart contracts (Bonsón & Bednárová, 2019). The access control system is implemented into smart contracts to protect the blockchain (Sultana et al., 2020).

To conclude, smart contracts enable blockchains to share databases among participants (Wang & Kogan, 2018) if transactions meet the pre-defined algorithm-based rules of smart contracts (Ji et al., 2022) without engaging any trusted third party (Khan et al., 2021b). The system declines the transactions if the information does not meet the pre-defined rules and requirements, thus smart contracts improve auditing quality and speed (Rozario & Vasarhelyi, 2018).

3.1.3 Blockchain Architecture

The following chapter analyzes the characteristics of blockchain architectures, segregation of blockchains into different layers, types of blockchains, user access management, changelogs, interoperability issues of blockchains, and cyber security of blockchains compared to ERP systems.

3.1.3.1 Overview of Blockchain Architecture

Blockchains require an appropriate IT architecture (Vishnia & Peters, 2020). Blockchain architectures must consider a decentralized peer-to-peer network node

(Vincent et al., 2020), and complex components such as consensus algorithms, cryptography (Gauthier & Brender, 2021), and aspects of scalability with increasing size or volume of transactions must be implemented into e (Khan et al., 2021a). The architecture requires a plan for linking all blockchain system components to integrate the requirements of auditees, auditors, regulators, and other stakeholders (Vincent et al., 2020). It must also respect compliance requirements towards laws, business rules, and regulations for auditing procedures and audit firms' requirements (Vincent et al., 2020).

Blockchain architectures consist of a block, chain, consensus protocol, miner, node, and transaction:

1. *Blocks* are data structures that store transactions distributed among all blockchain nodes.
2. *Chains* consist of sequences of blocks arranged in specific orders.
3. *Consensuses* consist of predefined rules and agreements for performing blockchain operations.
4. *Miners* are specific nodes engaged in verification processes before adding new blocks to the blockchain.
5. *Nodes* are computers located inside blockchain architecture.
6. *Transactions* provide records that serve the purpose of blockchains records, information, etc. (Pahlajani et al., 2019).

3.1.3.2 Considering Auditing Purposes

The blockchain architecture has to encompass the audit firms' and clients' business requirements (Dyball & Seethamraju, 2021). An adequate architecture consisting of a blockchain-based transaction processing system using a zero-knowledge proof method in a distributed ledger technology must ensure the confidentiality of data and records for

accounting and auditing purposes (Wang & Kogan, 2018). Blockchains must enable continuous auditing procedures by considering requirements for auditors' professional judgment (Barandi et al., 2020).

Blockchain architecture design must comply with audit assertions of occurrence, completeness, classification, cutoff, and accuracy to meet relevant audit objectives (Freiman et al., 2022). For audit firms collecting sufficient and appropriate audit evidence within a blockchain system is essential (Vincent et al., 2020). Clients need an IT environment that provides their data security, privacy, confidentiality, and immutability (Vincent et al., 2020), while audit clients and firms maintain identical copies of the distributed ledger with permanent access to the ledger (Bonsón & Bednárová, 2019).

3.1.3.3 Separation of Blockchain Systems into Different Layers

Wang et al. (2020) recommend separating blockchain systems into four layers daily business activities layer, blockchain data and server (network) layer, audit application service layer, and auditors" (Wang et al., 2020). All business activities of auditees shall take place in the daily business activities layer, where transactions are recognized as the flow of information, physical goods, capital, and cash, while unified data and related information of all transactions are routed through financial and accounting systems toward the network layer (Wang et al., 2020).

Transactions in the day-to-day business activities layer are verified among participants on the blockchain (Pimentel et al., 2021). After verification of transactions, smart contracts trigger transactions according to pre-defined logic (Feng et al., 2019). Network layers include network equipment, database, PC service layer, storage equipment, and consensus mechanisms. Transaction information storage occurs after transactions in the transaction pool located on the blockchain data and server layer (Zeng

& Zhang, 2019). Verification procedures involve the automated authenticity of transactions and the correctness of computerized bookkeeping (Rozario & Thomas, 2019).

The application service layer, regarded as the most important part of a blockchain-based auditing information system, provides the environment for real-time and continuous auditing as it covers auditing functions, an audit early warning system, a continuous monitoring system, an enterprise agreement analysis system, an analysis system for a suspicious transaction, a method for the collection of audit evidence and the audit reporting system (Wang et al., 2020). Continuous auditing towards the quality of financial data is performed in this layer before recording and immutable storage of transactions on the blockchain (Wang et al., 2020). Auditors log into the auditor's layer with electronic devices to perform audit procedures to supervise and inspect the audited client firm (Dewi, 2022). Smart auditing tools inspect all executed transactions while generating auditing reports on the blockchain (Schmitz & Leoni, 2019). The results of audits are packaged as fixed attachments with the timestamp and uploaded and recorded onto the blockchain (Wang et al., 2020).

3.1.3.4 Types of Blockchains

When establishing blockchain systems for auditing, decisions must arise about the most suitable type of blockchain (Wang et al., 2020). The following chapter describes the three blockchain types public, private, and consortium blockchains.

3.1.3.4.1 Public Blockchains

Public or permissionless blockchains follow the principle of decentralization (Zheng et al., 2019). Intermediaries or central authorities are obsolete in a permissionless blockchain (Lombardi et al., 2022). Permissionless blockchains are not controlled by one or several participants, as all participants are authorized to access all blockchain data

monitored by all users (Smith, 2015 as cited in Liu et al., 2019). In public ledgers, all records of transactions and consensus protocols are accessible to anybody; thus, all participants may authorize and verify transactions on the blockchain without implemented access controls for users, which may impair the security of distributed ledgers (Ghiro et al., 2021).

The major advantages of permissionless blockchains lay in their decentralization characteristics. All blockchain copies are permanently synchronized to keep data consistent and actual (Lombardi et al., 2022). Blockchain mechanisms ensure immutability, as any change to the blockchain would be inconsistent with copies of the other participants (Ismail et al., 2019). To counteract the lack of trust by providing adequate security, consensus protocols of permissionless ledgers impose strict conditions when verifying new transaction blocks (Ghiro et al., 2021). In contrast, disadvantages result from low transaction speed if many participants access the blockchain, and lack of data privacy, as all permissionless blockchain users have access to all data (Liu et al., 2019).

3.1.3.4.2 Private Blockchain

Private respective permissioned blockchains are controlled by a trusted center and characterized by centralization (Zheng et al., 2019). Permissioned blockchains focus on restrictions in membership and implemented control procedures, as individual roles, participants' access, and approval of new users lie under the control of the trusted center (AICPA & CPA Canada, 2017). At the same time, the trusted center grants authorized individuals access to the blockchain and rights to perform transactions, where the central organization rules strict control of nodes (Zheng et al., 2019).

These blockchains are not completely transparent, as the master copy is not accessible to all blockchain members (Crosby et al., 2016). Recorded transactions are encrypted by public and private encryption keys (Liu et al., 2019). Moreover, blockchain technology provides audit trails to research special items (Dasaklis et al., 2019). In conclusion, permissioned blockchains require a reliable consensus protocol to ensure trustworthiness and immutability due to the rights of the central authority (Ismail et al., 2019).

3.1.3.4.3 Consortium Blockchains

Consortium-respective federated blockchains are hybrid blockchains that combine elements of private and public blockchains (Dib et al., 2018) with partial decentralization of the federated database, while authorized institutions or organizations also have access to the blockchain (Zheng et al., 2019). Power in consortium blockchains is shared among the members (Dib et al., 2018). Dib et al. (2018) criticized that data immutability in consortium blockchains could be tampered with, although the majority of the participants (or miners) have reached a consensus on a transaction (Dib et al., 2018). To sum up, the advantages of federated blockchains lie in the control aspect, where a group of participants' respective nodes controls transactions, while a known number of nodes authorize transactions (Albaroodi & Anbar, 2022).

3.1.3.4.4 Summary of Blockchain Types

Establishing blockchain systems for auditing requires decisions about the most suitable type of blockchain (Wang et al., 2020). Permissioned and permissionless blockchains differ between authorized participants, consensus protocol execution, and shared database maintenance (Jayachandran, 2017 as cited in Bonsón & Bednárová, 2019). Due to confidentiality and data privacy, public blockchains are unsuitable tools for

recording accounting-related data and information, as all transactions in a public blockchain are visible to all participants without restrictions (Bonyuet, 2020). Permissionless blockchains proved to be disadvantageous for auditing purposes that no reversal of erroneous transactions is possible, and no authority verifies the ownership and the existence of blockchain data (Liu et al., 2019).

With access restrictions, implemented control procedures, security and privacy of data, and compliance with business and regulations, permissioned blockchains are more suitable for audit and accounting purposes than permissionless blockchains (Bonsón & Bednárová, 2019). Zheng et al. (2019) affirmed private blockchains as most suitable for auditing and accounting purposes (Zheng et al., 2019). In contrast, Liu et al. (2019) considered it critical when the central authority has the power to override blockchain mechanisms and information (Liu et al., 2019).

For security reasons, permissioned distributed ledger networks based on smart contracts with user account management as consensus protocols are preferable against permissionless blockchains (Bashir, 2020). As a disadvantage, permissioned blockchains face higher risks towards the credibility and integrity of the blockchain, as a central authority has privileges to override implemented rules of the blockchain system (Liu et al., 2019). Consortium blockchains that combine elements of private and public blockchains provide the highest disruptive potential for blockchain-based auditing, as auditors can access the auditors' and their customers' data (Zheng et al., 2019). Thus, the doctoral thesis focuses on this hybrid respective federated type of blockchain.

3.1.3.5 Interoperability of Blockchains

The interoperability of blockchains with other ERP or blockchain systems is critical (Kayıkcı & Subramanian, 2022). Currently, no single standard for blockchain

design is codified, and further research is needed on interoperability issues between blockchains (Hardjono et al., 2018). Different blockchain systems exhibit different transaction formats; no uniform transaction format exists between blockchains (Kan et al., 2018). The architecture of decentralized blockchain applications lacks interoperability, which means blockchain systems and existing technologies cannot be easily integrated into a consistent framework (Besançon et al., 2019). The inability of independent blockchain systems to communicate among themselves represents an inherent problem of distributed systems (Pillai et al., 2020). Decentralized blockchain applications have interoperability issues, as they cannot easily integrate into a unified framework due to architecture specifics (Besançon et al., 2019). A multi-tier architecture can help to improve communication between different blockchain systems (Jin et al., 2018).

3.1.3.6 Recording of Transaction and Changes in Changelogs

The infrastructure of blockchain systems must ensure secure logging to record all changes in changelogs (Putz et al., 2019). For traceability, immutability, security, non-repudiation, and privacy for clients and traceability, auditability, and automated auditing, changelogs connect the database tier to the application tier (Ahmad et al., 2019). Records are stored in changelogs in a systematic order and by date by adding the hash, a timestamp, and a signature, among others access (Vincent et al., 2020). To address security and privacy concerns and to reduce the data to be stored, only the hash is recorded in the changelog (Ismail et al., 2019).

The sender's digital signature and the transaction's origin ensure non-repudiation (Wang et al., 2021). After hashing the data towards the changelog, a transaction can no longer be modified (Ateniese et al., 2017). By digitally signing transactions by the preparer and submitting a hash of the changelog entries, it is linked to the blockchain

(Borah et al., 2020). Protecting changelogs with adequate data encryption and retaining them in-house can mitigate risks of unauthorized access or data leakage of sensitive information (Algarni et al., 2021). Changelogs create a traceable and immutable audit trail function for auditors (Vincent et al., 2020), as all changes to the blockchain are stored in the changelog (Oakley et al., 2021). They enable the identification of fraudulent actions toward the blockchain (Dujak & Sajter, 2019).

3.1.4 Cybersecurity of Blockchains versus ERP Systems

ERP systems integrate accounting and financial solutions for auditee's financial information processing (Faccia & Petratos, 2021). While ERP systems operate in a centralized architecture, blockchains use a distributed database to verify, store and organize transactions by incorporating a group of nodes (Farcane & Deliu, 2020). Unlike ERP systems, which have a high risk of tampering, blockchains distribute the process of transaction verification, storage, and organization among a group of computers to reduce the risk of tampering (Dai & Vasarhelyi, 2017).

Blockchains are expected to be deployed alongside existing ERP systems (Fuller & Markelevich, 2020). Blockchains operate automatically through smart contracts and offer the potential to reduce the costs of ERP systems significantly (Sokolov & Kolosov, 2018). Blockchains provide better security and authentication procedures as all nodes are up-to-date, whereas the data is immutable (Banerjee, 2018). The proof-of-work consensus of blockchain architecture that influences the speed of processing the transactions is responsible for ascertaining the integrity of blocks and preventing attached blocks may contain malicious data, whereby BFT, a consensus protocol, where just a set of authenticated devices' respective nodes within a network are selected, provides a promising technological alternative (Alfandi et al., 2020). To conclude, blockchains

provide a higher level of cybersecurity than ERP systems due to the decentralized infrastructure and implemented blockchain mechanisms (Dai & Vasarhelyi, 2017).

3.1.5 User Access Management for Blockchains

Blockchain systems require a basic authentication and authorization process regarding granting and revoking credentials for logging into the system, updating the blockchain, and performing transactions (Mikula & Jacobsen, 2018). Using blockchain technology to control access to personal data potentially supports compliance with GDPR (Cichosz et al., 2019). Data stored in the blockchain must be protected against unauthorized access (Mikula & Jacobsen, 2018). Smart contracts with dedicated access rules execute transactions autonomously on the blockchain (Yavari et al., 2020). Blockchains require dedicated user access management (Maesa et al., 2019; Mikula & Jacobsen, 2018).

3.1.6 Summary of Blockchain Technology´s Characteristics

3.1.6.1 Critical Perspectives on Blockchain Suitability for Audits

Several authors are identified by the literature review that provides a critical view of the suitability of blockchains for auditing purposes. Nordgren et al. (2019) complain about the high uncertainty toward blockchain applications, as very little real-world research has been performed so far (Nordgren et al., 2019). Furthermore, Nordgren et al. (2019) miss measures on how the existing technical systems can address the ever-increasing data and the number of transactions in blockchains (Nordgren et al., 2019) - for this reason, they question if blockchains indeed depict the most suitable technology to disrupt the audit industry (Nordgren et al., 2019).

Boireau (2018) criticizes the 51 percent attack; if one node or a group of participants controls more than 50 percent of the blockchain power, these nodes can

modify data or manipulate the blockchain to steal digital assets (Boireau, 2018). Sayeed & Marco-Gisbert affirm this issue (Sayeed & Marco-Gisbert, 2019). Graham and Sherwood (2021) are concerned that management assertions on financial statements blockchains could be impacted adversely by blockchains (Graham & Sherwood, 2021). Catalini & Tucker (2018) stress that, to some extent, blockchains potentially lack transparency as persons engaged in security breaches could remain anonymous (Catalini & Tucker, 2018).

Pillai outlines that federated blockchain systems often need help communicating correctly among themselves (Pillai et al., 2020). These issues lead to interoperability problems among blockchains and other ERP systems (Besançon et al., 2019). Graham & Sherwood (2021) emphasize that blockchain technology will likely play a significant role in auditing and accounting in the future; however, it remains to be determined in what way blockchains will be engaged in accounting and auditing (Graham & Sherwood, 2021). Some authors as Stinchcombe (2018), doubt that transactions in blockchains and the respective data are integer and accurate, whereas questions arise concerning responsibility for errors from smart contracts (Stinchcombe, 2018).

Further counterproductive issues for auditing procedures could result from a lack of standardization if different jurisdictions treat digital assets diverse (Accounting Blockchain Coalition Internal Controls Working Group, 2019, as cited in Egiyi & Okafor, 2021). Sarmah (2018) fault that challenges for the widespread employment of blockchains results from their complexity and irreversibility of records if reversal bookings are required (Sarmah, 2018). He also complains that the more nodes participate in the blockchain mechanisms to authorize and verify transactions, the slower the blockchain will operate (Sarmah, 2018).

Rozario and Vasarhelyi (2018) refuse permissionless blockchains to be applied for auditing purposes where all participants have access to all data, while confidentiality of financial data is not ensured; thus, permissionless blockchains are less suitable for auditing (Rozario & Vasarhelyi, 2018). Barandi et al. (2020) stress the risk of collusion in a permissioned blockchain with few participants (Barandi et al., 2020). Heo et al. (2021) point out that the security of blockchains may be significantly harmed if one weak point is exploited, resulting in enormous cybersecurity risks for all other participants (Heo et al., 2021). According to Puri et al. (2021), further security issues arise from hackers manipulating the blockchain code, which can lead to negative snowball effects (Puri et al., 2021).

3.1.6.2 Synthesis of Blockchain Suitability for Audits

Blockchains provide digital, distributed, and decentralized data structures that enable the development of transactional blocks that support digital transactions without requirements for a central authority (Lashkari & Musilek, 2021). Their features include distributed ledgers, time series data, consensus mechanisms, hashes, and asymmetric encryption (Cheng & Huang, 2019). Blockchain systems require a standardized blockchain framework to avoid interoperability issues (Hardjono et al., 2018).

DLT enables the recording of transactions in chronological order using encryption, and progressive algorithms, by applying massive computational resources in public or private types of ledgers (Lashkari & Musilek, 2021). Central authorities become obsolete, while recorded data are stored immutable, permanently, and tamper-proof in the distributed database (Lashkari & Musilek, 2021). In essence, blockchain technology represents a distributed repository of data whose contents are open to verification and authorization by each member with access to the chain (Graham & Sherwood, 2021).

After starting new transactions (Ghiro et al., 2021), most network nodes validate the transaction based on the implemented consensus mechanisms (Carrara et al., 2020). Suppose most peer-to-peer nodes reach a consensus on the appropriateness of transactions (Inghirami, 2019); data of encrypted and validated transactions are attached as a new block on the blockchain (Lashkari & Musilek, 2021). All participants of blockchains require an encryption key when uploading transactions in a transparent way on private or public blockchains (Müller et al., 2022).

Blockchain technology provides immutability of transactions, traceability, and transparency as promising features for auditing purposes (Gauthier & Brender, 2021). Irreversibility of records for purposes of audit (Das et al., 2022) is enabled by hash methods and decentralized blockchain consensus mechanisms (Stetsenko & Khalimov, (2020). Blockchain transactions, in general, are performed automatically with smart contracts, authorized and verified by consensus mechanisms, whereas fraudulent activities are easily detected in peer-to-peer networks (Sarmah, 2018). Smart contracts depict computer codes stored on a blockchain to execute transactions under pre-defined conditions without human intervention (Gans, 2019). Smart contracts provide the potential to reduce manual faults through automated validation and execution of blockchain transactions (Thakur et al., 2021).

Concerning suitable blockchain types, public blockchains provide a decentral structure (Zheng et al., 2019) without any central authority (Lombardi et al., 2022), while all data in a public blockchain is accessible to all participants with no access to management controls (Ghiro et al., 2021). Private blockchains are operated under the supervision of a central authority (Ismail et al., 2019), while the central authority has exclusive access to the master data (Crosby et al., 2016). For audit purposes, consortium

blockchains are the most suitable combinations of private and public blockchains (Wang et al., 2020); under the power of a central authority, transactions are verified and authorized by other blockchain participants. (Albaroodi & Anbar, 2022).

Blockchain technology provides authentication and authorization (Mikula & Jacobsen, 2018) for dedicated user access management (Cichosz et al., 2019), depending on the role of the participants (Copigneaux et al., 2020). Access Management on Blockchains is technically performed by smart contracts that grant or deny access (Yavari et al., 2020). Appropriate blockchain architecture supports the confidentiality of data and records for accounting and auditing purposes in distributed ledgers (Wang & Kogan, 2018). It enables logging all blockchain changes in changelogs (Putz et al., 2019), providing a valuable audit trail function for auditors (Oakley et al., 2021).

Furthermore, an appropriate architecture design facilitates continuous auditing procedures (Barandi et al., 2020) by implementing audit assertions of occurrence, completeness, classification, cutoff, and accuracy (Freiman et al., 2022). Consequently, the appropriate architecture gathers and collaborates among auditees, their auditors, their customers, auditors of the customers, and regulators (Vincent et al., 2020). Blockchain technology eliminates the requirement to rely on third parties outside the blockchain to assure the integrity and safety of transactional data (Demirkan et al., 2020).

Blockchain characteristics such as decentralization, immutability, near real-time reporting, audit trails, transparency, and accountability render blockchain technology an incredibly suitable tool for auditing (Rozario & Thomas, 2019). Traceable, immutable, secure, unarguably, and protected data render blockchains audible (Ahmad et al., 2019). The separation of blockchain systems into four different layers, the daily business activities layer, blockchain data, server (network) layer, audit application service layer,

and auditors' layer, helps to reduce communication and interoperability issues between different blockchain systems (Jin et al., 2018).

3.2 Blockchains Eliminate Weaknesses of Traditional Auditing

The following paragraphs discuss the superiority of blockchain-based audit procedures in contrast to traditional audits by eliminating weaknesses of manual audit procedures. The doctoral thesis is researching the suitability of blockchain technology for auditing procedures, in general, to eliminate weaknesses of contemporary auditing and to analyze if blockchain technology can improve audit quality, efficiency, and reliability (Farcane & Deliu, 2020). Applying the blockchain enables automated audits, shortening the audits' duration (Brender & Gauthier, 2018). Blockchain technology must comply with IFRS accounting requirements as comparability, relevance, reliability, understandability, timeliness, and true and fair view regarding accrual accounting and revenue recognition for accounts receivable (Zülch, 2020).

3.2.1 Audit Functions

The function of auditing is presented concerning the auditing procedures and regulations of the USA.

3.2.1.1 Definitions of Auditing

The external audit function is defined as follows:

"…audit refers to inspection or examination performed by someone other than the preparer or performer." (Graham & Sherwood, p. 118, 2021). "…external auditor contributes to proper accountability, especially considering that the intended function of the external audit is to lend credibility to financial reports." (Maama & Marimuthu, p. 476, 2021). "The audit function plays a crucial role not only to monitor managerial actions

but also to create a better information environment as well as providing a secondary source of assurance against corporate failures." (Soyemi et al., p. 46, 2021).

3.2.1.2 Characteristics of External Auditing

Audit firms are engaged by businesses subject to examination by laws and regulations (AICPA & CPA Canada, 2017). The role of external auditing is to confirm the true fair view of auditees´ financial statements, to evaluate whether the auditee's accounting has followed the relevant GAAP accounting standards in recording its business activities and whether amounts in the financial statements are materially correct (Graham & Sherwood, 2021). Auditee's managements make assertions about the financial statements, whereby external auditors check the appropriateness of these assertions (Graham & Sherwood, 2021).

Furthermore, auditors of public interest entities must understand the auditee's internal controls and assess potential fraud risks (Hamshari et al., 2021). They must report on the auditees' internal financial reporting controls if these controls operate effectively during the fiscal period under audit (Aksoy & Aksoy, 2020). Throughout an audit of financial statements, auditors and their teams perform substantive audit procedures to be able to assess to a reasonable degree of assurance whether financial statements are free from error or material misstatements (Vincent & Wilkins, 2020) while they must obtain sufficient and appropriate audit evidence through interviews, physical inspections, observations, third-party confirmations, examinations, and analytical procedures (Arefin, 2020). They also confirm amounts and disclosures of financial statements (Blanco et al., 2021).

Based on the audit results, external auditors express an opinion thereon whether financial statements are in all material respects compliant with the applicable financial

reporting framework (Palmrose & Kinney, 2018) and issue the audit report (Graham & Sherwood, 2021). Finally, the auditee transfers the auditor's report and the financial statements to the regulatory authority (Graham & Sherwood, 2021). Auditors' confidence in their abilities to successfully discuss and defend discretionary financial reporting issues with clients affect the extent to which auditors objectively judge the client's financial reporting (Svanberg et al., 2019).

The purpose of the audit function is to contribute to trust in the validity of financial information, as auditors perform their audit under the very strict supervision of the boards of accountancy, the legislation, and standard-setting organizations (Akther & Xu, 2020). CPA's respective audit firms must follow the relevant GAAS audit standards and the ethical code of professional conduct (Dobrowolski, 2021). They have to perform their audit work based on professional skepticism and objectivity to provide reasonable but not absolute assurance that financial statements under audit are free from material misstatements by fraud, error, or omissions (AICPA & CPA Canada, 2017).

By performing an audit engagement, all auditors must preserve independence, honesty, and objectivity (Salih & Flayyihb, 2020); otherwise, they may not perform the audit engagement (Alderman & Jollineau, 2020). Thus, external users of financial statements rely on the auditor's opinion, while there are always risks related to the inadequacy of the opinion presented (Salih & Flayyihb, 2020). To sum up, the external audit function renders the audited entity's financial information highly trustworthy and prompt, which is why audited financial statements provide the most reliable accounting information for external users (Frazer, 2020).

3.2.2 Weaknesses of Contemporary Auditing

Traditional audit procedures exhibit several weaknesses (Wang et al., 2020). The discussion of such weaknesses is the subject of the following paragraphs.

3.2.2.1 Outline of Traditional Auditing Weaknesses

Traditional substantive audit procedures consist of a periodic and backward-looking audit approach from the balance sheet date back until the beginning of the period under audit by using risk-oriented manual and semi-manual sampling methods to examine auditees' transactions by collecting appropriate audit evidence for assessing the risk of material misstatement in financial statements and to express an audit opinion thereon (Rozario & Vasarhelyi, 2018). Audit procedures such as acceptance of the audit engagement and investigation of risk associated with the engagement, requests for third-party confirmations, and internal control testing are generally performed on a manual audit approach (Byrnes et al., 2018).

3.2.2.2 Traditional Auditing Weaknesses in Particular

3.2.2.2.1 Risk-oriented Periodic Sampling Procedures

At the start of any audit, the auditors receive journal entries, spreadsheet files, and other documents in electronic and manual formats from the auditee (Schmitz & Leonie, 2019). Under traditional audit procedures, the required audit evidence is obtained by a risk-oriented audit approach based on sampling methods on a pre-selected population of the auditee's financial data while testing only a fraction of the relevant population (Lombardi et al., 2022). The result of the sampling method is extrapolated across all transactions of the specified population (Ekin, 2019). Therefore, the audit opinion is solely based on testing samples of account balances or transactions instead of auditing entire populations (Barandi et al., 2020).

According to US audit standard AU-C 350, sampling results in audit risks that arise from the limitation of a control audit action or a substantive audit to a sample, in that the auditor's conclusions could potentially reach a different conclusion if the complete database were audited (AICPA, 2006). Due to the characteristic limitations of sampling audits in contrast to auditing of whole populations, an inherent risk remains that material misstatements in financial statements remain undetected even though the auditor complies with GAAS standards and principles (Barandi et al., 2020).

Additional weaknesses result from the backward-looking periodic audit approach, as key activities and risks were often identified weeks or months after the balance sheet date (Byrnes et al., 2018). Some samples may be one year old when auditing annual financial statements under a periodic audit approach (Appelbaum & Nehmer, 2017).

3.2.2.2.2 Work-intensive Audit Procedures at High Costs

Manual auditing is labor-intensive, costly, and requires large audit teams of more than ten people (Lombardi et al., 2022). A considerable portion of the audit cost mainly relates to the verification of authenticity and accuracy of the data of the transactions performed by the auditee since a large number of audit procedures must be performed manually or semi-manually (Cheng & Huang, 2019). At the same time, audit teams spend several weeks to several months, depending on the size and complexity of the auditees' business on-site at the auditee's premises (Cheng & Huang, 2019). Due to this issue, the frequency of traditional audits is typically performed on a quarterly or annual basis (Kahyaoğlu et al., 2020).

3.2.3 Blockchain-based Auditing

3.2.3.1 Blockchains Require External Auditing

Blockchains require external audits as complex accounting-related proceedings based on auditees' management assertions, such as measuring the fair value of assets or testing for impairment of goodwill, fixed and intangible assets, or receivables, require human expertise and judgment on the part of accountants and auditors (Schmitz & Leonie, 2019). Appelbaum & Nehmer (2020) advocate external audits of blockchains considering data reliability, data security, and transaction transparency of accounting transactions (Appelbaum & Nehmer, 2020).

Smith and Castonguay (2020) state that auditors must assess blockchain technology risks using the blockchain audit trail (Smith & Castonguay, 2020). Wang et al. (2020) also endorse the approach of a blockchain-based audit information system by aiming for the transformation to a continuous and intelligent real-time audit approach (Wang et al., 2020). Bonyuet (2020) anticipates auditors must manage blockchain risks by adopting new standards and incorporating audit modules into new blockchain systems to ensure efficient auditing (Bonyuet, 2020).

3.2.3.2 Characteristics of Blockchain-based Auditing

Databases under audit are increasingly exposed to cybersecurity attacks, and the complexity and amount of business transactions are rising; thus, audit firms need to transform their manual and semi-manual audit approach into automated and tool-based auditing (Rozario & Vasarhelyi, 2018). Another technological driver provides increased outsourcing of customer data to a cloud computing environment (Fan et al., 2020). Further innovation arose from the innovation of smart contracts for blockchain systems that enable automated transactions on the blockchain when predefined rules are met as

prescribed by Rozario and Thomas (Rozario & Thomas, 2019). Smart contracts allow the performing of smart audit procedures to enable automated continuous audit procedures almost in real-time to enhance the effectiveness of audit procedures (Rozario & Thomas, 2019). Beneath performing continuous auditing procedures, auditors must apply their professional judgment on accounting and management estimates on the financial statements (Kahyaoğlu et al., 2020).

As an advantage of blockchain-based audits, stakeholders receive the audit information quicker and more accurately at a more detailed level of knowledge (Alarcon & Ng, 2018). Blockchains grant auditors access to all required information almost in one place (Schmitz & Leoni, 2019) as soon as a transaction has been performed (Lombardi et al., 2022), while the recognition of transactions and their auditing can be accomplished almost in real-time (Pimentel et al., 2021). Evidence from blockchains is obtained electronically, whereby IT environments and their impact on the audit evidence must be considered (Vincent et al., 2020).

Auditors benefit from the ability to perform their analytical data procedures in real-time, while real-time information provides auditees greater confidence in the accuracy of accounting-related data (Appelbaum & Smith, 2018). Financial statements that receive financial data directly from the blockchain are updated every business day, enabling a quick and efficient closing of accounting periods, as the data is trusted (Appelbaum & Smith, 2018). Thus, blockchain technology enhances substantive auditing procedures, sampling methods, and audit testing processes (Wang et al., 2020).

3.2.3.3 Smart Audit Procedures on Blockchains

Verifying the ownership and the valuation of digital assets in a blockchain requires new approaches and different substantive audit procedures (Liu et al., 2019). This chapter analyzes smart audit procedures.

3.2.3.3.1 Continuous Auditing with Smart Audit Procedures

Blockchains that contain complete audit trails of all transactions since their implementation (Kokina et al., 2017) provide the platform for smart audit tools that execute predefined audit procedures autonomously, identify material items, and provide real-time audit reporting to the external auditor (Rozario & Vasarhelyi, 2018). The specific business risks of the auditee, new emerging risks, and the reliability of quality control processes are incorporated into the automated smart audit procedures that provide real-time audit reporting to the external auditor (Rozario & Vasarhelyi, 2018). Smart audit tools enable near real-time continuous audit procedures throughout the year on all transactions (Bonyuet, 2020; Liu et al., 2019). Auditors are granted access to all accounting-relevant data of the auditee in the blockchain on a read-only basis (Rozario & Thomas, 2019). Thus, auditors have permanent access to the accounting data in the blockchain databases, while data will be monitored, extracted, and analyzed ongoing by the auditor (Smith & Castonguay, 2020).

Auditors examine entire populations of transactions by smart audit tools in the period under audit by performing continuous audit procedures on reliable data instead of sampling methods on a risk-based approach (Kokina et al., 2017). Smart audit procedures are applied to examine dual-purpose procedures to identify key terms in contracts and to evaluate intangible assets, to analyze access management of blockchains and adequacy of participant's access rights, to analyze sales and inventories, to retest identified errors, to

evaluate consensus mechanisms, to verify that no participant controls more than 51 percent of the blockchain, and to match auditee's contracts with smart contracts (Rozario & Vasarhelyi, 2018). Smart audit procedures also enable autonomous audit procedures, including independent internal control tests and autonomous analytical methods of the accounting relevant data based on predefined conditions (Rozario & Vasarhelyi, 2018). In addition to smart audit procedures, external auditors inspect consensus protocols' compliance with conditions defined in smart audit procedures, blockchain codes, blockchain access management, and access to cryptographic keys (Rozario & Vasarhelyi, 2018).

Smart audit procedures under the control of auditors check the risks of erroneous protocols in audit evidence and the creation of alerts in case of faults (Rozario & Vasarhelyi, 2018). This raises a heightened expectation that financial statements are potentially free from material errors or fraud, as all accounting-related data has been examined (Appelbaum & Smith, 2018). As auditors perform data analytics by smart audit procedures based on entire data populations in real-time, statistical sampling techniques are no longer required (Bonyuet, 2020).

Furthermore, smart audit procedures enable almost real-time reporting to the audit committee, regulators, investors, suppliers, and audit inspectors (Farcane & Deliu, 2020). Expectation gaps among auditors and stakeholders are minimized (Iwanowicz & Iwanowicz, 2019). External auditors inspect, in addition, consensus protocols' compliance with conditions defined in smart audit procedures, blockchain codes, blockchain access management, and access to cryptographic keys (Rozario & Vasarhelyi, 2018). Blockchain technology with smart audit tools allows audit firms to shift from end-of-year audits to continuous real-time audits throughout the year (Psaila, 2017).

Smart audit procedures improve audit quality as auditors perform audit procedures more efficiently, while in particular areas of higher risks, the whole population of transactions is audited (Yebi & Cudjoe, 2022). They autonomously predict sales using financial and non-financial data and compare them to the actual sales while identified errors are analyzed (Rozario & Vasarhelyi, 2018). Smart audit procedures and smart internal control tests are performed to address current and new audit risks of fictitious, unauthorized, or erroneous transactions, inaccurate recording of goods, inaccurate recording of cash receipts, inappropriate blockchain mechanisms, posting of unauthorized transactions in blockchains, unauthorized creation of smart client contracts, and improper application of outdated client smart contracts (Rozario & Vasarhelyi, 2018).

Thus, auditors have permanent access to the accounting data in the blockchain databases, while data will be monitored, extracted, and analyzed ongoing by the auditor (Smith & Castonguay, 2020). Adequately implemented blockchains with integer smart contracts are the most reliable digital systems containing accounting-related data and information (Appelbaum & Smith, 2018). Transactions in blockchain systems are automatically recorded, encrypted, and immutable (Appelbaum & Smith, 2018). Smart audit tools must consider scalability, flexibility, and risks from incorrect codes in smart audit procedures (Bonyuet, 2020). Consequently, audits with blockchains are performed by continuous auditing procedures (Barandi et al., 2020), reducing audits' costs (Schmidt & Wagner, 2019).

3.2.3.3.2 Auditing of Internal Controls by Smart Audit Procedures

Blockchain data alone do not assure the reliability of a company's financial reporting (Liu et al., 2019), as they cannot verify if transactions are booked and accounted for appropriately according to respective rules or the appropriateness of the transaction

purpose (Pimentel et al., 2021). Accounting-related internal controls must ensure the accuracy and completeness of transactions and identify false, fraudulent, or misleading financial information not addressed by the blockchain's consensus mechanisms (Centobelli et al., 2021). Thus, auditees must implement an effective accounting-related ICS that grants the completeness and accuracy of blockchain transactions (Castonguay, 2021). The ICS must contain internal controls towards the existence, design, and operational effectiveness of internal control systems and test the consensus mechanisms of blockchains to ensure adequate accounting processes (Smith & Castonguay, 2020).

The effectiveness of accounting-related internal controls surrounding the blockchains must be tested by auditors (Liu et al., 2019). Internal control tests are performed with smart audit tools to automatically evaluate blockchains' consensus mechanisms and verify if blockchain participants control 51 percent of blockchain nodes (Omar et al., 2021). Control testing assures the completeness of accounting-related data that off-chain transactions are ruled out and by cut-off testing that all accounting-related assets and transactions in the blockchains are reported in the correct fiscal period (Pimentel et al., 2021). Moreover, they are performed to automatically match several initial clients' smart contracts towards the number of clients' smart contracts in periods under audit (Rozario & Vasarhelyi, 2018).

Furthermore, internal control tests enable automatically matching customer node access levels when initiating blockchain transactions (Castonguay, 2021). Testing the ITGC that protects sensitive information in blockchains assures information security, system availability, process integrity, and privacy and confidentiality issues, while ITGC (AICPA & CPA Canada, 2017). Weaknesses of internal controls increase the risks of

material misstatements in financial reporting by management fraud (Donelson et al., 2017).

3.2.3.4 Audits in Addition to Smart Audit Procedures

Despite auditing all accounting-relevant transactions with smart audit procedures, supplementing audit procedures are required (Cangemi & Brennan, 2019), as transactions in blockchains do not guarantee reliable financial reporting, as agreed and verified transactions on the blockchain could be based on fraudulent agreements or misleading transactions (AICPA & CPA Canada, 2017). Therefore, in blockchain systems, auditors inspect documents supporting the blockchain code, configuration, and governance of the peer network that operates blockchain processes (Demirkan et al., 2020). Whether a blockchain can be relied upon depends on factors such as the robustness of the consensus mechanism and the reliability of the cryptography used, whereas simply relying on the adequacy and accuracy of blockchains is not an option (Pimentel et al., 2021).

Blockchain's consensus mechanisms ensure the integrity of transactions (Rozario & Vasarhelyi, 2018), while smart contracts enable automated performing and monitoring of transactions based on predefined contract terms (Yermack, 2017). In an appropriately designed blockchain, consensus mechanisms integrated into smart contracts authenticate, verify, and perform data automatically and assure the integrity and accuracy of the recorded and stored transactions on the blockchain (Wang et al., 2020). If no consensus is reached, concerning transactions are classified as suspicious transactions, and then, information on new blocks is rejected and classified as invalid (Pimentel et al., 2021). Then, auditors must analyze reasons for abnormality and again pass consensus mechanisms, as it serves as an alert function of blockchain-based auditing systems (Pimentel et al., 2021).

