The United States' Experience in Utilizing Blockchain to Enhance Data Security in Internal Auditing

Abdelhak ZIANI [1] ♦, Kheira MEDJDOUB [2]

[1] Ibn Khaldoun University of Tiaret (Algeria), abdelhak.ziani@univ-tiaret.dz

ORCID: https://orcid.org/0009-0000-7041-2017

[2] Ibn Khaldoun University of Tiaret (Algeria), Kheira.medjdoub@univ-tiaret.dz

ORCID: https://orcid.org/0009-0005-2141-8603

Received: 26/05/2025 Accepted: 14/07/2025 Published:20/07/2025

Abstract:

This study explores the role of blockchain technology in enhancing data security within internal auditing in the United States. Blockchain, as a decentralized and immutable ledger system, offers significant benefits in maintaining data integrity and transparency. The paper discusses how blockchain can automate certain auditing functions, provide real-time assurance, and ensure the security of sensitive audit data. It highlights case studies involving federal agencies and private companies that have implemented blockchain to enhance secure auditing practices. Despite the potential benefits, challenges such as regulatory compliance, technology adoption costs, and infrastructure adequacy are identified. The study concludes that blockchain technology can significantly enhance data security and efficiency in internal auditing but requires further research and strategic planning to overcome existing challenges.

Keywords: Blockchain Technology, Internal Auditing,Data Security, DigitaTransformation

♦ **Corresponding author.**

I- Introduction:

With today's fast evolving technology, organisations are being forced to reconsider the traditional means through which auditing was performed and subsequently met with significant challenges in the area of network security and data integrity (Arquam et al., 2022). By contrast, Blockchain has been proposed to distribute responsibilities and secure sensitive information on tamper-evident ledgers. Yet, the use in the auditing area is relatively unclear, which creates avenues for research desired by academics and professionals (The Duy et al., 2020).

This shift in technology has led to a rearrangement of power and has compelled both national and international regulation to adapt. Existing measures that include control mechanisms based on mutual trust between internal auditors and external auditors usually do not go deeply enough into data sharing. In this context, the Sarbanes-Oxley Act (SOX) of 2002 underscores the significance of internal controls and external auditor independence (Bansal, 2024). In the meantime, IIA standards and frameworks such as COBIT and COSO offer critically important governance guidance, but must be continuously retooled to line up with ever evolving compliance regulations (Álvarez-Foronda et al., 2023; Lowenstein & Cao, 2023).

Internal audit data is sensitive as it may reveal operational flaws and confidential strategies, and present serious risks (The Duy et al., 2020). Ias a result, old ways of protecting your data are no longer considered good enough under the SOX Act Section 404. Auditors' opinions have been closely scrutinized for data security, even resulting in large annual fines to the corporate sector for their non-performance in this regard (Saha et al., 2023).

Despite advances in technology, the same old security concerns remain just as relevant today, such as authorized users breaking the rules, and unauthorized sharing of information. There is a general agreement that in order to mitigate these risks the right strategy is to adopt sound physical, procedural and personnel security.

The digital transformation has exposed the inherent vulnerabilities of conventional auditing systems in safeguarding sensitive data and adhering to evolving regulatory frameworks, such as the Sarbanes-Oxley Act of 2002, necessitating innovative approaches. Consequently, the central question arises: **How can blockchain technology bolster data security in internal auditing within the United States?**

To address the research problem, the study is guided by the following sub-questions:

1. What specific security and efficiency benefits does blockchain technology offer to internal auditing processes?
2. What are the primary technological, regulatory, and organizational challenges impeding blockchain adoption in U.S. internal auditing?
3. How do existing national and international regulatory frameworks, such as SOX and GDPR, shape the implementation of blockchain in auditing?
4. What practical insights can be derived from U.S.-based case studies of blockchain applications in internal auditing?

These questions provide a structured framework for analyzing the multifaceted role of blockchain in auditing, ensuring a rigorous and systematic investigation. To test the relationships and assumptions embedded within this inquiry, the study puts forward several hypotheses that will guide the subsequent analysis and data interpretation.

The study proposes the following hypotheses:

H_1: The adoption of blockchain technology is associated with enhanced data security in internal auditing through its core features of decentralization, immutability, and cryptographic security.

- **H_2:** Implementing blockchain in internal auditing can lead to greater audit efficiency by automating verification processes, enabling real-time assurance, and executing smart contracts.
- **H_3:** The primary barriers hindering widespread blockchain implementation in U.S. internal auditing include high technological adoption costs, regulatory uncertainties, and the need for significant upgrades to existing IT infrastructure.
- **H_4:** Strategic planning and structured collaboration among auditors, technologists, and regulatory bodies are key factors that can mitigate adoption challenges and facilitate the effective integration of blockchain into auditing practices.

These hypotheses guide the investigation, testing the potential benefits and obstacles of blockchain in the auditing domain. Consequently, this study carries profound implications for both academic research and professional practice in internal auditing. By exploring blockchain's role in enhancing data security, it addresses a critical gap in the literature, where the application of emerging technologies in auditing remains underexplored. Practically, the findings provide actionable insights for organizations seeking to strengthen governance, mitigate data security risks, and comply with regulatory mandates in an era of digital transformation. The study's focus on U.S.-based case studies offers context-specific evidence that can inform policymakers, auditors, and technologists in developing strategies to harness blockchain's potential. Moreover, by bridging the divide between technological innovation and auditing methodologies, the research contributes to the evolution of auditing standards, fostering resilience and trust in organizational data management.

