applied sciences

MDPI

Article

A Blockchain-Enabled Framework for Improving the Software Audit Process

Mohammed Assiri [1,2,*] and Mamoona Humayun [3,*]

[1] Department of Computer Science, College of Sciences and Humanities, Aflaj, Prince Sattam bin Abdulaziz University, Al-Kharj 16273, Saudi Arabia
[2] Department of Software Engineering, College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Al-Kharj 16273, Saudi Arabia
[3] Department of Information Systems, College of Computer and Information Sciences, Jouf University, Al-Jouf 72388, Saudi Arabia
[*] Correspondence: m.assiri@psau.edu.sa (M.A.); mahumayun@ju.edu.sa (M.H.)

Abstract: Audits are an essential component of every organization, particularly those involving software development. In addition to several testing cycles, software auditing has become an essential software development milestone. Software auditing is a continual activity that enables a business to remain ahead of the curve and predict potential software problems. Audits, whether undertaken in-house or by external auditors, entail a significant amount of time and work. Consistent audits provide financial and economic benefits, as well as legal benefits. The most essential advantage of audits is safeguarding your system from internal and external assaults. Audit logs serve a crucial role in the auditing process; they typically capture all system operations and occurrences. They are used as evidence providers during an inquiry and by auditors to monitor the privacy and security of information and systems. Auditors confirm the accuracy of data pertaining to businesses and their activities. To determine if these acts exceed the limitations established by organizations, governments, and other parties, dependable information is essential. Infractions of such rules or corporate standards may be indicative of fraud, malpractice, risk, or inefficiency. Despite the existence of automated audit tools, audit policy, and audit logs, many audit frauds are reported on a daily basis. To make the audit process transparent and secure, this research proposes a blockchain-enabled framework SSFTA to aid software auditors in conducting a transparent and effective audit process. The proposed framework is evaluated using a case study. The findings demonstrated that the suggested framework makes the auditing process simple and transparent.

Keywords: software audit; audit logs; security; blockchain; audit frauds

check for updates

Citation: Assiri, M.; Humayun, M. A Blockchain-Enabled Framework for Improving the Software Audit Process. *Appl. Sci.* **2023**, *13*, 3437. https://doi.org/10.3390/app13063437

Academic Editor: Gianluca Lax

Received: 23 February 2023
Revised: 6 March 2023
Accepted: 7 March 2023
Published: 8 March 2023

1. Introduction

A software audit (SA) is a systematic examination of the software's design, implementation, and results in relation to predetermined criteria (such as quality, progress, or conformity with goals, standards, and laws) [1,2]. Audits of software may be performed either in-house by organizations such as development teams or by external entities. For larger audits, it may be necessary for many people to work together under the direction of a single lead auditor. In most cases, certain tools are used to collect the necessary data for a SA. Audits of functionality or security might be performed with the use of various analytic tools [3–7]. Proprietary tools may be reviewed as part of a compliance audit if and when software is sold or its status has to be confirmed. Audits are necessary for ensuring consistent software quality, removing unused licenses, optimizing corporate processes, and meeting regulatory and compliance needs [6,8,9].

There are usually two types of audits that are commonly used in software organizations: those conducted inside an organization by its staff, and those conducted by an outside party [10]. SA performed by an outside party might be helpful when in-house knowledge is lacking or when you need a second, unbiased opinion. It may also be necessary to bring in an outside auditor if your internal team is overburdened, inexperienced, or otherwise unable to complete the audit on time. Internal audits are crucial and should be conducted on a regular basis, but they frequently lack the rigor and expertise that may be provided by external specialists. Because both sorts are necessary, it is important to note that external auditors, thanks to their objectivity and thoroughness, often find more genuine concerns. As developers often do not know what to look for in terms of legal and compliance concerns, it is useful to have an outside party perform an audit of the software [11–13].

Auditing is the procedure of examining the documents and records of a software development organization for errors and discrepancies. Data stored here must accurately reflect the workings of the program and the transactions that have taken place inside it. As these files are maintained internally, there is a great potential for fraud or manipulation on the part of employees with access to them [6,14,15]. Due to the many incentives for falsifying these documents, audits are essential for ensuring accuracy. In accordance with current auditing standards, auditors must have reasonable confidence that the organization's records, when considered as a whole, are free from serious misrepresentation, whether due to simple mistakes or fraud. In order to offer a clean or qualified opinion, auditors must satisfy themselves that the financial statements of the business are free of substantial errors.