Auditees must establish blockchain access controls to ensure the confidentiality and integrity of data and the blockchain code, whereby all levels of access and the granting of access rights must be defined by the auditee, considering internal requirements and policies (Popchev et al., 2021). Hereof, the integrity and adequacy of access controls and approval processes must be audited annually (Popchev et al., 2021). Therefore, auditors must evaluate blockchains' reliability by examining the blockchain's source code, access mechanisms, and cryptography (Pimentel et al., 2021). Audit procedures have to encompass the quality of the blockchain code, the protocols for changes, and the power allocation between the blockchain members (Liu et al., 2019).

3.2.4 Comparison of Traditional versus Blockchain-based Auditing

Under traditional audit methods, auditors interview the responsible staff of auditees and observe control processing (Paggi, 2022). In a blockchain system, audit procedures differ significantly from traditional audit approaches, as they are performed continuously to improve the assurance level of the auditing activity and the obtained audit evidence by substantially reducing the time lag between the date of a transaction and the related audit procedures (Wang et al., 2020). Physical inspection of accounting records, invoices, and vouchers, e.g., by walkthroughs, physical inventory procedures, and audit sampling under traditional audits, are replaced by examination of the accuracy of blockchain inputs based on entire data by Radio Frequency Identification (Appelbaum & Smith, 2018).

Auditors of blockchains examine the existence of timestamps, hashes, and consensus among nodes and perform data analysis of blockchain data (Wang et al., 2020). While today's audits examine the approval of transactions and balances at the end of reporting periods, blockchains provide validated transaction records almost in real time

after the trades have been executed (Rozario & Vasarhelyi, 2018). Blockchain-based auditing is less work-intensive than traditional audit practice (Schmitz & Leonie, 2019).

Instead of manual recalculation of accounting entries and re-performance of control procedures by manual audit procedures, all data on transactions on the blockchain are permanently monitored and calculated for accuracy (Wang et al., 2020). In blockchain environments, built-in blockchain mechanisms monitor workflows and control processes while process violations are identified by the system (Paggi, 2022). Analytical procedures are performed in the blockchain in real-time using special filters for continuity equations and statistics (Appelbaum & Smith, 2018). Table A2 shows the differences between traditional and blockchain-based auditing in the form of a comparison of the requirements for particular audit techniques.

3.2.5 Blockchain Impact on the Audit Profession and Auditor's Role

The audit profession and the role of the auditors will face challenges from innovative technologies such as blockchains (Bonyuet, 2020). This technology will change how auditors perform their audit engagements in the future; therefore, the audit profession has to generate new assurance opportunities (Calderón & Stratopoulos, 2020). Bonsón and Bednárová (2019) outlined that blockchain technology has the power to change our business and social life over decades and worked out its potential impacts on auditing and accounting (Bonsón & Bednárová, 2019). Dai and Vasarhely (2017) analyzed blockchain technology early on, and they argued that blockchains empower the potential to disrupt contemporary substantive auditing procedures with an automatic audit approach (Dai & Vasarhely, 2017).

To perform a blockchain-based audit appropriately, auditors and their staff must acquire sufficient knowledge about blockchain technology to understand the blockchain

mechanisms and the underlying assumptions and estimates (Wang et al., 2020). More talents with high professionalism and strategic foresight will be required in the future (Cheng & Huang, 2019). Thus, CPAs and their audit staff need further training to understand at least one technical programming language and the basic functions of blockchain technology (Selg, 2022b). Auditors unable to gain appropriate knowledge must refrain from audits on blockchains (Pimentel et al., 2021).

The expected increased audit efficiency will enable auditors to engage more time in predictive analytics, internal control improvements, and problem-solving complex aspects (Alarcon & Ng, 2018). Financial statements and valuation methods are often based on estimates rather than facts; thus, an auditor´s judgment is still necessary for a blockchain environment to evaluate if the management´s estimated values are reasonable (Bible et al., 2017). Participants in blockchains need CPAs as arbitration functions, a legal framework, to settle disputes among the blockchain participants in permissioned blockchains to enforce contractual terms if the code of smart contracts deviates from legal documents or contractual agreements (AICPA & CPA Canada, 2017).

Counterparties using the blockchain can engage the services of CPAs to ensure smart contracts are implemented through an independent assessment, whereby risks to blockchain users related to undetected errors or vulnerabilities can be significantly reduced (Farcane & Deliu, 2020). Despite the ability of blockchains to perform and verify transactions automatically, the requirement for an auditor´s professional judgment will not be obsolete (Barandi et al., 2020). Also, external auditors in the blockchain must perform audits independently (Rozario & Thomas, 2019). Currently, auditors fear using the blockchain due to their lack of experience and are unsure as the training will be difficult (Pimentel et al., 2021). Therefore, auditors are reluctant due to a lack of skills to

assess the implied risks appropriately and to evaluate the auditees' estimates (Pimentel et al., 2021).

Further challenges to blockchain-based audits that must be discussed arise from statutory requirements in the audit profession (Rozario & Vasarhelyi, 2018). From the perspective of standard setters, the role of auditors in a blockchain environment has to be regulated by prospective audit standards and statements of position (AICPA & CPA Canada, 2017). Safety concerns regarding this important new technology emerged, especially given that it is still in its infancy and has a high potential for disruption (Cumming et al., 2019).

3.2.6 Effective Auditing of Accounts Receivable with Blockchains

This chapter examines and presents the superiority of blockchain-based auditing on the accounts receivable balance sheet position. Beginning with accounting principles and accounting procedures on accounts receivable, traditional auditing concerning requests for external confirmation is outlined, followed by characteristics and benefits of auditing accounts receivable with blockchains.

3.2.6.1 Accounting of Accounts Receivable

3.2.6.1.1 IFRS Accounting Principles on Accounts Receivable

Except for lease contracts, all contracts with customers as accounts receivable apply to the accounting standard IFRS 15, "Revenue from Contracts with Customers" (Zülch, 2020). The scope of IFRS 15 determines the principles for reporting financial information by an entity concerning the amount, nature, uncertainty, and timing of cash flows and revenues out of contracts with its customers (Haggenmüller, 2019). According to IFRS 15.9, an entity shall recognize contracts with its customers only if all participating parties approve contracts and commit to grant the related obligations, each party's rights

for delivery of goods and services from the contract can be identified, payment terms for all goods and services to be transferred can be identified, the commercial substance of the agreement is undisputed, and collection of the consideration in exchange for the goods and services transferred to the customer is probable (Zülch, 2020).

3.2.6.1.2 Accounting Procedures of Accounts Receivable

Whenever suppliers transfer goods and services to their customers before payment of the consideration, accounts receivable in the form of short-term assets are booked at the supplier firm as outstanding payments (Brata et al., 2021). Accounts receivable show the amounts that the auditee's customers owe for goods or services delivered (Sarferaz, 2022). After making bookkeeping and payments, ledgers and accounts are reconciled (Farcane & Deliu, 2020). If customers cannot pay for compensation, supplier firms have to recognize such receivables as bad debts (Savchenko et al., 2018). If these receivables are unrecoverable, they can be eliminated (Rey-Ares et al., 2021). Allowance for bad debts indicates if an entity faces a structural deficiency in collecting customer payments or compensation (Nurdiansyah & Manda, 2018). Sharp increases in bad debts may indicate requirements for large write-offs (Jayaraman & Bhuyan, 2020).

3.2.6.2 Contemporary Auditing Procedures of Accounts Receivable

3.2.6.2.1 Current Regulation of Accounts Receivable under GAAS

Audits of accounts receivable require a framework to comply with relevant rules and regulations (Vasarhelyi et al., 2012). Sole testing of accounting records on accounts receivable does not provide sufficient and appropriate audit evidence; therefore, auditors must examine other information (AICPA, 2021). Audit evidence from external sources is more reliable than internal sources of the auditee (Appelbaum et al., 2020). AU-C 505.03

outlines that evaluating accounts receivable by third-party confirmations contributes to reducing risks of material misstatement in financial statements (Nouri, 2018).

Requests for obtaining external confirmations are regulated under the GAAS auditing standard AU-C 505 (AICPA, 2012b). The scope of AU-C 505 is providing manual rules for requesting external auditing confirmations by positive or negative confirmations (Flood, 2021). In addition, AU-C 505 regulates cases of management's refusal to request the auditee's customers for confirmation of balances, alternative audit procedures when lacking appropriate response, and the evaluation of the confirmation results (Flood, 2021).

Based on the auditor's discretion by considering the materiality of the balance sheet position as well as control risks and the inherent risks, auditors have to evaluate based on AU-C 330.20 (AICPA, 2012c), if the procedures to obtain external confirmations have to be performed (Flood, 2021). According to audit standard AU-C 330.20, external confirmations are not required if the balance sheet positions are immaterial, the risks of material misstatements are low, and these risks are mitigated by other audit procedures (AICPA, 2012c). If auditors do not request third-party confirmations (Piercy & Levy, 2021), the reasons for omission must be documented (Flood, 2021).

3.2.6.2.2 Preliminary Considerations on External Confirmations

The purpose of the audit of accounts receivable lies in the determination of their actual value, their existence of overdue receivables, verification of the correctness of the write-off of receivables, and completeness as well as the correctness of accounts receivable in the accounting records (Melnychenko & Mishina, 2022). Under materiality aspects, auditors have to decide if third-party confirmations for accounts receivable will

reduce the audit risk towards material misstatements of the financial statements (AICPA,2012b). If the accounts receivable position is material, and the auditor's evaluation identifies risks, external confirmations of the respective balances are requested from the auditees' customers (Nouri, 2018).

Additionally, the auditor must understand the nature of the client's transactions to identify potential unusual transactions (Raschke et al., 2018). To ensure orderly audit procedures, auditors must take control of the confirmation process without engaging the auditee, which requires considerable audit effort (Flood, 2021). External confirmations must be received in written form by AU-C 505.A27 (Pereira et al., 2022).

Requests may be designed as positive or negative confirmations (AICPA, 2012b). Positive confirmations require the respondent to confirm positions, and in case of substantial deviations, confirmations should be requested once again (Westland, 2020). Negative request confirmations that require confirmations only in the event of material deviations from the balances to be confirmed are generally less reliable than positive confirmation requests (Flood, 2021).

3.2.6.2.3 Traditional Procedures to Verify Accounts Receivable

The audit standard AU-C 505 requires auditors to select accounts to be confirmed that are material toward the account balances, accounts with zero balances, old unpaid items, written-off accounts, and accounts of unaudited entities (AICPA, 2012b). Requests for external confirmations require auditors to send many letters or e-mails regarding the correctness of accounts receivable balances to auditee's customers to verify the authenticity and accuracy of the receivables (Cheng & Huang, 2020). The written confirmation requests must contain a numbering of the accounts, addresses, amounts of

balances, a total of all accounts receivable selected, and a percentage of the total amount receivables (Flood, 2021).

After receiving external confirmations, auditors must examine whether the audit evidence provided is sufficient and appropriate for the identified risks on financial statements (AICPA, 2012b). They must evaluate the results, determine the reliability of the confirmed information, and compare the confirmed balances with totals on the relevant ledgers to evaluate the confirmation results for any differences or deviations (Nouri, 2018). For testing completeness of the accounts receivable, sales of the current period under audit are added to the beginning balance of the accounts receivable ledger, while accounts receivable receipts are subtracted, resulting in the ending balance of the accounts receivable ledger (Rozario et al., 2022). Cutoff procedures must also be conducted to determine if the transactions are recognized in the appropriate accounting periods and that there are no issues regarding the auditee's bookkeeping methods (Appelbaum & Smith, 2018).

In the event of deviations, inappropriate third-party confirmations, or unusual transactions, auditors must perform alternative audit procedures (Andiola et al., 2022), such as testing subsequent cash receipts or shipping documents (Lureau, 2020). By the end of the confirmation process, auditors document the confirmation results by indicating the number of requests, amounts of confirmations, and percentages toward receivables in total (AICPA, 2012b). If auditors are faced with client management's refusal to request third-party confirmations, the management's refusal must be documented by AU-C 505.08 (AICPA, 2012b). In contrast, the auditor should ask management for reasons for the refusal and inspect any evidence to evaluate the reasons (Flood, 2021). The auditors

also have to assess the impact of the refusal on the validity of the audit (Edmonds et al., 2019).

3.2.6.3 Blockchain-based Audit Procedures on Accounts Receivable

Applying blockchain technology for audits of accounts receivable results in shifting from manual to automated audit procedures (Schmitz & Leonie, 2019). In consortium blockchain systems, auditors have dedicated access to the accounting-related data of the auditee (Hayrettin & Karaburun, 2020). Accounts receivable of the auditee, corresponding accounts payable of its customers, and confirmations of underlying transactions are recorded and stored (Lombardi et al., 2022); thus, consortium blockchains provide all required information and data concerning outstanding receivables and payment terms (Rijanto, 2021).

Blockchain systems check accounts receivable data automatically by the implemented consensus mechanisms, which assure the accuracy and immutability of recorded transactions (Rijanto, 2021). As soon as transactional data concerning the selling of goods and services are authorized and verified by blockchain participants, data are added as new blocks to the existing blockchain (Torky & Hassanein, 2020). Accounts receivable are verified by smart audit procedures based on business logic towards agreed-upon predefined and pre-approved audit procedures that deal with risks, such that shipped goods need to be correctly booked and recorded in the relevant ledgers (Rozario & Thomas, 2019). Smart audit procedures include rules to check if accounts receivable exist, reasonable amounts, and good aging (Schmitz & Leonie, 2019).

They automatically match the auditee's accounts receivable data with their clients' accounts payable data in consortium blockchains (Ozlanski et al., 2020). Blockchain's block hashes are recalculated to verify the data's correctness (Waldo, 2019). Thus,

external confirmations are obsolete in an effectively functioning blockchain system because the blockchain ledger contains all the relevant data, allowing the auditors to check the hash for a particular transaction to verify the existence, occurrence, and valuation (Rozario & Vasarhelyi, 2018).

Blockchain technology reduces efforts and costs when reconciling the data of a supplier with the corresponding data of the buyer, as supplier and buyer use the same database, while inefficiencies toward the reconciliation of accounts or the request for paper-based or electronic confirmations will become obsolete (Schmitz & Leonie, 2019). Although blockchain data is tamper-proof, there are risks to the integrity of the data while extracting data from the blockchain (Sheldon, 2019).

Alternatively, verification of accounts receivable in a federated blockchain system by a supplier auditor and another client firm auditor towards the corresponding accounts payable is performed based on zero-knowledge protocol (Cao et al., 2018). Such protocols in the form of an algorithm that enables participants of blockchains to prove a certain value to another participant without conveying any further information can be applied for purposes of accounts receivable confirmation (Harris, 2019). Regarding transactions that different audit firms audit, Auditor A sends requests to the federated blockchain, which can only be confirmed by auditor B, auditing the counterpart of the transactions (Cao et al., 2018). Request and confirmation are encrypted by following a zero-knowledge proof protocol without revealing client-specific information, while the verification process is automated to eliminate requirements for human interventions (Cao et al., 2019).

3.2.6.4 Blockchains Eliminate Requests for External Confirmations

Auditing third-party confirmations is where blockchain technology provides higher efficiency toward manual substantive audit procedures, as blockchains contain

recorded transactions and related invoices, sales orders, shipping documents, and receipts of goods and services (Appelbaum & Nehmer, 2017). As transactions on the blockchain must be confirmed by all network participants, blockchains eliminate requirements to ensure that transaction records match transactions of counterparts on the other side of a deal (Thakur et al., 2020). Consequently, if the blockchain protocol ensures that consensus mechanisms of the blockchain are operating appropriately and no client participant of the blockchain controls more than 51 percent of the blockchain (Appelbaum & Nehmer, 2017), blockchain technology eliminates tedious and time-consuming audit procedures to collect paper-based third-party confirmations on accounts receivable (Elommal & Manita, 2021).

Third-party confirmations from customer firms of the auditee are no longer required in a blockchain environment (Castonguay, 2021), as counterparties and auditors have real-time insight into the transactions (Appelbaum & Smith, 2018). As a benefit of blockchain technology, the data is immutable, and efforts to reconcile receivable accounts and verify the transaction data will decrease significantly (Septiawan, 2022). In addition, audits have become more efficient and less work-intensive (Cao et al., 2019).

3.2.7 Summary of Elimination of Audit Weaknesses by Blockchains

3.2.7.1 Critical Perspectives on Elimination of Audit Weaknesses

According to Lombardi et al. (2022), blockchain technology in auditing is still very early; thus, the topic needs to be more deeply researched (Lombardi et al., 2022). Skeptics argue that the technology needs to be more mature and scalable to replace traditional audit and accounting procedures (Alarcon & Ng, 2018). Alarcon and Ng (2018) outline in addition that blockchains currently lack the trust of regulators and audit firms due to the complexity of architecture and mechanisms, as there are still risks that

data or assets of blockchains can be stolen or corrupted due to unidentified vulnerability risks, programming errors, or system weaknesses (Alarcon & Ng, 2018). Blockchain-based auditing with smart audit tools faces risks from ineffective internal controls on accounting-related processes such as the account receivable cycles (Alarcon & Ng, 2018). To bring up an objection to these constraints, verifying transactions on blockchains is just one aspect of a trusted system (Vincent et al., 2020).

By performing an audit, auditors must evaluate if recorded transactions are based on accurate, relevant, objective, verifiable, and reliable audit evidence (Tuxtabaevich, 2022). Blockchains can support assertions of completeness and occurrence, but blockchains provide no information on the quality and characteristics of goods and services underlying recognized transactions (AICPA & CPA Canada, 2017). When testing blockchain data, there is no information on potential additional off-chain transaction agreements or if transactions violate the arm's length principle among related parties (Brownsword, 2020).

Accounting-related transactions are often based on estimated values under IFRS accounting which deviate from their historical costs (AICPA & CPA Canada, 2017). Thus, auditors still need to evaluate management's estimates of the recorded transactions in the blockchain (Bonyuet, 2020). Even if auditors perform their audit work with direct access to blockchains (Cetinoglu, 2021), there are risks that financial statement assertions are inaccurate (Graham & Sherwood, 2021).

Blockchains do not ensure that transactions are free from being illegal, fraudulent, or unauthorized; (Bonyuet, 2020). Blockchain consensus mechanisms do not validate whether a transaction has been correctly accounted for under the GAAP and GAAS rules, nor whether the business purpose is legitimate since blockchain-based transactions are

exclusively authorized and checked for existence, correct date, and several transactions (Pimentel et al., 2021). Auditees must implement internal controls to address such risks (Dyball & Seethamraju, 2021). The CPA must examine if these controls operate effectively (Frazer, 2020) and perform data analytics on the blockchain data by including the blockchain environment's ITGC (Sheldon, 2019).

A further problem to be solved concerns the legal validity of smart contracts for business agreements; they have not been resolved since no international case law currently applies (Duke, 2019). To assess the reliability of blockchains, auditors have to examine the appropriateness of the logic in smart contracts and to evaluate if any manipulation is possible or has been done on the consensus algorithms and mechanisms (AICPA & CPA Canada, 2017).

Some authors of blockchains outline that blockchains could abandon requirements for an audit of financial statements by auditors, that audit work of a CPA is no longer required when all accounting transactions of the auditee are recognized as immutable in blockchains (AICPA & CPA Canada, 2017). Auditors shall prevent relying too much on blockchains (Tušek et al., 2021). Schmitz and Leonie (2019) stress that blockchain mechanisms eliminate limitations of double-entry bookkeeping, making an external audit of companies' financial statements obsolete (Schmitz & Leonie, 2019).

An audit is not just a review of routine transactions, as it includes a holistic assessment of the robustness of internal controls, the accounting policies, and the reasonableness of material estimates made by the management of the auditee; thus, the external audit work cannot be replaced by blockchains (Pimentel et al., 2021). Blockchain verification processes cannot replace the verification function or the role of independent external auditors as they do not address controls to detect fraud, errors, or omissions

(Desplebin et al., 2021). As blockchains potentially compromise the role of auditors and auditing firms lack sufficient knowledge (Estep, 2021), blockchain-related training of auditors and their audit staff is critical for auditor acceptance (Manita et al., 2020).

Graham and Sherwood (2021) are critical of blockchain-based auditing as blockchain technology, on the one hand, can provide benefits in terms of continuous audits at lower costs; however, on the other hand, they argue these benefits are limited, whereby a higher effort for the audit of internal controls will nullify the reduction of testing auditee's transactions (Graham & Sherwood, 2021).

3.2.7.2 Synthesis of Results from the Literature Review

Traditional substantive audit procedures are periodically performed by sampling (Rozario & Vasarhelyi, 2018). Such audit approaches that do not continuously audit entire data populations entail risks that material misstatements and fraud in financial statements remain undetected (Barandi et al., 2020). Consequently, such manual audit procedures prove costly and work-intensive; thus, unnecessary large audit teams often require more than ten persons compared to digitalized audits (Lombardi et al., 2022).

Emerging blockchain technology provides the potential to disrupt and overcome these issues of the traditional auditing procedures by enabling permanent auditing procedures almost in real-time based on automated tools for data analysis with direct access to all relevant data, while all nodes authorize transactions, and data are immutable and traceable (Lombardi et al., 2022). Auditing accounts receivable in a blockchain environment makes requests for third-party confirmations obsolete as counterparties and auditors provide insight into all auditee transactions (Castonguay, 2021).

Smart audit procedures perform fully automated continuous audits without human intervention (Barandi et al., 2020), including automated internal control tests and

autonomous analytical procedures (Rozario & Vasarhelyi, 2018). In contrast to traditional manual substantive audit procedures, smart audit procedures evaluate entire populations of all accounting-relevant transactions of the auditee almost in real-time; thus, risk-oriented audit sampling becomes obsolete (Bonyuet, 2020). Consequently, blockchain-based auditing provides more assurance than the risk-oriented audit approach (Guzov et al., 2019). While auditing costs can be significantly reduced (Schmidt & Wagner, 2019). Furthermore, by evaluating all accounting-relevant transaction data in real-time, all relevant audit and fraud risks can be identified (Rozario & Vasarhelyi, 2018).

In addition to smart audit procedures, auditors must perform yearly tests of the blockchain code (Pimentel et al., 2021) and the blockchain access controls (Popchev et al., 2021). In addition, auditors must evaluate every year the appropriateness of the implemented blockchain consensus mechanisms (Pimentel et al., 2021). Blockchain systems need additional internal control testing to ensure the completeness of blockchain data so that entire accounting-relevant transactions are authenticated, verified, and performed, as well as accurately recognized in the blockchain (Liu et al., 2019). Due to these new digital requirements, blockchain technology will have major impacts on the audit profession and the role of auditors (Cheng & Huang, 2019). The audit profession must identify new business models while auditors face new audit procedures (Calderón & Stratopoulos, 2020).

3.3 Compliance of Blockchain-based Auditing toward AU-C 505

Chapter 3.3 examines compliance toward current GAAS by the example of accounts receivable if blockchain-based auditing of auditing accounts receivable complies with the regulations under GAAS standard AU-C 505 or potential gaps towards AU-C 505 exists.

3.3.1 Audit Framework for Blockchain-based Auditing

Blockchain-based audits, like traditional audits, require a framework to comply with relevant rules and regulations (Vasarhelyi et al., 2012) and to ensure appropriate audit work (Kend & Nguyen, 2020). Audit procedures based on blockchain technology under US legislation must comply with the GAAS audit principles codified in the AU Section 150 (AICPA, 2001). Under GAAS, auditing accounts receivable is regulated by AU-C 505 (AICPA, 2012b). In 2009 the IAASB codified the audit standard ISA 505 (IAASB, 2009). GAAS standard AU-C 505 was released by AICPA in 2012 (AICPA, 2012b).

According to Armitage and File (2014), the audit standards ISA 505 (IAASB, 2009) and AU-C 505 (AICPA, 2012b) represent the authoritative literature and guidance for auditors for requesting external confirmations in audits (Armitage & File, (2014). The German standard-setting body IDW adopted ISA standards in 2021 (Eltweri et al., 2022). Amended by German specifics, ISA [DE] 505 agrees largely with ISA 505 and AU-C 505 (AICPA, 2012b). Gauthier and Brender (2021) pointed out that under the current GAAS, no audit standards for blockchain-based auditing are codified (Gauthier & Brender, 2021).

3.3.2 Identification of Literature Gap toward AU-C 505

The research aimed to determine if orderly blockchain-based audits on accounts receivable can be carried out under the current GAAS auditing standard AU-C 505, which in detail describes manual substantive audit procedures to obtain third-party confirmations to evaluate the appropriateness of accounts receivable (AICPA, 2012b). Tool-based audit procedures and continuous real-time audits by blockchains, where data has to be extracted from the blockchain and analyzed by smart audit tools, require different procedures than manual auditing (Gauthier & Brender, 2021). AU-C 505 does

not address the auditor's procedures to evaluate controls of blockchains for accuracy and completeness of accounts receivable balances (Mantelaers et al., 2019).

GAAS standard for external confirmation does not address inspections of records in blockchains by evaluating entire data sets, nor inquiry procedures by monitoring processes and controls to identify any violations, confirmations by linking of data streams, recalculation of data by running calculations or to perform analytical procedures to verify the blockchain data (Appelbaum & Nehmer, 2017). Auditors' tasks to check if a blockchain grows over time are also not addressed (Appelbaum & Nehmer, 2017). Specific confirmation regarding blockchain process components in the form of an agreement with members of the peer network regarding the design and functioning of the hashing algorithm and the blockchain mechanisms (Carrara et al., 2020) are neither addressed under this auditing standard (AICPA, 2012b). The current regulation of external auditing confirmations respective accounts receivable under AU-C 505 in particular but under GAAS overall is insufficient (Gauthier & Brender, 2021).

3.3.3 Codification of New Blockchain-based Audit Standards

Lombardi et al. (2021) conducted interviews about GAAS audit standards for blockchains, confirming that no unique direction or authoritative guidance towards blockchain-based auditing exists under GAAS (Lombardi et al., 2022). Gauthier and Brender (2021) similarly concluded that there is a regulatory gap for blockchain-based auditing under the current GAAS as no blockchain-specific audit standards are codified (Gauthier & Brender, 2021). Furthermore, no regulation on assessing an internal control environment based on a blockchain toward accounts receivable exists (Dyball & Seethamraju, 2021).

Therefore, new or revised blockchain-based audit standards must consider the special requirements for the design of blockchains to meet the solicitation of GAAS (De Haes et al., 2020). Toward auditing accounts receivable, new or revised GAAS audit standards must be codified to enable adequate audits on accounts receivable with blockchains (Elommal & Manita, 2022). According to Gauthier and Brender (2021), issuing and codifying new audit standards generally takes ten years (Gauthier & Brender, 2021). Standard setters can address this issue by releasing best practice comments and recommendations during the transition phase to guide the auditors that apply blockchain-based auditing procedures (Gauthier & Brender, 2021).

3.3.4 Summary of Compliance Gaps towards AU-C 505

The relevant framework for blockchain-based auditing provides the US GAAS as codified in AU Section 150 (AICPA, 2001). GAAS audit standard AU-C 505 regulates manual audit procedures to obtain and evaluate external confirmations when auditing accounts receivable (Flood, 2021). According to the research of Gauthier and Brender (2021) and Lombardi et al., no blockchain audit standards are currently codified (Gauthier & Brender, 2021). Thus, a literature gap could be identified by auditing accounts receivable with blockchains toward AU-C 505. Consequently, to perform orderly audits on accounts receivable with blockchains, and smart audit tools, new or revised GAAS audit standards must be codified to enable adequate audits with blockchains (Elommal & Manita, 2022).

3.4 Key Points of the Literature Review

3.4.1 Summary of Blockchain Suitability toward Auditing

Blockchains consist of a decentralized ledger distributed across the blockchain network of computer systems, with data duplicated in distributed databases (Shobanadevi

et al., 2022). Blockchain technology's main pillars include the decentralization of databases, peer-to-peer networks, transparency, and traceability of blockchain transactions, the immutability of recorded data, and automated transactions with smart contracts (Lombardi et al., 2022). Bonsón and Bednárová (2019) and others considered that blockchains provide a suitable technology for auditing purposes, as all transactions are tamper-proof, immutable, recorded, and traceable in the distributed database (Bonsón & Bednárová, 2019).

Blockchains are highly secure systems, as most nodes authorize and verify the transactions (Appelbaum & Smith, 2018). Smart contracts automatically trigger pre-defined transactions by the implemented consensus mechanisms (Luo et al., 2019). The immutability feature of blockchains serves audit purposes, while recorded transactions cannot be modified or deleted (Bonyuet, 2020). Blockchain data are asymmetrically encrypted and protected (da Rosa Righi et al., 2020). Data in each block is protected by a hash, while the previous block's hash value is embedded into the current blockhead by forming a Merkle tree (Zheng et al., 2019).

The greatest benefit of blockchain technology results from implemented smart contracts, whereby manual tasks can be automated, thus improving the speed, accuracy, and cost efficiency of accounting-relevant transactions (Bonyuet, 2020). Consortium blockchains proved to be the most suitable blockchain systems for auditing due to their personal and public character (Wang et al., 2020). Blockchains prevent fraud, while smart contracts enable continuous auditing with smart audit tools (Lombardi et al., 2022).

The blockchain continuously records transactions (Jayathilake & Seneviratne, 2022). Blockchains provide a complete and immutable audit trail, as blocks on the blockchain cannot be altered after they were added to the chain (Arruñada, 2018). If

auditees delete or falsify financial data, this will leave traces in the blockchain system, and auditors can easily identify and analyze any changes (Cheng & Huang, 2019). When relevant supervisory authorities are integrated into the blockchain network, they can monitor all transactions of auditees in real time to identify abnormal behavior at any time and take on some oversight function to counter fraudulent behavior (Cheng & Huang, 2019).

3.4.2 Summary of Elimination of Audit Weaknesses by Blockchains

Blockchain-based auditing eliminates the weaknesses of traditional audit procedures (Farcane & Deliu, 2020). Substantive audit procedures for testing transactions are replaced by smart audit procedures (Fan et al., 2020) while shifting from a retroactive, point-in-time audit to ongoing, real-time auditing and data analytics (Elommal & Manita, 2022). In contrast to the risk-oriented audit approach, blockchain-based auditing procedures cover whole populations of accounting-relevant data, information, and records (Guzov et al., 2019).

Smart audit tool-based methods for obtaining appropriate audit evidence enable more efficient data extraction and analysis (Sastry Musti et al., 2021). By applying smart audit tools, audits of financial statements can be performed almost in real-time with continuous testing of all transactions in the blockchain by reducing costs for audits by smart audit tools (Barandi et al., 2020). In addition, smart audit procedures increase audits' efficiency and quality (Barandi et al., 2020). With smart audit procedures, fictitious, unauthorized, or incorrect sales contracts can be distinguished from actual ones (Rozario & Vasarhelyi, 2018).

Research shows that testing internal controls are very important to ensure the completeness of the accounting-related data in the blockchain and the appropriateness of

management assertions (Selg, 2022a). In a blockchain environment, the auditee´s management is responsible for implementing accounting-related internal controls that monitor compliance of the smart contract source code toward consistency with the intended business logic (Wang, 2018). Auditors assess the auditee's internal controls with smart audit tools, the policies and guidelines toward financial reporting, and the appropriateness of the auditee´s management estimates (Pimentel et al., 2021).

In addition, auditors must examine whether these controls operate effectively in the blockchain during the audit period (Rozario & Thomas, 2019). Audit evidence from blockchains exhibits high quality due to the implemented consensus mechanisms (Wang & Kogan, 2018). Due to the continuous auditing of all transactions, periodic audit procedures at the end of a year or quarter are reduced significantly, as only the blockchain code, access management, cryptography, and hashing have to be audited (Pimentel et al., 2021). However, the ability of blockchains to identify fraudulent transactions remains limited as long as auditees do not implement effective internal controls that ensure completeness toward recording all accounting-relevant transactions in the blockchain (Schmitz & Leonie, 2019).

The emergence of blockchain-based auditing poses new requirements for auditors' roles and the audit profession (Farcane & Deliu, 2020). To cope with new techniques and blockchain requirements, auditors must acquire new skills, master technical programming languages, and study the main functions of blockchain systems (Farcane & Deliu, 2020). External audits are still required in a blockchain environment, as consensus mechanisms cannot replace external audit functions (Pimentel et al., 2021).

To summarize, the focus of auditing activities in a blockchain system is shifting from tracing and verifying records and internal controls by mainly manual substantive

audit procedures to a systemic evaluation of transactions, internal control testing, testing of blockchain mechanisms, risk assessment of blockchain-based accounting, and fraud detection (Bonyuet, 2020) with smart audit procedures, and testing of blockchain codes and mechanisms (Elommal & Manita, 2021). Continuously auditing all transactions reduces audit procedures significantly at a year or quarter end, as only the blockchain code, access management, cryptography, and hashing have to be audited (Pimentel et al., 2021). Blockchain technology is enhancing audit efficiency, quality, effectiveness, and reliability by concurrently reducing auditing costs of collecting sufficient and appropriate audit evidence and improving the level of assurance, which will contribute to a much higher reputation for the audit profession (Barandi et al., 2020). Since transactions in the blockchain are recorded automatically, encrypted, and unchangeable, they will become the source of truth for auditing purposes (Appelbaum & Schmidt, 2018).

3.4.3 Recapitulation of Compliance Gaps toward AU-C 505

Blockchain-based auditing requires US CPAs to follow relevant GAAS audit standards (Ortman, 2018). However, under current GAAS standards, no auditing standards for blockchains are codified (Appelbaum et al., 2022). Audit standard AU-C 505 (AICPA, 2012b), which regulates current audits of accounts receivable (Flood, 2021), is not appropriate to guide audit procedures with blockchains, as blockchains require different audit procedures on audit sampling and new roles for the auditors (Zemánková, 2019). Thus, no regulation for blockchain-based auditing exists (Gauthier & Brender, 2021). This lack of compliance concerning blockchain-based auditing was identified as a literature gap. The study focused particularly on compliance gaps in GAAS audit standard AU-C 505 when auditing the balance sheet position accounts receivable.

Chapter three presents the research methodology of the doctoral thesis. It follows a qualitative research approach. The research methodology contains the research method, the research design, the approach to theory development, research techniques to obtain primary and secondary data, data analysis, coding procedures, and ethical considerations when performing interviews.

CHAPTER III: RESEARCH METHODOLOGY

The subject of chapter three is the description of the research methodology based on a qualitative research methodology by an overview of the research methods applied, the theoretical research model, the research approach, data collection and analysis, the data population, the validation strategies of the research results, limitations and delimitations, and ethical considerations.

1. Recapitulation of Research Problem and Research Questions

1.1 Restate the Research Problem

Traditional manual and semi-manual audits procedures based on a risk-oriented audit approach provide several weaknesses as too much workload caused by mainly manual substantive audit procedures that require very large teams resulting in very high costs while just auditing periodically at the end of quarterly or annual periods (Barandi et al., 2020; Wang et al., 2020). Risk-oriented auditing not covering entire populations provides the risk that material misstatements or fraud in financial data are not detected (Cheng & Huang, 2019). Furthermore, it is unknown if blockchain-based auditing, by the example of accounts receivable, is compliant with GAAS standard AU-C 505.

1.2 Restate the Research Questions

The qualitative research methodology aims to answer the following three research questions.

RQ1: How must blockchain technology be designed to serve as a suitable digital tool for auditing?

RQ2: How do blockchain-based audit procedures eliminate weaknesses of manual and semi-manual auditing and requirements for external confirmations?

RQ3: How is blockchain-based auditing toward accounts receivable compliant with GAAS standard AU-C 505?

2. Research Design

The doctoral thesis performs a qualitative research methodology to analyze the suitability, efficiency, and compliance of blockchain-based auditing. Primary data is collected through interviews with auditors familiar with blockchains and IT-related audits based to verify the literature review results. The research methodology and design follow the theoretical model of Saunders´ research onion (Saunders et al., 2019).

2.1 Qualitative Study as Phenomenology

The research is designed as phenomenology that examines phenomena in the way researchers experience things and the meanings of those things in their own experience (Neubauer et al., 2019). Qualitative research aims to analyze phenomena in a particular context based on the experiences of specifically selected individuals rather than attempting to generalize to the population based on the sample (Johnson et al., 2020). The research on the suitability of blockchain-based auditing, its ability to eliminate weaknesses of traditional auditing, and to explore compliance of auditing accounts receivable with blockchains toward AU-C 505, follows an approach as phenomenology (Ward et al., 2018). This phenomenon is analyzed and evaluated by relying on the experience of 22 auditors and their answers to a set of 13 questions in a semi-structured questionnaire. Thus, the research design as a qualitative study is the appropriate research method for the phenomenology approach.

2.2 Research Philosophy

The research philosophy follows an inductive study based on the theory of positivism, as it enables the researcher to operate in an observable social reality to

generate law-like generalizations and produce detailed and accurate knowledge (Saunders et al., 2019). Any social reality is based on individuals´ experiences of that special reality (Gray, 2021). Verification of research results by interviews follows the philosophical theory of phenomenology, as it is designed as an inquiry by a questionnaire, whereby experiences and descriptions of auditors towards the blockchain technology as a unique phenomenon are being analyzed and narrowed down into observable law-like statements by the researcher (Creswell & Creswell, (2018).

2.3 Research Approach

The research approach for the doctoral thesis is performed as an induction to collect relevant data for the topic in two different phases:

Phase 1: A literature review mainly by researching articles in audit and accounting-related journals, publications of US standard setters, and large audit firms by synthesizing and comparing evidence collected to answer three research questions defined by the researcher. Google Scholar serves as the main data source.

Phase 2: Performing semi-structured interviews based on a pre-defined questionnaire and examining the interviewee's answers to verify the results from the literature review. The interviews are recorded and transcribed, while the transcripts are manually coded and analyzed by the software application Atlas.ti (Kalpokas & Radivojevic, 2021).

2.4 Methodological Choice and Research Strategy

The methodological choice of the study follows a monomethod qualitative approach, whereas no quantitative research is performed (Askarzai & Unhelkar, 2017). The research strategy is designed as a narrative inquiry based on several interviews being recorded and transcribed into written representation, whereas researchers are engaged in

data collection, data analysis, and the presentation of the results (Byrne, 2017). The timely aspect of the thesis is performed as a cross-sectional study in which the data collection is conducted on the same target population of 22 interviewees at one point in time, whereby in cross-sectional studies, participants are not surveyed over an extended period (Wang & Cheng, 2020).