To realize these contributions and provide a clear roadmap for the research, the study pursues the following objectives:

1. To evaluate the role of blockchain technology in enhancing data security and transparency in internal auditing processes.
2. To analyze the practical applications of blockchain in internal auditing through case studies of U.S. federal agencies and private companies.
3. To identify the technological, regulatory, and organizational challenges associated with blockchain adoption in auditing.
4. To propose strategic recommendations for overcoming adoption barriers and integrating blockchain effectively into internal auditing practices.

These objectives provide a clear roadmap for the research, ensuring a comprehensive exploration of blockchain's potential and limitations.

To fulfill these objectives, the study adopts a qualitative research approach to investigate blockchain's application in internal auditing. It employs a dual methodology, combining a systematic literature review with case study analysis. The literature review synthesizes academic and industry sources to examine blockchain's technical features and their relevance to auditing, while the case study analysis focuses on real-world applications in the U.S. to provide empirical evidence. Data is collected from publicly available reports, peer-reviewed journals, and industry publications, and the analysis integrates theoretical frameworks like COBIT and COSO with practical insights.

To analyze the collected data, a **thematic analysis** approach was employed to systematically identify, analyze, and report patterns (themes) within the data, derived directly from the research questions. This comprehensive methodology ensures a contextually grounded exploration of blockchain's role, moving beyond mere description to offer a structured analytical interpretation and actionable recommendations for stakeholders.

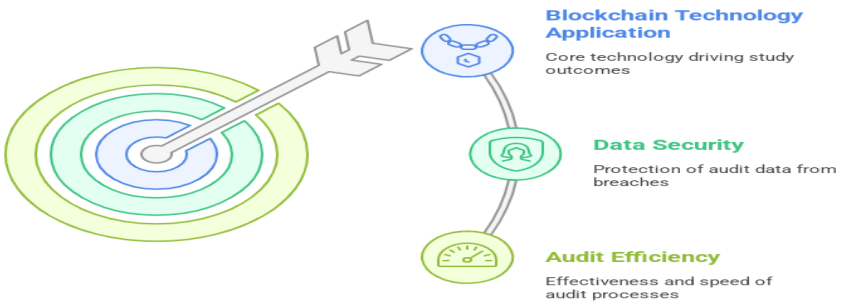
1. The theoretical framework of the study.

This section establishes the theoretical foundations of the study. To operationalize the research inquiry, it begins by defining the core variables, setting the stage for a detailed analysis of how blockchain technology influences internal auditing practices and laying the groundwork for the conceptual model.

1.1. Definition of Study Variables:

The study examines blockchain technology's role in enhancing data security in U.S. internal auditing. The following variables are defined to analyze its impact and challenges:

Figure (1): Study Variables



Source: Prepared by researchers

- **Blockchain Technology Application (Independent Variable)**: Utilization of blockchain in internal auditing, encompassing distributed ledgers, cryptographic hashing, and smart contracts. It drives the study's examination of security and efficiency outcomes.

- **Data Security (Dependent Variable)**: Protection of sensitive audit data from breaches or tampering, ensuring integrity and confidentiality. Measured by reduced security incidents and robust audit trails.

- **Audit Efficiency (Dependent Variable)**: Effectiveness and speed of auditing processes, enhanced by blockchain's automation. Assessed via time savings and error reduction.

Based on the theoretical review, this study proposes a conceptual model (Figure 1) that illustrates the relationship between blockchain technology features and internal auditing objectives. The model posits that key blockchain characteristics (Decentralization, Immutability, Transparency) directly influence core data security attributes (Integrity, Confidentiality, Availability), which in turn enhance overall audit quality and efficiency. This model will serve as an analytical framework for interpreting the case study finding.

1.2. Understanding Blockchain Technology.

Blockchain is a peer-to-peer, decentralized, and distributed digital ledger system introduced by the pseudonym of Satoshi Nakamoto in 2008 and realized as the basis of Bitcoin in 2009 (GURGU). Blockchain plays a crucial role in maintaining a tamper-proof record of chronological transactions for cryptocurrencies. (Zenagui B & al, 2024) Since its inception, blockchain and its variations have been utilized to deliver functionalities that entail secure and tamper-proof processes and operations. Despite its potential, blockchain remains misunderstood. Misconceptions have prevented blockchain from being effectively deployed in applications outside of cryptocurrencies. In the context of auditing, this section aims to dissect blockchain and its popular misconceptions and illuminate blockchain for auditing or managerial decision making. One crucial deterrent to initiating blockchain deployments involved blockchain's ambiguities and common misconceptions as well as the charming but unrealistic propaganda and HYPE that surrounds this already contentious technology (Zolanvari et al., 2018). Blockchain technology is compared against traditional database systems to highlight motivation, objective, and its strengths, as well as concerns. This paper also offers a brief but meaningful description about crowd-favorite blockchain. consensus mechanisms, cryptographic backing and smart contract, and the blockchain industry's open secrets, "challenges and issues".

1.2.1. Definition and Basics of Blockchain

Blockchain is becoming an emerging technology that extends possibilities for securing data in wide application domains. Blockchain itself is a decentralized, distributed ledger because every computer or node in its network keeps a copy of the transaction data. Each transaction consists of a block that is accumulated like a chain, forming a 'blockchain'. Because the blockchain network is decentralized, no single entity can control the blocks, leading to a high level of security. Data security is further enhanced by linking every new block with the hash of the previous block, forming a chain of blocks that is at the same time unchanging and secure (Mansour et al., 2024). In summary, the decentralized, distributed system of blockchain is composed of various computers or nodes that store identical data, called a node or block. Nodes are connected by peer-to-peer technology, which means that they exchange data directly, without passing through a central server.