Since the audit is becoming more crucial to the stability of the software marketplaces, major efforts have been undertaken in recent years to increase its efficacy. The adoption of new auditing standards, maintaining audit records, and adopting computer-assisted audit tools and procedures are notable among the primary endeavors [16–18]. Despite all these efforts and strict regulation by the government, audit fraud persist globally. In order to make SA free from fraudulent behavior, there is a need for an end-to-end transparent system that could detect any fraudulent activity by internal or external auditors. To address this gap, this study provides a blockchain-based solution for securing the audit process from internal or external fraud. Blockchain technology (BCT) has the ability to affect all recordkeeping activities, including the initiation, processing, authorization, recording, and reporting of transactions [19–21]. When new blockchain-based methodologies and processes arise, the function and skill sets of auditors may shift. For instance, techniques for getting adequate audit evidence must consider both conventional stand-alone general ledgers and blockchain-based ledgers. In addition, reporting and accounting might benefit from improved consistency and openness, allowing for more effective data extraction and analysis. BCT may have a substantial influence on how auditors carry out their engagements. It helps in automation and data analytics. Keeping in view the importance of blockchain and some other cutting-edge technologies such as 5G and cloud, we propose a framework named smart and secure framework for transparent auditing (SSFTA). The explicit contribution of the paper is as follows:

1. Proving the detailed overview/taxonomy of the audit process, including audit types, features, principles, and steps of conducting the audit process;
2. Reviewing and evaluating the research on the influence of BCT on auditing;
3. Proposed SSFTA as a framework that would aid auditors in using 5G, Cloud, and BCT to enhance company information systems, save time, and avoid fraudulent activities during software auditing;
4. Using smart contracts and digital ledger (DTL) for transparency and accountability.

The organization of the paper is briefly elaborated in Figure 1. Table 1 provides the details of important abbreviations used in the paper.

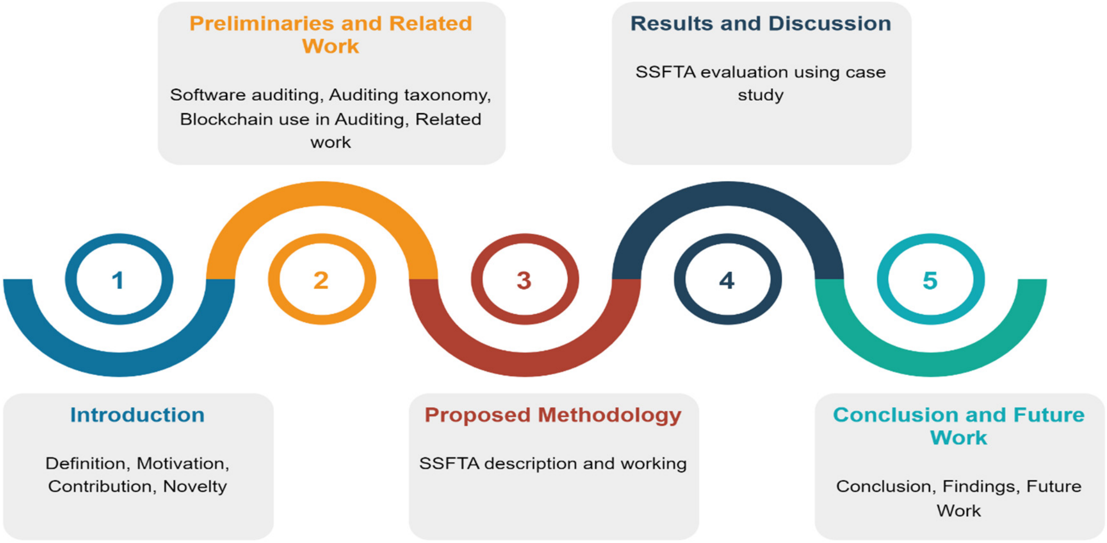
Preliminaries and Related Work
Software auditing, Auditing taxonomy, Blockchain use in Auditing, Related work
Results and Discussion
SSFTA evaluation using case study
1
2
3
4
5
Introduction
Definition, Motivation, Contribution, Novelty
Proposed Methodology
SSFTA description and working
Conclusion and Future Work
Conclusion, Findings, Future Work

Figure 1. Paper organization.

Table 1. List of acronyms and their details.