3 Population and Sample of Research

3.1 Population of Study

The general population consists of experienced auditors, as seen in Table A4. Table A5 provides further details on education, experience with audits and blockchains, and employment status. The target population concerns auditors focused on IT-related audits that received experience with blockchain technology in the area of auditing in Europe and the USA. The selected sample consisted of 22 auditors from Germany, Austria, Switzerland, the Czech Republic, the UK, and the USA, as seen in Table A6. 13 participants have more than three years of experience with blockchains. At the same time, nine panelists have up to two years of experience.

Apart from one recipient with seven years of experience with auditing, 21 participants have worked for more than ten years in auditing. 16 of the 22 interviewees are employed as owners, respective executives, or at a senior management level in their audit firms. 18 of the 22 recipients hold a master´s degree or a Ph.D., while three of the panelists hold Bachelor´s Degrees, and one preferred not to say. Eight of the interviewees are females; the other 14 are males. See Table A6 for further details.

3.2 Sample Selection for the Phenomenology

The sampling procedures are purposive based on the professional relationships of the researcher with experienced auditors. The researcher contacted participants in his

professional network via phone, email, and video conferencing to convince them to participate in the study. In addition, the researcher asked his contacts to use their professional relationships with other auditors to ask them to participate in the interviews.

Therefore, through the personal interaction of the researcher with potential candidates for the interviews, and in some cases, their willingness to ask other auditors to participate, 22 auditors gave permission to participate. The researcher ensured the participants' confidentiality regarding their statements and full anonymity. Due to the personal contacts of the researcher with other auditors, most of the participants came from Germany. Some German auditors established contacts with auditors in Austria, the Czech Republic, Switzerland, the UK, and the USA. The 22 interviews lasted between 48 and 72 minutes, as provided in Table A2.

Mason (2010) explores the appropriate sample sizes for qualitative research while outlining the saturation problem (Mason, 2010). After a certain amount of data is collected, saturation occurs because no further data relevant to the study can be found because similarities keep occurring (Mason, 2010). Creswell (1998) recommends for research on the phenomenology method a sample size for interviews of five to 25 panelists (Creswell, 1998 as cited in Mason, 2010). Therefore, the sample size of twenty-two experienced auditors as panelists for the interviews is appropriate for phenomenology. An overview of the interviewees, the duration of the interviews, and the size of the transcripts can be seen in Table A3.

4 Data Sources

Collecting primary data through interviews answers the doctoral thesis's research questions (DeJonckheere & Vaughn, 2019). Primary data from interviews provide one of the most effective methods of obtaining such data (Adhabi & Anozie, 2017). Semi-

structured interviews are preferable for qualitative research projects (Adhabi & Anozie, 2017).

5 Trustworthiness of the Research

Trustworthiness of research means the degree to which readers can judge whether the research was conducted honestly and whether reasonable conclusions were drawn (Pratt et al., 2020). Korstjens and Moser (2018), among other authors, take the position that credibility, confirmability, reliability, and transferability represent the relevant quality criteria of any qualitative research (Korstjens & Moser, 2018).

Credibility is ensured by approaches such as

1. prolonged engagement to draw conclusions from the research topic,
2. persistent observation to develop the codes to analyze the data,
3. member check by adjusting transcripts after feedback from the interviewees, and
4. method triangulation by using multiple approaches for collecting data (Korstjens & Moser, 2018).

Transferability will be preserved while patterns and descriptions from one research context also apply to other research projects (Stahl & King, 2020). Confirmability is maintained using consistent and traceable research (Korstjens & Moser, 2018). Multiple coding steps enable the preservation of the reliability requirement of qualitative research (Gray, 2021).

To ensure the qualitative research's reliability, the interviews' transcripts are checked using consistent coding through constant comparison of the collected data with the identified codes and the written transcripts (Memon et al., 2017). The interviews are recorded to avoid researcher bias, whereas their results are documented in transcripts. Afterward, the researcher compares ongoing the results documented in the transcripts

with the findings from the literature review. Finally, the researcher evaluates and compares findings from interviews and the literature review with professional experience in auditing and blockchains.

6 Data Collection and Analysis

Qualitative data analysis is performed by preparing, organizing, transcribing, coding, categorizing, and verifying research data (Lester et al., 2020). The results of the interviews are documented, checked and analyzed, and compared with the literature review results for verification (Saunders et al., 2019).

6.1 Procedures for Data collection

All respondents received an electronic invitation via email, with appointments for the survey made in advance. By electronically confirming the appointment invitation, the interviews could be scheduled accordingly. Before the interviews began, the researcher obtained permission to record the interviews, which was agreed to by all interview participants. Data collection of all interviews was based on remote video conferences via Microsoft Teams on the internet, whereas the implemented recording function in Microsoft Teams recorded the interviews. The researcher shared the screen so that the researcher and interviewees had common access to the questionnaire. During the interviews, the researcher and the participants ensured they were each alone in a private room or office with a locked door. Each interview took place in a single interview session.

The interviews were performed by a semi-structured questionnaire of 13 questions applied to all the interviews. In case of queries by the interviewees, the researcher provided a short explanation of the topic or the respective questions. After performing the 22 interviews, the interviews were recorded and converted into written transcripts (Loubere, 2017) by the researcher into a Word document of approximately three pages.

The conversations are converted into text through transcription, simplifying the analysis process and helping the researcher evaluate the interviewees' statements (Nascimento & Steinbruch, 2019). The transcribed interviews were emailed to respondents for review to determine the extent to which their responses were accurately reflected. Apart from minor corrections, the participants agreed with the transcripts.

The participants are not informed about the other participants' opinions to keep the answers as neutral as possible. Transcripts of interviews serve as a data basis for a narrative analysis (Nasheeda et al., 2019). In qualitative research, data obtained from interviews are transcribed verbatim to enable analytic procedures of primary data (Lester et al., 2020). Transcription allows researchers to better and more capture and recognize evidence obtained (Zakaria et al., 2015). Transcription into written form helps the researcher to structure data for reporting purposes (Zakaria et al., 2015).

6.2 Data Analysis by Coding

Coding can be defined as follows: "Coding is a key structural operation in qualitative research, enabling data analysis and successive steps to serve the purpose of the study." (Williams & Moser, 2019, p. 45). The coding process is performed in three steps first-order analysis, second-order analysis, and aggregated dimensions. Further details of the different codes are presented in Appendix E.

6.2.1 First-Order Analysis

The first steps in the qualitative analysis encompass preparing and organizing data towards the thematical approach to blockchain-based auditing by gathering data from the 22 interviews and preparing transcripts for analysis (Lester et al., 2020). First-order analysis or open coding procedures distill data, sort it, and allow comparisons with other segments of data (Friese, 2022). Important for the efficiency of open coding is a

systematic approach to the identified thematic fragments and concepts (Williams & Moser, 2019).

In first-order coding, the researcher aims to formulate data and phenomena regarding concepts by screening the responses and organizing similar words and phrases into broad thematic areas (Williams & Moser, 2019). A first-order analysis serves to identify important patterns in the data, then mark them accordingly, and identify patterns in the data to clarify the research questions and the reviewed literature (Mohajan, 2018). The coded transcripts support the researcher by structuring the obtained data, finding tendencies and similarities, and drawing appropriate conclusions from the qualitative data.

6.2.2 Second-Order Analysis

In the subsequent second-order data analysis, identified patterns from the first-order analysis are developed and transcribed into thematic descriptive categories (Mohajan, 2018). Codes or themes identified by first-order coding are further refined and categorized to develop core codes by an inductive analysis to explain the research findings (Williams & Moser, 2019). Specific categories are developed from core codes through condensation (Williams & Moser, 2019).

6.2.3 Aggregated Dimensions

Different motivational drivers of different interaction outcomes are grouped into aggregated dimensions (Löher, 2019). Selective coding allows the researcher to select and integrate categories of the selected data into real phenomena (Williams & Moser, 2019). Aggregating the analyzed data allows the formation of progress results in the form of theoretical concepts and the interpretation of the meaning of the results and the theories developed from them (Williams & Moser, 2019).

7. Adherence with Ethical Requirements

Ethical considerations for undertaking qualitative research methods require guidelines to protect sensitive data obtained within the study (Arifin, 2018). All the participants were professionals in the field of auditing. The youngest participant is 32 years old. Fulfilling these criteria qualified them as appropriate participants for this study. The interviews are performed in accordance with the AICPA Code of Professional Conduct (Mintz, 2020), whereby an ethical standard serves as a guideline. After answering the questionnaire, interview participants are assured by the researcher that ethical standards will be adhered to.

Participants are warranted anonymity and confidentiality regarding their statements. Their names and identities will not be published during data collection on the occasion of data analysis or by reporting the study results. The recorded materials will be deleted after the successful defense and publication of the work. This ensures that their data are protected appropriately. Thus, throughout the study, the researcher assigns the aspect of ethics a very high priority.

8. Limitations and Delimitations of Study

Limitations related to the research methods, the sample, the instruments, the process of data collection, and the data analysis are described in this section. Research limitations and delimitations are addressed to ensure the quality of findings and the interpretation of the evidence presented (Theofanidis & Fountouki, 2018). The study aims to classify the appropriateness of the research activities in an overall context by examining the collected information with the findings of other authors (Creswell & Creswell, 2018).

8.1 Limitations

Blockchain-based auditing provides a highly specialized area of knowledge. Thus, it is difficult to identify suitable panelists of auditors while encouraging their participation. The lack of practical experience of interviewees in auditing with blockchains limits the scope of the study. Auditing with blockchains overall and accounts receivable to some extent is a mere academic discussion due to a lack of in-depth practical experience. Few interviewees have in-depth practical experience with blockchain-based auditing of accounts receivable. As another limitation, the dataset includes mostly peer-reviewed articles in journals from the Google Scholar database. However, Google Scholar has a high reputation and encompasses many peer-reviewed journals.

8.2 Delimitations

As research by authors as Mason (2010) and others has shown, a population of 5 to 25 interviewees is appropriate in qualitative research (Mason, 2010). The population of interviewees is limited to 22 participants by the researcher. To compensate for some interviewees' lack of experience with blockchains, the researcher interviewed only auditors with deep knowledge of IT-based auditing. These auditors are more able to empathize with the subject matter of blockchain-based auditing.

Geographic limitations on auditors from Germany will not be an issue, as auditing accounts receivable procedures are similar to AU-C 505 procedures. In 2008 the IAASB codified ISA standard 505 (IAASB, 2008) "External confirmations." AICPA codified in 2012 audit standard AU-C 505 "External confirmations." In 2021 the German IDW codified audit standard ISA [DE] 505. Interviewing German and other European auditors regarding U.S. auditing standard AU-C 505 will not result in misleading conclusions, as

requirements and procedures for auditing accounts receivable according to ISA 505 and ISA [DE] 505 are very similar to AU-C 505 procedures.

9. Summary of the Research Methodology

Chapter III presents a detailed description of the qualitative research methodology employed to answer the three research questions of the study. This chapter describes the qualitative research approach, the philosophy of positivism, the approach of working with the literature, the questionnaire design, the methods of data collection to obtain primary and secondary data, and data analysis. The obtained data from the interviews are transcribed, whereas the transcripts are evaluated by a narrative analysis based on coding by first and second-order analysis and aggregated dimensions.

The results from the literature review are assessed by content analysis. The sample of interviewees consists of 22 participants who answered a semi-structured questionnaire of 13 questions. All study participants contributed to the research by sharing their profound experiences with IT-based auditing and blockchains. The next chapter four presents the research results of the interviews. Moreover, chapter IV aims to demonstrate that the research method outlined in chapter III has been adhered to.

CHAPTER IV: RESEARCH RESULTS

Chapter four of the doctoral thesis presents the interviews by analyzing the questionnaire data. It addresses the three research questions of the thesis and provides an overview of the number of interviewees, their backgrounds, and their geographical location.

1. Introduction to Data Analysis and Research Results

1.1 Aim of Research to Answer the Research Questions

Chapter four contains the results of the study on the phenomenology research that was performed to answer the three research questions of the doctoral thesis:

RQ1: How must blockchain technology be designed to serve as a suitable digital tool for auditing?

RQ2: How do blockchain-based audit procedures eliminate weaknesses of manual and semi-manual auditing and requirements for external confirmations?

RQ3: How is blockchain-based auditing toward accounts receivable compliant with GAAS standard AU-C 505?

1.2 Addressing the Research Problem

The literature review revealed that traditional manual auditing provides weaknesses (Wang et al., 2020). The study focused on improvements in audit quality and efficiency through a digital audit approach by blockchains. At the beginning of the research, it was unknown how or to what extent weaknesses of traditional audit procedures in general and toward accounts receivable could be solved. Research has shown that the full potential of blockchain technology is not exploited, as virtually only

a few auditors owned practical knowledge of how to apply it (Wongthongtham et al., 2021).

1.3 Purpose of the Doctoral Study

From the background of identified audit weaknesses, the study aims to explore the characteristics of blockchain technology to evaluate auditing with blockchains that provide the potential to eliminate shortcomings of current manual and semi-manual audits. The study further examined whether there are any regulatory gaps in blockchain-based auditing concerning the existing AU-C 505 in the der current GAAS. The research approach aims to add knowledge to the academic body, to guide audit firms on how to implement and operate blockchain-based auditing, to outline the efficiency of blockchain-based auditing towards accounts receivable, and to provide information for standard setters concerning regulatory gaps by blockchain-based auditing, and requirements for new and revised audit standards for blockchains.

1.4 Demographics

Twenty-two auditors participated in the interviews for the doctoral study. The sample size of 22 interviewees fulfills the requirement of five to 25 interviews, as indicated under the research methodology in chapter III. The questionnaire is based on 13 questions focused on answering the research questions and nine questions concerning demographics. Five questions dealt with the suitability of blockchains, and six further questions focused on eliminating audit weaknesses by blockchains. In comparison, two questions concerned the identified literature gap on blockchains' compliance with audit standard AU-C 505.

Concerning the age of the interviewees, fourteen of the interviewed persons were male, and eight interviewees were female. Among the 22 interviewees, ten participants

were between 36 and 45 years old. Five of the participants are between 46 and 55 years old. Four interviewees are aged older than 56 years. Two of the respondents are aged between 26 to 35 years.

By qualification, all interview participants are certified as auditors. Six interviewees are licensed as German CPAs. Another five panelists are approved as Certified Information Systems Auditors. Two participants held a license as ISO 27001 Lead Auditor. Two panelists hold ACCA licensure. One attendee of the interviews qualified as an ITIL Professional. Two persons are licensed as US CPAs. One recipient had a Swiss CPA, and one panelist holds an Austrian CPA license.

All participants of the interviews are very experienced in auditing, with at least eight years of experience in auditing to more than 15 years of experience with audit work. Twelve interview attendees had a good experience with blockchains of over three years. Ten panelists had extensive experience in IT-related audits but little experience with blockchains of up to two years. Almost all interviewees gained more than nine years of professional experience with auditing, whereas one interviewee had six to eight years of professional experience with blockchains.

The size of the audit firms of the interviewed persons varied from very large to medium-sized. Two of the interviewed auditors were employed at the so-called very large Big Four audit firms. Two more panelists are employed at one of the next ten largest audit firms after the four largest ones. One recipient is employed at a larger audit firm of up to 500 employees. The other 17 interviewees worked at medium-sized firms with up to 200 employees.

Thus, most interviewees are employed at medium-sized audit firms. Concerning the countries of origin, the plurality of interviewees, 16 participants, come from Germany.

Two panelists are from the USA, one from Switzerland, one from Austria, one from the UK, and one from the Czech Republic. Table 5, Table 6, and Table 7 show further details on the demographics of the 22 interviewees.

1.5 Data Collection

For data collection, a pre-defined semi-structured questionnaire was designed to obtain primary data through the interviews. The results of the interviews were transcribed and coded. The interviews with 22 auditors employed at large and medium-sized audit firms from Austria, Germany, Norway, Switzerland, the UK, and the USA were the primary source to answer the research questions. The demographic questions were used as supporting data for the research.

1.6 Data Analysis

Chapter IV includes tables and graphs to present the results of individual interviews. A narrative analysis was performed to analyze the interview answers concerning the three research questions. The interviews were analyzed per question. The research procedures for evaluating the interviews were conducted in three levels of analysis first-level coding, second-level coding, and aggregate dimensions.

First, the 22 interviews were manually coded per question using first-order coding. The researcher coded the responses according to categories or themes in this process. Transcripts of the interviews were uploaded into the software application Atlas.ti and evaluated. The implemented functions coded data from the interviews in Atlas.ti. Matching manual and software-based coding helped the researcher consistently highlight key elements during coding through a thematic analysis concerning the three research questions. This allowed relevant codes to be identified. As a result of the first-order coding, 43 codes resulted, as shown in Appendix E.

The results of the open coding were used in the subsequent second-order coding phase to identify similarities regarding the identified codes toward the relevant audit area respective questions on interviews. The second-order analysis showed categories towards blockchains, audits with blockchains, and compliance of blockchain-based audits of accounts receivable. Afterward, the selected codes were grouped into aggregated dimensions that formed the foundation for the research questions.

To answer RQ1, data was collected with five questions from the questionnaire. Data by answers from questions six to 11 of the questionnaire aimed to answer RQ2. Answers to questions 12 and 13 were collected to address RQ3. The data analysis process was performed by coding the research questions as shown in Appendix E. Toward RQ1, coding was done, among others, by the words “suitable tool,” “distributed database,” “peer-to-peer network,” and “smart contracts.” To address RQ2, coding was done, among others, by “eliminating weaknesses,” “manual auditing,” and “semi-manual auditing.”, “smart audit procedures,” “accounts receivable,” and “external confirmations.” To answer RQ3, coding was done, among others, by “ISA 505”, “AU-C 505”, “ISA [DE] 505”, and “compliance gaps.” The interpretation of the data collected was made by graphical and statistical evaluation.

Data collection was based on 22 interviewees. The population of interview respondents was sufficient to conclude. The quality of the data collected is appropriate as all interviewees are experienced auditors. The quantity of the data is sufficient to answer the three research questions. The suitability of blockchains for auditing could be revealed. The results showed a tendency to the existing weaknesses of traditional auditing and the superiority of blockchain-based auditing. The questions helped to identify a compliance

respective literature gap. At the same time, all interviewees agreed on the need for revised or new audit standards dealing with blockchains.

2 Results of Qualitative Research

The following chapter presents the results of the interviews regarding the doctoral study's research questions. All interviewees answered the complete questionnaire. To illustrate the respondents' statements, in general, 2-3 representative participants' responses on each relevant topic were described in more detail. An overview of the questionnaire concerning the interviewees is attached in Appendix D. The assigned codes for the respective research areas are provided in Appendix E.

2.1 Objective 1: Suitability of Blockchains for Audits

Appendix C presents in section I an overview of the five questions to evaluate the suitability of blockchains for audit purposes by 22 participants.

2.1.1 Blockchain Knowledge and Relevant Blockchain Features

To evaluate the interviewees' knowledge level, the researcher inquired about their knowledge of blockchains. Although the recipients gained different experiences, all were familiar with blockchains' basic concepts. They generally characterized blockchains as digital tools for collecting data in blocks and affirmed that new blocks attach data to the existing blockchain. The interview participants understand that blockchain nodes interact with each other. They assume that blockchains provide a higher security level than common accounting systems. In addition, the researcher interviewed the participants on the blockchain attributes of distributed databases, peer-to-peer transmission, irreversibility of records, and smart contracts.

Regarding distributed databases, participant 15, one of the interviewees' most experienced auditors, points out that it is more difficult to corrupt a distributed database

than a centralized ERP database. Interviewee 22 emphasizes that from her background as an IT auditor, the advantage of distributed databases is that all blockchain participants, their auditors, and the customers of the auditee and their auditors have direct access to all accounting-related data they require. Recipient 13 appreciates the lower cybersecurity risks of decentral databases than centralized data management in ERP systems, as all blockchain data are asymmetrically encrypted and hashed. She outlines that no blockchain node owns full control of the blockchain data. Thus, federated databases render blockchains tamper-proof and data immutable as 51 percent of attacks become less probable, while modifications or deletions of blockchain are almost impossible.

Panelist 7 talks about his experience on peer-to-peer networks in a blockchain test environment. He confirms the outcome of testing that peer-to-peer transmission is highly effective for exchanging information directly among the involved blockchain peers by exchanging data anonymously. Participant 15 outlines the value of peer-to-peer transmission for blockchains, whereas most peers authorize and verify blockchain transactions. Participants 6 and 20 underscore their skeptics of the effectiveness of peer-to-peer networks. They indicate that potential IT incidents more often lead to disruptions in the blockchain mechanisms, whereas the effectiveness of peer-to-peer networks is challenged.

Most of the interview participants confirm the concept of the immutability of blockchain data. Panelist 7 summarizes the opinion of the other participants by stating that the basic functions of blockchains ensure the irreversibility of records. Panelists one and three disagree. They outline that in a private blockchain, the owner can change data. Recipients 10 and 14 neither agree nor disagree. They outline that it depends on the blockchain type if the data is immutable. According to panelists one and three, they refer

that the owner may change the date in a private blockchain. In a public blockchain where no one controls the blockchain, there is a higher chance that intruders affect the blockchain adversely.

Seventeen interviewees agree on the increased speed and quality of blockchain transactions by applying smart contracts. Participant 13 highly appreciates the benefits of smart contracts. He means there is no human intervention when blockchains are combined with smart contracts, as the smart contract performs authorization and verification. The tool checks the predefined rules. The application of smart contracts highly improves the speed and quality of blockchain transactions.

Recipient 22 stresses that auditors must check the integrity of smart contracts´ logic yearly to ensure that the computerized logic remains unchanged. Interviewee four does not provide a clear statement, as he is indecisive about the benefits of smart contracts on the efficiency of blockchain technology. He means that technical issues might impact the effectiveness of smart contracts. On the other hand, errors in the programming of the implemented logic will result in serious economic damage.

To sum up, as shown in Figure B1, most interviewees agree on the relevance of the specific blockchain features for auditing. Seven codes are assigned to these attributes that form the subsumption of blockchain features.

2.1.2 Most Suitable Blockchain Type for Auditing

Three codes were identified concerning the three different blockchain types: public, private, and consortium. The responses from participant 17 reflected, to a large extent, the views of the 16 supporters of consortium blockchains as the most appropriate type for auditing. She reasoned that a public blockchain is unsuitable for audit and accounting purposes, as all participants can access all data. Private blockchains are too

influenced by one party, whereas the risk of control is too high. Thus, she affirmed consortium blockchains as the most suitable audit type. Participant 11, a very experienced German CPA, points out that only public blockchains can be accepted for auditing as no central authority or auditee controls the blockchain. In this way, he adequately reflects the opinion of the minority of six examiners.

In summary, Figure B2 indicates consortium blockchains as the most suitable blockchain type. No interviewee rates private blockchains as a suitable blockchain type due to the major influence of an auditee firm respectively, a central authority on the blockchain. At the same time, some participants mean that public blockchains are most suitable. The researcher identifies three codes in this examination field.

2.1.3 IT-Security of Blockchains in contrast to ERP Systems

Participant 4 affirms blockchains' higher level of cybersecurity compared to ERP systems. He means blockchains are more difficult to corrupt. Threats from hostile encryption of blockchains are lower as a second party executes other protection mechanisms. Backward changes are not possible. In case of an attack, only one database might be corrupted and not the blockchain as long as no one owns more than 50 percent of the blockchain power. In the case of cyberattacks, when hackers try to encrypt databases to extort money, they do not even get access to payment data. The risk of extortion is lower than in ERP systems as intruders cannot encrypt all blockchain nodes due to the distributed database, as redundant ledgers provide more stability. Thus, blockchains are more stable than ERP systems against cyber security risks.

Panelist 13 confirms this point of view. He underlines that blockchains are more secure than traditional ERP systems. In case intruders manipulate data, these data are no

longer identical to the databases' respective ledgers of the other participants. The other blockchain participants would realize that blockchain data was changed.

Controversial opinion towards a higher level of security holds participant 22. He outlines that blockchains are exposed to cybersecurity risks just as ERP systems. In data-intensive industries such as auditing, blockchain technology also harbors risks beneath several benefits. If hackers could perform a 51 percent attack and gain control over the blockchain, they would be able to alter the blockchain data. In such instances, blockchains are threatened by much higher cybersecurity risks than ERP systems. Panelist 14 remains indecisive due to a lack of profound knowledge.

As seen in Figure B3, blockchains provide a higher level of security than ERP systems. Although a majority holds this view, no explicit statement is emerging. The research reveals three codes concerning the protection of blockchains.

2.1.4 User Access Management on Blockchains

The interviews reveal that the plurality of recipients affirms the requirement of reliable user access management when auditing with blockchains. Participant eight share his professional experience regarding the audit of digital accounting systems. Representative of the others, he states that blockchains, just as ERP systems require access controls based on the need-to-know and need-to-do principles. In a consortium blockchain counterparts shall only get access to the data they need for their tasks. Auditors need access to the corresponding accounts payable data of their auditee´s accounts receivable when testing accounts receivable. Participants 16 and 21 decline specific user management for blockchains. They outline that user management is no longer required on blockchains due to implemented blockchain mechanisms. Participant 17 is unsure if the blockchain mechanisms would operate effectively. Therefore, she remains indecisive.

To summarize, Figure B4 reveals that dedicated user access management is required for blockchain systems. Nineteen interviewees agree that blockchains require proper user access management for auditing, while two recipients disagree, and one provides no clear answer. Two codes are assigned to this research area.

2.1.5 Appropriate Architecture for Blockchains

The researcher interviewed the recipients on appropriate blockchain architecture, including interoperability issues, changelogs, and blockchain segregation. Representative of the interviewees, attendee seven, a Ph.D. with long years of business experience in audits and blockchains, underlined the benefits of an appropriate IT architecture. The architecture must consider the business needs of the auditee and the audit firm. It must enable auditors to implement smart audit tools that perform continuous audit procedures.

Concerning blockchain architecture, several auditors raise concerns about interoperability problems. Interviewee 15 holds a master’s degree in Computer Science, which means that a blockchain's dependency on the infrastructure's reliability is lower than in centralized ERP systems, as database administrators do not have access to the blockchain data. He outlines that the risks of blockchains are lower as they do not need a secure operating system and no protected database and applications. However, he means that a protected IT environment in a blockchain system is still required. Two other participants are indifferent.

Panelist 11, a very experienced German CPA with a special focus on IT audits teaching audit classes, points out that interoperability problems exist among blockchains and ERP systems, as no IT regulations govern common standards for IT architecture blockchains. Participant seven is among the two indecisive auditors who neither agree nor disagree. He means that there are technical challenges concerning interoperability

among different IT systems that an API can solve. However, he refuses general interoperability problems concerning the connectivity of blockchain systems. Overall, the interviewees provide a clear statement on interoperability problems when applying blockchains with other blockchains or ERP systems.

The architecture must enable the traceability of transactions and changes to the blockchains. The changelogs record all changes to the blockchain, whereas they create an audit trail to track fraudulent actions toward the blockchain. 19 of the 22 interviewed auditors affirm the necessity of implementing changelogs to blockchains, while three disagree. Participant 15 agrees that all transactions and changes on blockchains must be logged. He outlines that distributed ledgers are less risky than centralized databases. However, he means that change management is still required, as it is important to understand all changes to a blockchain system. Auditor 12, an Austrian CPA, disagrees. She means that blockchains contain all data from the beginning. Thus, additional changelogs are optional in addition to the blocks that contain all data and information.

Most of the interviewees affirm the requirement of separating blockchains into different layers. Participant 13, a US CPA with some blockchain experience but extensive auditing experience, agrees on the blockchain segmentation. He explains that blockchains need a basis layer for infrastructure to run the blockchain. Also, connectivity requires a different layer and the storage layer that records the transactions. Another layer serves for authentication and authorization. The business logic for business processes needs a separate layer as well. Furthermore, he outlines that blockchains require ERP functionalities, even if data is not stored in a central database but in a distributed database.

Participant four, a specialized IT auditor, is expressing different opinions. He is among the few that decline the segmentation requirement. He insists that as the other

recipients deny a separation, blockchains provide a complete system based on blockchain mechanisms that authorize, verify transactions, and regulate themselves. Blockchains require platforms to implement smart contracts and smart audit procedures.

In conclusion, as shown in Figure B5, the interviewees clearly state interoperability problems when applying blockchains with other blockchains or ERP systems. The interviews reveal that changelogs significantly increase the auditability of blockchains. Furthermore, the segmentation of blockchains into different layers is favored as it improves the understanding of this technology and expands its applicability. Four codes are identified in this research area.

2.1.6 Summary of Findings on Blockchain´s Suitability for Auditing

The interview results revealed that most participants affirm the usefulness of the distributed database, peer-to-peer transmissions, irreversibility of records, and higher speed and quality by smart contracts for auditing purposes. Most interviewees affirm consortium blockchains as the most useful type for auditing. Most attendees agree on the higher security level of blockchains for ERP systems, but several panelists need clarification or deny a higher security level.

Almost all respondents affirm the requirements for dedicated user management and an adequate IT architecture considering interoperability issues, recording all blockchain changes in changelogs, and separating the blockchains into different layers. The results of the interviews do not provide a large variance, as auditors engaged in IT-related audits are familiar with the major IT frameworks such as COBIT 2019, ISO 27001, or ITIL. To summarize, most interviewees agree on the suitability of blockchains for auditing. Only a few attendees in the interviews disagree. Second-Order-Coding reveals

the three attributes of blockchain features and blockchain characteristics as prerequisites for auditing and the most suitable blockchain type, as outlined in Appendix E.

2.2 Objective 2: Eliminating Audit Weaknesses by Blockchains

Section II in Appendix D provides the six questions twenty-two participants answered concerning audit weaknesses and their elimination with blockchain-based auditing.

2.2.1 Weaknesses of Traditional Auditing

The interviewees had to evaluate potential weaknesses of traditional audits that are mainly manual or semi-manual. Participant two, one of the strong supporters of traditional audit weaknesses, admits to most interviewees that sampling procedures are less valid than auditing entire populations. He means that audit evidence is obtained by a risk-oriented sampling approach covering only a portion of the population. Because auditing only covers a fraction of the population of accounting-related data, risks remain that material misstatements or fraud remain undetected.

As further weaknesses, he underlines that manual substantive audit procedures are costly and work-intensive compared to automated ones. He also affirms that the high workload results in too large audit teams. Recipient 15 agrees with the opinion of participant two that sampling cannot ensure that all material deviations, misstatements, or fraud can be identified. Furthermore, he outlines that manual or semi-manual audit procedures are costly and work-intensive, requiring unnecessarily large audit teams.

However, panelist 22 holds a differentiated opinion. He means that traditional auditing based on sampling procedures by periodic auditing provides some weaknesses as sampling is not as valid as auditing entire populations. However, in general, he confirms the ability of traditional audits to address all relevant misstatements or fraud.

Concerning auditing costs, he emphasizes that universal automated audit tools such as blockchains only work if all rules and decisions are automated. Relating to the high costs of manual auditing, he insists that digital devices such as CAATs cause other costs. Regarding audit staff, he supports the view that tool-based audits require less audit staff.

Panelists 2 and 11, both German CPAs, do not answer clearly. They claim that current audit procedures could identify material misstatements and most fraud in financial statements. Otherwise, they admit that manual audit procedures might be inferior to automated auditing. To sum up, Figure B6 reveals that most interviewed auditors affirm such weaknesses. Five codes were identified during the research.

2.2.2 The Necessity for External Auditing on Blockchains

Recipient 13, a US CPA with long experience in auditing and good knowledge of blockchains, strongly agrees with the requirements of external audits. He means blockchains evaluate the authorization to execute transactions and verify the appropriateness of these transactions. Still, blockchains cannot assess the fair value of goodwill, the need for depreciation of accounts receivable or fixed assets, nor the extent of contingent liabilities if the auditee is sued for any form of compensation for damages. Auditors are still required to evaluate management estimates. Furthermore, he outlines that we may no longer need external audits if there is a worldwide standard for all IT systems to be certified. Nevertheless, he adds that such a standard is far from utilization.

Participant five, an auditor with some experience with blockchains, points out that blockchain mechanisms alone cannot guarantee the completeness of accounting-related transactions. He emphasizes that blockchains require an effective ICS, whose effectiveness in terms of the completeness of the accounting-relevant transactions must be confirmed by an external auditor. Interviewee 21 amends that audit standards require

quarterly or yearly audits. She disagrees as nodes control themselves why external audits are no longer needed. The interviews reveal, as shown in Figure B7, that the plurality of auditors affirms the requirement for external audits on blockchains. The analysis of data identifies two codes.

2.2.3 Superiority of Smart Audit Procedures

Smart audit tools enable continuous auditing procedures of all blockchain transactions almost in real-time and internal controls. Thus, smart audit procedures cover entire populations of accounting-relevant data. Participant 22, a CISA with in-depth knowledge of IT-related audits and good knowledge about blockchains, agrees that smart audit procedures could perform transactions and control attitudes continuously when relevant information is inside the database. Before an audit engagement is accepted, risk factors can be systematically captured and assessed by smart audit tools to facilitate the early identification of necessary quality assurance measures that enable more accurate auditing of accounting and compliance issues. In his view, continuous auditing works for most transactions based on data reliability, but not all issues can be audited automatically, respectively continuously. In general, he affirms that smart audit procedures that cover all transactional data on blockchains render sampling procedures obsolete if internal controls ensure that all accounting-relevant data is recorded in the blockchain. In this regard, he states that if smart audit tools inspect transaction by transaction, it is probably not sure that all relevant audit and fraud risks are addressed.

In case smart audit tools check transactions backward and compare them with the actual transaction, they can manage all appropriate audit and fraud risks. Concerning the high costs of manual auditing, he points out that digital audit tools are also costly, whereas

they have to compensate for their costs over time. So, one part of the costs is offsetting another part of the costs. He affirms that it is smarter to offset staff against digital tools.

Participant 13, a US CPA who encounters blockchain technology during his professional practice, supports this view. He means that ensuring the completeness and integrity of accounting-relevant data is very important. Blockchains show the current status of recorded transactions but do not assure the completeness or integrity of accounting. Therefore, auditees must implement additional internal controls beneath the existing blockchain. Otherwise, blockchains are not useful tools for auditing purposes.

Participant 20, a German CPA with profound knowledge of IT-based audits, is skeptical about the operability of blockchains in auditing. Participant 13 states the importance of completeness of data and that auditors must understand the outcome of blockchain data. He sees risks that employees lever out the ICS. Therefore, he affirms that without establishing an effective ICS, he rejects to accept blockchains in auditing and accounting. Recipient 22 points out that auditees require an effective ICS without further addressing possible blockchain weaknesses. Based on the implemented ICS, he supposes blockchain could replace traditional auditing tools and procedures.

Participant 11, a highly skilled German CPA and IT auditor familiar with blockchain-based auditing is skeptical and disagrees with eliminating sampling procedures by smart audit tools. He means that it depends on the origin of transactions. In a complete blockchain-based system where all processes and transactions are based on blockchains, it is appropriate to omit sampling procedures. If transactions and data are generated from outside the blockchain, the auditor has to perform sampling procedures to understand transactions substantially. He agrees that smart audit tools provide the potential to detect all fraud. In blockchain systems, risks remain if two or three employees

collude to lever out the ICS. Participants one and 19 decline to provide a clear answer as they point out that the risks of smart audit tools have yet to be researched in-depth. However, they affirm the high potential of continuous audit procedures.

To conclude, Figure B8 shows that smart audit procedures are effective, but auditors must evaluate whether to invest in human engagement or implement digital tools. Furthermore, the research reveals the requirement of auditing the ICS of the auditee in addition to smart audit procedures, as provided in Figure B9. The research identifies five codes concerning the application of smart audit procedures.

2.2.4 Audit of Blockchain Code, Mechanisms, and Access Controls

Interviewee 15 states that transactions in a blockchain do not guarantee reliable financial reporting, as blockchain mechanisms do not verify the appropriateness of the underlying contractual agreements. Thus, under continuous audit procedures, at least yearly testing of the integrity of the blockchain code, the access mechanisms, and the effectiveness of access controls on the blockchain are required. He underlines the need for these additional audit procedures to provide more reliability so that no changes to the blockchain code are made. Participant nine also agrees to perform additional audits under continuous auditing. She also confirms that auditors must test the integrity of the blockchain mechanisms at least once per year, as disagreements in the blockchain could indicate an attack. Moreover, there is more reliability if smart audit tools confirm that no changes to the blockchain code were made. Yearly testing of access controls ensures that no unauthorized access happens.

Participant 19 disagrees with additional audits as he means that smart audit tools inspect all accounting-relevant transactions and check internal controls on the completeness of transactions and data integrity. Participants two and nine neither agree

nor disagree. They mean that smart audit tools would be useful in audits by processing large amounts of data. However, data quality must continue to meet the highest standards, be applicable and user-friendly in practice, and that technologies are compatible with existing systems, processes, and ways of working. Thus, they have arguments for additional audits and against them.

In summary, a plurality of interview participants affirms the requirement of yearly audits of blockchain codes, mechanisms, and access controls, as seen in Figure B10. Some interviewees disagree, while few panelists remain indecisive. The transcript analysis reveals three codes.

2.2.5 Blockchain Impacts on Audit Profession and Auditor´s Role

Participant 18, a female CISA, had intensively studied digitalization's impacts on the audit profession. She means that the requirements and tasks of auditors would change by blockchains. Mainly manual substantive audit procedures will turn into continuous audits. The auditor´s role will change from testing transactions to testing controls and merely evaluating management assertions. Concerning regulations, she outlines the requirements for new audit standards and modified regulations that address specific blockchain features. Participant 21, an ISO 27001 Lead Auditor and data analyst that supports audit firms on IT-related procedures as part of the audit of the financial statements, considers the large impacts of blockchain technology on the role of the auditors when auditing blockchains and the audit profession itself. She stresses that data analysis with tools such as IDEA would become paramount for auditors that perform additional testing of data and internal controls beneath continuous auditing. He also notes that current regulation needs to cover blockchain requirements adequately.