Blockchain provides a solution by keeping integrity in an open book. This is because a blockchain ID is derived from a combination of transactions that are not easily forged. This way, the entire data chain can be confirmed from the beginning. The

functionality of the blockchain digital ledger is based on a decentralized and distributed system of computers storing identical data called a block or node (Zarrin et al., 2021). Whole nodes are connected by peer-to-peer technology, meaning they exchange data straight without intermediaries (Kogon, 2017). Every new transaction is saved to a block as a chain of blocks that link and secure previous data. The complexity of the functions of the blockchain can be perceived as something difficult. Nevertheless, the basics of blockchain are not hard to comprehend but relatively easy to put into practice. Toward that end, a comprehensive definition of blockchain is provided as well as a concept description of what blockchain is, its foundations of work, and how the blocks themselves function.

1.2.2. Key Features and Components.

There are fundamental aspects that create trust in a blockchain system: (1) Transparency from the decentralized feature, (2) Security from the cryptographic and hashing algorithm, inset of each transaction block, (3) Immutability from the chaining design such that once a block is added, it is extremely difficult to change it, and (4) Trust from the connected network. The part of blockchain that guarantees the cryptographic and hashing algorithm inset of each transaction block is the consensus mechanism (Zolanvari et al., 2018). This part is important in enhancing trust in the blockchain they are creating. Additionally, some of the financial regulatory bodies may need encryption and privacy with sensitive data. The blockchain design is integrated with encryption algorithms AES and X.509, which respectively represent data encryption and digital signature for improving data security and privacy.

One of this blockchain is the Ethereum protocol. It offers protocol extensions with decentralized, encryption, privacy, access control solutions, and a high-level language for the tasks described by “smart contracts.” A smart contract is simply a computer code running on top of a blockchain containing the “terms” for the contract execution. It is self-executing with the terms directly written into code. Once deployed on the blockchain, the code can be triggered by transactions, and when pre-defined conditions are met, the outcome is automatically executed ensuring an automated, “if-then” consensus. Regarding the transaction history support, it is found that the alternative blockchain has only TxIndex. All of the detailed information for each payment in the transaction log of Ethereum is supported by parameter fromTx.

1.2. Applications of Blockchain in Various Industries.

Beyond its origins in cryptocurrency, blockchain technology has demonstrated significant transformative potential across a wide range of industries. This section explores its practical applications in several key sectors, beginning with its foundational role in financial services, followed by its impact on supply chain management, and its emerging use in securing sensitive data within the healthcare industry.

1.2.1. Financial Services.

The first instance of blockchain technology was found in the financial services industry since public blockchain is established and maintained by a network of diverse participants, including financial service firms. The financial services industry also

demonstrated the significance of blockchain technology, albeit largely as the innovators. Numerous startups and international corporations embraced this technology to transform financial services. One startup effectively turned its blockchain platform into an industry standard. To date, more than 100 financial institutions from different countries have adopted this platform to process cross-border payments. The international landscape illustrates blockchain's ability to significantly advance a particular function of the enterprise risk management framework – compliance. The industry's blockchain interest posed less of a dilemma, and it is one such function piloting others.

Today, leading financial institutions have implemented several pilot projects testing the application of blockchain for various functions. AITCA was also founded to provide a voice for the emerging market stakeholders seeking to influence policy and technology that may impact the future adoption of blockchain-related technology. Their cloud-based solution platform has more than 2,000 pilot projects to date, making it the world's most comprehensive database of blockchain pilot projects. This data is furthered by examining how internal auditing applies blockchain. Although limited to 20 articles listed, ten industries stand out, each taking a different utilization angle to the public blockchain.

1.2.2. Supply Chain Management.

Various supply chain management developments by blockchain companies, such as for supply chain financing, for luxury goods, and for Byzantine-resistant functionalities, for pharmaceutical products, for multinational merchandise, and for speed clearing and settlement in the financial industry. applied blockchain technology in digitizing supply chain finance to ensure the security of supply chain financing information by adopting a reliable consensus algorithm and privately controlled supply chain data. By doing so, information on the accounts payable and accounts receivable cycles can now exist credibly on the same blockchain.

set up a blockchain network with 15 global banks to share trade finance data effectively, with the aim of cutting funding risks and fraud. was co-founded by several companies and launched by the blockchain improvement upon silhouette, to redesign the global trade process via a blockchain-led digital operating model across the supply chain of customers' products. The procurement process is detailed in supply chain, while novel block programming paradigm can help analyze well-known brands across digital electronic products, fashion retail, and logistics (Hrouga & Sbihi, 2023). Surveys have also focused on the application of the blockchain system in the fresh food supply chain. The decentralization and Internet of Things are still used or mentioned frequently.

1.2.3. Healthcare.

In 2017, a decentralized platform combining a novel trinary hash function with blockchain was introduced, designed to exchange and secure sensitive medical data. Termed Healthchain, it was suggested that healthcare industries use the system to enable physicians at different medical institutions to share patient data safely and to enable collaboration among doctors in providing patient care. The platform allows health data to be stored securely through the use of distributed ledger technology, and patient medical records can be disclosed only upon permission from patients through cryptographic access control. After analyzing the characteristics of the Healthchain platform to compare it with

conventional healthcare data storage service alternatives, it was discovered that the design is more appropriate for patient data disclosure during a clinic visit than for typical patient care.

A solution was presented designed to securely protect the privacy of big data that uses machine learning within hospitals, leveraging blockchain technology. This system provided hospital owners with the freedom to encrypt and outsource data to be shared among potentially competing hospitals without risking patient privacy. Machine learning capabilities were preserved in this system using a secure human intervention mechanism, which was integrated into smart contracts. It was stated that the system allows sharing of models for AI with the local population to speed up next-generation precision medicine research, tailored to the treatment needs of individual patients. Based on the readings, the blockchain, which allows storage of records across multiple secure nodes, is appropriate for healthcare. (Adere, 2022) The Healthchain and big data models both offer a secure and decentralized platform that allows hospital owners to share sensitive data submitted by multiple organizations using blockchain technology.