Participant 12 disagrees with the high impact. She outlines that the auditor would continue to be the focal point of an audit because much of the higher-value audit work remains with the auditor himself. She agrees with some support but declines a disruption of the audit industry and major changes in the role of auditors by blockchain technology. Attendee one does not provide a clear answer. She is sure about the potential effects of the blockchains, but he means that currently, we are so far away from widespread adoption of blockchains in auditing that it is too far to provide a clear statement. She indicates blockchains represent a "job enrichment" and not a "job replacement" for auditors. As seen in Figure B11, almost all interviewees expect major disruption from blockchains on auditing and the auditors´ role.

2.2.6 Blockchains Render External Confirmations Obsolete

Participant 9, a very experienced Swiss CPA, means consortium blockchains host the auditees and their customers. She points out that all relevant information is available for the auditor when auditing accounts receivable in consortium blockchains. Auditors get access to the receivable data and additional information, such as invoices and transport documents. Due to consortium blockchains' characteristics, the auditors can also access the corresponding accounts payable data of the auditees´ customers. In addition, he states that the consortium nodes must monitor the integrity of the blockchain system. She recommends that the consortium blockchain be certified or checked once per year, similar to a SWIFT audit, to ensure a high quality of accounting-related processes, then requests for external confirmations become obsolete.

Interviewee 19, a highly skilled auditor focused on IT, emphasizes that if blockchain systems are implemented properly, requests for external confirmations are no longer required. He outlines that only consortium blockchains are suitable for auditing

accounts receivable in one blockchain system. Private blockchains do not support connections to external data, while public blockchains do not protect confidential accounting data against unauthorized access. According to him, reviewing one sample per year is still recommendable.

Participants one, eleven, 15, and 22 decline that auditing of blockchains renders third-party confirmations as obsolete. They mean that blockchains, like other IT-based accounting systems, are threatened by cybersecurity risks. In the case of 51 percent attacks, intruders could tamper with or steal blockchain data. If no special audit standards exist for blockchains, the requirement to audit accounts receivable in addition to blockchain procedures remains. Two recipients are unsure, as it depends on the blockchain type.

Finally, as provided in Figure B12, most participants agree that requests for external confirmations when auditing accounts receivable are no longer required in a consortium blockchain. However, most recipients decline to apply for private or public blockchains. Three codes are assigned on external confirmations.

2.2.7 Summary of Eliminating Audit Weaknesses by Blockchains

Most interviewees agree on the weaknesses of traditional sampling-based audit procedures. In contrast, most interview participants considered periodic auditing at the end of fiscal periods inappropriate to detect all material misstatements and fraud. According to most interview panelists, manual auditing is considered too expensive by requiring unnecessary large audit teams. Most of the interviewees affirm the requirement for external auditing of blockchain systems. Furthermore, most interview respondents agree that smart audit procedures enable auditing of all transactions almost in real-time,

and smart audit procedures support lower audit costs. Whereas a plurality agrees that smart audit procedures render sampling to obtain audit evidence obsolete.

Similar results raise the question of whether smart audit procedures performed throughout the year on all accounting-related transactions effectively address all relevant audit and fraud risks. Almost all interviewees confirm that testing the blockchain code, IAM, and blockchain mechanisms is required at least once per year. Most of the attendees of the interviews consider establishing an effective ICS very important. Most panelists at the interviews agree on the large influence of blockchains on the role of the auditors and the audit profession. Most interviewees affirm the need for blockchains to enable proper automated verification of receivables to render requests for external third-party confirmations of accounts receivable obsolete. Second-order coding shows audit weakness of traditional auditing, benefits from continuous auditing with blockchains, and the requirement of supplementary auditing procedures, as shown in Appendix E.

2.3 Objective 3: Compliance Gaps by Blockchains towards AU-C 505

Appendix D presents in section III the two questions concerning the compliance of blockchain-based auditing with current GAAS.

2.3.1 Compliance of Blockchain-based Audits toward AU-C 505

Participant 22, a very experienced professional in auditing with a special focus on IT audits and good experience with blockchains, also teaches auditing classes outlines that blockchains provide a digital approach to data analysis by tools that extract all the relevant data to examine accounts receivable from consortium blockchains. He points out that any abandonment from external confirmation requests by digital blockchain-based procedures cannot comply with the audit standard AU-C 505, as the standard provides “must” requirements.

Panelist 12 confirms the opinion of participant 22, who also possesses deep experience in traditional and IT-related audits and blockchains. Based on her experience, she insists that the audit standard not refers to any tool-based procedures. She stresses that most parts of AU-C 505 deal with guidelines on obtaining external confirmations by manual procedures, evaluating the results, further procedures if the response rate is too low, handling nonresponses, and decisions on positive or negative confirmations. Consequently, there are compliance gaps in auditing accounts receivable automatically with blockchains.

Participants 13, 19, and 21, who gained comprehensive experience with auditing accounts receivable, are among the five auditors who neither agree nor disagree and remain skeptical about the regulation gap. Concerning regulation gaps of blockchains with AU-C 505, they mean that it depends on how the blockchain is applied. Only in a properly implemented and certified consortium blockchain that operates in a blockchain environment where the auditee and all customers are engaged, auditors use adequate smart audit procedures, and blockchain-based audit procedures are not compliant with AU-C 505. They state that such a blockchain environment is far but provides great potential for the future. Therefore, they decline to give a clear statement. None of the interviewees confirm that continuous auditing with smart audit tools complies with AU-C 505. They claim that compliance gaps exist.

The results on compliance of auditing accounts receivable with blockchains toward GAAS audit standard AU-C 505 are shown in Figure B13. Auditing accounts receivable with blockchains is not compliant with AU-C 505. Thus, a compliance gap exists. Furthermore, all auditors confirm that only consortium blockchains are suitable for auditing accounts receivable. The data analysis reveals three codes.

2.3.2 Elements of Blockchain Audit Standard on Accounts Receivable

Interviewees 15 and 18 are among the few that gave detailed responses. Participant 15 means that soon audit standards must be codified that regulate audit procedures toward accounts receivable with blockchains. Therefore, the standard setters must take up this issue promptly; otherwise, the widespread adoption of blockchain technology in auditing will be slowed down. He means that the audit standard should guide collecting appropriate audit evidence and evaluating data. In addition, he points out that the future audit standard should show reasonable digital audit procedures with smart audit tools that enable continuous auditing. Finally, he also emphasizes that the prospective audit standard shall regulate the role and responsibility of the auditors.

Participant 18, a CISA with long years of professional experience with IT-related audits, underlines that current audit standards regulate tests of details that are in the future no longer required due to the blockchain features and mechanisms if auditors rely on them. She emphasizes that current audit standards must implement automated procedures based on blockchains. In doing so, she criticizes, from the perspective of an IT auditor, that existing audit standards do not even regulate performing data analytics. She means that under continuous audit procedures, additional procedures to inspect the auditee's internal controls, access mechanisms, and periodical transaction sampling must be regulated by the audit standard.

Due to the very specific question, most interviewees provide rather generalizing answers. Research on auditing accounts receivable with blockchains reveals compliance gaps toward GAAS standard AU-C 505. Based on these findings, interviewees outline that auditing accounts receivable with blockchains require, in general, codification of a new audit standard. All interview panelists affirm such requirements and demonstrate the

compliance gap. Overall, the interviews reveal that the interviewees have some idea about the required elements of a blockchain standard, but they have yet to study the matter in much more detail. The codes are identified.

2.3.3 Summary of Compliance Gaps on AU-C 505 with Blockchains

Because of the broad consistency of AU-C 505 with ISA 505, or ISA [DE] 505, the identified compliance gaps toward AU-C 505 also apply to these two audit standards. Therefore, the majority of the interviewees affirm the existence of potential compliance gaps when auditing accounts receivable with blockchains toward audit standard AU-C 505. Consequently, the interviewees agree on the requirement to codify new or revised auditing standards especially designed for blockchain-based auditing procedures on accounts receivable. Second-Order-Coding reveals in Appendix E compliance gaps of blockchain-based auditing toward GAAS.

3 Recapitulation of Research Results

Data from the interviews are based on a semi-structured questionnaire, and the results of the data analysis are presented in chapter four. The collected data are summarized and analyzed for the three research questions. 16 of the 22 interviewees come from Germany. Respectively one panelist comes from Austria, the Czech Republic, Switzerland, and the UK. Two panelists come from the USA.

For answering RQ1, interviewees responded to five questions about the suitability of blockchain technology for auditing. The interviewees affirm specific blockchain features as basic requirements for auditing. Consortium blockchains are assessed as the most suitable type, whereas blockchains require an adequate IT architecture. Most interviewees agree on the worthiness of blockchain features for auditing purposes. Furthermore, they affirm the improved speed and quality of blockchain transactions by

applying smart contracts. To enable blockchains for auditing, the interview participants stress the need for dedicated user access management for blockchain systems to protect the data and blockchain separation into different layers. In summary, the interviews reveal that blockchain technology is a suitable tool for auditing.

To answer RQ2, the recipients answered seven questions concerning eliminating weaknesses of traditional auditing by blockchains in general and by the example of the balance sheet position accounts receivable. Most interviewees affirm that risk-oriented audit procedures based on sampling provide weaknesses, whereas sole periodical auditing at the end of fiscal periods is inappropriate to detect all material misstatements and fraud. They confirm the requirement for external auditing for blockchain systems. Furthermore, most interview panelists agree that applying smart audit procedures enables auditing of all transactions almost in real-time, thus rendering sampling to obtain audit evidence obsolete. Despite continuous auditing with smart audit procedures, most respondents affirm that testing the blockchain code, IAM, and blockchain mechanisms is necessary at least once per year. Interviews also show that blockchain systems alone are not sufficient for auditing. Audits with blockchains require an effective ICS to ensure the completeness and appropriateness of blockchain transactions. Blockchains will significantly influence the audit profession and the auditors' role in the future. Finally, most interviewees affirm that requests for third-party confirmations of accounts receivable become obsolete by blockchains. To conclude, blockchains eliminate weaknesses of traditional auditing and improve audit quality.

Two questions addressed RQ3. Most interviewees disagree on compliance with blockchain-based auditing towards the current GAAS standard AU-C 505. The plurality of interview recipients affirms that existing audit standards require new or modified audit

standards to address auditing with blockchains. To summarize, research shows that auditing accounts receivable with blockchains is not compliant with AU-C 505, and there is a need for the codification of new or modified audit standards.

The following chapter five contains discussions and conclusions about the research results. The researcher verifies the interview conclusions toward the literature review findings. Furthermore, chapter five contains implications of the study, a section for further research, and suggestions for a potential continuation of the thesis.

CHAPTER V: SUMMARY AND CONCLUSIONS

Chapter five contains a discussion of the findings and conclusions of the study on the mechanics of blockchain technology, the suitability of blockchains to eliminate weaknesses of substantial auditing procedures, the effectiveness of blockchains, and compliance gaps on AU-C 505. Additionally, further areas for research are outlined. A sample of a blockchain-based audit standard is discussed regarding the compliance gap.

1 Introduction and Recapitulation of Study

1.1 Research Approach

The purpose of the phenomenology was to explore if blockchains are suitable tools for auditing and, in the event of suitability, to investigate if audits with blockchains eliminate weaknesses of traditional audits. With this background, the study investigated whether blockchain-based auditing, particularly on accounts receivable, comply with audit standard AU-C 505. In light of the research findings, the researcher analyzed whether, under GAAS, new or revised audit standards are required to govern audits with blockchains duly.

The study reveals that the blockchain features of distributed databases, peer-to-peer transmissions, irreversibility of records, and computational logic by smart contracts render blockchain technology an appropriate tool for auditing. Interviewees affirm consortium blockchains as the most suitable type for audit purposes. Periodical traditional auditing based on sampling methods provides weaknesses in detecting material misstatements and fraud. Therefore, sampling methods become obsolete by auditing with smart audit tools that enable continuous audit procedures.

Thus, requests for external confirmations are no longer required when auditing accounts receivable, as all relevant data is available in a consortium blockchain. From a regulatory perspective, auditing accounts receivable with blockchains is not compliant with audit standard AU-C 505. Consequently, new or modified audits must be codified to enable compliant blockchain-based auditing.

1.2 Research Questions and Data Analysis

Chapter five contains discussions on the major research findings that address the problem statement and purpose of the study to answer three research questions:

RQ1: How must blockchain technology be designed to serve as a suitable digital tool for auditing?

RQ2: How do blockchain-based audit procedures eliminate weaknesses of manual and semi-manual auditing and requirements for external confirmations?

RQ3: How is blockchain-based auditing toward accounts receivable compliant with GAAS standard AU-C 505?

Thereby, four objectives were analyzed.

1. Analysis of the blockchain technology
2. Elimination of audit weaknesses by blockchains
3. Blockchain-based auditing of accounts receivable
4. Compliance Gaps towards AU-C 505 by auditing accounts receivable with blockchains.

The most suitable ways to answer the research questions are to perform semi-structured interviews to collect primary data (Farooq & de Villiers, 2017), followed by a detailed literature review of secondary data to verify the findings (Kalu et al., 2019). Data analysis for the literature review was performed by a thematic content analysis based on

the CAQDAS software Atlas.ti (Friese et al., 2018). The interview data was evaluated by preparing transcripts within a narrative analysis (Nasheeda et al., 2019).

1.3 Importance of the Doctoral Study

Traditional audit procedures consist of a backward-looking audit approach by using manual and semi-manually sampling methods to examine audit clients´ transactions to collect sufficient appropriate audit evidence for being able to assess the risk of material misstatement in financial statements and to express an audit opinion thereon (Rozario & Vasarhelyi, 2018). As databases with data under audit are increasingly exposed to cybersecurity attacks, and the complexity and amount of business transactions are rising, audit firms need to transform their audit approach into automated and tool-based auditing procedures (Rozario & Vasarhelyi, 2018).

New technologies such as Big Data, artificial intelligence, the Internet of Things, and blockchain support digitalization (Farcane & Deliu, 2020). Among these technologies, blockchain technology provides the disruptive functionality of a collaborative audit process based on a federated blockchain (Cao et. al., 2018) concerning real-time accounting, continuous monitoring, and fraud prevention (Wang & Kogan, 2018) by reducing costs for audits (Barandi et al., 2020).

Due to the process of digital transformation (Dengler & Matthes, 2018), it is vital for audit firms, academia, regulators, and standard-setters to reflect recent technological developments, such as blockchain technology, that provide the potential to disrupt the audit and accounting profession (Rozario & Vasarhelyi, 2018). Especially the convergence of auditing and accounting with blockchain technology provides a potential for increasing the speed of transactions, whereas manual efforts for audit sampling and

record tracking are reduced, and fraud risks in financial reporting decrease (Wang & Kogan, 2018).

2. Interpretation of Findings and Conclusions

Finally, the research findings are discussed and evaluated concerning the three research questions by evaluating findings from the interviews in contrast to results from the literature review.

2.1 Findings on Objective 1 – RQ1 Audit Suitability of Blockchains

Below, the suitability of blockchain technology for auditing is discussed and evaluated toward RQ1.

2.1.1 Discussion of Blockchain Features

The researcher evaluated the characteristics of the blockchain features for auditing purposes. The interview results reveal that the blockchain features distributed database, peer-to-peer transmission, immutability of records, smart contracts are essential blockchain features as prerequisites for auditing purposes. Lombardi et al. (2021) outline that decentralized distributed databases contain all recorded transactions while identical blockchain data is accessible to any blockchain participants (Lombardi et al., 2022). Data in distributed databases are protected by asymmetric encryption that ensures high security against cybersecurity threats (Da Xu et al., 2021).

Lashkari and Musilek (2021) emphasize that data in distributed databases is tamper-proof (Lashkari & Musilek, 2021). Schmitz and Leonie (2019) point out that DLT provides the potential to support and improve auditing procedures (Schmitz & Leonie, 2019). However, Pillai et al. (2020) outlines that distributed databases more often experience technical problems (Pillai et al., 2020), leading to interoperability problems among blockchains (Besançon et al., 2019).

The literature review also confirms the effectiveness of peer-to-peer networks and reveals that by the blockchain consensus mechanisms, most blockchain nodes authorize and validate transactions (Masood et al., 2018). All peers are notified when initiating transactions (Ghiro et al., 2021). A new block is attached to the blockchain if most nodes reach a consensus on transactions (Liu et al., 2019). These features render distributed data difficult to tamper with (Varma, 2019).

The immutability of blockchain data is a core aspect of blockchain technology, which ensures that transactions, including metadata, cannot be altered after the transaction has taken place (Graham & Sherwood, 2021). The literature discussion confirms the interviewees′ view on immutability as long as no participant controls more than 50 percent of the network power or no 51 percent attacks happen (Boirau, 2018). Authors such as Zheng et al. (2019) emphasize the protection of blockchains by hashing (Zheng et al., 2019), which contributes to a large extent to the immutability of blockchain data (Bhushan et al., 2021).

(Ghiro et al., 2021) outline that the application of hashes makes it easy to verify the integrity of blockchains (Ghiro et al., 2021). If blockchain hashes are unchanged, blockchain data remain integer (Ortman, 2018). Hashing methods (Stetsenko & Khalimov, 2020) and the decentralized blockchain consensus mechanisms render blockchain data irreversible and thus suitable for audit purposes (Das et al., 2022). By linking all blocks in blockchains to previous blocks, recorded transactions can no longer be modified or deleted (Bonyuet, 2020).

Results from the literature show that smart contracts support automated validation and execution of blockchain transactions (Barandi et al., 2020). Smart contracts enable blockchains to share databases among strange participants (Wang & Kogan, 2018) if pre-

defined and agreed-upon contractual agreements match with algorithm-based rules of smart contracts (Ji et al., 2022) without engaging any trusted third party (Khan et al., 2021b). If the information does not meet the pre-defined rules and requirements, transactions are declined by the system, and an error message is generated (Rozario & Vasarhelyi, 2018). Performing transactions by smart contracts decreases costs, significantly reducing the potential for human error and error risks (Alarcon & Ng, 2018). To protect the implemented logic, smart contracts are equipped with access controls (Sultana et al., 2020). Central authorities become obsolete through smart contracts (Bonsón & Bednárová, 2019).

However, some question the benefits of distributed ledger technology (Dow, 2019). Boireau (2018) criticizes blockchains for risks of 51 percent attacks as nodes, in such cases, can manipulate blockchain data (Boireau, 2018). Singh et al. (2021) state in contrast to distributed databases that, no blockchain participant owns full control due to the decentralized structure of the database (Singh et al., 2021). Despite the expectation of distributed ledger technology regarding cost reduction, velocity, and efficiency, distributed ledger technologies are not ready for mass transactions yet (Seretakis, 2017).

To conclude, the research reveals that distributed databases provide a valuable blockchain feature to enhance auditing purposes. Asymmetric encryption renders distributed databases a high level of cybersecurity. Blockchain technology enables an effective and secure exchange of data and information among blockchain peers. Smart contracts are a very important feature that significantly improves blockchain technology. As a result, blockchain data cannot be tampered with or modified after adding a new block. These four features enable blockchain-based auditing and provide a prerequisite for continuous audit procedures.

2.1.2 Conclusion toward most suitable Blockchain Type for Auditing

Different opinions about which blockchain type is most appropriate for auditing are prevalent in the literature. Zheng et al. (2019) affirm that private blockchains as most suitable for auditing and accounting purposes (Zheng et al., 2019). Due to the power of the central authority to override blockchain data and mechanisms, this blockchain type needs a consensus protocol that affirms the trustworthiness and immutability of blockchain data (Ismail et al., 2019). Liu et al. (2019) and others criticize the central authority in private blockchains, whereby a public blockchain is not preferable (Liu et al., 2019). Bonyuet (2020) evaluates public blockchains as inappropriate for auditing due to a lack of confidentiality, data privacy issues, and access controls (Bonyuet, 2020).

The literature review reveals that for auditing purposes, whether solely private blockchains (Lombardi et al., 2022) nor public blockchains are appropriate tools to record accounting-related data and information accordingly (Bonyuet, 2020). Copigneaux et al. (2020) prefer the semi-decentralized consortium blockchains as most suitable for auditing, where some participants verify and record data of transactions (Copigneaux et al., 2020). Li et al. (2020) confirm this view, as they combine elements of private and public blockchains while all relevant data and information are accessible by respecting confidentiality and data privacy aspects (Li et al., 2020). In summary, the researcher agrees with the interviewees and authors as Albaroodi & Anbar (2022) and others, that consortium blockchains are the most suitable blockchain type, where one group of nodes controls the transactions while others approve the transactions (Albaroodi & Anbar, 2022).

2.1.3 Discussing Cybersecurity of Blockchains versus ERP Systems

Interview results are as mixed as the findings from the literature review. Heo et al. (2021) express the concern that exploiting the weak points of a blockchain would cause

massive damage to the whole blockchain (Heo et al., 2021). Puri et al. (2021) mean that explicit security issues result from tampering with blockchain codes (Puri et al., 2021). In contrast, Dai and Vasarhelyi (2017) outline that blockchains disperse the authorization, verification, and storage of data among the blockchain node, whereby risks of falsifying the blockchain data are significantly lower in ERP systems (Dai & Vasarhelyi, 2017). ERP systems face higher risks of tampering due to the centralized database (Farcane & Deliu, 2020), while consortium blockchains provide a higher level of security than ERP systems with a combination of private and public blockchain elements (Banerjee, 2018).

To summarize the interview results and the literature review findings, blockchains are more secure against cyber security risks than traditional ERP systems. Blockchain systems are more difficult to corrupt, whereas past transactions in ERP systems are subject to a higher risk of tampering. Threats such as risks from hostile encryption of blockchains are lower as a second party owns another protection mechanism. Furthermore, only one database might be corrupted, not the blockchain, as long as no one owns more than 50 percent. In the case of cyberattacks, hackers try to encrypt databases to extort money so that they would release encrypted data. They do not get access to payment data. The risk of extortion is lower as intruders cannot encrypt all blockchain nodes due to the distributed database, which provides more stability due to redundant ledgers. In case intruders manipulate data, these data are no longer identical to the databases' respective ledgers of the other participants.

2.1.4 Discussion on User Access Management for Blockchains

The recipients of the interviews affirm the necessity of adequate user access management for blockchains. The findings of the literature review confirm the results of the interviews. Mikula and Jacobsen (2018) emphasize that blockchains need user

management based on authentication and authorization processes as confidential accounting-related blockchain data require protection (Mikula & Jacobsen, 2018). Yavari et al. (2020) stress that smart contracts that perform transactions autonomously require appropriate user access management (Yavari et al., 2020). In conclusion, confidential blockchain data must be protected like data on ERP systems, whereas user access controls must regulate access to the data.

2.1.5 Conclusion on Appropriate Architecture

Most panelists of the interviews agree on the requirement of an adequate blockchain architecture to enable orderly audit procedures. Several interviewees outline interoperability issues of blockchain systems with ERP systems or other blockchains. Most of the 17 participants emphasize that blockchains need a basic infrastructure layer to run the blockchain. The business logic for business processes needs a separate layer as well. All blockchains require ERP functionalities.

The literature review results are similar to the findings of the interviews. The literature review reveals that the architecture of a distributed ledger technology must serve the confidentiality of data and records for accounting and auditing purposes (Wang & Kogan, 2018). According to Vincent et al. (2020), the IT environment and architecture must create an environment that ensures confidentiality, data security, immutability, and privacy (Vincent et al., 2020). Furthermore, an appropriate blockchain architecture must allow continuous auditing procedures (Barandi et al., 2020). It must comply with the relevant audit assertions of accuracy, classification, completeness, occurrence, and cutoff to support the achievement of pertinent audit objectives (Freiman et al., 2022).

Faccia and Petratos (2021) identify interoperability problems of blockchain systems toward other blockchain or ERP systems (Faccia & Petratos, 2021). Kan et al.

(2018) emphasize the lack of uniform transaction format among blockchain systems (Kan et al., 2018), which Hardjono et al. (2018) in addition explicitly criticize (Hardjono et al., 2018). Thus, integration into a unique framework proves to be very difficult (Besançon et al., 2019). Federated blockchains have a general communication problem (Pillai et al., 2020). A solution to interoperability issues provides an architecture based on several layers (Jin et al., 2018).

The literature likewise takes the same view that all blockchain changes require recording in changelogs, whereas Ahmad et al. (2019) are among the proponents that recommend changelogs as connecting pieces between the database tier and the application tier (Ahmad et al., 2019). Likewise, Vincent et al. (2020) outline the specific value of changelogs as an audit trail (Vincent et al., 2020) since all changelogs record all changes to the blockchain (Oakley et al., 2021). Thus, changelogs significantly reduce the risks of illegitimate access or data breaches (Algarni et al., 2021). Changelogs are important in improving the auditability of blockchain transactions and safety against cybersecurity risks(Wang et al., 2020). The conception of the literature recommends the separation of blockchains into the daily business activities layer, blockchain data, server (network) layer, audit application service layer, and auditors for auditing purposes (Wang et al., 2020).

In summary, only adequate architecture blockchains enable orderly continuous audit procedures. Changelogs render blockchains more audible, and different layers improve the applicability of blockchains. Just as IT systems in general, blockchains shall be divided into different layers. The separation into different layers reduces interoperability issues of blockchains. However, the topic of interoperability issues requires further research in the future.

2.1.6 Summary of Suitability of Blockchains for Auditing

A thoroughly performed literature review and the interview results reveal the suitability of blockchains for auditing purposes. Blockchains are suitable tools for auditing as the distributed database supports accounting requirements for recording transactions in chronological order. The decentral characteristics and encryption of blocks and hashing methods render blockchains immutable and tamper-proof. Blockchain data is stored safely and shared among all nodes by real-time updating data.

Transaction numbers, time stamps, and IDs make blockchains auditable. Transactions are performed automatically by smart contracts based on consensus mechanisms. Smart contracts based on computational logic and consensus mechanisms enable automatic transactions if predefined conditions are met, while no trusted authority is required. Major advantages of smart contracts result in reduced fault potentials by replacing manual procedures through autonomous transactions.

As all participants own an identical copy and most nodes in the peer-to peer-to-peer authorize and verify transactions based on consensus mechanisms, blockchains provide a high level of security towards completeness and integrity of accounting-related data in contrast to ERP systems. Blocks are encrypted and protected by hashes, whereas every block is linked by hashing with previous blocks by forming a Merkle tree. These mechanisms prevent, in general, recorded transactions from being tampered with. Fraudulent activities can be detected more easily in peer-to-peer networks than in traditional accounting systems.

2.2 Discussion of Objective 2 – RQ2 Elimination of Audit Weaknesses

Proceeding from the identified suitability of the blockchain technology for auditing, final considerations are discussed on whether blockchains eliminate weaknesses of manual and semi-manual audits.

2.2.1 Conclusions on Weaknesses of Traditional Audits

Most interviewees agree on the weaknesses of traditional auditing, whereas three panelists disagree. These weaknesses result from risk-based sampling procedures that examine only a portion of the accounting-relevant data, sole periodical audits at the end of fiscal periods, and mainly manual substantive audit procedures at high costs that are very work-intensive, whereas too large audit teams are required.

The literature review reveals that this topic is discussed controversially. The results outline the weaknesses of traditional auditing, mainly results from sampling procedures (Barandi et al., 2020). Evaluating a fraction of data populations does not guarantee that all material misstatements and fraud in financial data could be identified (Barandi et al., 2020). Faccia et al. 2022 confirm the weaknesses of sampling procedures combined with an inefficient and work-intensive audit approach, as risks often remain undetected and controls do not address the relevant risks (Faccia et al., 2022).

Barandi et al. (2020) point out that periodic audits may not detect all material misstatements and fraud in financial statements (Barandi et al., 2020). Lombardi et al. (2021) outline that traditional auditing requires too large audit teams (Lombardi et al., 2022). Lombardi et al. (2021) and others emphasize the high costs and the heavy workload of traditional audit procedures (Lombardi et al., 2022). Blockchain-based audits provide a high potential to solve traditional audit procedures' issues, making audits more comprehensive (He & Chen 2021).

Authors as Marei and Iskandar (2019) evaluate the current audit approach as appropriate, whereas using audit technologies such as CAATs instead of manual audit techniques allows auditors to perform more effective and efficient IT audit work, resulting in reduced audit time (Marei & Iskandar, 2019). Thus, CAATs have become more popular under traditional auditing since the beginning of the 21st century (Byrnes et al., 2018). In contrast to CAATs, the implementation of blockchains shows a significant positive effect on audit quality, while the auditor's use of CAATs has no significant positive impact on audit quality (Sujanto et al., 2021).

To conclude, traditional auditing provides weaknesses, as risk-oriented sampling cannot ensure that all material deviations, misstatements, or fraud can be identified. Sole periodical audits are inappropriate for detecting all relevant material misstatements or fraud. Results from the literature review confirmed this perspective. Manual audit procedures have high costs and workloads, requiring unnecessarily large audit teams compared to a blockchain-based approach. The interviews and literature review findings affirm that traditional audits implicate significant weaknesses. In conclusion, as outlined in Appendix E, aggregate dimensions show the suitability of blockchains for auditing.

2.2.2 Discussion of External Audit Requirements for Blockchains

The findings from the literature review confirm the results of the research on primary data. Most interview participants affirm the necessity of external audits for blockchains, as auditors are always required to evaluate management estimates, e.g., toward depreciation of fixed and intangible assets, goodwill impairment, or bad debt depreciation. Blockchain verification mechanisms cannot replace the audit function or the role of independent external auditors, as they do not address controls for detecting fraud, errors, or omissions (Desplebin et al., 2021). Authors such as Schmitz and Leoni (2019),

Appelbaum & Nehmer (2020), Smith and Castonguay (2020), and Wang et al., 2020 to name a few, emphasize explicitly the requirement to perform external audits on blockchains. In summary, the proponents of external audits on blockchains are to be agreed upon, consistent with the statements of the interviews. In any case, external audits are required to fulfill regulatory requirements.

2.2.3 Discussing the Superiority of Smart Audit Procedures

Most interview respondents believe that smart audit tools render manual or semi-manual procedures obsolete, as almost all material misstatements or fraudulent activity will be detected, while auditing costs, in contrast to substantive manual procedures, decrease. The interviewees also affirm that ensuring the completeness and integrity of accounting-relevant blockchain data by an effective ICS implemented by the auditees is very important.

The literature opinion confirms the interviewees on the benefits of smart audit procedures compared to manual substantive ones. Rozario & Vasarhelyi (2018) outline, besides other authors, that smart audit procedures were designed to perform continuous audit activities on blockchains (Rozario & Vasarhelyi, 2018). Authors as Gauthier and Brender (2021) conclude that smart audit procedures do not require specific sampling methods, as the whole accounting-relevant data for the period under audit will be evaluated and tested continuously in contrast to the traditional risk-based approach (Gauthier & Brender, 2021). Appelbaum and Smith (2018) discover that most material misstatements or frauds could be eliminated by continuous auditing (Appelbaum & Smith, 2018). Rozario & Vasarhelyi (2018) emphasize that smart audit tools enable the detection of all relevant audit and fraud risks by automatically auditing all transactional data (Rozario & Vasarhelyi, 2018).

Besides other authors, Liu et al. (2019) claim that blockchains need additional internal control testing to ensure the completeness and integrity of the blockchain data (Liu et al., 2019). According to Pimentel et al. (2021), blockchain mechanisms alone cannot verify if transactions are accounted for appropriately according to the transaction covenant (Pimentel et al., 2021). By evaluating blockchain data, management assertions on the required depreciation of accounts receivable cannot be determined appropriately (Barandi et al., 2020).

Therefore, authors as Liu et al. (2019) and Castonguay (2021) outline that auditees require an effective accounting-related ICS (Castonguay, 2021) to gain sufficient audit assurance that blockchain data are accurate and complete (Liu et al., 2019). Smith and Castonguay (2020) pointed out that control testing of auditors must focus on the design to fulfill control objectives, their existence, and operational effectiveness during the period under audit (Smith & Castonguay, 2020). Testing the accounting-related ICS and the ITGC ensures high information security, process integrity, system availability, and data privacy (AICPA & CPA Canada, 2017).

To summarize, smart audit procedures that are prerequisites for continuous auditing provide great potential to improve auditing speed and quality by inspecting entire data pools that render sampling procedures obsolete. Smart audit procedures provide a high potential to improve audit quality significantly by detecting the relevant audit and fraud risks. Auditing costs will decrease with mainly automated audit procedures as blockchain transactions are automatically executed. The interviewed auditors and the plurality of the reviewed authors agreed that blockchain-based auditing requires testing of internal controls beneath continuous audits of transactions.

2.2.4 Discussing Blockchain Code, Mechanisms, and Access Controls

The interviewees mainly agree that despite continuous auditing by smart audit tools, auditors must test the integrity of the blockchain code, the appropriateness of the implemented blockchain mechanisms, and the integrity of the access controls at least yearly. The findings from the literature review confirmed the interview outcomes. Among other representatives of the literature, Graham & Sherwood (2021) and Popchev et al. (2021) highlight that auditors need to review the blockchain code, the smart contract codes, and the access controls to ensure that the contractual terms reflected in them are appropriate, and then perform relevant tests, that the contracts are executed as intended (Graham & Sherwood, 2021; Popchev et al.,2021). Blockchain transactions provide no guarantee that the agreed and verified transactions on the blockchain are integer (AICPA & CPA Canada, 2017).

In summary, to gain a higher quality of audits, the integrity of the blockchain code, the effectiveness of access controls, and the power allocation between the blockchain members must be tested at least once per year (Liu et al., 2019). Furthermore, blockchains require testing the integrity of the consensus mechanisms integrated into smart contracts to ensure the integrity and accuracy of the recorded data (Wang et al., 2020). The research reveals that despite continuous auditing with smart audit tools, the requirement for at least yearly audits of blockchain codes, consensus mechanisms, and access controls toward blockchains is highly important.

2.2.5 Discussion on Impacts on Audit Profession and Role of Auditors

Cheng & Huang (2019), as well as Calderón & Stratopoulos (2020), the representative for the opinion expressed in the literature represented, agree with the results from the plurality of interviews that major changes for the audit profession and the

auditor´s role will result from the blockchain technology (Cheng & Huang, 2019); Calderón & Stratopoulos, 2020). Standard setters such as AICPA and CPA Canada (2017) assume that the role of auditors in blockchain environments requires new regulations concerning specific blockchain audit standards and the auditor´s role (AICPA & CPA Canada, 2017). Auditors must acquire appropriate knowledge of blockchain features (Selg, 2022b).

In conclusion, implementing blockchain technology will significantly change the strategic audit approach and procedures. Due to the shift from manual and semi-manual audit procedures to a digital audit approach based on continuous procedures with smart audit tools, all interview respondents expect significant impacts from blockchain technology on the audit profession and the role of the auditors. The audit profession has to develop new audit strategies that consider the change from manual toward digital substantive procedures. The auditors' main role will shift from testing transactions and controls to an increased evaluation of management assertions towards the appropriateness of depreciation of fixed and intangible assets and assessments of impairment on the goodwill, among others.

2.2.6 Conclusions of Waiving External Confirmations by Blockchains

Most interviewees mean that auditing with blockchains renders requests for external confirmation obsolete if blockchain systems are technically properly implemented. The results from the literature research arrive at the same conclusion. A representative for several authors, Appelbaum and Nehmer (2017) are among the first ones to outline the superiority of blockchains in contrast to ERP systems when auditing accounts receivable, as requests for external confirmations become obsolete, whereas blockchains record all transactional data and the related invoices and shipping documents

(Appelbaum & Nehmer, 2017). Castonguay (2021) also emphasizes that requests for third-party confirmations are no longer needed in a consortium blockchain environment as counterparties and auditors get access to all auditee's related transactional data (Castonguay, 2021).

To summarize, the superiority of auditing with blockchains compared to manual or semi-manual substantive audit procedures becomes obvious by the balance sheet position accounts receivable. Research findings confirm that costly and time-consuming requests for external confirmations with often low response rates are no longer required in consortium blockchain environments. However, an adequate and certified consortium blockchain environment is a prerequisite.

2.2.7 Summary of Elimination of Audit Weaknesses by Blockchains

The research shows that traditional risk-oriented auditing based on sampling provides weaknesses as substantive audit procedures only cover some data populations. Sampling approaches and sole periodical audits do not provide absolute assurance to identify all material misstatements or fraud. As a further disadvantage, manual and semi-manual audit procedures generate high costs with an excessive workload by engaging unnecessary large audit teams. Aggregate Dimensions, as shown in Appendix E, reveal that smart audit procedures implemented into blockchains can eliminate weaknesses of traditional audits through a continuous audit approach that covers entire data pools by detecting material audit and fraud risks at reduced audit costs.

Sampling methods will become obsolete with smart audit tools. The example of accounts receivable shows the superiority of blockchain-based auditing. Costly and time-consuming requests for third-party confirmations to confirm accounts receivable balances are no longer required in a blockchain environment. External auditing is still needed

despite implementing blockchain mechanisms to authorize and verify transactions. However, smart audit procedures still require yearly audits of blockchain codes, mechanisms, and access controls toward blockchains. In addition, auditors must test internal controls at least yearly to ensure the completeness and integrity of blockchain data. The adoption of blockchain technology will greatly impact the audit profession and the role of the auditors.

2.3 Discussion of Objective 3 – RQ3 Compliance Gaps on AU-C 505

Upon discovering that blockchain-based audits eliminate weaknesses of traditional audits is discussed whether auditing accounts receivable with blockchain can be performed in compliance with GAAS audit standard AU-C 505 and whether audits with blockchains require new or modified audit standards.

2.3.1 Conclusions on Compliance toward AU-C 505 with Blockchains

Audit standard AU-C 505 was analyzed towards accounts receivable if this standard can provide relevant guidance for blockchain-based audits. Almost all the auditors engaged in the interviews doubt that blockchain-based auditing is fully compliant with the requirements of the audit standard AU-C 505. The literature did not explicitly outline a compliance gap in AU-C 505 when auditing accounts receivable with blockchains. The identified gap on AU-C 505 by the plurality of the interviewees is not addressed in the literature on auditing, in the publications of standard setters, nor in the professional practice of auditors. Some authors, such as Barandi et al. (2020), outlined that no audit standards under GAAS for blockchain-based are codified (Barandi et al., 2020). Table A7 assesses from the researcher's perspective how individual paragraphs of the AU-C 505 auditing standard (AICPA, 2012b) provide appropriate regulation for a blockchain-based accounts receivable audit.