1.3.Blockchain in Internal Auditing.

There is consensus in the professional literature that blockchain technology can enhance data security side of the internal auditing function. In terms of the auditing strategy and audit program design stages of internal auditing, blockchain technology can play a supportive role in the stage of audit implementation.

(a) Processes, transactions, and events. Data must be transformed into a transaction before it is written to the blockchain. Such transactions can carry any kind of data. With the help of certain protocols, blockchains can write a descriptive event and execute actions within systems based on this written action. Such capabilities might enable the automation of certain auditing functions and, in turn, lead to more controls and real-time assurance. An external blockchain-internal system query function can be used to extract a blockchain transaction and audit the event performed.

(b) Independent party. Normally, an external blockchain node operator will be needed for audit, given the need for party broader independence. It is especially important in data security circumstances. From a data security standpoint, it is critical that auditing be carried out by an external blockchain node operator as an independent party and organization (Ortman, 2018).

Auditors verify the integrity of a data set by comparing a calculated hash of that data set with the non-fungible blockchain hash. (Naderi et al.2025) Without such a preference, the integrity of the record verifying the event written in the block will be questioned. In that case, the importance and benefits of the transparency and immutability advantages of the blockchain will be eliminated. Within the field of auditing, transaction data sets on blockchains may be needed to be controlled. Before data is written on chain there is a window of time that malicious behavior can occur while data becomes an immutable, permanent part of a blockchain. However, a safe period is provided and care and actions will take place within that time frame. At this point, internal auditors and auditors will have written a report verifying the data, as expected, correctly reflected on the blockchain.

In the opinion of internal auditors and auditors, there is discredit in the context of the required formats and standards, and more researches are needed when it comes to concrete examples. Also, do not have a process tool that can convert blockchain transaction data to human-readable data and output. On possible internal control questions that blockchain technology can bring to organizations, cases #1, #2, #3, #4, and #5 are presented. Checks are not occurring on a monthly basis. Besides, the regulatory authority can not read the data written into their chain in case a legal dispute arises.

Blockchain can be used at certain step(s), detecting and providing resources of possible applications. Contracts to be implemented on the HI function or regulations to be enacted. For immediate compliance this year, there is the need for development. Leverage smart contracts to facilitate compliance with the desired ongoing monitoring functions, control the completion of the HI plan, and input relevant data, and automate evidences collected. However, parts of HI process where a human judgment is needed do not seem reasonable. For continuous updating and improvement of audit methodologies. Yet there is no commercial product, served as a niche industry, written in the profession of audit, that better standardizes the complicated terminology of the blockchain in the background industry, the question of how to make the input-output format of the blockchain clairvoyant is not absolute. Examples of possible audit procedures and methodologies to be performed in each of the six-stage HI stages or as a whole can include Bitcoin, Ethereum, Ripple, and request client on funding by the investments made on blockchain. Offering blockchain database services to businesses and thus requested to contract the accounting department to get a yearly financial status certificate of a blockchain company. During the inventory count requested to note the hash of last blocks of data assigned to the warehouse to later verify the integrity of the set. On the ongoing private placement, see if all investor information remains confidential during the buyout agreement on DLTL investments. To third parties which warehouse will be used for storing products transfer is performed by blockchain. In addition, the traditional HI methodologies are not suited and adaptable to the revolutions in information technology. A proactive and futuristic vision need to be developed by the HI function already on the area of blockchain when adapting audit methodologies or drafting new regulations and have increased attention to the potential developments in the field. Currently, there is a lack of commercial products that cater to the specialized, niche industry. Additionally, it is not certain that this particular industry has been written in the audit professional literature and therefore aids the discredit of the required formatting and standardization of complicated terminology in the technology in the auditing profession.

1.3.1. Benefits and Challenges.

Blockchain technology, originally developed as a public transaction ledger for cryptocurrencies, is a digitized, decentralized, and distributed ledger that records transactions across the internet. Companies and organizations have adopted this technology for various practices aimed at enhancing data security. Audit professionals assert that this technology can advance the fundamental auditing process by bolstering data security and fostering a more efficient audit environment (Imjai et al., 2024).

This research provides evidence of these benefits by analyzing the United States' experience in using blockchain technology to enhance data security in internal auditing.

Experimental results conducted by practicing accountants demonstrate that adapting blockchain in the internal auditing process not only enhances the level of audit assurance but also increases the efficiency of audit tasks.

Despite these promising benefits, the study reveals that various challenges may arise during implementation. These include the costs of technology adoption and employee training, the adequacy of existing IT infrastructures, and the need to secure regulatory consent and ensure compliance.

Furthermore, the rapid advancement of blockchain technology can outpace the auditing field's ability to respond and adapt. Accordingly, this paper provides further discussion on the preventive measures required to overcome these challenges, aiming to secure effective and long-lasting benefits from the application of blockchain in internal auditing.