To conclude, by comparing the requirements of AU-C 505 toward accounts receivable by traditional substantive audit procedures with blockchain-based auditing, the researcher identifies and reveals several compliance gaps, confirming the interview findings. Thus, it is recommended for standard setters under GAAS to codify a new auditing standard that encompasses specific requirements of blockchain-based auditing on accounts receivable. Based on the findings in Table A7, a potential structure of a future standard for auditing accounts receivable with blockchains is outlined in chapter 2.3.2.2.

2.3.2 Blockchain-based Audit Standard on Accounts Receivable

2.3.2.1 Discussion on Blockchain-based Audit Standard

Most interviewees outline that new or modified audit standards must be codified to address specific blockchain features. The literature review confirms the interviews' findings whereby few authors, such as Elommal and Manita (2022) and Gauthier and Brender (2021), stress that no audit standards for blockchains exist nowadays (Elommal & Manita, 2022); Gauthier & Brender, 2021). Centobelli et al. (2021) emphasize that blockchain audit standards must respect increasing automation, analysis, and machine learning functions (Centobelli et al., 2021). According to AICPA and CPA Canada (2017), future blockchain-based audit standards, e.g., towards accounts receivable, require testing the logic of smart contracts in comparison with the relevant business logic of accounts receivable processes and auditing of interfaces between smart contracts that trigger business events, and external data sources (AICPA & CPA Canada, 2017).

As a result of research on the GAAS framework under AU Section 150 (AICPA, 2001) and of AU-C 505, audit standards under GAAS that regulate audit of external confirmations (AICPA, 2012b), it can be stated that the current audit regulation under GAAS is not appropriate to provide appropriate guidance for blockchain-based auditing.

Elommal and Manita (2022) are correct in that new audit standards must be codified to provide an approved framework for blockchain-based auditing and to enhance audit practices with this technology (Elommal & Manita, 2022).

2.3.2.2 Proposal for Blockchain Audit Standard

Following is a proposal toward structure and elements for a prospective audit standard for blockchain-based auditing on accounts receivable derived from the interviews' results and the researcher's specific knowledge.

2.3.2.2.1 Scope of the Blockchain-based Audit Standard

When performing statutory audits in accordance with GAAS, requirements of AU Section 200, "Overall Objectives of the Independent Auditor and the Conduct of an audit following GAAS," provisions of Section 330, "Performing Audit Procedures in Response to Assessed Risks," and "Evaluating Audit Evidence Obtained" of section 500 Audit Evidence must be observed. (AICPA, 2020).

2.3.2.2.2 Evaluating Blockchain-based Information

Auditors shall assess the suitability of blockchain-based information as audit evidence by considering,

a) relevance and reliability of the information, and
b) whether such information confirms or contradicts assertions of financial statements (AICPA, 2020).

Auditor's assessment of the information to be used as evidence should consider whether

a) the information obtained is sufficiently precise and detailed for audit purposes and
b) the information obtained is accurate and complete to serve as audit evidence (AICPA, 2020).

2.3.2.2.3 Regulation for Blockchain-based Auditing Procedures

The auditor shall maintain control over blockchain-based audit procedures, including (AICPA, 2012b)

a) continuous auditing of records or documents by entire auditing populations of accounting-related data with smart audit tools under the auditor´s control;
b) monitoring of processes and internal controls to identify process violations and off-chain transactions by an in-depth examination (Appelbaum & Nehmer, 2017);
c) monitoring of all accounting-related data and running of automatic calculations on permanent intervals;
d) automatic replication of all recognized transactions in the blockchain to identify exceptions for purposes of re-performance;
e) analytical procedures for scanning of real-time data by pre-defined KPIs, ratios, and statistics (Appelbaum & Nehmer, 2017);
f) testing the design of smart contracts, hash encryption, blockchain code, consensus mechanisms, and hashing algorithm used by the distributed ledger (Wang & Kogan, 2018) in case of first-time audits of a blockchain.

2.3.2.2.4 Auditor Responsibility

AU-C section 330 outlines the auditor's responsibility

a) to design and implement appropriate audit procedures to address the assessed risks of a material misstatement by the auditor at the financial statement level and
b) to design and perform additional audit procedures whose nature, extent, and timing are based and responsive to assess risks of off-chain transactions (AICPA, 2012c).

Auditing of blockchains, in addition, requires the auditor´s evaluation of the auditee´s management estimates according to section AU-C 540, “Auditing Accounting Estimates,” including Fair Value Accounting Estimates, and Related Disclosures in

conjunction with AU-C section 342 Auditing Accounting Estimates (AICPA, 2020). The auditor's consideration of the reliability of audit evidence obtained from blockchains shall include reviews of risks if the integrity of blockchain information has been compromised due to off-chain arrangements and security issues (AICPA, 2012b).

2.3.2.2.5 Blockchain-Based Procedures to Obtain Audit Evidence

This section is intended to guide auditors in designing and performing testing procedures to obtain sufficient, relevant, appropriate, and reliable audit evidence to form the audit opinion (Perera & Abeygunasekera, 2022).

Continuous Auditing: Accounting-relevant data and transactions are evaluated by smart audit tools that enable continuous auditing procedures based on smart audit procedures by gathering digital audit evidence (Lombardi et al., 2022). For auditing accounts receivable, all relevant accounting records and other information, such as invoices, vouchers, and shipping documents, are accessible in consortium blockchains (Lombardi et al., 2022).

Auditing Internal Controls: To evaluate the integrity and completeness of accounting-relevant data and transactions, the auditee must implement an appropriately designed ICS that enables recording all accounting-relevant data and controls access on the blockchain by an adequate IAM (Liu et al., 2019).

Additional Audit Procedures: In addition to continuous auditing procedures, at least once per fiscal period, audit evidence shall be obtained by testing

a) blockchain- and accounting-related internal controls of the auditee as access controls,
b) the integrity of the blockchain code,
c) the integrity of smart contracts´ logic, and
d) blockchain mechanisms (Rozario & Thomas, 2019).

2.3.3 Conclusion on Compliance Gaps towards AU-C 505

Aggregate dimensions as provided in Appendix E, reveal compliance gaps when auditing accounts receivable with blockchains. Interviewees outline that automated and continuous blockchain procedures require different regulations, unlike manual or semi-manual auditing. No authors that explicitly address this issue could be found by researching the literature. In addition to the interviews, the researcher compared specific requirements of AU-C 505 toward blockchain features and specifics and revealed that auditing with blockchains is not sufficiently regulated under AU-C 505. Based on the identified knowledge respective compliance gap toward AU-C 505, all the interviewed auditors affirm the necessity to codify new or revised audit standards.

3. Key Points of the Doctoral Research

As a research result on blockchain suitability, the study reveals that blockchains provide innovative technology. Although the adoption will raise new challenges for auditees, audit firms, and auditing standard setters, blockchains are a suitable tool for auditing, while consortium blockchains represent the most appropriate blockchain type.

Furthermore, the research shows that the traditional manual and semi-manual risk-oriented audit approach by sampling could be improved. Blockchain technology, in conjunction with smart audit tools, provides a high potential to eliminate such weaknesses by continuously auditing all relevant accounting transactions and auditing internal controls with smart auditing procedures. The speed and quality of audits will increase through smart audit procedures. At the same time, costs will decrease, and requests for third-party confirmation to confirm the accounts receivable ledger will become obsolete in a consortium blockchain.

The research on compliance of blockchain-based auditing of accounts receivable toward the codified GAAS audit standard AU-C 505 “External Confirmations” unveiled compliance issues. Requirements of continuous auditing with smart audit tools on blockchains are not addressed by AU-C 505, as it rules mainly solely manual procedures to obtain external confirmations. Consequently, standard setters must codify new or revised audit standards for auditing accounts receivable with blockchains. Therefore, the dissertation includes a proposal of the components that could be included in a future auditing standard for blockchain-based auditing of accounts receivable.

4. Implications

4.1 Theoretical Implications

The study approach can answer the study's three research questions. Regarding RQ1, the research shows that blockchain technology is a suitable tool for auditing. Answering RQ2 reveals that traditional material audit procedures have weaknesses that Blockchain-based auditing eliminates. Labor-intensive and costly audit procedures, such as obtaining third-party confirmations to verify the accounts receivable line item, are rendered obsolete by blockchains. Answers toward RQ3 identify a literature gap, as auditing with blockchains is not addressed by the GAAS standard AU-C 505.

Based on the study's findings, the theoretical framework of GAAS presented in chapter two must be revised to consider the requirements of audits with blockchains. GAAS standards are focused on manual or semi-manual audit procedures. In contrast, digital blockchain procedures require different aspects due to the continuous audit approach and the application of smart audit tools. Thus, new blockchain-based audit standards must be codified. The role of the auditors in a blockchain system differs from

the traditional role. In the blockchain, the inspection of single transactions will shift from single testing transactions done by tools to continuous testing of transactions and controls.

In contrast, the outlined blockchain framework is adequate. The study outlines the suitability of decentralized infrastructures of blockchains based on software solutions, as well as peer-to-peer transmission with different nodes, consensus protocols, application of smart contracts, specific blockchain architecture, and requirements for IAM as prerequisites for auditing. Smart audit tools enable blockchain-based auditing.

The dissertation conclusion provides credibility concerning the conceptual framework. The study confirms the research topic of the thesis that blockchains are a suitable tool for auditing. Furthermore, the study approves blockchains' thesis statement concerning higher audit quality. The literature review findings confirm blockchains' suitability for auditing and the higher quality and effectiveness of blockchain-based auditing. The findings and results of the doctoral thesis add knowledge to the academic body and for auditing practice, guide audit firms implementing and operating blockchain-based auditing, increase efficiency on blockchain-based auditing towards accounts receivable, and outline regulatory gaps concerning AU-C 505. The impact of the doctoral thesis is on a broader education of students and audit staff toward deeper knowledge and understanding of blockchain technology.

4.2 Practical Implications

The possible future implications of the study focus on two aspects. The future professional practice of auditing will increasingly rely on digital tools to test all accounting-relevant transactions toward entire pools of financial data and data analysis by smart audit tools that enable continuous auditing. This contributes to a higher level of audit quality and reduced costs of audits in less time. Continuous auditing supports the

identification of all material misstatements and fraud toward financial data. Limitations and weaknesses of traditional manual or semi-manual substantive audit procedures are eliminated.

Other implications concern the standard audit setters. Currently, specific audit standards for blockchain-based auditing have yet to be codified. Different audit procedures and other conditions of the auditor's role must be regulated to address the particular requirements of digital audits with blockchains. In coordination with the responsible persons from different large and medium-sized audit firms, the standard setters must establish a legitimate framework for auditing with blockchains. As part of establishing a framework, the audit firms shall adopt the blockchain-based audit approach to incorporate the specification from the new audit standards. These two approaches represent the most promising future developments emerging from the research.

4.3 Thesis´ Strengths and Weaknesses

To some degree, motivating interview partners to participate was not easy. Written and telephone inquiries to U.S. audit firms were either not answered or rejected concerning the high workload of the employees in the so-called busy season. Thanks to personal and professional contacts and the support of other auditors, the researcher persuaded interview partners to participate in the interviews. Therefore, the researcher conducted 22 interviews with auditors from several countries.

Interviewees from Europe are not familiar with GAAS standard AU-C 505. To close the knowledge gap, reference was made to the still valid audit international audit standard ISA 505 from 2009 and the current codified German audit standard ISA [DE] 505, which are largely identical to AU-C 505 to address this issue. Other restrictions arose from limited access to academic sources. The literature sources examined resulted

predominantly from "Google Scholar." More than 300 literary sources from 2017 to 2022 were included in the literature review to counteract a possible limitation. Available references of the examined journal articles were also included in the literature review where appropriate to expand the search.

4.4 Future Implications from the Thesis

This section provides recommendations for future studies in blockchain-based auditing by the dissertation research results. The doctoral thesis provides a basic and general approach to the suitability of blockchain technology as an appropriate tool to eliminate weaknesses of traditional auditing, to outline higher effectiveness for auditing of accounts receivable in contrast to conventional substantive procedures, and compliance gaps of blockchain-based audits with the codified GAAS and in particular audit standard AU-C 505, and the future role of the auditor. Research in academia and practical experience with blockchains in auditing and accounting are in an early stage of development. As almost no one has gained appropriate practical experience with blockchains, future research has to amend and continue the study.

5 Recommendations for Future Research and Practice

Subsequent sections provide an outlook on areas for future research projects. Furthermore, the example of a possible future audit standard shows how the research project could be continued.

5.1 Areas for Future Research

Subsequent sections provide an outlook on areas for future research projects.

5.1.1 Impact on Audit Profession and New Roles for Auditors

The expected high impact of blockchain technology on the audit and accounting profession has to be evaluated by future research. The effects on accounting and auditing

procedures with blockchains should be worked out more intensively. Beneath the impacts on the audit and accounting profession, further requirements on the auditor's role must be evaluated.

5.1.2 Issues on Blockchain Architecture

Research has to examine what kind of blockchain architectures support complex auditing and accounting procedures with large numbers of blockchain participants and high transaction volume with information of regulators and legislators. As auditing firms need more staff with IT-related knowledge, training audit staff towards using blockchain technology will be among the critical issues for a broad acceptance among auditors that requires further research. In addition, interoperability issues must be respected. Scalability and flexibility issues must also be in the frequency of testing smart audit procedures, acting on outdated systems, and processing error messages.

5.1.3 Requirements of External Audits on Blockchains

Further detailed research shall examine how blockchain mechanisms provide the potential to replace the audit opinion respective performing of external audits. Other analyses can be performed on the relevance of additional periodic assurance by auditors when the results of smart audit procedures are quantifiable. Additionally, the research shall refer to a potential worldwide blockchain standard that renders external audits obsolete.

5.1.4 New Areas for Auditing Purposes

New areas of auditing are emerging in the wake of ongoing digitalization. Enterprises are increasingly moving the operation of their accounting-related applications from on-premises servers to cloud environments provided by specialized service companies. Furthermore, cryptocurrencies, as new kinds of digital intangible assets also

subject to extremely strong price fluctuations, represent new areas for auditing. These areas shall be analyzed for possible applications for blockchain-based audit procedures.

5.2 Future Practice - Specific Audit Standard on Accounts Receivable

This section provides recommendations for future practice by potentially continuing the study based on the results and findings from blockchain-based auditing research. No specific blockchain audit standards are codified under existing GAAS regulations (Alarcon & Ng, 2018). Thus, standard setters must codify new or modified audit standards concerning all relevant elements of the balance sheet and the income statement that enable orderly blockchain-based auditing.

6. New Insights from the Research

Research conducted as part of the dissertation yielded new findings not found by the literature review respective literature gaps as follows.

6.1 Compliance Gap of Auditing with Blockchains on AU-C 505

For auditing accounts receivable under the current GAAS, auditors must follow the audit standard AU-C 505, "External Confirmations." This standard provides rules on how to request, collect and evaluate third-party confirmations that enable verifying the correctness of the accounts receivable ledgers. These procedures are mainly manually performed. Research has shown that auditing with blockchains based on a digital approach is not compliant with GAAS audit standard AU-C 505 nor any other of the GAAS audit standards. Thus, the research revealed a literature gap in that no regulation is coded under AU-C 505. No articles on auditing accounts receivable with blockchains were found in the available literature.

6.2 Proposal for Structure of a Blockchain-based Audit Standard

As a result of the identified compliance gap based on the research results, in accordance with typical GAAS standards, the researcher was able to design the structure and relevant elements of a possible future audit standard for auditing accounts receivable as described in paragraph 2.3.2.2 and paragraph 4.2 within this chapter five. Nowhere in the literature were indications of elements or any structure of a blockchain-based audit standard. However, this proposed audit standard represents a basic structure that needs further research.

7 Final Thoughts

We are on the threshold of an emerging digitized economic environment driven by novel technologies such as blockchain. Blockchain-based auditing can potentially disrupt the audit profession and how audits will be performed. As a result, the audit, financial reporting, and key business processes will undergo fundamental transformations. Ultimately, businesses and their employees will experience sustained disruption by automating and digitizing business processes, workflows, and transactions in which employees increasingly lose influence. In the decades to come, in the end, this development, which will be massively driven by digitalization, is expected to result in a shift from manual and semi-manual processes to far-reaching automatization, not only in auditing but in the entire world of business.

References

Abreu, P. W., Aparicio, M., & Costa, C. J. (2018). Blockchain technology in the auditing environment. In *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, 1-6. IEEE.

Adam, I., & Fazekas, M. (2021). Are emerging technologies helping win the fight against corruption? A review of the state of evidence. *Information Economics and Policy*, *57*, 100950.

Adhabi, E., & Anozie, C. B. (2017). Literature review for the type of interview in qualitative research. *International Journal of Education*, *9*(3), 86-97.

Aggarwal, S., & Kumar, N. (2021). Attacks on blockchain. In *Advances in Computers* , 399–410, Elsevier.

Ahmad, A., Saad, M., & Mohaisen, A. (2019). Secure and transparent audit logs with BlockAudit. *Journal of network and computer applications*, *145*, 102406.

Aksoy, T., & Aksoy, L. (2020). Increasing importance of internal control in the light of global developments, national and international standards and regulations. *Sayıştay Dergisi*, (118), 9-40.

Akther, T., & Xu, F. (2020). Existence of the audit expectation gap and its impact on stakeholders' confidence: The moderating role of the financial reporting council. *International Journal of Financial Studies*, *8*(1), 4.

Alarcon, J. L., & Ng, C. (2018). Blockchain and the Future of Accounting. *Pennsylvania CPA Journal,* 2018, 3-7.

Albaroodi, H. A., & Anbar, M. (2022). ETHEREUM-INSPIRED ACCESS MANAGEMENT ACCOUNT CONTROL FOR A SECURED DECENTRALIZED CLOUD STORAGE. *Journal of Theoretical and Applied Information Technology*, *100*(7).

Alderman, J., & Jollineau, S. J. (2020). Can audit committee expertise increase external auditors' litigation risk? The moderating effect of audit committee independence. *Contemporary Accounting Research*, *37*(2), 717-740.

Alfandi, O., Khanji, S., Ahmad, L., & Khattak, A. (2021). A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues. *Cluster Computing*, *24*, 37-55.

Algarni, A. M., Thayananthan, V., & Malaiya, Y. K. (2021). Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems. *Applied* Sciences, 11(8), 3678.

Alston, E., Law, W., Murtazashvili, I., & Weiss, M. (2022). Blockchain networks as constitutional and competitive polycentric orders. *Journal of Institutional Economics*, *18*(5), 707-723.

American Institute of Certified Public Accountants (AICPA) (1989). Reports on Audited Financial Statements. AU-C Section 508. AICPA, New York.

American Institute of Certified Public Accountants (AICPA) (2001). Generally Accepted Auditing Standards. AU-C Section 150. AICPA, New York.

American Institute of Certified Public Accountants (AICPA) (2006). Audit Sampling. AU-C Section 350. AICPA, New York.

American Institute of Certified Public Accountants (AICPA) (2012a). Consideration of Fraud in a Financial Statement Audit. AU-C Section 240.

American Institute of Certified Public Accountants (AICPA) (2012b). External Confirmations. AU-C Section 505.

American Institute of Certified Public Accountants (AICPA) (2012c). Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained. AU-C Section 330.

American Institute of Certified Public Accountants (AICPA) (2016). Forming an Opinion and Reporting on Financial Statements. AU-C Section 700A.

American Institute of Certified Public Accountants (AICPA) (2019). Accounting for and auditing of digital assets. *Digital Assets Working Group; AICPA Senior Committees; AICPA staff*, 1-40.

American Institute of Certified Public Accountants (AICPA) (2020). *AU-C Section 200. Overall objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards.* New York.

American Institute of Certified Public Accountants (AICPA) (2021). Audit Evidence. AU-C Section 500.

American Institute of Certified Public Accountants and the Chartered Professional Accountants of Canada (AICPA & CPA Canada). (2017). Blockchain technology and its potential impact on the audit and assurance profession.

Andiola, L. M., Downey, D. H., Earley, C. E., & Jefferson, D. (2022). Wealthy watches inc.: the substantive testing of accounts receivable in the evolving audit environment. *Issues in Accounting Education*, *37*(2), 37-51.

Andoni, M., Robu, V., Flynn, D., Abram, D. Geach, D. Jenkins, McCallum, P. & Peacock, A. (2019). ‘‘*Blockchain technology in the energy sector: A systematic review of challenges and opportunities*,’’ Renew. Sustain. Energy Rev., Vol. 100, 143–174.

Appelbaum, D., Budnik, S., & Vasarhelyi, M. (2020). Auditing and accounting during and after the COVID-19 crisis. *The CPA Journal*, *90*(6), 14-19.

Appelbaum, D., Cohen, E., Kinory, E., & Smith, S. S. (2022). Impediments to Blockchain Adoption. *Journal of Emerging Technologies in Accounting*.

Appelbaum, D., & Nehmer, R. A. (2017). Using drones in internal and external audits: An exploratory framework. *Journal of Emerging Technologies in Accounting*, *14*(1), 99-113.

Appelbaum, D., & Nehmer, R. A. (2020). Auditing cloud-based blockchain accounting systems. *Journal of information systems*, *34*(2), 5-21.

Appelbaum, D., & Smith, S. S. (2018). Blockchain Basics and Hands-on Guidance: Taking the Next Step toward Implementation and Adoption. *The CPA Journal, 88*(6), 28-37.

Arefin, S. (2020). Internship report on audit procedures in Bangladesh: An experience in Hawlader Yunus Co. and Chartered Accountants.

Arifin, S. R. (2018). Ethical Considerations in Qualitative Study. *International Journal* of Care Scholars, 1(2), 30-33.

Armitage, J., & File, R. (2014). An examination of the return of confirmation requests containing fictitious names and/or addresses. *Studii Economice*, (2), 18-28.

Arruñada, B. (2018). Blockchain's struggle to deliver impersonal exchange. *Minn. JL Sci. & Tech.*, *19*, 55.

Askarzai, W., & Unhelkar, B. (2017). Research methodologies: An extensive overview. *International Journal of Science and Research Methodology*, *6*(4), 21.

Ateniese, G., Magri, B., Venturi, D., & Andrade, E. (2017, April). Redactable blockchain–or–rewriting history in bitcoin and friends. In *2017 IEEE European symposium on security and privacy (EuroS&P)*, 111-126. IEEE.

Attia, O., Khoufi, I., Laouiti, A., & Adjih, C. (2019, June). An IoT-blockchain architecture based on hyperledger framework for health care monitoring application. In *NTMS 2019-10th IFIP International Conference on New Technologies, Mobility and Security*, 1-5. IEEE Computer Society.

Baloch, Q. B. (2011). Writing of Research Proposal. *Abasyn University Journal of Social Sciences, 4*(1).

Banerjee, P., Nikam, N., & Ruj, S. (2019). Blockchain enabled privacy preserving data audit. *arXiv preprint arXiv:1904.12362*.

Bansal, G., Chamola, V., Kaddoum, G., Piran, M. J., & Alrashoud, M. (2021). Next generation stock exchange: Recurrent neural learning model for distributed ledger transactions. *Computer Networks*, *193*, 107998.

Barandi, Z., Lawson-Body, L., & Willoughby, L. (2020). Impact of the Blockchain Technology on the Continous Auditing: Mediation Role of Transaction Cost Theory. *Issues in Information Systems*, 206-212.

Barenji, R. V. (2021). A blockchain technology based trust system for cloud manufacturing. Journal of Intelligent Manufacturing, 1-15.

Barenji, A. V., & Montreuil, B. (2022). Open Logistics: Blockchain-Enabled Trusted Hyperconnected Logistics Platform. *Sensors*, *22*(13), 4699. Open Logistics: Blockchain-Enabled Trusted Hyperconnected Logistics Platform. *Sensors*, *22*(13), 4699.

Bashir, I. (2020). *Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more*. Packt Publishing Ltd.

Besançon, L., Da Silva, C. F., & Ghodous, P. (2019, May). Towards blockchain interoperability: Improving video games data exchange. In *2019 IEEE international conference on blockchain and cryptocurrency (ICBC)*, 81-85. IEEE.

Bhushan, B., Sinha, P., Sagayam, K. M., & Andrew, J. (2021). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Computers & Electrical Engineering*, *90*, 106897.

Bible, W., Raphael, J., Riviello, M., Taylor, P., & Oris Valiente, I. (2017). Blockchain technology and its potential impact on the audit and assurance profession. Aicpa.org.

Blanco, B., Coram, P., Dhole, S., & Kent, P. (2021). How do auditors respond to low annual report readability?. *Journal of Accounting and Public Policy*, *40*(3), 106769.

Boireau, O. (2018). Securing the blockchain against hackers. *Network Security*, *2018*(1), 8-11.

Bonsón, E., & Bednárová, M. (2019). Blockchain and its implications for accounting and auditing. *Meditari Accountancy Research*, *27*(5), 725-740.

Bonyuet, D. (2020). Overview and impact of blockchain on auditing. *International Journal of Digital Accounting Research*, *20*, 31-43.

Borah, M. D., Naik, V. B., Patgiri, R., Bhargav, A., Phukan, B., & Basani, S. G. (2020). Supply chain management in agriculture using blockchain and IoT. In *Advanced applications of blockchain technology*, 227-242). Springer, Singapore.

Brata, I. O. D., Rahmawati, V. A., Ardiansyah, R. S. M., Andriyani, A. D., Kautsar, M. D., Pangeran, M. D., & Roespinoedji, D. (2021). How Of Credit Sales System Influence On Internal Control Receivables of a Pharmacy in Bandung City, West Java. *Review of International Geographical Education Online*, *11*(3), 1446-1452.

Brender, N., & Gauthier, M. (2018). Impacts of blockchain on the auditing profession. *ISACA journal*, *5*, 27-32.

Brownsword, R. (2020). Automated transactions and the law of contract: When codes are not congruent. In *The Future of the Law of Contract* (pp. 94-111). Informa Law from Routledge.

Byrne, G. (2017). Narrative inquiry and the problem of representation:'giving voice', making meaning. *International Journal of Research & Method in Education*, *40*(1), 36-52.

Byrnes, P. E., Al-Awadhi, A., Gullvist, B., Brown-Liburd, H., Teeter, R., Warren, J. D., & Vasarhelyi, M. (2018). Evolution of Auditing: From the Traditional Approach to the Future Audit1. In *Continuous auditing*. Emerald Publishing Limited.

Calderón, J., & Stratopoulos, T. C. (2020). What accountants need to know about blockchain. *Accounting Perspectives*, *19*(4), 303-323.

Cangemi, M. P., & Brennan, G. (2019). Blockchain auditing–accelerating the need for automated audits!. *EDPACS*, *59*(4), 1-11.

Cao, S., Cong, L. W., & Yang, B. (2018). Auditing and blockchains: Pricing, misstatements, and regulation. *Misstatements, and Regulation.*

Cao, S., Cong, L. W., & Yang, B. (2019). Financial reporting and blockchains: Audit pricing, misstatements, and regulation. *Misstatements, and Regulation*.

Carnegie, G. D., & Napier, C. J. (2010). Traditional accountants and business professionals: Portraying the accounting profession after Enron. *Accounting, organizations and society*, *35*(3), 360-376.

Carrara, G. R., Burle, L. M., Medeiros, D. S., de Albuquerque, C. V. N., & Mattos, D. M. (2020). Consistency, availability, and partition tolerance in blockchain: a survey on the consensus mechanism over peer-to-peer networking. *Annals of Telecommunications*, *75*(3), 163-174.

Castonguay, J. (2021). Auditing and Examining Blockchain Information. *The Emerald Handbook of Blockchain for Business, Emerald Publishing Limited, Bingley*, 359-372.

Catalini, C., & Tucker, C. (2018). Antitrust and costless verification: an optimistic and a pessimistic view of the implications of blockchain technology. *SSRN Electronic Journal*.

Centobelli, P., Cerchione, R., Esposito, E., & Oropallo, E. (2021). Surfing blockchain wave, or drowning? Shaping the future of distributed ledgers and decentralized technologies. *Technological Forecasting and Social Change*, *165*, 120463.

Cetinoglu, T. (2021). Reflections of Developments in Information Technologies to Internal Audit: Blockchain Technology and Continuous Auditing. In *Auditing Ecosystem and Strategic Accounting in the Digital Era: Global Approaches and New Opportunities* (pp. 339-359). Cham: Springer International Publishing.

Cheng, C., & Huang, Q. (2020). Exploration on the application of blockchain audit. In *5th International Conference on Economics, Management, Law and Education (EMLE 2019),* 63-68. Atlantis Press.

Cichosz, S. L., Stausholm, M. N., Kronborg, T., Vestergaard, P., & Hejlesen, O. (2019). How to use blockchain for diabetes health care data and access management: an operational concept. *Journal of diabetes science and technology*, *13*(2), 248-253.

Copigneaux, B., Vlasov, N., Bani, E., Tcholtchev, N., Lämmel, P., Fuenfzig, M., ... & Frazzani, S. (2020). Blockchain for supply chains and international trade.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches.* Sage publications.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), 71.

Cumming, D. J., Johan, S., & Pant, A. (2019). Regulation of the crypto-economy: Managing risks, challenges, and regulatory uncertainty. *Journal of Risk and Financial Management*, *12*(3), 126.

Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of information systems*, *31*(3), 5-21.

da Rosa Righi, R., Alberti, A. M., & Singh, M. (2020). *Blockchain technology for Industry 4.0*. Springer Singapore.

Das, M., Tao, X., Liu, Y., & Cheng, J. C. (2022). A blockchain-based integrated document management framework for construction applications. *Automation in Construction*, *133*, 104001.

Dasaklis, T. K., Casino, F., Patsakis, C., & Douligeris, C. (2019). A framework for supply chain traceability based on blockchain tokens. In *International Conference on Business Process Management* (pp. 704-716). Springer, Cham.

Da Xu, L., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. *IEEE Internet of Things Journal*, *8*(13), 10452-10473.

De Andrés, J., & Lorca, P. (2021). On the impact of smart contracts on auditing. *International Journal of Digital Accounting Research*, *21*.

De Haes, S., Van Grembergen, W., Joshi, A., Huygh, T., De Haes, S., Van Grembergen, W., ... & Huygh, T. (2020). COBIT as a Framework for Enterprise Governance of IT. *Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations*, 125-162.

DeJonckheere, M., & Vaughn, L. M. (2019). Semistructured interviewing in primary care research: a balance of relationship and rigour. *Family medicine and community health*, *7*(2).

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics, 7*(2), 189-208.

Dengler, K., & Matthes, B. (2018). The impacts of digital transformation on the labour market: Substitution potentials of occupations in Germany. *Technological Forecasting and Social Change*, *137*, 304-316.

Desplebin, O., Lux, G., & Petit, N. (2021). To be or not to be: blockchain and the future of accounting and auditing. *Accounting Perspectives*, *20*(4), 743-769.

Dewi, A. R. (2022). THE ROLE OF INFORMATION TECHNOLOGY IN THE DEVELOPMENT OF COMPUTERIZED AUDIT. *Jurnal Ilmiah MEA* (Manajemen, Ekonomi, & Akuntansi), 6(2), 1947-1964.

Dib, O., Brousmiche, K. L., Durand, A., Thea, E., & Hamida, E. B. (2018). Consortium blockchains: Overview, applications and challenges. *Int. J. Adv. Telecommun*, *11*(1), 51-64.

Dobrowolski, Z. (2021). Principles of entrepreneurship auditing: a framework for understanding audit efficacy. *European Research Studies*, *24*(2B).

Donelson, D. C., Ege, M. S., & McInnis, J. M. (2017). Internal control weaknesses and financial reporting fraud. *Auditing: A Journal of Practice & Theory*, *36*(3), 45-69.

dos Santos, R. P. (2019). Consensus algorithms: A matter of complexity. *Between Science and Economics*, 147-170.

Dow, S. (2019). Monetary reform, central banks, and digital currencies. *International Journal of Political Economy*, *48*(2), 153-173.

Dujak, D., & Sajter, D. (2019). Blockchain applications in supply chain. *SMART supply network*, 21-46.

Duke, A. (2019). What Does the CISG Have to Say about Smart Contracts: A Legal Analysis. *Chi. J. Int'l L.*, *20*, 141.

Dyball, M. C., & Seethamraju, R. (2021). The impact of client use of blockchain technology on audit risk and audit approach—An exploratory study. *International Journal of Auditing*, *25*(2), 602-615.

Edmonds, M., Miller, T., & Savage, A. (2019). Accounts receivable: An audit simulation. *Journal of Accounting Education*, *47*, 75-92.

Egiyi, M. A., & Okafor, V. I. (2021). Blockchain: The Building Block to the Future of Accounting. *European Journal of Finance and Management Sciences*, *5*(3), 1-8.

Ekin, T. (2019). An Integrated Decision Making Framework for Medical Audit Sampling.

Elommal, N., & Manita, R. (2022). How Blockchain Innovation could affect the Audit Profession: A Qualitative Study. *Journal of Innovation Economics Management*, *37*(1), 37-63.

Eltweri, A., Faccia, A., & Foster, S. (2022). International Standards on Auditing (ISAs) Adoption: An Institutional Perspective. *Administrative Sciences*, *12*(3), 119.

Engelen, K. C. (2021). Germany's Wirecard Scandal. *The International Economy*, *35*(1), 9-12.

Estep, C. (2021). Auditor integration of IT specialist input on internal control issues: How a weaker team identity can be beneficial. *The Accounting Review*, *96*(5), 263-289.

Faccia, A., & Petratos, P. (2021). Blockchain, enterprise resource planning (ERP) and accounting information systems (AIS): Research on e-procurement and system integration. *Applied Sciences*, *11*(15), 6792.

Faccia, A., Pandey, V., & Banga, C. (2022). Is permissioned blockchain the key to support the external audit shift to entirely open innovation paradigm?. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(2), 85.

Fan, K., Bao, Z., Liu, M., Vasilakos, A. V., & Shi, W. (2020). Dredas: Decentralized, reliable and efficient remote outsourced data auditing scheme with blockchain smart contract for industrial IoT. *Future Generation Computer Systems*, *110*, 665-674.

Farcane, N., & Deliu, D. (2020). Stakes and Challenges Regarding the Financial Auditor's Activity in the Blockchain Era. *Audit Financiar, 18*(157), 154-181.

Farooq, M. B., & De Villiers, C. (2017). The market for sustainability assurance services: A comprehensive literature review and future avenues for research. *Pacific Accounting Review*.

Feng, T., Yu, X., Chai, Y., & Liu, Y. (2019). Smart contract model for complex reality transaction. *International Journal of Crowd Science*, *3*(2), 184-197.

Flood, J. M. (2021). *Wiley Practitioner's Guide to GAAS 2021: Covering all SASs, SSAEs, SSARSs, and Interpretations.* John Wiley & Sons.

Frazer, L. (2020). Does internal control improve the attestation function and by extension assurance services? A Practical Approach. *Journal of Accounting and Finance*, *20*(1), 28-38.

Freiman, J. W., Kim, Y., & Vasarhelyi, M. A. (2022). Full population testing: Applying multidimensional audit data sampling (MADS) to general ledger data auditing. *International Journal of Accounting Information Systems*, *46*, 100573.

Friese, S., Soratto, J., & Pires, D. (2018). Carrying out a computer-aided thematic content analysis with ATLAS. ti.

Fuller, S. H., & Markelevich, A. (2020). Should accountants care about blockchain?. *Journal of Corporate Accounting & Finance*, *31*(2), 34-46.

Gans, J. S. (2019). *The fine print in smart contracts* (No. w25443). National Bureau of Economic Research.

Gauthier, M. P., & Brender, N. (2021). How do the current auditing standards fit the emergent use of blockchain?. *Managerial auditing journal*, *36*(3), 365-385.

Ghiro, L., Restuccia, F., D'Oro, S., Basagni, S., Melodia, T., Maccari, L., & Cigno, R. L. (2021). What is a Blockchain? A Definition to Clarify the Role of the Blockchain in the Internet of Things. *arXiv preprint arXiv:2102.03750*.

Graham, G. A. L., & Sherwood, M. (2021). The External Financial Statement Audit Process and Blockchain Technology. *TIDE AcademIA Research*, *3*(1), 103-140.

Gray, D. E. (2021). Doing research in the real world. *Doing research in the real world*, 1-100.

Guo, J., Kinory, E., & Zhou, Y. (2021). Examining PCAOB disciplinary orders on small audit firms: Evidence from 2005 to 2018. *International Journal of Auditing*, *25*(1), 103-116.

Gupta, M. (2017). Blockchain For Dummies, John Wiley & Sons, Inc.

Guzov, I., Soboleva, G., & Artemova, D. (2019, November). Digital technologies in accounting and taxation: Some issues from Russian literature and experience. In *Third International Economic Symposium (IES 2018)* (pp. 258-263). Atlantis Press.

Haggenmüller, S. (2019). *Revenue recognition under IFRS 15: A critical evaluation of predefined purposes and implications for improvement* (Doctoral dissertation, University of Gloucestershire).

Hammoudeh, M., Adebisi, B., Unal, D., & Laouid, A. (2021). Bringing Coordination Languages Back to the Future Using Blockchain Smart Contracts. In *The 5th International Conference on Future Networks & Distributed Systems,* 299-304.

Hamshari, Y. M., Ali, H. Y., & Alqam, M. A. (2021). The relationship of professional skepticism to the risks of auditing and internal control, and the discovery of fraud and core errors in the financial statements in Jordan. *Academic Journal of Interdisciplinary Studies*, *10*(2), 105-105.

Hardjono, T., Lipton, A., & Pentland, A. (2018). Towards a design philosophy for interoperable blockchain systems. *arXiv preprint arXiv:1805.05934*.

Harris, C. G. (2019). Consensus-based secret sharing in blockchain smart contracts. In *2019 International Workshop on Big Data and Information Security (IWBIS),* 79-84. IEEE.

Hayrettin, U. S. U. L., & Karaburun, G. (2020). Changes in the professional profile of auditors in the light of blockchain technology. *European Journal of Digital Economy Research*, *1*(1), 5-12.

He, L. J., & Chen, J. (2021). Does mandatory audit partner rotation influence auditor selection strategies?. *Sustainability*, *13*(4), 2058.

Heo, G., Yang, D., Doh, I., & Chae, K. (2021). Efficient and secure blockchain system for digital content trading. *IEEE Access*, *9*, 77438-77450.

Homoliak, I., Venugopalan, S., Hum, Q., & Szalachowski, P. (2019). A security reference architecture for blockchains. In *2019 IEEE international Conference on blockchain (blockchain)*, 390-397. IEEE.

Howell, B. E., & Potgieter, P. H. (2021). Uncertainty and dispute resolution for blockchain and smart contract institutions. *Journal of Institutional Economics*, *17*(4), 545-559.

Huang, J., Kong, L., Chen, G., Wu, M. Y., Liu, X., & Zeng, P. (2019). Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. *IEEE Transactions on Industrial Informatics*, *15*(6), 3680-3689.

Inghirami, I. E. (2019). Accounting information systems in the time of blockchain. In *Conference: İtaıs 2018 Conference* (pp. 1-16).

International Auditing and Assurance Standards Board (IAASB) (2009). ISA 505, External Confirmations.

Ismail, L., Materwala, H., & Zeadally, S. (2019). Lightweight blockchain for healthcare. *IEEE Access*, *7*, 149935-149951.

Iwanowicz, T., & Iwanowicz, B. (2019). ISA 701 and materiality disclosure as methods to minimize the audit expectation gap. *Journal of Risk and Financial Management*, *12*(4), 161.

Jamil, F., Ahmad, S., Iqbal, N., & Kim, D. H. (2020). Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals. *Sensors*, *20*(8), 2195.

Jayaraman, A. R., & Bhuyan, P. (2020). Impact of NPA and loan write-offs on the profit efficiency of Indian banks. *Decision*, *47*(1), 35-48.

Jayathilake, N. D., & Seneviratne, S. C. (2022). The Investigation of the Awareness of Implementing Blockchain Technology in Audit Trails among the Auditors. *Journal of Accounting Research, Organization and Economics*, *5*(2), 109-123.

Ji, S., Zhu, S., Zhang, P., Dong, H., & Yu, J. (2022). Test-Case Generation for Data Flow Testing of Smart Contracts Based on Improved Genetic Algorithm. *IEEE Transactions on Reliability*.

Jin, H., Dai, X., & Xiao, J. (2018). Towards a novel architecture for enabling interoperability amongst multiple blockchains. In *2018 IEEE 38th International* Conference on Distributed Computing Systems (ICDCS), 1203-1211). IEEE.

Johnson, J. L., Adkins, D., & Chauvin, S. (2020). A review of the quality indicators of rigor in qualitative research. *American journal of pharmaceutical education*, *84*(1).

Kahyaoğlu, S. B., Sarikaya, R., & Topal, B. (2020). Continuous auditing as a strategic tool in public sector internal audit: The Turkish case. *Selçuk Üniversitesi Sosyal Bilimler Meslek Yüksekokulu Dergisi*, *23*(1), 208-225.

Kalpokas, N., & Radivojevic, I. (2021). Adapting practices from qualitative research to tell a compelling story: A practical framework for conducting a literature review. *The Qualitative Report*, *26*(5), 1546-1566.

Kalu, A. O. U., Unachukwu, L. C., & Ibiam, O. (2019). Accessing secondary data: A literature review.

Kan, L., Wei, Y., Muhammad, A. H., Siyuan, W., Gao, L. C., & Kai, H. (2018). A multiple blockchains architecture on inter-blockchain communication. In *2018 IEEE international conference on software quality, reliability and security companion (QRS-C),* 139-145). IEEE.

Kayıkcı, Y., & Subramanian, N. (2022). Blockchain Interoperability Issues in Supply Chain: Exploration of Mass Adoption Procedures. In *Big Data and Blockchain for Service Operations Management* (pp. 309-328). Cham: Springer International Publishing.

Kend, M., & Nguyen, L. A. (2020). Big data analytics and other emerging technologies: the impact on the Australian audit and assurance profession. *Australian Accounting Review*, *30*(4), 269-282.

Khalaf, O. I., & Abdulsahib, G. M. (2021). Optimized dynamic storage of data (ODSD) in IoT based on blockchain for wireless sensor networks. *Peer-to-Peer Networking and Applications*, *14*(5), 2858-2873.

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021a). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-peer Networking and Applications*, *14*(5), 2901-2925.

Khan, D., Jung, L. T., & Hashmani, M. A. (2021b). Systematic Literature Review of Challenges in Blockchain Scalability. *Applied Sciences*, *11*(20), 9372.

Kivunja, C. (2018). Distinguishing between theory, theoretical framework, and conceptual framework: A systematic review of lessons from the field. *International journal of higher education*, *7*(6), 44-53.

Kokina,J., Mancha, R. & Pachamanova, D. (2017). Blockchain: Emergent industry adoption and implication for accounting. *Journal of Emerging Technologies in Accounting, 14*(2), 91-100.

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1), 120-124.

Lashkari, B., & Musilek, P. (2021). A comprehensive review of blockchain consensus mechanisms. *IEEE Access*, *9*, 43620-43652.

Lester, J. N., Cho, Y., & Lochmiller, C. R. (2020). Learning to do qualitative data analysis: A starting point. *Human Resource Development Review*, *19*(1), 94-106.

Li, D., Hu, Y., & Lan, M. (2020). IoT device location information storage system based on blockchain. *Future Generation computer systems*, *109*, 95-102.

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.

Löher, J. (2019). *MATCHING FOUNDERS AND FUNDERS IN EQUITY CROWDFUNDING* Doctoral dissertation, Universiät Siegen, Siegen, Germany.

Lombardi, R., de Villiers, C., Moscariello, N., & Pizzo, M. (2022). The disruption of blockchain in auditing–a systematic literature review and an agenda for future research. *Accounting, Auditing & Accountability Journal*, *35*(7), 1534-1565.

Loubere, N. (2017). Questioning transcription: The case for the systematic and reflexive interviewing and reporting (SRIR) method. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research* (Vol. 18, No. 2, p. 22). DEU.

Loughran, M. (2020). *Financial accounting for Dummies*. John Wiley & Sons.

Lu, H., Tang, Y., & Sun, Y. (2021). DRRS-BC: Decentralized routing registration system based on blockchain. *IEEE/CAA Journal of Automatica Sinica*, *8*(12), 1868-1876.

Luo, H., Das, M., Wang, J., & Cheng, J. C. (2019). Construction payment automation through smart contract-based blockchain framework. In *ISARC. Proceedings of the International Symposium on Automation and Robotics in Construction (36),* 1254-1260). IAARC Publications.

Lureau, S. S. (2020). Auditing Accounts Receivable and Allowance for Doubtful Accounts at Cardinal Corporation. *The North American Accounting Studies*, *3*(1), 4.

Maama, H., & Marimuthu, F. (2021). Accountability in the Ghanaian local governance structure: Probing the role of external auditing. *Problems and Perspectives in Management*, *18*(4), 475.

Maesa, D. D. F., Mori, P., & Ricci, L. (2019). A blockchain based approach for the definition of auditable access control systems. *Computers & Security*, *84*, 93-119.

Mahindrakar, A., & Joshi, K. P. (2020, May). Automating GDPR compliance using policy integrated blockchain. In *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, 86-93. IEEE.

Manita, R., Elommal, N., Baudier, P., & Hikkerova, L. (2020). The digital transformation of external audit and its impact on corporate governance. *Technological Forecasting and Social Change*, *150*, 119751.

Mantelaers, E., Zoet, M., & Smit, K. (2019). The impact of blockchain on the auditor's audit approach. *Proceedings of the 2019 3rd International Conference on Software and e-Business*, 183-187.

Marei, A., & Iskandar, E. D. T. B. M. (2019). The impact of Computer Assisted Auditing Techniques (CAATs) on development of audit process: an assessment of Performance Expectancy of by the auditors. *International Journal of Management and Commerce Innovations*, *7*(2), 1199-1205.

Mason, M. (2010). Sample size and saturation in PhD studies using qualitative interviews. In *Forum qualitative Sozialforschung/Forum: qualitative social research* (Vol. 11, No. 3).

Masood, S., Shahid, M. A., Sharif, M., & Yasmin, M. (2018). Comparative analysis of peer to peer networks. *International Journal of Advanced Networking and Applications*, *9*(4), 3477-3491.

Mayan, M. J. (2016). *Essentials of qualitative inquiry*. Routledge.

McGaghie, W. C., Bordage, G., & Shea, J. A. (2001). Problem statement, conceptual framework, and research question. *Academic medicine*, *76*(9), 923-924.

Melnychenko, O., & Mishina, A. (2022). Key issues of the planning process of the audit of receivables.

Memon, S., Umrani, S., & Pathan, H. (2017). Application of constant comparison method in social sciences: a useful technique to analyze interviews. *Grassroots*, *51*(1).

Mijoska, M., & Ristevski, B. (2021). Possibilities for applying blockchain technology–a survey. *Informatica*, *45*(3).

Mikula, T., & Jacobsen, R. H. (2018). Identity and access management with blockchain in electronic healthcare records. In *2018 21st Euromicro conference on digital system design (DSD),* 699-706. IEEE.

Mintz, S. (2020). Codifying the Fundamental Principles of'Professional Behavior': Strengthening Professionalism by Enhancing Moral Conduct. *The CPA Journal*, *90*(3), 20-27.

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People*, *7*(1), 23-48.

Montenegro, T. M., & Brás, F. A. (2018). A review of the concept and measures of audit quality across three decades of research. *International Journal of Accounting, Auditing and Performance Evaluation*, *14*(2-3), 183-253.

Morse, J. M., & Richards, L. (2013). Qualitative research design. *Readme first for a user's guide to qualitative methods. 3rd ed. Los Angeles: Sage*, 87-116.

Müller, R., Kanso, A., & Adler, F. (2022). An Approach to Integrate a Blockchain-Based Payment Model and Independent Secure Documentation for a Robot as a Service. *Annals of Scientific Society for Assembly, Handling and Industrial Robotics 2021*, 177.

Nair, R., Gupta, S., Soni, M., Shukla, P. K., & Dhiman, G. (2020). An approach to minimize the energy consumption during blockchain transaction. *Materials Today: Proceedings*.

Nascimento, L. D. S., & Steinbruch, F. K. (2019). “The interviews were transcribed”, but how? Reflections on management research. *RAUSP Management Journal*, *54*, 413-429.

Nasheeda, A., Abdullah, H. B., Krauss, S. E., & Ahmed, N. B. (2019). Transforming transcripts into stories: A multimethod approach to narrative analysis. *International Journal of Qualitative Methods*, *18*, 1609406919856797.

Neubauer, B. E., Witkop, C. T., & Varpio, L. (2019). How phenomenology can help us learn from the experiences of others. *Perspectives on medical education*, *8*, 90-97.

Nordgren, A. I. N. O., Weckström, E. L. L. E. N., Martikainen, M. I. N. N. A., & Lehner, O. M. (2019). Blockchain in the fields of finance and accounting: a disruptive technology or an overhyped phenomenon. *ACRN Journal of Finance and Risk Perspectives*, *8*, 47-58.

Nouri, H. (2018). Auditor-to-Auditor Confirmations: A New Approach in Obtaining Accounts Receivable Confirmation and Its Empirical Investigation.

Nurdiansyah, D. H., & Manda, G. S. (2018). The effect of allowance for bad debt loss to the level of profitability (case study in local bank Indonesia). *ECONOMICS-Innovative and Economic Research*, *6*(1), 125-139.

Oakley, J., Worley, C., Yu, L., Brooks, R. R., Özçelik, İ. L. K. E. R., Skjellum, A., & Obeid, J. S. (2021). Scrybe: A Secure Audit Trail for Clinical Trial Data Fusion. *Digital Threats: Research and Practice*.

O'leary, Z. (2004). The essential guide to doing research. Sage Publishing Inc., London.

Ølnes, S., & Jansen, A. (2018, May). Blockchain technology as infrastructure in public sector: an analytical framework. In *Proceedings of the 19th annual international conference on digital government research: governance in the data age* (pp. 1-10).

Omar, I. A., Jayaraman, R., Salah, K., Yaqoob, I., & Ellahham, S. (2021). Applications of blockchain technology in clinical trials: review and open challenges. *Arabian Journal for Science and Engineering*, *46*(4), 3001-3015.

Ortman, C. (2018). Blockchain and the Future of the Audit.

Ozlanski, M. E., Negangard, E. M., & Fay, R. G. (2020). Kabbage: A fresh approach to understanding fundamental auditing concepts and the effects of disruptive technology. *Issues in Accounting Education Teaching Notes*, *35*(2), 26-38.

Paggi, E. (2022). Blockchain in finance: focus on securitization.

Pahlajani, S., Kshirsagar, A., & Pachghare, V. (2019). Survey on private blockchain consensus algorithms. In *2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT),* 1-6). IEEE.

Palmrose, Z. V., & Kinney Jr, W. R. (2018). Auditor and FASB responsibilities for representing underlying economics—What US standards actually say. *Accounting Horizons*, *32*(3), 83-90.

Pamungkas, B., Ibtida, R., & Avrian, C. (2018). Factors influencing audit opinion of the Indonesian municipal governments' financial statements. *Cogent Business & Management*, *5*(1), 1540256.

Park, J., & Jeong, E. (2019). Service quality in tourism: A systematic literature review and keyword network analysis. *Sustainability*, *11*(13), 3665.

Peng, L., Feng, W., Yan, Z., Li, Y., Zhou, X., & Shimizu, S. (2021). Privacy preservation in permissionless blockchain: A survey. *Digital Communications and Networks*, *7*(3), 295-307.

Pereira, A., Vaz, Â., & Silva, E. S. (2022). Sales, Services and Debts Receivable. *International Journal of Social Sciences and Management Review, 05* (1), 37-43.

Perera, P. A. S. N., & Abeygunasekera, A. W. J. C. (2022). Blockchain Adoption in Accounting and Auditing: A Qualitative Inquiry in Sri Lanka. *Colombo Business Journal*, *13*(1).

Piercy, L. R., & Levy, H. B. (2021). To Confirm or Not to Confirm-Risk Assessment is the Answer. *The CPA Journal*, *91*(12), 54-57.

Pillai, B., Biswas, K., & Muthukkumarasamy, V. (2020). Cross-chain interoperability among blockchain-based systems using transactions. *The Knowledge Engineering Review*, *35*.

Pimentel, E., Boulianne, E., Eskandari, S., & Clark, J. (2021). Systemizing the challenges of auditing blockchain-based assets. *Journal of Information Systems, 35*(2), 61-75.

Popchev, I., Radeva, I., & Velichkova, V. (2021, October). The impact of blockchain on internal audit. In *2021 Big Data, Knowledge and Control Systems Engineering* (BdKCSE), 1-8. IEEE.

Poucher, Z. A., Tamminen, K. A., Caron, J. G., & Sweet, S. N. (2020). Thinking through and designing qualitative research studies: A focused mapping review of 30 years of qualitative research in sport psychology. *International Review of Sport and Exercise Psychology*, *13*(1), 163-186.

Pratt, M. G., Kaplan, S., & Whittington, R. (2020). Editorial essay: The tumult over transparency: Decoupling transparency from replication in establishing trustworthy qualitative research. *Administrative Science Quarterly*, *65*(1), 1-19.

Psaila, S. (2017). Blockchain: A game changer for audit processes. *Deloitte Malta Article*, 1-4.

Puri, V., Priyadarshini, I., Kumar, R., & Van Le, C. (2021). Smart contract based policies for the Internet of Things. *Cluster Computing*, *24*(3), 1675-1694.

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). The blockchain as a decentralized security framework [future directions]. *EEE Consumer Electronics Magazine, 7*(2), 18-21.

Putz, B., Menges, F., & Pernul, G. (2019). A secure and auditable logging infrastructure based on a permissioned blockchain. *Computers & Security.*(Vol 87).

Qasim, A., & Kharbat, F. F. (2020). Blockchain technology, business data analytics, and artificial intelligence: Use in the accounting profession and ideas for inclusion into the accounting curriculum. *Journal of Emerging Technologies in Accounting, 17*(1), 107–117.

Raikwar, M., Mazumdar, S., Ruj, S., Gupta, S. S., Chattopadhyay, A., & Lam, K. Y. (2018). A blockchain framework for insurance processes. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS),* 1-4. IEEE.

Raschke, R. L., Saiewitz, A., Kachroo, P., & Lennard, J. B. (2018). AI-enhanced audit inquiry: A research note. *Journal of Emerging Technologies in Accounting*, *15*(2), 111-116.

Rey-Ares, L., Fernández-López, S., & Rodeiro-Pazos, D. (2021). Impact of working capital management on profitability for Spanish fish canning companies. *Marine Policy*, *130*, 104583.

Rijanto, A. (2021). Blockchain technology adoption in supply chain finance. *Journal of Theoretical and Applied Electronic Commerce Research*, *16*(7), 3078-3098.

Rozario, A. M., & Thomas, C. (2019). Reengineering the audit with blockchain and smart contracts. *Journal of emerging technologies in accounting*, *16*(1), 21-35.

Rozario, A. M., & Vasarhelyi, M. A. (2018). Auditing with Smart Contracts. *International Journal of Digital Accounting Research, 18*.

Rozario, A. M., Vasarhelyi, M. A., & Wang, T. D. (2022). On the Use of Consumer Tweets to Assess the Risk of Misstated Revenue in Consumer-Facing Industries: Evidence from Analytical Procedures. *AUDITING: A Journal of Practice & Theory*.

Salih, J. I., & Flayyihb, H. H. (2020). Impact of audit quality in reducing external audit profession risks. *International Journal of Innovation, Creativity and Change*, *13*(7), 176-197.

Sarferaz, S. (2022). Process of Finance. In *Compendium on Enterprise Resource Planning,* 233-251). Springer, Cham.

Sarmah, S. S. (2018). Understanding blockchain technology. *Computer Science and Engineering, 8*(2), 23-29.

Sastry Musti, K. S., Paulus, G. N., & Katende, J. (2021). A Novel Framework for Energy Audit Based on Crowdsourcing Principles. *Crowdfunding in the Public Sector: Theory and Best Practices*, 167-186.

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods. Business Students* (4th edition ed.). Harlow, United Kingdom: Pearson Education Limited.

Savchenko, A., Saliamon-Mikhieieva, K., & Holynska, M. (2018). Analysis and audit of key economic indicators of economic entities (a case study of the dairy industry). *Baltic journal of economic studies*, *4*(3), 271-275.

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

Schmidt, C. G., & Wagner, S. M. (2019). Blockchain and supply chain relations: A transaction cost theory perspective. *Journal of Purchasing and Supply Management, 25*(4).

Schmitz, J., & Leoni, G. (2019). Accounting and auditing at the time of blockchain technology: a research agenda. *Australian Accounting Review, 29*(2), 331-342.

Selg, M. (2022a). Dissertation Design on Blockchain Technology in Auditing. *Journal of International DBA Studies*, *2*(003).

Selg, M. (2022b). Characteristics and Functionality of the Blockchain Technology. *Journal of International DBA Studies*, *2*(003).

Septiawan, B. (2022). Application Of Triple-Entry Bookkeeping with Blockchain Technology as an Effort to Prevent Accounting Fraud. *Akuntansi Dewantara*, *6*(2), 42-47.

Seretakis, A. L. (2019). Blockchain, securities markets and central banking.

Sheldon, M. D. (2019). A primer for information technology general control considerations on a private and permissioned blockchain audit. *Current Issues in Auditing*, *13*(1), A15-A29.

Shields, P. M., Rangarajan, N., & Casula, M. (2019). It is a Working Hypothesis: Searching for Truth in a Post-Truth World.

Shobanadevi, A., Tharewal, S., Soni, M., Kumar, D. D., Khan, I. R., & Kumar, P. (2022). Novel identity management system using smart blockchain technology. *International Journal of System Assurance Engineering and Management*, *13*(1), 496-505.

Singh, K. K. (2022). Application of Blockchain Smart Contracts in E-Commerce and Government. *arXiv preprint arXiv:2208.01350*.

Smith, S. S., & Castonguay, J. J. (2020). Blockchain and accounting governance: Emerging issues and considerations for accounting and assurance professionals. *Journal of Emerging Technologies in Accounting, 17*(1), 119-131.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of business research*, *104*, 333-339.

Sokolov, B., & Kolosov, A. (2018). Comparison of ERP systems with blockchain platform. In *Proceedings of the Computational Methods in Systems and Software*, 240-247. Springer, Cham.

Soonawalla, K., & Stroehle, J. C. (2022). Old Saddles for New Horses: How Non-Financial Assurance Reinforces Traditional Firm Boundaries. *Available at SSRN 4230387*.

Soyemi, K., Afolabi, O. V., & Obigbemi, I. F. (2021). External audit quality and clients' corporate governance mechanisms in Nigeria: Any nexus?. *Journal of Research in Emerging Markets*, *3*(2), 44-59.

Stahl, N. A., & King, J. R. (2020). Expanding approaches for research: Understanding and using trustworthiness in qualitative research. *Journal of Developmental Education*, *44*(1), 26-28.

Stetsenko, P., & Khalimov, G. (2020). Blockchain-Based Protocol for Ensuring Authenticity of Data Origin in Cloud Environments. In *ICST* (pp. 176-190).

Stinchcombe, K. (2018). Blockchain is not only crappy technology but a bad vision for the future. *Medium. Apr*, *5*.

Sujanto, M., Lindawati, A. S. L., Zulkarnain, A., & Liawatimena, S. (2021). Auditor's Perception on Technology Transformation: Blockchain and CAATs on Audit Quality in Indonesia. *International Journal of Advanced Computer Science and Applications*, *12*(8).

Sultana, T., Almogren, A., Akbar, M., Zuair, M., Ullah, I., & Javaid, N. (2020). Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices. *Applied Sciences*, *10*(2), 488.

Svanberg, M., Santén, V., Hörteborn, A., Holm, H., & Finnsgård, C. (2019). AIS in maritime research. *Marine Policy*, *106*, 103520.

Thakur, T., Mehra, A., Hassija, V., Chamola, V., Srinivas, R., Gupta, K. K., & Singh, A. P. (2021). Smart water conservation through a machine learning and blockchain-enabled decentralized edge computing network. *Applied Soft Computing*, *106*, 107274.

Thakur, V., Doja, M. N., Dwivedi, Y. K., Ahmad, T., & Khadanga, G. (2020). Land records on blockchain for implementation of land titling in India. *International Journal of Information Management*, *52*, 101940.

Theofanidis, D., & Fountouki, A. (2018). Limitations and delimitations in the research process. P*erioperative Nursing-Quarterly scientific, online official journal of GORNA, 7*, 155-163.

Torky, M., & Hassanein, A. E. (2020). Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges. *Computers and* Electronics in Agriculture, 178, 105476.

Tušek, B., Ježovita, A., & Halar, P. (2021). The importance and differences of analytical procedures' application for auditing blockchain technology between external and internal auditors in Croatia. *Economic Research-Ekonomska Istraživanja*, *34*(1), 1385-1408.

Tuxtabaevich, E. I. (2022). Theoretical Bases of Application of Audit Procedures in the Process of Collecting Audit Evidence. *Spanish Journal of Innovation and Integrity*, *4*, 64-68.

Vasarhelyi, M. A., Alles, M., Kuenkaikaew, S., & Littley, J. (2012). The acceptance and adoption of continuous auditing by internal auditors: A micro analysis. *International journal of accounting information systems*, *13*(3), 267-281.

Varma, J. (2019). Blockchain in Finance. *Vikalpa, 44*(1), 1-11.

Vincent, N. E., Skjellum, A., & Medury, S. (2020). Blockchain architecture: A design that helps CPA firms leverage the technology. *International Journal of Accounting Information Systems, 38*. doi:100466.

Vincent, N. E., & Wilkins, A. M. (2020). Challenges when auditing cryptocurrencies. *Current Issues in Auditing*, *14*(1), A46-A58.

Vishnia, G. R., & Peters, G. W. (2020). AuditChain: A trading audit platform over blockchain. *Frontiers in Blockchain, 3*(14), 1-14.

Waldo, J. (2019). A hitchhiker's guide to the blockchain universe. *Communications of the ACM*, *62*(3), 38-42.

Wang, Y. (2018). *Designing continuous audit analytics and fraud prevention systems using emerging technologies* (Doctoral dissertation, Rutgers University-Graduate School-Newark).

Wang, X., & Cheng, Z. (2020). Cross-sectional studies: strengths, weaknesses, and recommendations. *Chest*, *158*(1), S65-S71.

Wang, Y., & Kogan, A. (2018). Designing confidentiality-preserving Blockchain-based transaction. *International Journal of Accounting Information, 30*, 1-18.

Wang, L., Liu, J., & Liu, W. (2021). Staged data delivery protocol: A blockchain-based two-stage protocol for non-repudiation data delivery. *Concurrency and Computation: Practice and Experience*, *33*(13), e6240.

Wang, K., Zhang, Y., & Chang, E. (2020). A conceptual model for blockchain-based auditing information system. Proceedings of the 2020 2nd International Electronics Communication Conference. 101-107.

Ward, J. K., Comer, U., & Stone, S. (2018). On qualifying qualitative research: Emerging perspectives and the "Deer"(descriptive, exploratory, evolutionary, repeat) paradigm. *Interchange*, *49*, 133-146.

Westland, J. C. (2020). Substantive Tests. In *Audit Analytics*, 189-241. Springer, Cham.

Williams, M., & Moser, T. (2019). The art of coding and thematic exploration in qualitative research. *International Management Review*, *15*(1), 45-55.

Wongthongtham, P., Marrable, D., Abu-Salih, B., Liu, X., & Morrison, G. (2021). Blockchain-enabled Peer-to-Peer energy trading. *Computers & Electrical Engineering*, *94*, 107299.

Woodside, J. M., Augustine Jr., F. K., & Giberson, W. (2017). Blockchain technology adoption status and strategies. *Journal of International Technology and Information Management, 26*(2).

Yavari, M., Safkhani, M., Kumari, S., Kumar, S., & Chen, C. M. (2020). An improved blockchain-based authentication protocol for iot network management. *Security and Communication Networks*, *2020*, 1-16.

Yebi, D. K., & Cudjoe, E. K. (2022). Artificial Intelligence as a Disruptive Business Model in Auditing. A study of the impact of artificial intelligence on auditors' skills and competence, audit process, and audit quality.

Yermack, D. (2017). Corporate governance and blockchains. *Review of finance*, *21*(1), 7-31.

Zakaria, R., Hatib Musta'amal, A., & Amin, N. F. M. (2015). Transcribing with Atlas.ti. In *ATLAS.Ti user conference,* 1-15.

Zemánková, A. (2019). Artificial Intelligence and Blockchain in Audit and Accounting: Literature Review. *WSEAS Transactions on Business and Economics, 16*,(1)*,* 568-581.

Zeng, Y., & Zhang, Y. (2019). Review of research on blockchain application development method. In *Journal of Physics: Conference Series* (Vol. 1187, No. 5, p. 052005). IOP Publishing.

Zeng, Y., Zhang, J. H., Zhang, J., & Zhang, M. (2021). Key audit matters reports in China: Their descriptions and implications of audit quality. *Accounting Horizons*, *35*(2), 167-192.

Zheng, R., Jiang, J., Hao, X., Ren, W., Xiong, F., & Ren, Y. (2019). bcBIM: A blockchain-based big data model for BIM modification audit and provenance in mobile cloud. *Mathematical Problems in Engineering*, *2019*.

Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, *105*, 475-491.

Zhong, B., Wu, H., Ding, L., Luo, H., Luo, Y., & Pan, X. (2020). Hyperledger fabric-based consortium blockchain for construction quality information management. *Frontiers of engineering management*, *7*(4), 512-527.

Zülch, H. (2020). International Financial Reporting Standards (IFRS) 2020: Deutsch-englische Textausgabe der von der EU gebilligten Standards und Interpretationen. 14. John Wiley & Sons.

Appendix A - Tables

Table A1

Generally Accepted Auditing Standards (GAAS)

General Standards	Standards of Fieldwork	Standards of Reporting
Technical training and proficiency in performing an audit (AICPA, 2001).	Adequately plan the work and properly supervise any assistants (AICPA, 2001).	A statement that financial statements are presented in accordance with GAAP (AICPA, 2001).
Independence in mental attitude relating to the audit (AICPA, 2001).	Obtain a sufficient under-standing of entities and their environment, including internal controls (AICPA, 2001).	Identification of inappropriate consistency in the application of GAAP (AICPA, 2001).
Exercise due professional care in the performance of audits and preparation of reports (AICPA, 2001).	Obtain sufficient appropriate audit evidence by performing audit procedures to form an opinion on financial statements under audit (AICPA, 2001).	Statement if informative disclosures are not reasonably adequate (AICPA, 2001).
		Express an opinion regarding the financial statements (AICPA, 2001).

Note: This table summarizes in tabular form the GAAS of AU-C 150 by AICPA, 2001, p. 1599-1600.

Table A2

Traditional versus Blockchain-based Audit Procedures

Audit Procedures	Traditional Auditing	Auditing with Blockchains
Inspection	Under traditional auditing, audit procedures for inspection of samples of accounting records and tracing them towards related invoices, vouchers, etc., for verification of the transactions and matching them with the other information are performed (Appelbaum & Nehmer, 2017).	In a blockchain system, audit procedures examine entire populations of accounting-related data in real-time and test internal controls (Appelbaum & Nehmer, 2017).
Observation	Substantive audit procedures focus on observing the auditee´s control activities by audit teams (Appelbaum & Nehmer, 2017).	Verification of workflows under audit is performed with blockchains (Appelbaum & Nehmer, 2017).
Inquiry	Substantive audit procedures focus on performing interviews with the responsible staff of the auditee (Appelbaum & Nehmer, 2017).	Monitoring of processes and internal controls to identify process violations are performed with blockchains (Appelbaum & Nehmer, 2017).
Confirmation	Substantive audit procedures focus on performing requests for third-party confirmations on account balances of accounts receivable (Appelbaum & Nehmer, 2017).	The linking of several data streams for confirming balances is performed by using blockchains (Appelbaum & Nehmer, 2017).
Recalculation	Substantive audit procedures focus on extracting data from accounting systems and recalculating e data for verification by audit teams (Appelbaum & Nehmer, 2017).	If required, monitoring all accounting-related data and running automatic calculations on permanent intervals are performed using blockchains (Appelbaum & Nehmer, 2017).
Re-performance	Substantive audit procedures focus on re-performing control procedures by the audit teams to verify the effectiveness of internal controls (Appelbaum & Nehmer, 2017).	Automatically replicates all recognized transactions in blockchains to identify if exceptions are performed using blockchains (Appelbaum & Nehmer, 2017).

Note: This table provides a comparison of traditional versus blockchain-based audit procedures following Appelbaum & Nehmer, 2017, p.103.

Table A3

Overview of Conducted Interviews

Interviewee	Duration of Interviews	Comments
1: ISO 27001 Lead Auditor	62 minutes	Good experience in auditing and with cryptocurrencies; Some experience with blockchain;
2: German CPA	49 minutes	Good experience in IT-related audits and with blockchains;
3: German CPA	68 minutes	Very deep experience in IT-related audits and good experience with blockchains
4: CISA	60 minutes	Long term experience in IT-related audits and good experience with blockchains
5: ITIL Professional	65 minutes	Highly experienced in IT-related audits; Good experience in blockchains; Trainer of auditors for tool-based auditing
6: CISA	69 minutes	Over 25 years of experience in IT-related audits and good blockchain knowledge;
7: ACCA	61 minutes	Good experience in IT-related audits; Some experience with blockchains;
8: US CPA	59 minutes	Good experience in auditing IT systems; Some experience with blockchain-based auditing;
9: Swiss CPA	48 minutes	Long experience in auditing; Newly engaged in IT-related audits on ISA 315; Some blockchain experience;
10: CISA	61 minutes	Very experienced in auditing with a special focus on IT audits; some blockchain knowledge;
11: German CPA	62 minutes	Very experienced in IT auditing; Teaching audit classes; Long experience with blockchains;
12: Austrian CPA	68 minutes	Good experience in auditing; Some experience with blockchain-based auditing;
13: US CPA	65 minutes	Very deep experience in IT-related audits; Some experience with blockchains; Involved in software development of ACL;
14: ACCA	67 minutes	Very deep experience in IT-related audits Some experience with blockchains;
15: CISA	64 minutes	Highly experienced in IT-related audits; Teaching auditing classes; Good experience with blockchains;
16: German CPA	68 minutes	Highly experienced in IT-related audits; Some experience with blockchains;
17: CIA	64 minutes	Highly experienced in IT-related audits; Some experience with blockchains;

18: CISA	57 minutes	Good experience in IT-related audits; Good experience with blockchains;
19: German CPA	68 minutes	Highly experienced in IT-related audits; Some experience with blockchains;
20: German CPA	62 minutes	Highly experienced in IT auditing and consulting; Good experience with blockchains; Teaching audit classes;
21: ISO 27001 Lead Auditor	52 minutes	Good experience in IT-related audits; Some experience with blockchains;
22: CISA	72 minutes	Highly experienced in IT-related audits; Long experience with blockchains; Motivator of implementing digital auditing in its public accounting firms;

Note: Data collected by the author in November 2022

Table A4

Demographics on Affiliation to the Researcher, Age, and Gender

Number	Affiliation to the Researcher	Age	Gender
1: ISO 27001 Lead Auditor	Former colleague	36-45	Male
2: German CPA	Business Partner	56+	Male
3: German CPA	Business Partner	56+	Male
4: CISA	Former colleague	36-45	Male
5: ITIL Professional	Former colleague	46-55	Male
6: CISA	Business Partner	36-45	Male
7: ACCA	Recommendation Group	36-45	Male
8: US CPA	Recommendation Group	46-55	Male
9: Swiss CPA	Recommendation Group	36-45	Female
10: CISA	Former colleague	36-45	Male
11: German CPA	Business Partner	36-45	Male
12: Austrian CPA	Recommendation Group	36-45	Female
13: US CPA	Recommendation Group	36-45	Male
14: ACCA	Recommendation Group	46-55	Female
15: CISA	Business Partner	46-55	Male
16: German CPA	Business Partner	56+	Male
17: CIA	Former customer	36-45	Female

18: CISA	Former colleague	26-35	Female
19: German CPA	Former colleague	56+	Male
20: German CPA	Business partner	46-55	Male
21: ISO 27001 Lead Auditor	Business partner	26-35	Female
22: CISA	Business partner	36-45	Male

Note: Data collected by the author in November 2022

Table A5

Demographics on Education, Experience with Blockchains, and Audit

Number	Education	Blockchain Experience	Experience with Auditing
1: ISO 27001 Lead Auditor	Prefer not to say	0-2 years	9 to 11 years
2: German CPA	Master´s Degree	0-2 years	9 to 11 years
3: German CPA	Master´s Degree	0-2 years	9 to 11 years
4: CISA	Master´s Degree	3 to 5 years	15+ years
5: ITIL Professional	Master´s Degree	6 to 8 years	15+ years
6: CISA	Master´s Degree	3 to 5 years	15+ years
7: ACCA	Ph.D.	3 to 5 years	9 to 11 years
8: US CPA	Master´s Degree	3 to 5 years	15+ years
9: Swiss CPA	Master´s Degree	0-2 years	9 to 11 years
10: CISA	Master´s Degree	3 to 5 years	9 to 11 years
11: German CPA	Master´s Degree	3 to 5 years	15+ years
12: Austrian CPA	Master´s Degree	0-2 years	9 to 11 years
13: US CPA	Master´s Degree	3 to 5 years	15+ years
14: ACCA	Master´s Degree	0-2 years	9 to 11 years
15: CISA	Master´s Degree	3 to 5 years	15+ years
16: German CPA	Master´s Degree	0-2 years	15+ years

17: CIA	Bachelor´s Degree	0-2 years	15+ years
18: CISA	Bachelor´s Degree	3 to 5 years	9 to 11 years
19: German CPA	Ph.D.	3 to 5 years	15+ years
20: German CPA	Master´s Degree	3 to 5 years	15+ years
21: ISO 27001 Lead Auditor	Bachelor´s Degree	0-2 years	6 to 8 years
22: CISA	Master´s Degree	3 to 5 years	15+ years

Note: Data collected by the author in November 2022

Table A6

Demographics on Office Location, Country of Origin, Firm Size, and Current Job Level

Number	Office Location	Country of Origin	Firm Size	Current Job Level
1: ISO 27001 Lead Auditor	Bad Kötzting	Germany	51 to 200	Owner / Executive
2: German CPA	Munich	Germany	more than 5001	Owner / Executive
3: German CPA	Cologne	Germany	1 to 10	Owner / Executive
4: CISA	Dusseldorf	Germany	1,001 to 5,000	Senior Management
5: ITIL Professional	Cologne	Germany	51 to 200	Senior Management
6: CISA	Dusseldorf	Germany	1,001 to 5,000	Senior Management
7: ACCA	Bristol	UK	51 to 200	Middle Management
8: US CPA	Saint Louis	USA	1 to 10	Owner / Executive
9: Swiss CPA	Zurich	CH	51 to 200	Middle Management
10: CISA	Nuremberg	Germany	1,001 to 5,000	Senior Management
11: German CPA	Bensberg	Germany	51 to 200	Owner / Executive
12: Austrian CPA	Vienna	Austria	11 to 50	Middle Management

13: US CPA	Chicago	USA	51 to 200	Senior Management
14: ACCA	Prague	Czech Republic	11 to 50	Middle Management
15: CISA	Frankfurt	Germany	51 to 200	Owner / Executive
16: German CPA	Cologne	Germany	51 to 200	Owner / Executive
17: CIA	Munich	Germany	51 to 200	Senior Management
18: CISA	Hamburg	Germany	201 to 999	Middle Management
19: German CPA	Munich	Germany	51 to 200	Owner / Executive
20: German CPA	Frankfurt	Germany	51 to 200	Owner / Executive
21: ISO 27001 Lead Auditor	Hamburg	Germany	more than 5001	Middle Management
22: CISA	Dusseldorf	Germany	1,001 to 5,000	Senior Management

Note: Data collected by the author in November 2022

Table A7

Traditional versus Blockchain-based Auditing toward AU-C 505

Traditional versus blockchain-based Auditing toward AU-C 505		
	Traditional procedures under AU-C 505	**Blockchain-based Auditing**
Procedures to obtain Audit Evidence AU-C 505.02		
Higher reliability of audit evidence obtained from external sources, by the auditor directly, and in written or electronic form	Auditors request external confirmations from third-party as audit evidence.	Audit evidence in consortium blockchains is available electronically, while auditors have direct and permanent access to the blockchain data. Auditors extract data from blockchains to obtain audit evidence and perform analytical procedures with smart audit procedures. **Result** Procedures to perform audits by blockchains with smart audit procedures do not address external confirmations.
Importance of external confirmations AU-C 505.02		
Reference on AU-C 330	AU-C 330 contains regulations for the auditor's reliability to design and implement audit procedures to obtain external confirmations to address risks of material misstatement of financial statements.	Smart audit procedures perform permanent audit procedures in real-time on blockchains. Additionally, auditors evaluate the consensus mechanisms of blockchains, the blockchain code, and access to blockchain nodes. Smart audit procedures do not require external confirmations. **Result** AU-C 330 needs to provide adequate guidance for blockchain-based auditing.
Reference on AU-C 240	AU-C 240 contains regulations to design and implement audit procedures to address fraud risks in financial statements (AICPA, 2012a).	Adequately designed and controlled blockchain systems face almost no fraud risk toward financial statements.