2. Case Studies.

The U.S. government has made strong investments in conducting and encouraging blockchain research and in utilizing blockchain technology for various applications. Privacy, security, transparency, and efficiency are the main objectives of implementing blockchain in auditing. State-of-the-art research demonstrates that the U.S. government and large companies are leading the way in implementing blockchain in data security, and there is much potential for this implementation to expand to various sectors (The Duy et al., 2020). Accordingly, based on national initiatives and the use of blockchain in the federal government, four real-world case studies are provided. Two of these studies involve federal agencies, and two involve leading public companies in the U.S. These studies often combine judicious analysis, synthesis, and development, emphasize practical implications, and analyze real-world problems (Angeles, 2019). To be more illustrative and insightful, this section provides the case studies in a step-by-step manner. Each case study first outlines the challenges, then describes the employed strategy, and finally presents the results, insights, or benefits. In the context of the federal government, blockchain has been utilized by federal agencies to enhance secure auditing information, prevent potential fraud and fabrication of financial data, render validation, and ease the trusted sharing of financial details between agencies, auditors, and firms. A block explorer and a Blockchain as a Service (BaaS) is set up by National Science Foundation to carefully record auditing details from the grant programs, and the BaaS facilitates the verification process. The PricewaterhouseCoopers, a famous U.S. auditor, and the auditing firms are granted access to the distributed ledger technologies of NSF to authenticate audit statistics (Baba et al.2021). This initiative, 3 years following the implementation, is echoed by the General Accounting Office as a constructive proposal for blockchain usage in auditing. The potential advantages and compliance directions are provided. Subsequently, the GAO looks forward to directing the government’s financial management services to undertake a collaborative effort to construct a Blockchain System that ensures trust-mediated sharing of procurement details across federal departments.

2.1. Government Agencies.

Government agencies are responsible for ensuring the rules and regulations of the state are followed by all its citizens. The recent emergence of blockchain technology has made it easier for government agencies to make records public and secure while still private, as in the case of the Commonwealth of Massachusetts' blockchain records pilot program (Mansour et al., 2024). The main benefit for the agencies could be the ability to make contracts and other records public so that citizens are able to see that an agency is running efficiently. Additionally, the requirement for data entry or management could be removed, saving time. Governments have a great deal of money. Theoretically, the security of this money could be greatly improved through blockchain and by making all records public. Funds and money are often stolen or embezzled through illegitimate contracts (Alexopoulos et al., 2019). If all parts of a contract are viewable on a blockchain ledger, the potential for theft is greatly reduced. A blockchain system was implemented in the city of Moscow to execute and manage contracts more efficiently, and they have already seen a decrease of 44% fraud in contracts involving suppliers.

The Moscow case demonstrates a direct application of blockchain's transparency feature (as outlined in our conceptual model) to mitigate fraud. By creating a public, immutable ledger for contracts, the opportunity for illegitimate modifications was significantly reduced, validating Proposition 1 (H_1) regarding enhanced data integrity.

For businesses in general, many benefits have been claimed regarding the use of blockchain. Despite this, the use of blockchain technology in the business world is relatively low. There are some concerns with privacy, regulations, speed, etc. An interview-based case study tries to criticize the practical learning from the blockchain project in a specific business, the Philips healthcare sector, and highlight how the various negative attributes of blockchain technology discourage its use in their business. By contrast, resetting the technical expectations to more pragmatic target values and by combining blockchain with existing technologies, a realistic foundation for a successful application could be formed.

2.2. Private Sector Companies

The private sector in the US represents a substantial contributor to the economy and opportunity for blockchain. Companies have the potential to work in different sectors, for example, technological corporations, automobile manufacturer, healthcare service provider, tire and rubber provider, management of industrial fasteners and components. All these types of companies widely differ from each other and can promote advances in using blockchain technology (Jiang, 2024). Moreover, this serves to underscore the broad influence of blockchain. The size of companies is varied, from General Electric with more than $95 billion in revenue to BH North America with less than $1 billion. The implementation of blockchain technology has been varied subject to exercises as well as industries. There are some companies that have implemented blockchain technology and additionally, have been the subject of exploration. Those investigations provide a contribution to the empirical literature as these case companies originate from multiple industrial sectors.

2.2.1. Case Studies of Private Sector Company

One of the companies runs as a technological corporation based in the United States. This corporation tends to look for advanced solutions, creating software, cloud solutions, workstations, and servers for businesses, educational departments, and the health sector. Another company focuses on innovation in mobility services, working as an automobile manufacturer from the USA. This multi-million-dollar company looks for smart transport with low pollution and high efficiency. Within the company's services belong robo-taxis available with an application. This provider has also developed a digital payment that works as an e-wallet with propositions of blockchain technology.

Yet another case is a provider of healthcare services established in the United States. Together with various hospitals, it has created a blockchain alliance. In addition, this company deals with alliances in the healthcare sector, which is supposed to mean sharing data about various treatments. The tire and rubber provider has factories in Asia, including the USA. The company has launched a project, which purpose is to implement a blockchain solution in the tire sector. The workflow related to car servicing is supposed to be easier, as verified information will be available, from the work done by the service.

Another example is the oldest company operating in the USA – management of industrial fasteners and components, with multiple contacts over the worldwide. The implementation of blockchain is a part of cooperation with another multi-billion-dollar company. The target of this project is to document data related to deliveries. Data originating from all shipments is to be placed on the blockchain. In the event of a dispute between the companies, there will be a lack of necessity for manual inspection, it will be possible to verify the whole shipment process. Moreover, another option should be that the data about the delivery could be securely sent to the recipient just after it is posted on the blockchain. It would allow for real-time verification of receipt.

3. Regulatory Framework and Compliance

Compliance can be a complex subject when looking at using blockchain technology in a sector with existing regulation that is yet far from fully defined. There have been local, national, and regional references about blockchain technology and its compliance implications. However, these regulatory frameworks lack the clarity needed to ensure that there can be covered compliance for all situations.

National and supranational organizations are taking steps to produce guidance, regulation, or recommendations about the use and implications of this technology in the industry. One organization created a working group to advise on its work in the area of automated and distributed ledger technology. Main points on the matter are disintermediation, risk and controls, ownership, and possibly best practices. Among the best practices, they would like to measure the use and gain of the new technology opportunity and the applicability of industry standards. A document was published on the ambitions to lead in the era of distributed ledger technologies. This document aims to provide legal clarity and certainty about existing regulations and solutions for compliance with developing technologies. Representatives about data protection make statements on how regulations should be read by those who work with blockchain technology. The same community also takes steps to produce guidelines and auditors in charge of auditing the reliability of the blockchain systems.

In the publication there are minor mentions of approaches to user data security and transparency. The edition includes discussion on policy of blockchain, regulation, and compliance. One of those settings is with the introduction of the blockchain technology and privacy law, one such privacy law being the General Data Protection Regulation.

3.1. SEC Regulations

In August 2017, the United States (US) Securities and Exchange Commission (SEC) issued a report stating that initial coin offerings (ICOs) may constitute the issuance of securities and are subject to federal securities laws regarding registration, offering, and trading. (Bourveau et al.2022) The risks of fraud and manipulation are highlighted, and it provides guidance for investors and markets participants to comply with federal securities laws. Thereafter, many important events involving the SEC and blockchain have occurred, and those most relevant to financial markets are discussed.

However, the blockchain technology does not fit well with current laws and regulations. The SEC continuously proposes and enforces regulations relevant to blockchain to foster transparent and efficient markets, thereby protecting investors. Because blockchain is a new technology, participants in blockchain markets are required to understand various SEC regulations. For internal auditors, examining business activities concerning blockchain from the viewpoint of regulatory compliance and risk management is important.

Though blockchain technology can bring benefits to securities markets, it also poses new risks that have not been addressed by existing securities laws. Therefore, the SEC consistently proposes new regulations relevant to financial markets. First, the SEC provided an official statement on blockchain and cryptocurrencies. It considers that they potentially implicate virtually every industry, including securities markets, and are subject to federal securities laws. Also, the fraud and manipulative practices in these areas are raised concerns (Wu et al., 2024). Thereafter, SEC regulations relevant to blockchain are discussed in detail.

3.2. GDPR and Other International Standards

The European General Data Protection Regulation (GDPR) became effective on May 25th, 2018, imposing stringent data privacy requirements that reverberate throughout the entire continent. As European data protection laws often set the benchmark for stringent standards worldwide, corporations, including many multinationals, have completely overhauled their data processing operations in widespread adaptation efforts (Vasconcelos et al.2024). The most contentious, perhaps, are the right-to-know and right-to-erasure regulations stipulated by the GDPR on stored personal data, which come to a crashing contradiction with the immutability properties of blockchain’s ledger. Other standards should also be considered in locking down goals to ensure data integrity and maintenance of private information not in the scope of an audit necessity. Blockchain ought to initially address these standards in partnership with regulators to negate hefty fines for inadequacies and ensure compatibility with the expected market environment (Belen-Saglam et al., 2022). Thus, internal auditors accommodate themselves to the changing times to better safeguard data and address inefficiencies, pivoting their areas of concern. Even a matter addressing customer validity criteria can be extended in terms of database logs and access

store visibility to circumvent tampering of cryptographic evidence. Here, the inherently public nature of blockchain could be transformed into an audit asset during an investigation through encryption in storage to only allow visible access to the hash output. Another situation of interest occurs during a contract work performed by the audit unit intended to guarantee data integrity is maintained by the organization in question; thus, one practical step the audit unit could autonomously take is supplementing the hash root data custodian entry with responses from an outside source. But the Chinese whispers protocol applied to the information must still be designed in consultation with IT to ensure visibility of data requests instituted.

4. Future Trends and Possibilities

The increasing speed of technological advancements can be a great pressure for internal audit. On the other hand, to wait and see basically costs opportunities for institutionalization. This text is aiming to try to anticipate some trends and possibilities may happen in internal audit practices in the near future. The text is divided into four main parts. The first part is an overview of the latest development of blockchain technology and its potential application in internal audit. The second part explores some trends and possibilities, with the combination of internal audit practices. The third part tries to use some fictional scenarios to describe how these possibilities may look like. Some challenges to implement these possibilities will be discussed in the last part, and also some advices to face these challenges.

For a majority of people, when mentioning blockchain, the first thing coming up is cryptocurrency, as blockchain is best known as the technology behind cryptocurrency (Brender et al., 2018). However, blockchain is essentially a decentralized and immutable ledger technology, and cryptocurrency is merely the first application of blockchain. In recent years, there are increasing experiments of adopting blockchain technology in various sectors. And with the rapid development of Industry 4.0, the need for data security and reliability is dramatically increasing. Blockchain technology is recognized as an innovative and reliable solution in aspects of data security, data integrity, decentralized storage, and distributed consensus mechanism. After the first design on the bitcoin in 2008, and first launched the following year as open-source software, the implementation of the blockchain technology has developed and diversified industry horizons. In 2016, the potential of this technology was reinforced by several high-profile adopters of the technology, noting its suitability in the significant fields.

4.1. Integration with AI and IoT

Technologies such as artificial intelligence (AI), the Internet of Things, and blockchain have the potential to transform internal auditing. Blockchain—when fully integrated with these digital tools—impacts the auditing process by enhancing the transparency, security, and efficiency of data exchange. Over the past decades, blockchain technology has attracted increasing interest due to its security features regarding distributed and transparent data records. More recent innovations—such as AI and IoT technologies—commingle with blockchain to make auditing environments more secure and efficient. It is worth noting that the synergy of blockchain, AI, and IoT is also transforming numerous

sectors and underlying structures. For example, in a blockchain-integrated AI framework for industrial environments, AI algorithms analyze real-time data through blockchain cloud services. By conducting data reconciliation and automated audit trials, the AI system assigns multiple audit functions automatically (Zheng et al., 2019). Moreover, blockchain and IoT technologies are also seen to have the potential to cultivate data integrity, leading to better-informed decision-making processes due to the multi-sourced and high-quality data inputs from IoT devices.