		Result Regulation by AU-C 240 towards accounting fraud generally is not relevant for blockchain-based auditing.
Reference on AU-C 500A	According to AU-C 500A, corroborating information from third-party contributes to a higher assurance of audit evidence obtained by the auditors.	Audit evidence obtained from an adequately designed and controlled blockchain system provides high assurance. **Result** AU-C 500A is irrelevant in blockchains, as evidence from blockchains generally provides a high level of assurance.
Objective of AU-C 505		
AU-C 505.05	AU-C 505.05 contains no regulations for designing and implementing blockchain-based audit procedures to obtain adequate and relevant audit evidence.	The design and implementation of continuous audit procedures differ from traditional substantive audit procedures. **Result** AU-C 505.05 contains no regulations for designing and implementing blockchain-based auditing procedures with smart audit tools.
Definitions of AU-C 505		
AU-C 505.06	The definition section of AU-C 505.06 defines audit procedures and behavior as requests for positive (the answer is required) or negative (the answer is required in case of deviations) confirmation requests, the nature of external confirmations, and the meaning of exceptions and non-responses.	Definitions for blockchain-based smart audit procedures are not provided under AU-C 505. **Result** AU-C 505.06 contains no definitions for blockchain-based auditing.
External Confirmation Procedures		
AU-C 505.07	AU-C 505.07 regulates procedures to obtain external confirmations:	Procedures to obtain third-party confirmations of supplier firms are irrelevant for blockchain-based auditing.

	▪ Determination of information to be requested and confirmed ▪ Selection of appropriate supplier firms ▪ Design of appropriate confirmation requests under the auditor´s control ▪ Sending of requests to obtain third-party confirmations	**Result** AU-C 505.07 contains no regulations for blockchain-based auditing procedures to evaluate accounts receivable AU-C 505.07.
Management's refusal to perform external confirmation procedures by auditors		
AU-C 505.08 - 09	AU-C 505.08-09 regulates procedures in case auditees' management refuses external confirmation procedures: ▪ Inquiry of management for reasons for to decline ▪ Evaluation for implications of the refusal of the audit ▪ Performing alternative audit procedures ▪ Information of those charged with governance, whether the refusal is unreasonable or alternative audit procedures lack reliable evidence.	Management's refusal to perform external confirmation procedures is irrelevant to blockchain-based auditing. In a consortium blockchain, auditors get access to all accounting-relevant data of the auditees and their customers. **Result** AU-C 505.08-09 is not relevant for blockchain-based auditing in consortium blockchains.
Evaluation of third-party confirmation procedures		
Reliability of the Responses to the Requests for Confirmation **AU-C 505.10 - 11**	In case of doubts about the evidence obtained, according to AU-C 505.10 - 11, auditors must gather further evidence and evaluate implications on relevant risks towards financial statements.	Rules for continuous auditing, the extraction of data from blockchains and their evaluation as required by blockchains are not addressed under AU-C 505.10-16. **Result** AU-C 505.10-11 contains no regulations for evaluating audit evidence obtained from blockchains.

Nonresponses and oral responses AU-C 505.12	In non-responses or oral responses, the auditor must perform alternative audit procedures according to AU-C 505.12.	External confirmations or responses on audit procedures are not relevant in an appropriate blockchain system. Rules for additional audit procedures are obsolete in blockchains. **Result** Regulations of AU-C 505.12 concerning non-responses and oral responses are inappropriate for blockchains-based auditing.
Necessity of positive confirmations AU-C 505.13 - 14	If positive confirmations are required, according to AU-C 505.13-14, sole alternative audit procedures are insufficient. Auditors must evaluate the lack of evidence in the audit opinion. Exceptions must be evaluated if they are identified as misstatements.	Auditors have access to all information of blockchain systems, thus all required audit evidence is available. Rules for the evaluation of missing evidence require updates. Exceptions as misstatements must be researched as well. **Result** AU-C 505.13-14 contains no rules for blockchain-based auditing related to AU-C 505.13-14.
Negative Confirmations AU-C 505.15	According to AU-C 505.15 negative third-party confirmations provide less pervasive audit evidence than positive confirmations. Auditors can use them, if risks of misstatements are low, populations are homogeneous by small balances, exception rates are low, and recipients will not disregard requests.	Auditors of the blockchain have permanent access to the accounting data. In a blockchain system, third-party confirmations are obsolete. **Result** AU-C 505 contains no regulations for blockchain-based auditing related to AU-C 505.15.
Evaluation of Evidence obtained by the auditor AU-C 505.16	According to AU-C 505.16, auditors must evaluate whether evidence from external confirmation procedures provides relevant	Due to the nature of the blockchain mechanisms, evidence obtained from blockchains provides relevant and reliable audit evidence.

	and reliable audit evidence or whether further audit procedures are necessary.	**Result** AU-C 505 contains no regulations for blockchain-based auditing related to AU-C 505.16.

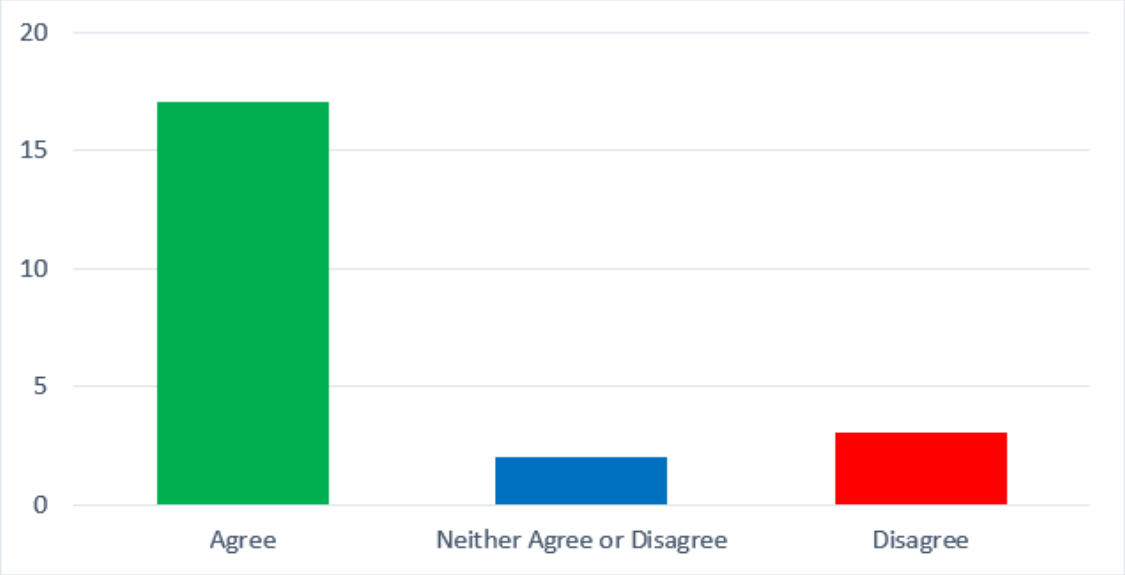
Note: Comparison of traditional auditing of accounts receivable under AU-C 505 by AICPA, 2012b compared with requirements of blockchain-based auditing as outlined by the author

Appendix B - Figures

After completing the questionnaire, the author requested the respondents to provide a brief statement on the individual questions. Their statements are presented in summary form in the following 13 figures.

Figure B1

Blockchain Features relevant for Auditing

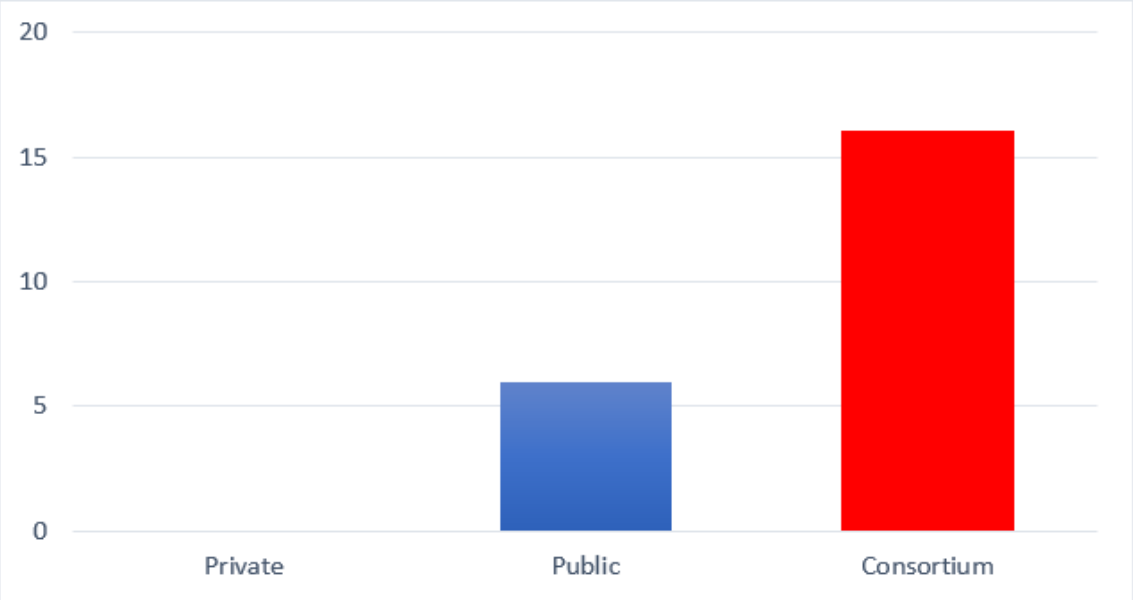


Answer Choices	Responses
Agree	17
Neither Agree or Disagree	2
Disagree	3
TOTAL	**22**

Note: Data collected by the author in November 2022

Figure B2

Most suitable Blockchain Type for Auditing

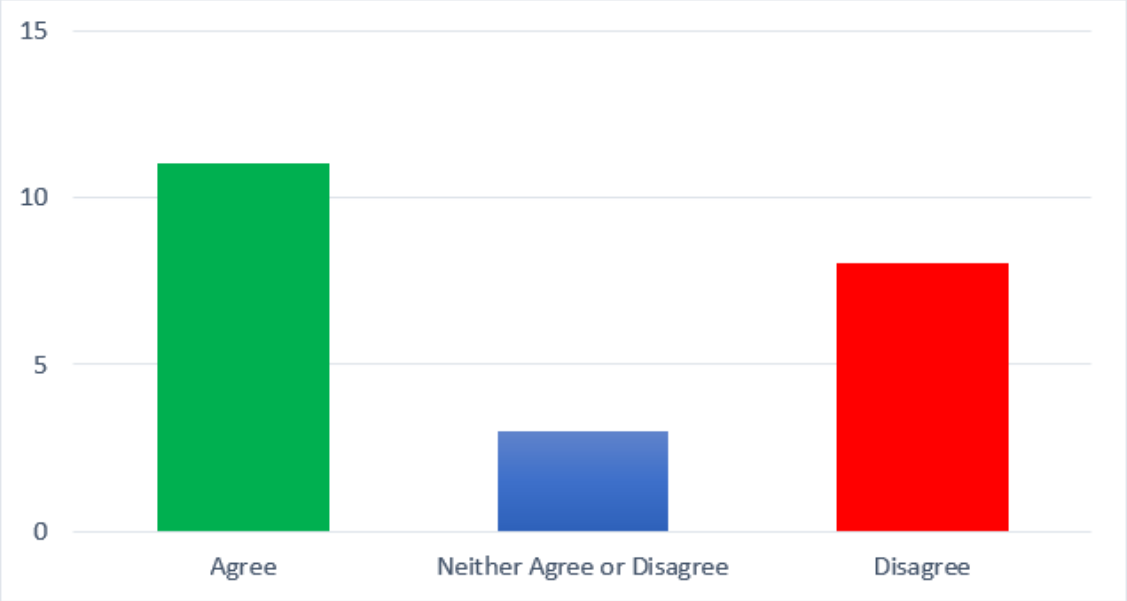


Answer Choices	Responses
Private	0
Public	6
Consortium	16
TOTAL	**22**

Note: Data collected by the author in November 2022

Figure B3

Higher Security of Blockchains against ERP-Systems

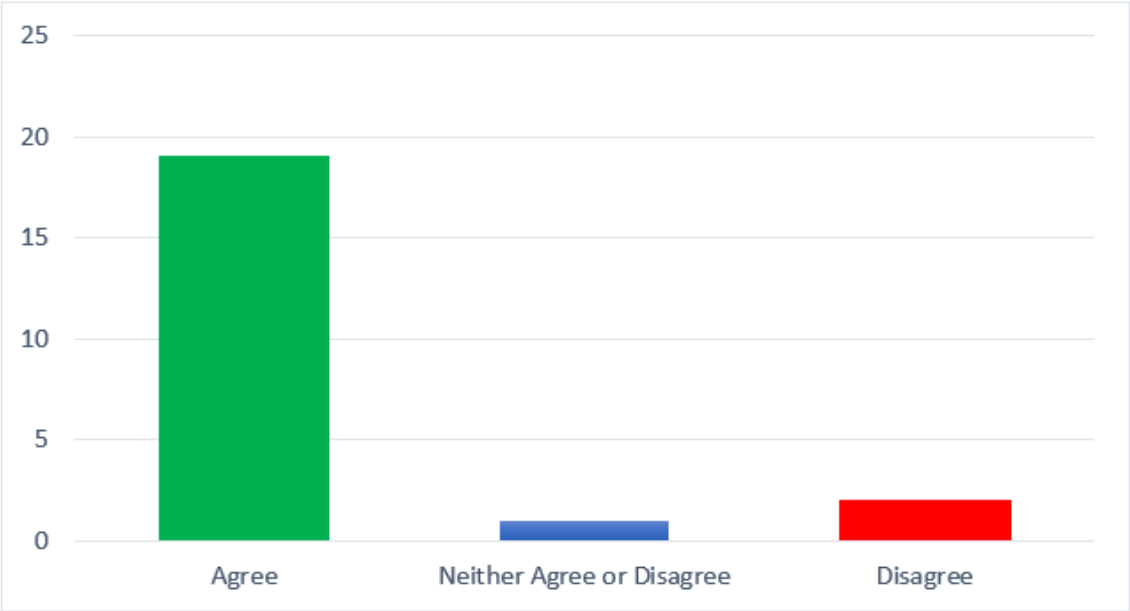


Answer Choices	Responses
Agree	11
Neither Agree or Disagree	3
Disagree	8
TOTAL	**22**

Note: Data collected by the author in November 2022

Figure B4

Need for User Access Management on Blockchains

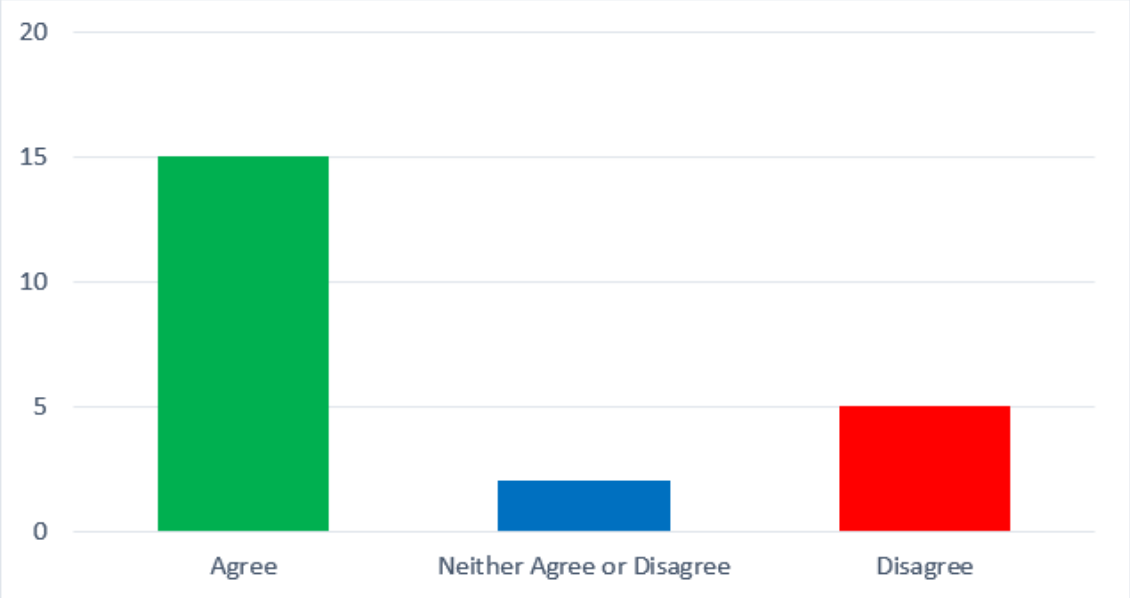


Answer Choices	Responses
Agree	19
Neither Agree or Disagree	1
Disagree	2
TOTAL	**22**

Note: Data collected by the author in November 2022

Figure B5

Adequate Blockchain Architecture enables Auditing and Interoperability among other Blockchains and ERP Systems

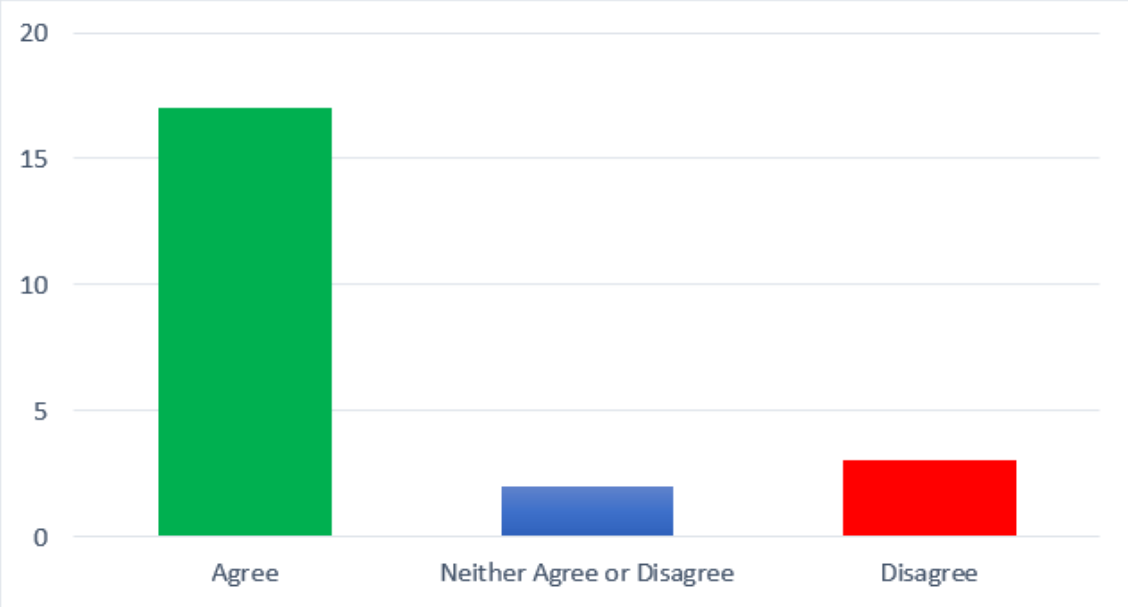


Answer Choices	Responses
Agree	15
Neither Agree or Disagree	2
Disagree	5
TOTAL	**22**

Note: Data collected by the author in November 2022

Figure B6

Weaknesses of Traditional Auditing

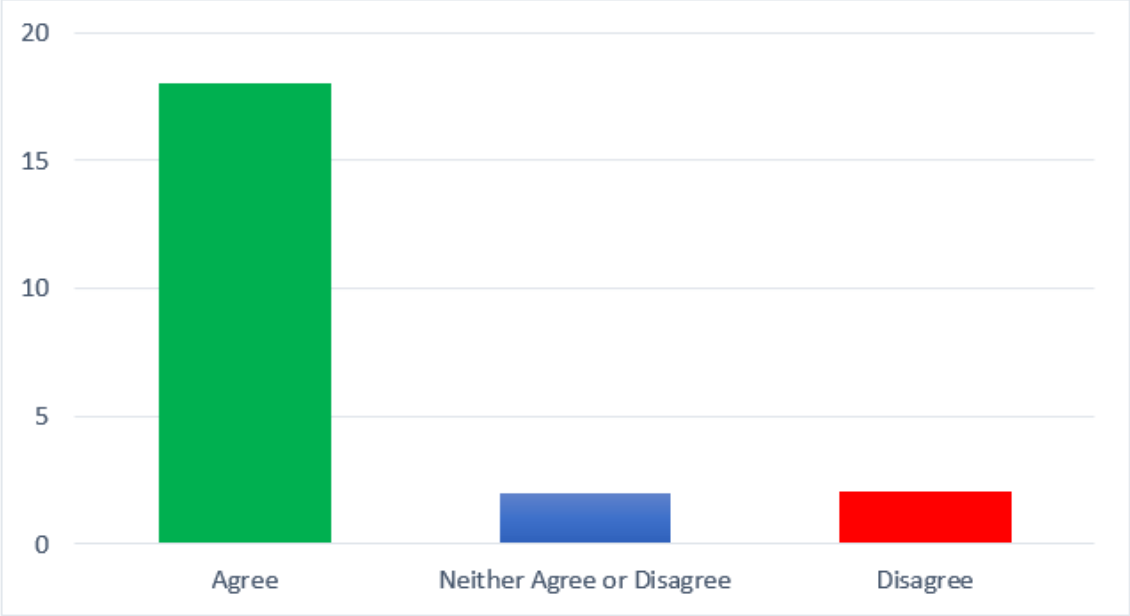


Answer Choices	Responses
Agree	17
Neither Agree or Disagree	2
Disagree	3
TOTAL	**22**

Note: Data collected by the author in November 2022

Figure B7

Blockchains Require External Auditing

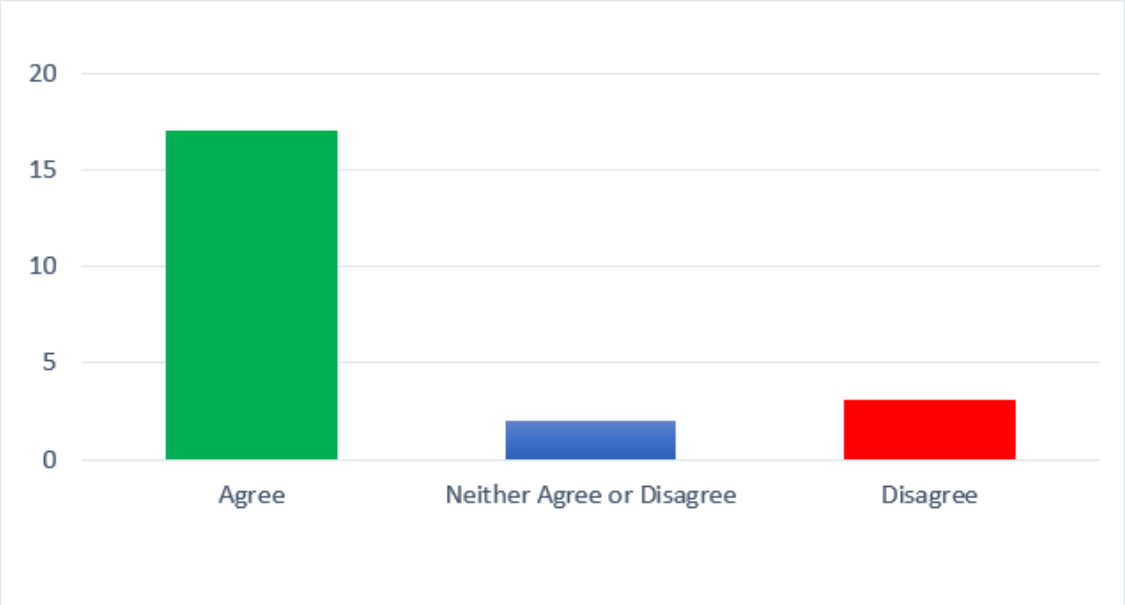


Answer Choices	Responses
Agree	18
Neither Agree or Disagree	2
Disagree	2
TOTAL	**22**

Note: Data collected by the author in November 2022

Figure B8

Smart Audit Procedures are Superior to Traditional Auditing

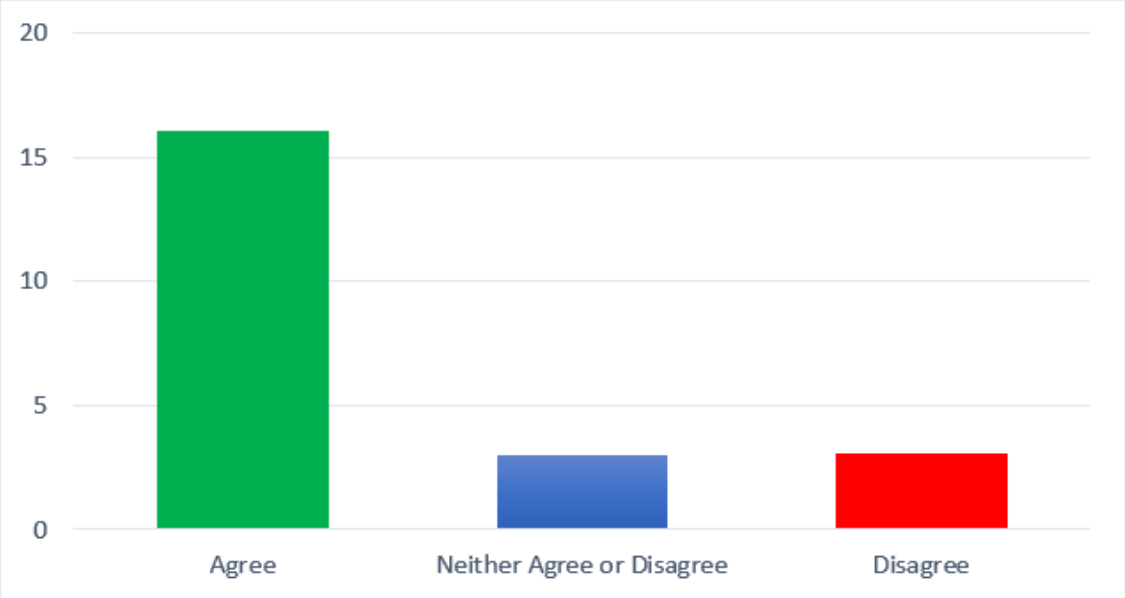


Answer Choices	Responses
Agree	17
Neither Agree or Disagree	2
Disagree	3
TOTAL	**22**

Note: Data collected by the author in November 2022

Figure B9

Auditing of Internal Controls by Smart Audit Procedures

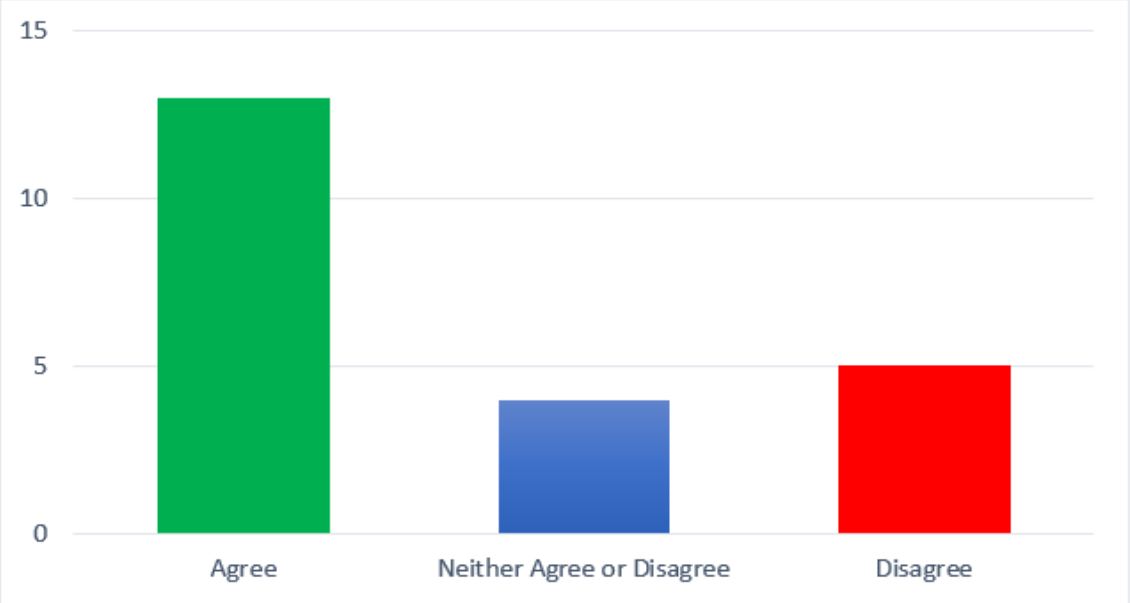


Answer Choices	Responses
Agree	16
Neither Agree or Disagree	3
Disagree	3
TOTAL	**22**

Note: Data collected by the author in November 2022

Figure B10

Smart Audit Procedures Require additional Audits on Blockchain Code, Mechanisms, and Access Controls

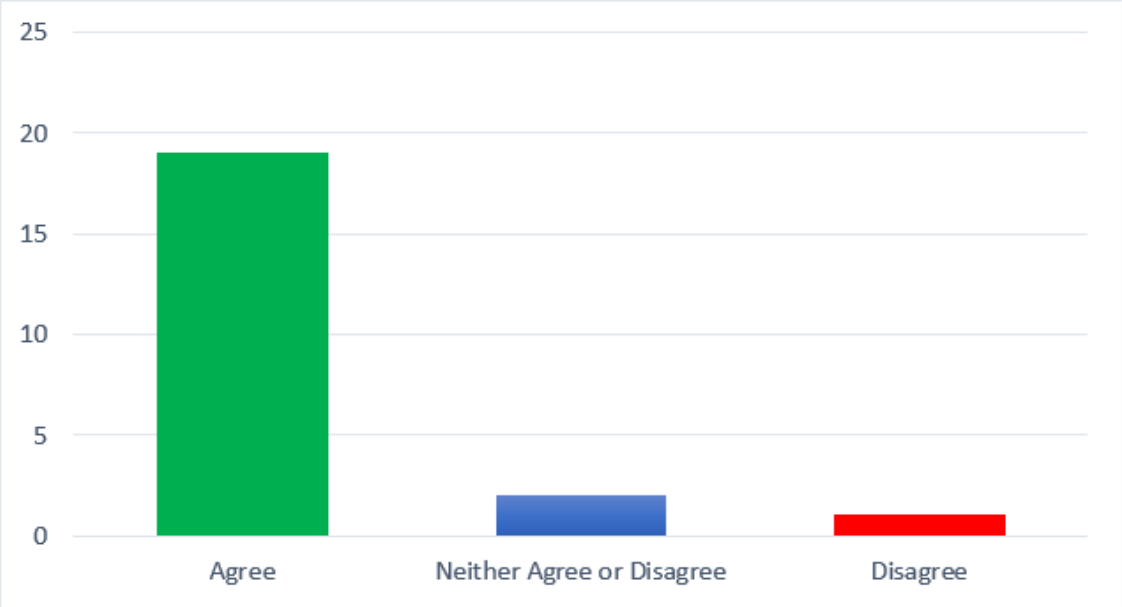


Answer Choices	Responses
Agree	13
Neither Agree or Disagree	4
Disagree	5
TOTAL	**22**

Note: Data collected by the author in November 2022

Figure B11

High Impact of Blockchains on Audit Profession and Role of Auditors

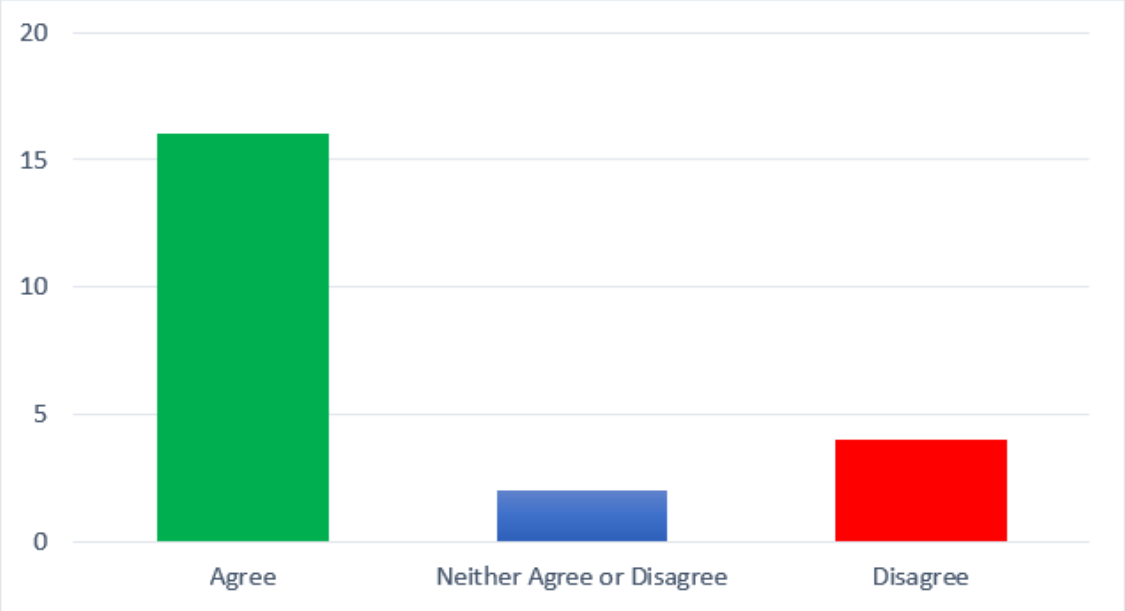


Answer Choices	Responses
Agree	19
Neither Agree or Disagree	2
Disagree	1
TOTAL	**22**

Note: Data collected by the author in November 2022

Figure B12

Blockchains Render Requests for External Confirmations Obsolete

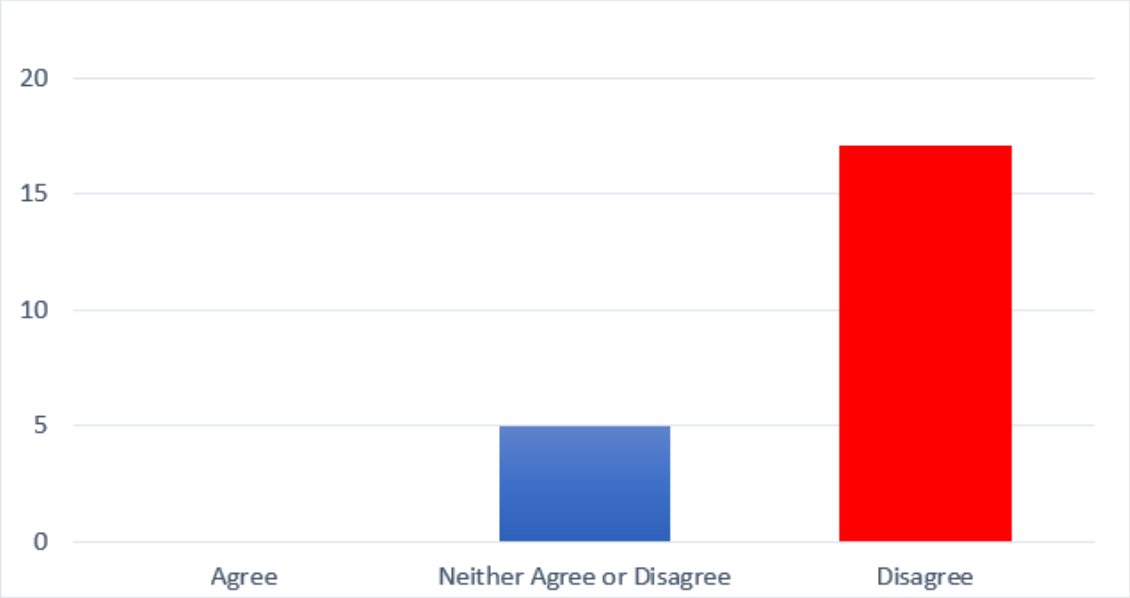


Answer Choices	Responses
Agree	16
Neither Agree or Disagree	2
Disagree	4
TOTAL	**22**

Note: Data collected by the author in November 2022

Figure B13

Compliance of Blockchain-based Auditing with AU-C 505



Answer Choices	Responses
Agree	0
Neither Agree or Disagree	5
Disagree	17
TOTAL	**22**

Note: Data collected by the author in November 2022

Appendix C - Audit Standards

Appendix C contains literal reproductions of the AICPA auditing standards "AU Section 150 General Accepted Auditing Standards (GAAS) and "AU-C Section 505 External Confirmations". AU Section 150 forms the theoretical framework of the doctoral thesis. AU-C Section 505 regulates procedures to obtain external confirmations among others when auditing accounts receivable. AU-C Section 505 is of importance as the doctoral thesis revealed a compliance and literature gap toward AU-C Section 505 when auditing accounts receivable with blockchains.

I. AU Section 150 General Accepted Auditing Standards

"(Supersedes SAS No. 1, section 150.)

Source: SAS No. 95; SAS No. 98; SAS No. 102; SAS No. 105; SAS No. 113.

Effective for audits of financial statements for periods beginning on or after December 15, 2001, unless otherwise indicated.

.01 An independent auditor plans, conducts, and reports the results of an audit in accordance with generally accepted auditing standards. Auditing standards provide a measure of audit quality and the objectives to be achieved in an audit. Auditing procedures differ from auditing standards. Auditing procedures are acts that the auditor performs during the course of an audit to comply with auditing standards.

Auditing Standards

.02 The general, field work, and reporting standards (the 10 standards) approved and adopted by the membership of the AICPA, as amended by the AICPA Auditing Standards Board (ASB), are as follows:

General Standards

1. The auditor must have adequate technical training and proficiency to perform the audit.

2. The auditor must maintain independence in mental attitude in all matters relating to the audit.

3. The auditor must exercise due professional care in the performance of the audit and the preparation of the report.

Standards of Field Work

1. The auditor must adequately plan the work and must properly supervise any assistants.

2. The auditor must obtain a sufficient understanding of the entity and its environment, including its internal control, to assess the risk of material misstatement of the financial statements whether due to error or fraud, and to design the nature, timing, and extent of further audit procedures.

3. The auditor must obtain sufficient appropriate[1] audit evidence by performing audit procedures to afford a reasonable basis for an opinion regarding the financial statements under audit

---

[1] See paragraph .06 of section 326, Audit Evidence, for the definition of the term appropriate. [Footnote added, effective for audits of financial statements for periods beginning on or after December 15, 2006, by Statement on Auditing Standards (SAS) No. 105.]

Standards of Reporting[2]

1 The auditor must state in the auditor's report whether the financial statements are presented in accordance with generally accepted accounting principles.[3]

2. The auditor must identify in the auditor's report those circumstances in which such principles have not been consistently observed in the current period in relation to the preceding period.

3. When the auditor determines that informative disclosures are not reasonably adequate, the auditor must state in the auditor's report.

4. The auditor must either express an opinion regarding the financial statements, taken as a whole, or state that an opinion cannot be expressed, in the auditor's report. When the auditor cannot express an overall opinion, the auditor should state the reasons therefor in the auditor's report. In all cases where an auditor's name is associated with financial statements, the auditor should clearly indicate the character of the auditor's work, if any, and the degree of responsibility the auditor is taking, in the auditor's report.

[As amended, effective for audits of financial statements for periods beginning on or after December 15, 2006, by Statement on Auditing Standards (SAS) No. 105. As amended, effective for audits of financial statements for periods beginning on or after December 15, 2006, by SAS No. 113.]

---

[2] The reporting standards apply only when the auditor issues a report. [Footnote added, effective for audits of financial statements for periods beginning on or after December 15, 2006, by SAS No. 113.]

[3] When an auditor reports on financial statements prepared in accordance with a comprehensive basis of accounting other than generally accepted accounting principles (GAAP), the first standard of reporting is satisfied by stating in the auditor's report that the basis of presentation is a comprehensive basis of accounting other than GAAP and by expressing an opinion (or disclaiming an opinion) on whether the financial statements are presented in conformity with the comprehensive basis of accounting used. [Footnote added, effective for audits of financial statements for periods beginning on or after December 15, 2006, by SAS No. 113.]

.03 Rule 202, Compliance With Standards, of the AICPA Code of Professional Conduct [ET section 202.01], requires an AICPA member who performs an audit (the auditor) to comply with standards promulgated by the ASB.[4] The ASB develops and issues standards in the form of SASs through a due process that includes deliberation in meetings open to the public, public exposure of proposed SASs, and a formal vote. The SASs are codified within the framework of the 10 standards.

.**04** The nature of the ten standards and the SASs requires the auditor to exercise professional judgment in applying them. Materiality and audit risk also underlie the application of the ten standards and the SASs, particularly those related to field work and reporting.[5] When, in rare circumstances, the auditor departs from a presumptively mandatory requirement, the auditor must document in the working papers his or her justification for the departure and how the alternative procedures performed in the circumstances were sufficient to achieve the objectives of the presumptively mandatory requirement. [As amended, effective December 2005, by SAS No. 102. As amended, effective for audits of financial statements for periods beginning on or after December 15, 2006, by SAS No. 113.]

Interpretive Publications

05 *Interpretive publications* consist of auditing interpretations of the SASs, appendixes to the SASs,[6] auditing guidance included in AICPA Audit and Accounting

---

[4] In certain engagements, the auditor also may be subject to other auditing requirements, such as Government Auditing Standards issued by the comptroller general of the United States, or rules and regulations promulgated by the U.S. Securities and Exchange Commission. [Footnote renumbered by the issuance of SAS No. 105, March 2006. Footnote subsequently renumbered by the issuance of SAS No. 113, November 2006.]

[5] See section 312, Audit Risk and Materiality in Conducting an Audit. [Footnote renumbered by the issuance of SAS No. 105, March 2006. Footnote subsequently renumbered by the issuance of SAS No. 113, November 2006.]

[6] Appendixes to SASs referred to in paragraph .05 of this section do not include previously issued appendixes to original pronouncements that when adopted modified other SASs. [Footnote added, effective September 2002, by SAS No. 98. Footnote renumbered by the issuance of SAS No. 105, March 2006. Footnote subsequently renumbered by the issuance of SAS No. 113, November 2006.]

Guides, and AICPA auditing Statements of Position.[7] Interpretive publications are not auditing standards. Interpretive publications are recommendations on the application of the SASs in specific circumstances, including engagements for entities in specialized industries. An interpretive publication is issued under the authority of the ASB after all ASB members have been provided an opportunity to consider and comment on whether the proposed interpretive publication is consistent with the SASs. [As amended, effective September 2002, by SAS No. 98.]

.06 The auditor should be aware of and consider interpretive publications applicable to his or her audit. If the auditor does not apply the auditing guidance included in an applicable interpretive publication, the auditor should be prepared to explain how he or she complied with the SAS provisions addressed by such auditing guidance

Other Auditing Publications

.07 Other auditing publications include AICPA auditing publications not referred to previously; auditing articles in the Journal of Accountancy and other professional journals; auditing articles in the AICPA CPA Letter; continuing professional education programs and other instruction materials, textbooks, guide books, audit programs, and checklists; and other auditing publications from state CPA societies, other organizations, and individuals.[8] Other auditing publications have no authoritative status; however, they may help the auditor understand and apply the SASs.

.08 If an auditor applies the auditing guidance included in another auditing publication, he or she should be satisfied that, in his or her judgment, it is both relevant to the circumstances of the audit, and appropriate. In determining whether another

---

[7] Auditing interpretations of the SASs are included in the codified version of the SASs. AICPA Audit and Accounting Guides and auditing Statements of Position are listed in appendix D. [Footnote renumbered by the issuance of SAS No. 98, September 2002. Footnote subsequently renumbered by the issuance of SAS No. 105, March 2006. Footnote subsequently renumbered by the issuance of SAS No. 113, November 2006.]

[8] The auditor is not expected to be aware of the full body of other auditing publications. [Footnote renumbered by the issuance of SAS No. 98, September 2002. Footnote subsequently renumbered by the issuance of SAS No. 105, March 2006. Footnote subsequently renumbered by the issuance of SAS No. 113, November 2006.]

auditing publication is appropriate, the auditor may wish to consider the degree to which the publication is recognized as being helpful in understanding and applying the SASs and the degree to which the issuer or author is recognized as an authority in auditing matters. Other auditing. Other auditing publications include AICPA auditing publications not referred to previously; auditing articles in the Journal of Accountancy and other professional journals; auditing articles in the AICPA CPA Letter; continuing professional education programs and other instruction materials, textbooks, guide books, audit programs, and checklists; and other auditing publications from state CPA societies, other organizations, and individuals. Other auditing publications have no authoritative status; however, they may help the auditor understand and apply the SASs.

Effective Date

.09 This section is effective for audits of financial statements for periods beginning on or after December 15, 2001 (AICPA, 2001).”

II. AU-C Section 505 External Confirmations

“Source: SAS No. 122.

Effective for audits of financial statements for periods ending on or after December 15, 2012.

Introduction

Scope of This Section

.01 This section addresses the auditor's use of external confirmation procedures to obtain audit evidence, in accordance with the requirements of section 330, Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained, and section 500A, Audit Evidence. It does not address inquiries regarding litigation, claims, and assessments, which are addressed in section 501A, Audit Evidence—Specific Considerations for Selected Items.

External Confirmation Procedures to Obtain Audit Evidence

.02 Section 500A indicates that the reliability of audit evidence is influenced by its source and nature and is dependent on the individual circumstances under which it is obtained.[9] Section 500A also includes the following generalizations applicable to audit evidence:[10]

- Audit evidence is more reliable when it is obtained from independent sources outside the entity.
- Audit evidence obtained directly by the auditor is more reliable than audit evidence obtained indirectly or by inference.
- Audit evidence is more reliable when it exists in documentary form, whether paper, electronic, or other medium.

---

[9] Paragraph .A5 of section 500A, Audit Evidence.

[10] Paragraph .A32 of section 500A.

Accordingly, depending on the circumstances of the audit, audit evidence in the form of external confirmations received directly by the auditor from confirming parties may be more reliable than evidence generated internally by the entity. This section is intended to assist the auditor in designing and performing external confirmation procedures to obtain relevant and reliable audit evidence.

.03 Other AU-C sections recognize the importance of external confirmations as audit evidence; for example

- section 330 discusses the auditor's responsibility (a) to design and implement overall responses to address the assessed risks of material misstatement at the financial statement level and (b) to design and perform further audit procedures whose nature, timing, and extent are based on, and are responsive to, the assessed risks of material misstatement at the relevant assertion level. [11] In addition, section 330 requires that, irrespective of the assessed risks of material misstatement, the auditor design and perform substantive procedures for all relevant assertions related to each material class of transactions, account balance, and disclosure. [12] The auditor is required to consider whether external confirmation procedures are to be performed as substantive audit procedures and is required to use external confirmation procedures for accounts receivable unless

  — the overall account balance is immaterial,

  — external confirmation procedures would be ineffective, or

---

[11] Paragraphs .05–.06 of section 330, Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained.

[12] Paragraph .18 of section 330.

— the auditor's assessed level of risk of material misstatement at the relevant assertion level is low, and the other planned substantive procedures address the assessed risk.[13]

- section 330 requires that the auditor obtain more persuasive audit evidence the higher the auditor's assessment of risk.[14] To do this, the auditor may increase the quantity of the evidence or obtain evidence that is more relevant or reliable, or both. For example, the auditor may place more emphasis on obtaining evidence directly from third parties or obtaining corroborating evidence from a number of independent sources. Section 330 also indicates that external confirmation procedures may assist the auditor in obtaining audit evidence with the high level of reliability that the auditor requires to respond to significant risks of material misstatement, whether due to fraud or error.[15]
- section 240, Consideration of Fraud in a Financial Statement Audit, indicates that the auditor may design confirmation requests to obtain additional corroborative information as a response to address the assessed risks of material misstatement due to fraud at the assertion level.[16]
- section 500A indicates that corroborating information obtained from a source independent of the entity (such as external confirmations) may increase the assurance the auditor obtains from evidence existing within the accounting records or representations made by management.[17]

Effective Date

.04 This section is effective for audits of financial statements for periods ending on or after December 15, 2012.

---

[13] Paragraphs .19–.20 of section 330.
[14] Paragraph .07b of section 330.
[15] Paragraph .A58 of section 330
[16] Paragraph .A43 of section 240, Consideration of Fraud in a Financial Statement Audit.
[17] Paragraph .A8 of section 500A.

Objective

.05 The objective of the auditor, when using external confirmation procedures, is to design and perform such procedures to obtain relevant and reliable audit evidence.

Definitions

.06 For purposes of generally accepted auditing standards, the following terms have the meanings attributed as follows:

Exception. A response that indicates a difference between information requested to be confirmed, or contained in the entity's records, and information provided by the confirming party.

External confirmation. Audit evidence obtained as a direct written response to the auditor from a third party (the confirming party), either in paper form or by electronic or other medium (for example, through the auditor's direct access to information held by a third party). (Ref: par. .A1)

Negative confirmation request. A request that the confirming party respond directly to the auditor only if the confirming party disagrees with the information provided in the request.

Nonresponse. A failure of the confirming party to respond, or fully respond, to a positive confirmation request or a confirmation request returned undelivered.

Positive confirmation request. A request that the confirming party respond directly to the auditor by providing the requested information or indicating whether the confirming party agrees or disagrees with the information in the request.

Requirements

External Confirmation Procedures

.07 When using external confirmation procedures, the auditor should maintain control over external confirmation requests, including

a. determining the information to be confirmed or requested; (Ref: par. .A2)

b. selecting the appropriate confirming party; (Ref: par. .A3)

c. designing the confirmation requests, including determining that requests are properly directed to the appropriate confirming party and provide for being responded to directly to the auditor; and (Ref: par. .A4–.A7)

d. sending the requests, including follow-up requests, when applicable, to the confirming party. (Ref: par. .A8)

Management's Refusal to Allow the Auditor to Perform External Confirmation Procedures

.08 If management refuses to allow the auditor to perform external confirmation procedures, the auditor should

a. inquire about management's reasons for the refusal and seek audit evidence about their validity and reasonableness; (Ref: par. .A9)

b. evaluate the implications of management's refusal on the auditor's assessment of the relevant risks of material misstatement, including the risk of fraud, and on the nature, timing, and extent of other audit procedures; and (Ref: par. .A10)

c. perform alternative audit procedures designed to obtain relevant and reliable audit evidence. (Ref: par. .A11)

.09 If the auditor concludes that management's refusal to allow the auditor to perform external confirmation procedures is unreasonable or the auditor is unable to

obtain relevant and reliable audit evidence from alternative audit procedures, the auditor should communicate with those charged with governance, in accordance with section 260, The Auditor's Communication With Those Charged With Governance.[18] The auditor also should determine the implications for the audit and the auditor's opinion, in accordance with section 705, Modifications to the Opinion in the Independent Auditor's Report.

Results of the External Confirmation Procedures

Reliability of Responses to Confirmation Requests

.10 If the auditor identifies factors that give rise to doubts about the reliability of the response to a confirmation request, the auditor should obtain further audit evidence to resolve those doubts. (Ref: par. .A12–.A22)

.11 If the auditor determines that a response to a confirmation request is not reliable, the auditor should evaluate the implications on the assessment of the relevant risks of material misstatement, including the risk of fraud, and on the related nature, timing, and extent of other audit procedures. (Ref: par. .A23)

Nonresponses and Oral Responses

.**12** In the case of each nonresponse, the auditor should perform alternative audit procedures to obtain relevant and reliable audit evidence. (Ref: par. .A24– .A27)

When a Written Response to a Positive Confirmation Request Is Necessary to Obtain Sufficient Appropriate Audit Evidence

.13 If the auditor has determined that a written response to a positive confirmation request is necessary to obtain sufficient appropriate audit evidence, alternative audit procedures will not provide the audit evidence the auditor requires. If the auditor does not

---

[18] Paragraph .12 of section 260, The Auditor's Communication With Those Charged With Governance

obtain such confirmation, the auditor should determine the implications for the audit and the auditor's opinion, in accordance with section 705. (Ref: par. .A28–.A29)

Exceptions

.14 The auditor should investigate exceptions to determine whether they are indicative of misstatements. (Ref: par. .A30–.A31

Negative Confirmations

.15 Negative confirmations provide less persuasive audit evidence than positive confirmations. Accordingly, the auditor should not use negative confirmation requests as the sole substantive audit procedure to address an assessed risk of material misstatement at the assertion level, unless all of the following are present:

a. The auditor has assessed the risk of material misstatement as low and has obtained sufficient appropriate audit evidence regarding the operating effectiveness of controls relevant to the assertion.

b. The population of items subject to negative confirmation procedures comprises a large number of small, homogeneous account balances, transactions, or conditions.

c. A very low exception rate is expected.

d. The auditor is not aware of circumstances or conditions that would cause recipients of negative confirmation requests to disregard such requests. (Ref: par. .A32)

Evaluating the Evidence Obtained

.16 The auditor should evaluate whether the results of the external confirmation procedures provide relevant and reliable audit evidence or whether further audit evidence is necessary. (Ref: par. .A33–.A34)

Application and Other Explanatory Material

Definitions

External Confirmation (Ref: par. .06)

.A1 The auditor's direct access to information held by a third party (the confirming party) may meet the definition of an external confirmation when, for example, the auditor is provided by the confirming party with the electronic access codes or information necessary to access a secure website where data that addresses the subject matter of the confirmation is held. The auditor's access to information held by the confirming party may also be facilitated by a third-party service provider. When access codes or information necessary to access the confirming party's data is provided to the auditor by management, evidence obtained by the auditor from access to such information does not meet the definition of an external confirmation.

External Confirmation Procedures

Determining the Information to Be Confirmed or Requested (Ref: par. .07a)

.A2 External confirmation procedures frequently are performed to confirm or request information regarding account balances, elements thereof, and disclosures. They also may be used to confirm the terms of agreements, contracts, or transactions between an entity and other parties or to confirm the absence of certain conditions, such as a "side agreement." Selecting the Appropriate Confirming Party (Ref: par. .07b)

.A3 Responses to confirmation requests provide more relevant and reliable audit evidence when confirmation requests are sent to a confirming party who the auditor believes is knowledgeable about the information to be confirmed. For example, a financial institution official who is knowledgeable about the transactions or arrangements for which confirmation is requested may be the most appropriate person at the financial institution from whom to request confirmation.

Designing Confirmation Requests (Ref: par. .07c)

.A4 The design of a confirmation request may directly affect the confirmation response rate and the reliability and nature of the audit evidence obtained from responses.

.A5 Factors to consider when designing confirmation requests include the following:

- The assertions being addressed.
- Specific identified risks of material misstatement, including fraud risks.
- The layout and presentation of the confirmation request.
- Prior experience on the audit or similar engagements.
- The method of communication (for example, in paper form or by electronic or other medium).
- Management's authorization or encouragement to the confirming parties to respond to the auditor. Confirming parties may only be willing to respond to a confirmation request containing management's authorization.
- The ability of the intended confirming party to confirm or provide the requested information (for example, individual invoice amount versus total balance).

.A6 A positive external confirmation request asks the confirming party to reply to the auditor in all cases, either by indicating the confirming party's agreement with the given information or asking the confirming party to provide information. A response to a properly designed positive confirmation request ordinarily is expected to provide reliable audit evidence. A risk exists, however, that a confirming party may reply to the confirmation request without verifying that the information is correct. The auditor may reduce this risk by using positive confirmation requests that do not state the amount (or other information) on the confirmation request and that ask the confirming party to fill in the amount or furnish other information. On the other hand, use of this type of "blank" confirmation request may result in lower response rates because additional effort is required from the confirming parties to provide the requested information.

.A7 Determining that requests are properly addressed includes verifying the accuracy of the addresses, including testing the validity of some or all of the addresses on the confirmation requests before they are sent out, regardless of the confirmation method used. When a confirmation request is sent by email, the auditor's determination that the request is being properly directed to the appropriate confirming party may include performing procedures to test the validity of some or all of the e-mail addresses supplied by management. The nature and extent of the necessary procedures is dependent on the risks associated with the particular type of confirmation or address. For example, a confirmation addressing a higher risk assertion or a confirmation address that appears to be potentially less reliable (for example, an electronic confirmation addressed in a manner that appears easier to falsify) may necessitate different or more extensive procedures to determine that the request is directed to the intended recipient. See further guidance in paragraphs .A14–.A15.

Follow-Up on Confirmation Requests (Ref: par. .07d)

.A8 The auditor may send an additional confirmation request when a reply to a previous request has not been received within a reasonable time. For example, the auditor may, having reverified the accuracy of the original address, send an additional or follow-up request.

Management's Refusal to Allow the Auditor to Perform External Confirmation Procedures

Reasonableness of Management's Refusal (Ref: par. .08a)

.A9 A refusal by management to allow the auditor to perform external confirmation procedures is a limitation on the audit evidence the auditor seeks to obtain; therefore, the auditor is required to inquire about the reasons for the limitation. A common reason offered by management is the existence of a legal dispute or ongoing negotiation with the intended confirming party, the resolution of which may be affected by an untimely confirmation request. The auditor is required to seek audit evidence about the validity and reasonableness of the reasons for management's refusal because of the risk

that management may be attempting to deny the auditor access to audit evidence that may reveal fraud or error.

Implications for the Assessment of Risks of Material Misstatement (Ref: par. .08b)

.A10 The auditor may conclude from the evaluation in paragraph .08b that it would be appropriate to revise the assessment of the risks of material misstatement at the assertion level and modify planned audit procedures, in accordance with section 315, Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement.[19] For example, if management's request to not confirm is unreasonable, this may indicate a fraud risk factor that requires evaluation, in accordance with section 240.[20] Alternative Audit Procedures (Ref: par. .08c)

.A11 The alternative audit procedures performed may be similar to those appropriate for a nonresponse, as set out in paragraphs .A24–.A27. Such procedures also would take into account the results of the auditor's evaluation in paragraph .08b.

Results of the External Confirmation Procedures

Reliability of Responses to Confirmation Requests (Ref: par. .10)

.A12 Section 500A indicates that even when audit evidence is obtained from sources external to the entity, circumstances may exist that affect its reliability.[21] All responses carry some risk of interception, alteration, or fraud. Such risk exists regardless of whether a response is obtained in paper form or by electronic or other medium. Factors that may indicate doubts about the reliability of a response include whether it

- was received by the auditor indirectly or
- appeared not to come from the originally intended confirming party.

---

[19] Paragraph .32 of section 315, Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement.

[20] Paragraph .24 of section 240.

[21] Paragraph .A32 of section 500A.

.A13 The auditor's consideration of the reliability of the information obtained through the confirmation process to be used as audit evidence includes consideration of the risks that

a. the information obtained may not be from an authentic source,

b. a respondent may not be knowledgeable about the information to be confirmed, and

c. the integrity of the information may have been compromised.

When an electronic confirmation process or system is used, the auditor's consideration of the risks described in a–c includes the consideration of risks that the electronic confirmation process is not secure or is improperly controlled.

.A14 Responses received electronically (for example, by fax or e-mail) involve risks relating to reliability because proof of origin or identity of the confirming party may be difficult to establish, and alterations may be difficult to detect. The auditor may determine that it is appropriate to address such risks by utilizing a system or process that validates the respondent or by directly contacting the purported sender (for example, by telephone) to validate the identity of the sender of the response and to validate that the information received by the auditor corresponds to what was transmitted by the sender.

.A15 An electronic confirmation system or process that creates a secure confirmation environment may mitigate the risks of interception or alteration. Creating a secure confirmation environment depends on the process or mechanism used by the auditor and the respondent to minimize the possibility that the results will be compromised because of interception or alteration of the confirmation. If the auditor is satisfied that such a system or process is secure and properly controlled, evidence provided by responses received using the system or process may be considered reliable. Various means might be used to validate the source of the electronic information. For example, the use of encryption, electronic digital signatures, and procedures to verify website authenticity may improve the security of the electronic confirmation system or process. If a system or process that facilitates electronic confirmation between the auditor

and the respondent is in place and the auditor plans to rely on the controls over such a system or process, an assurance trust services report (for example, Systrust) or another assurance report on that system or process may assist the auditor in assessing the design and operating effectiveness of the electronic and manual controls with respect to that system or process. Such an assurance report may address the risks described in paragraph .A13. If these risks are not adequately addressed in such a report, the auditor may perform additional procedures to address those risks.

.A16 The auditor is required by section 500A to determine whether to modify or add procedures to resolve doubts over the reliability of information to be used as audit evidence.[22] The auditor may choose to verify the source and contents of a response to a confirmation request by contacting the confirming party (for example, as described in paragraph .A14). When a response has been returned to the auditor indirectly (for example, because the confirming party incorrectly addressed it to the entity rather than the auditor), the auditor may request the confirming party to respond in writing directly to the auditor.

Disclaimers and Other Restrictions in Confirmation Responses

.A17 A response to a confirmation request may contain restrictive language regarding its use. Such restrictions do not necessarily invalidate the reliability of the response as audit evidence. Whether the auditor may rely on the information confirmed and the degree of such reliance will depend on the nature and substance of the restrictive language.

.A18 Restrictions that appear to be boilerplate disclaimers of liability may not affect the reliability of the information being confirmed. Examples of such disclaimers may include the following:

- Information is furnished as a matter of courtesy without a duty to do so and without responsibility, liability, or warranty, express or implied.

---

[22] Paragraph .10 of section 500A.

- The reply is given solely for the purpose of the audit without any responsibility on the part of the respondent, its employees, or its agents, and it does not relieve the auditor from any other inquiry or the performance of any other duty.

.A19 Other restrictive language also may not affect the reliability of a response if it does not relate to the assertion being tested. For example, in a confirmation of investments, a disclaimer regarding the valuation of the investments may not affect the reliability of the response if the auditor's objective in using the confirmation request is to obtain audit evidence regarding whether the investments exist.

.A20 Certain restrictive language may, however, cast doubt about the completeness or accuracy of the information contained in the response or on the auditor's ability to rely on such information. Examples of such restrictions may include the following:

- Information is obtained from electronic data sources, which may not contain all information in the respondent's possession.
- Information is not guaranteed to be accurate nor current and may be a matter of opinion.
- The recipient may not rely upon the information in the confirmation.

.A21 When the auditor has doubts about the reliability of the response as a result of restrictive language, then, in accordance with paragraph .10, the auditor is required to obtain further audit evidence to resolve those doubts. When the practical effect of the restrictive language is difficult to ascertain in the particular circumstances, the auditor may consider it appropriate to seek clarification from the respondent or seek legal advice.

.A22 If the auditor is unable to resolve the doubts about the reliability of a response as a result of restrictive language, then, in accordance with paragraph .11, the auditor is required to evaluate the implications on the assessment of the relevant risks of misstatement, including the risk of fraud, and on the related nature, timing, and extent of other audit procedures. The nature, timing, and extent of such procedures will depend on

factors such as the nature of the financial statement item, the assertion being tested, the nature and substance of the restrictive language, and relevant information obtained through other audit procedures.

Unreliable Responses (Ref: par. .11)

.A23 When the auditor concludes that a response is unreliable, the auditor may need to revise the assessment of the risks of material misstatement at the assertion level and modify planned audit procedures accordingly, in accordance with section 315.[23] For example, an unreliable response may indicate a fraud risk factor that requires evaluation, in accordance with section 240.[24]

Nonresponses and Oral Responses (Ref: par. .12)

.A24 The nature and extent of alternative procedures are affected by the account and assertion in question. Examples of alternative audit procedures the auditor may perform include the following:

- For accounts receivable balances, examining specific subsequent cash receipts (including matching such receipts with the actual items being paid), shipping documentation, or other client documentation providing evidence for the existence assertion
- For accounts payable balances, examining subsequent cash disbursements or correspondence from third parties and other records, such as receiving reports and statements that the client receives from vendors providing evidence for the completeness assertion

.A25 A nonresponse to a confirmation request may indicate a previously unidentified risk of material misstatement. In such situations, the auditor may need to revise the assessed risk of material misstatement at the assertion level and modify planned

---

[23] Paragraph .32 of section 315.

[24] Paragraph .24 of section 240.

audit procedures, in accordance with section 315.[25] For example, a fewer or greater number of responses to confirmation requests than anticipated may indicate a previously unidentified fraud risk factor that requires evaluation, in accordance with section 240.[26]

.A26 The auditor may determine that it is not necessary to perform additional alternative audit procedures beyond the evaluation of the confirmation results if such evaluation indicates that relevant and reliable audit evidence has already been obtained. This may be the case when testing for overstatement of amounts and (a) the nonresponses in the aggregate, projected as 100 percent misstatements to the population and added to the sum of all other unadjusted differences, would not affect the auditor's decision about whether the financial statements are materially misstated and (b) the auditor has not identified unusual qualitative factors or systematic characteristics related to the nonresponses, such as that all nonresponses pertain to year-end transactions.

.A27 An oral response to a confirmation request does not meet the definition of an external confirmation because it is not a direct written response to the auditor. Provided that the auditor has not concluded that a direct written response to a positive confirmation is necessary to obtain sufficient appropriate audit evidence, the auditor may take the receipt of an oral response to a confirmation request into consideration when determining the nature and extent of alternative audit procedures required to be performed for nonresponses, in accordance with paragraph .12. The auditor may perform additional procedures to address the reliability of the evidence provided by the oral response, such as initiating a call to the respondent using a telephone number that the auditor has independently verified as being associated with the entity. For example, the auditor might call the main telephone number obtained from a reliable source and ask to be directed to the named respondent instead of calling a direct extension provided by the client or included in the statement or other correspondence received by the entity. The auditor may determine that the additional evidence provided by contacting the respondent directly, together with the evidence upon which the original confirmation request is based (for

---

[25] Paragraph .32 of section 315.

[26] Paragraph .24 of section 240

example, a statement or other correspondence received by the entity), is sufficient appropriate audit evidence. In appropriately documenting the oral response, the auditor may include specific details, such as the identity of the person from whom the response was received, his or her position, and the date and time of the conversation.

When a Written Response to a Positive Confirmation Request Is Necessary to Obtain Sufficient Appropriate Audit Evidence (Ref: par. .13)

.A28 In certain circumstances, the auditor may identify an assessed risk of material misstatement at the assertion level for which a response to a positive confirmation request is necessary to obtain sufficient appropriate audit evidence. Such circumstances may include the following:

- The information available to corroborate management's assertion(s) is only available outside the entity.
- Specific fraud risk factors, such as the risk of management override of controls or the risk of collusion, which can involve employee(s) or management, or both, prevent the auditor from relying on evidence from the entity.

.A29 When the auditor has determined that a written response is necessary to obtain sufficient appropriate audit evidence and the auditor has obtained only an oral response to a confirmation request, the auditor may request the confirming party to respond in writing directly to the auditor. If no such response is received, in accordance with paragraph .13, alternative audit procedures will not provide the audit evidence the auditor requires, and the auditor is required to determine the implications for the audit and the auditor's opinion, in accordance with section 705.

Exceptions (Ref: par. .14)

.A30 Exceptions noted in responses to confirmation requests may indicate misstatements or potential misstatements in the financial statements. When a misstatement is identified, the auditor is required by section 240 to evaluate whether such

misstatement is indicative of fraud.[27] Exceptions may provide a guide to the quality of responses from similar confirming parties or for similar accounts. Exceptions also may indicate a deficiency, or deficiencies, in the entity's internal control over financial reporting.

.A31 Some exceptions do not represent misstatements. For example, the auditor may conclude that differences in responses to confirmation requests are due to timing, measurement, or clerical errors in the external confirmation procedures.

Negative Confirmations (Ref: par. .15)

.A32 The failure to receive a response to a negative confirmation request does not indicate receipt by the intended confirming party of the confirmation request or verification of the accuracy of the information contained in the request. Accordingly, a failure of a confirming party to respond to a negative confirmation request provides significantly less persuasive audit evidence than does a response to a positive confirmation request. Confirming parties also may be more likely to respond indicating their disagreement with a confirmation request when the information in the request is not in their favor but less likely to respond otherwise. For example, holders of bank deposit accounts may be more likely to respond if they believe that the balance in their account is understated in the confirmation request but less likely to respond when they believe the balance is overstated. Therefore, sending negative confirmation requests to holders of bank deposit accounts may be a useful procedure in considering whether such balances may be understated but is unlikely to be effective if the auditor is seeking evidence regarding overstatement.

---

[27] Paragraph .35 of section 240.

Evaluating the Evidence Obtained (Ref: par. .16)

.A33 When evaluating the results of individual external confirmation requests, the auditor may categorize such results as follows:

a. A response by the appropriate confirming party indicating agreement with the information provided in the confirmation request or providing requested information without exception

b. A response deemed unreliable

c. A nonresponse

d. A response indicating an exception

.A34 The auditor's evaluation, when taken into account with other audit procedures the auditor may have performed, may assist the auditor in concluding whether sufficient appropriate audit evidence has been obtained further audit evidence is necessary, as required by section 330.[28] (AICPA, 2012b)."

---

[28] Paragraphs .28–.29 of section 330.

Appendix D - Questionnaire

I. Suitability of Blockchain Technology for Auditing

Question 1.1: What do you know about blockchain features and principles and how relevant are these features for auditing?

Hints:

- Decentral databases
- Peer-to-peer transmission
- Irreversibility of records
- Smart contracts

Question 1.2: What blockchain type is most suitable for auditing purposes?

Hints:

- Private Blockchains
- Public Blockchains
- Consortium Blockchains

Question 1.3: How do you rate the security of blockchain technology against cyber security threats in contrast to ERP systems?

Hints:

- Asymmetric encryption
- 51 percent attack
- Blockchain mechanisms

Question 1.4: How user access management shall be implemented to protect blockchain systems appropriately?

Hints:

- Access controls
- Peer-to-peer mechanisms

Question 1.5: In what way the architecture of blockchain systems shall be designed to serve audit purposes?

Hints:

- Architecture
- Interoperability issues
- Changelogs
- Segregation in different layers

II. Elimination of Audit Weaknesses by Blockchain-based Auditing

Question 2.1: Do you think that traditional auditing provides weaknesses? If yes, what kind of weaknesses?

Hints:

- Risk-oriented audit approach
- Sampling procedures
- Periodical Auditing
- High costs
- Large audit teams

Question 2.2: How will blockchain technology be designed to audit itself, or is external auditing still required?

Hints:

- Audit standards
- Reliability
- Audit risk
- Inherent risks

Question 2.3: In what way must smart audit procedures be designed to audit accounting-related financial information so that sampling procedures become fully obsolete?

Hints:

- Continuous auditing
- Auditing internal controls
- Entire populations
- Consortium blockchains

Question 2.4: What audit procedures beneath smart audit tools decrease audit risks on blockchains?

Hints:

- Blockchain code
- Access controls
- Blockchain mechanisms

Question 2.5: Do you expect high impacts from blockchain technology on the auditing profession and the auditor's role?

Hints:

- New business models
- Disruption of audit procedures
- Auditor to examine merely management assertions

Question 2.6: How blockchain-based auditing must be designed to render requests for external confirmations obsolete.

Hints:

- Consortium blockchains
- Dedicated access
- Blockchain environment of auditees and their customers

III Compliance on AU-C 505 with Blockchains

Question 3.1: Are blockchain-based audit procedures toward accounts receivable compliant with GAAS audit standard AU-C 505?

Hints:

- Guidance on manual requests for external confirmations
- Management´s refusal to perform request procedures
- Positive and negative requests
- Evaluation of results
- Alternative audit procedures in case of a low response rate

Question 3.2: What structure and elements require audit standards concerning audits of accounts receivable with blockchains?

Hints:

- Consortium blockchains
- Guidance on smart audit procedures
- Obtaining audit evidence
- Data analysis

Appendix E - Coding

I First-Order Coding

<table>
<tr><th colspan="3">Characteristics of Blockchains</th></tr>
<tr>
<td>Blockchain Features
▪ Decentralized data
▪ Direct exchange
▪ Anonymous interaction
▪ Tamper-proof data
▪ Immutable data
▪ Blockchain mechanisms
▪ Asymmetric encryption

Security Level

▪ Asymmetric encryption
▪ 51 percent-attack
▪ Asymmetric encryption</td>
<td>User Access
▪ Authorization & Validation
▪ Confidentiality of data

Architecture
▪ Blockchain architecture
▪ Interoperability
▪ Changelog / Audit trail
▪ Blockchain layer</td>
<td>Blockchain Type

▪ Public Blockchain
▪ Private Blockchain
▪ Consortium Blockchain</td>
</tr>
<tr><th colspan="3">Elimination of Audit Weaknesses with Blockchains</th></tr>
<tr>
<td>Audit Weaknesses
▪ Risk-oriented approach
▪ Sampling
▪ Very high costs
▪ Too work-intensive
▪ Too large audit teams

External Audits
▪ External assurance
▪ Assessment of inherent, control and audit risks</td>
<td>Smart Auditing of Transactions
▪ Completeness
▪ Entire populations
▪ Misstatements/fraud
▪ No external confirm.
▪ Data analysis

Smart Auditing of Internal Controls
▪ Internal controls
▪ Completeness
▪ Data integrity</td>
<td>Additional Audits
▪ Automatic controls/ITGC
▪ Management Assertions
▪ Impact on auditing</td>
</tr>
</table>

Compliance with Blockchain-based Auditing	
Compliance of Blockchains with AU-C 505 ▪ Non-compliance with AU-C 505 ▪ New audit standards for blockchains ▪ Revised Audit Standards	**Elements of a Blockchain Standard** ▪ Guideline on blockchain procedures ▪ Obtaining audit evidence ▪ Data analysis procedures

II Second-Order Coding

Characteristics of Blockchains		
▪ Blockchain features	▪ Blockchain characteristics	▪ Most suitable blockchain type
Elimination of Audit Weaknesses with Blockchains		
▪ Audit weaknesses	▪ Continuous auditing with blockchains	▪ Supplementary auditing procedures on blockchains
Compliance with Blockchain-based Auditing		
▪ Compliance gaps of blockchain-based auditing toward GAAS		

III Aggregate Dimensions

Suitability of the Blockchain technology for auditing purposes
Elimination of Audit Weaknesses with Blockchains
Compliance Gaps of Blockchain-based Auditing toward AU-C 505

Appendix F - List of Abbreviations

Abbreviation	Explanation
ACCA	Association of Chartered Certified Accountants
AICPA	American Institute of Certified Public Accountants
API	Application Programming Interface
ASB	Auditing Standards Board
AU	Audit
AU-C	Audit Clarity Identifier
BFT	Byzantine Fault Tolerance
CAQDAS	Computer-Aided Qualitative Data Analysis Software
CISA	Certified Information Systems Auditor:
COBIT	Control Objectives for Information and Related Technology
CPA	Certified Public Accountant
DLT	Distributed ledger technology
e.g.	For Example
ERP	Enterprise Research Planning
EY	Ernst & Young
FASB	Financial Accounting Standards Board
GAAP	General Accepted Accounting Principles
GAAS	Generally Accepted Auditing Standards
GDPR	European General Data Data Protection Regulation
IAASB	International Auditing and Assurance Standards Board

IAM	Identity Access Management
ICS	Internal Control System
IDEA	Interactive Data Extraction and Analysis
IDW	Institut der Wirtschaftspruefer
IFRS	International Financial Reporting Standards
ISA	International Standards on Auditing
ISO	International Organization for Standardization
ITGC	IT General Controls
ITIL	Information Technology Infrastructure Library
PCAOB	Public Companies Accounting Oversight Board
Ph.D.	Doctor of Philosophy
RQ	Research question
SAS	Statements on Auditing Standards
SWIFT	Society for Worldwide Interbank Financial Telecommunication
UK	United Kingdom
US	United States
USA	United States of America