However, a range of challenges is likely to arise pertaining to data accuracy, privacy, and regulatory compliance—and space is emerging for how to govern potential risks and limitations. Standardized protocols have not yet been widely established for the seamless integration between blockchain and the overarching environment of AI or IoT. Yet with underlying process automation, the integration of blockchain and AI advances diverse sectors, including supply chain management, handling AR/AP processes, and addressing workforce strategies through real-time anomaly detection. Similarly, innovation in the healthcare, banking, and energy industries showcase various successful integrations of blockchain and IoT.

5. Conclusion

In conclusion, this study provides an in-depth analysis of the dual role of blockchain technology in the field of internal auditing in the United States. It emerges as a promising tool for enhancing data security and operational efficiency, yet it is simultaneously surrounded by significant challenges. The research findings, supported by case studies from both the public and private sectors, have shown that adopting blockchain can tangibly enhance data integrity and transparency, thereby supporting **Hypothesis 1 (H1)** and **Hypothesis 2 (H2)**.

However, the study confirms that the path to widespread adoption is not without obstacles. High costs, regulatory ambiguity, and the need for advanced infrastructures present real barriers, which validates **Hypothesis 3 (H3)**. More importantly, the analysis concludes that overcoming these challenges is not merely a technical issue but a strategic one that requires meticulous planning and structured collaboration among auditors, technologists, and regulatory bodies. This provides clear support for **Hypothesis 4 (H4)**.

Ultimately, the transition to blockchain-based auditing necessitates an evolution in the internal auditor's mindset and methodology. Their role is no longer confined to retrospective review but is shifting toward proactive participation in control design and continuous verification. Investing in education and continuous knowledge sharing among all stakeholders is not just a recommendation but an imperative to ensure that the audit profession keeps pace with technological innovation and reaps lasting, reliable benefits.

5.1. Summary of Key Findings

This study presents a set of key findings that highlight the potential and challenges of applying blockchain technology in internal auditing:

- **Enhanced Data Security and Audit Efficiency:** Evidence from the case studies demonstrates that blockchain applications significantly enhance the security of audit data through their core features of decentralization and immutability. The findings

also show that process automation via smart contracts contributes to improving the efficiency of audit tasks and reducing manual errors. This directly supports **Hypotheses H1** and **H2**.

- **Identification of Key Adoption Barriers:** The study reveals three primary barriers impeding the widespread adoption of blockchain: (1) high costs associated with the technology and training, (2) a state of regulatory uncertainty, particularly concerning securities laws and data protection regulations like GDPR, and (3) the inadequacy of IT infrastructures in many organizations. These findings confirm **Hypothesis 3 (H3)**.
- **The Importance of Strategic Planning and Collaboration to Overcome Challenges:** Despite these barriers, the findings implicitly indicate that successful blockchain implementation critically depends on strategic factors. The successful pilot projects launched by federal agencies underscore the importance of upfront planning and phased implementation. Moreover, the regulatory and technical challenges highlight the necessity of structured collaboration among auditors, developers, and regulatory bodies. The findings, therefore, support **Hypothesis 4 (H4)**, which posits that these factors are key to mitigating adoption challenges and facilitating the effective integration of the technology.

5.2. Recommendations for Future Research

Given that blockchain is a relatively new technology, many fundamental questions remain regarding its effective integration and utilization within the internal audit context. Accordingly, this section presents a sequential list of recommendations for future researchers, aiming to guide scholarly efforts toward bridging existing knowledge gaps and exploring the full potential of this promising technology:

1. Conduct research aimed at developing unified frameworks for integrating blockchain technology with existing audit methodologies, rather than relying on fragmented solutions (Brender et al., 2018).
2. Explore how blockchain can enable continuous auditing and real-time assurance models, and analyze the resulting impact on the traditional role of the auditor.
3. Develop systematic standards and procedures for auditing smart contracts, with a focus on assessing their programming logic, security, and executability.
4. Research how blockchain can be used to automate traditional audit procedures, such as external confirmations and asset tracking, and measure the impact of this automation on efficiency and reliability.
5. Conduct in-depth studies on the unique security risks of blockchain environments (such as 51% attacks and smart contract vulnerabilities) and develop effective audit controls to mitigate them.
6. Analyze the impact of scalability challenges in blockchain networks on the performance of audit processes and propose solutions to address them.
7. Study the challenges and opportunities of interoperability between different blockchain networks and its effect on the auditor's ability to form a comprehensive view.

8. Continuously analyze the impact of evolving regulations and new legislation (such as privacy laws) on the design and use of blockchain applications in auditing.
9. Investigate the most effective ways to enhance the technical literacy of auditors and design effective educational programs to empower them to understand blockchain and cryptographic technologies.
10. Conduct research that explores mechanisms for promoting effective collaboration between auditors, technical developers, and legal experts to ensure a comprehensive understanding of the technology.
11. Conduct longitudinal studies to track and evaluate the long-term impacts of blockchain adoption on the audit profession and the quality of financial reporting.
12. Analyze the organizational and cultural factors that may hinder the adoption of blockchain technology in internal audit departments and propose effective change management strategies.
13. Work on producing research and scholarly articles that can explain blockchain technology in a simplified and accessible manner for a broader, non-specialist audience.
14. Perform more comparative case studies that evaluate blockchain applications across different sectors to identify best practices and success factors.
15. Build maturity models that help organizations assess their readiness to adopt blockchain in their audit functions and define a clear roadmap for development.

References

Arquam, M., Patel, A., & Nand, P. (2022). The security strength of Blockchain technology: A Survey Report: https://www.researchgate.net/publication/360699350_The_security_strength_of_Blockchain_technology_A_Survey_Report

The Duy, P., Thi Thu Hien, D., & Pham, V. H. (2020). A survey on Blockchain-based applications for reforming data protection, privacy and security: https://www.researchgate.net/publication/344038420_A_survey_on_Blockchain-based_applications_for_reforming_data_protection_privacy_and_security

Bansal, M. (2024). Earnings management: a three-decade analysis and future prospects. Journal of Accounting Literature, Vol.47 No.4, pp.630-670.

Álvarez-Foronda, R., De-Pablos-Heredero, C., & Rodríguez-Sánchez, J. L. (2023). Implementation model of data analytics as a tool for improving internal audit processes. Front. Psychol. 14:1140972. doi: 10.3389/fpsyg.2023.1140972

Lowenstein, M. & Cao, S. (2023). Business accounting at fengshengtai in late imperial China: is there new evidence of double-entry bookkeeping? Business History Review. cambridge.org

Saha, B., Mehedi Hasan, M., Anjum, N., Tahora, S., Siddika, A., & Shahriar, H. (2023). Protecting the Decentralized Future: An Exploration of Common Blockchain Attacks and their Countermeasures: http://dx.doi.org/10.48550/arXiv.2306.11884

Gurgu, E. (). Distributed Ledger Systems History: The Blockchain Milestones. Annals of Spiru Haret University Economic Series. researchgate.net

Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2018). Security Services Using Blockchains: A State-of-the-Art Survey: https://core.ac.uk/download/233233862.pdf.
Mansour, M., Salama, M., Helmi, H., & Mursi, M. (2024). A Survey on Blockchain in E-Government Services: Status and Challenges: https://core.ac.uk/download/233233862.pdf.
Zarrin, J., Wen Phang, H., Babu Saheer, L., & Zarrin, B. (2021). Blockchain for decentralization of internet: prospects, trends, and challenges. Cluster Computing 24, pp. 281-2866.
Kogon, J. (2017). Blockchain Technology: An Analysis of Potential Applications and Uses: https://core.ac.uk/download/212892322.pdf.
Hrouga, M. & Sbihi, A. (2023). Logistics 4.0 for supply chain performance: perspectives from a retailing case study, Business Process Management Journal, Vol. 29 No. 6, pp. 1892-1919. https://doi.org/10.1108/BPMJ-03-2023-0183.
Adere, E. M. (2022). Blockchain in healthcare and IoT: A systematic literature review. Array, Vol. 14: https://doi.org/10.1016/j.array.2022.100139.
Ortman, C. (2018). Blockchain and the Future of the Audit. CMC Senior Theses. 1983: http://scholarship.claremont.edu/cmc_theses/1983
Naderi, H., Shojaei, A., & Heydari, M. H. (2025). Automated Energy Performance Monitoring and Occupant Engagement in Buildings through Blockchain-Enabled Non-Fungible Tokens. Journal of Information Technology in Construction (ITcon), 30(7), 133-158.
Imjai, N., Swatdikun, T., Rungruang, P., Basiruddin, R., & Aujirapongpan, S. (2024). Empowering generation z accountants in the era of data complexity and open innovation: Nurturing big data analytics, diagnostic, and forensic accounting skills. Journal of Open Innovation: Technology, Market, and Complexity, 10(2), 100308. sciencedirect.com
Angeles, R. (2019). Blockchain-Based Healthcare: Three Successful Proof-of-Concept Pilots Worth Considering, Journal of International Technology and Information Management, Vol.27 No.3, Article 4: https://scholarworks.lib.csusb.edu/jitim/vol27/iss3/4
Baba, A. I., Neupane, S., Wu, F., & Yaroh, F. F. (2021). Blockchain in accounting: challenges and future prospects. International Journal of Blockchains and Cryptocurrencies, 2(1), 44-67: https://par.nsf.gov/servlets/purl/10293122.
Alexopoulos, C., Charalabidis, Y., Androutsopoulou, A., Avgerinos Loutsaris, M., & Lachana, Z. (2019). Benefits and Obstacles of Blockchain Applications in e-Government: https://core.ac.uk/download/211327481.pdf.
Jiang, L. (2024). The use of blockchain technology in enterprise financial accounting information sharing. ncbi.nlm.nih.gov
Bourveau, T., De George, E. T., Ellahie, A., & Macciocchi, D. (2022). The role of disclosure and information intermediaries in an unregulated capital market: Evidence from initial coin offerings. Journal of Accounting Research, 60(1), 129-167.
Wu, H., Yao, Q., Liu, Z., Huang, B., Zhuang, Y., Tang, H., & Liu, E. (2024). Blockchain for Finance: A Survey, IET Research Journal, pp.1-17.
Vasconcelos, A. A., Lima, M. G. B., Gardner, T. A., & McDermott, C. L. (2024). Prospects and challenges for policy convergence between the EU and China to address imported deforestation. Forest Policy and Economics, 162, 103183: https://doi.org/10.1016/j.forpol.2024.103183

Belen-Saglam, R., Altuncu, E., Lu, Y., & Li, S. (2022). A Systematic Literature Review of the Tension between the GDPR and Public Blockchain Systems: https://doi.org/10.1016/j.bcra.2023.100129

Brender, N., Gauthier, M., Morin, J. H., & Salihi, A. (2018). The Potential Impact of Blockchain Technology on Audit Practice: https://core.ac.uk/download/211326847.pdf.

Zheng, Z., Dai, H. N., & Wu, J. (2019). Blockchain Intelligence: When Blockchain Meets Artificial Intelligence: https://www.academia.edu/104935857/Blockchain_Intelligence_When_Blockchain_Meets_Artificial_Intelligence

Zenagui, B., Hadjadj, C., Chekifi M. (2024). Blockchain technology in the field of banana global supply chains Bachir, Journal of Contemporary Business and Economic Studies, Vol (07) N0. (01). pp 53-67.