Acronyms	Used for
BCT	Blockchain technology
AI	Artificial intelligence
ML	Machine learning
SA	Software audit(s)
SSFTA	Smart and secure framework for transparent auditing
IA	Internal audit
XA	External audit
DTL	Digital ledger

2. Preliminaries and Related Work

This section will provide an overview of the audit process, BCT, and its impact on the audit process, and an overview of some existing studies to provide a state-of-the-art picture of the area under study. Figure 2 provides the taxonomy of SA to provide a general overview of the area under study.

2.1. Software Auditing

SA is the inspection of software conducted internally or by a third party to evaluate its compliance with rules and licenses, legal requirements, product quality, industry standards, and others. SA may include a wide variety of tasks. Often, they are specialized audits customized to the organization's present requirements. As mentioned before, there are two types of audits: those conducted inside an organization by its staff, and those conducted by an outside party. External SA may be helpful when a company either does not have the requisite knowledge in-house or would want a second pair of impartial eyes. An organization may also need to bring in an outside auditor if its internal staff is too swamped with work or inexperienced to complete the job properly [22,23]. Regular internal audits (IA) should be conducted, but they typically fall short of the depth and expertise that may be gained by hiring outside specialists. Both kinds of audits are necessary, but due to the objective and comprehensive nature of an external audit (XA), the majority of the issues are discovered by them. Additionally, it is beneficial to have experts outside of the development team audit the program, since the development team often lacks the expertise to check for regulatory compliance and legal difficulties [24–26]. In the below subsections, we discuss when an audit should be performed, the benefits of performing an audit, and the types of SA.

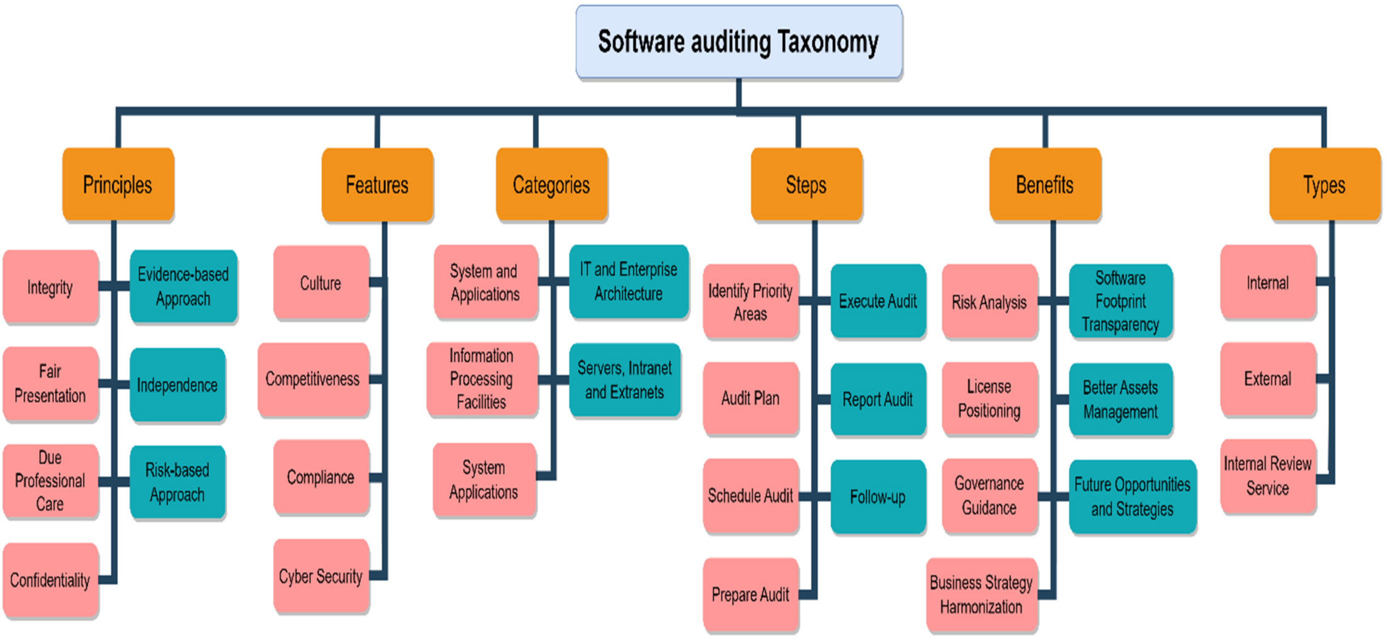

Figure 2. Software audit taxonomy.

2.1.1. When to Perform a Software Audit

SA is recommended on a regular basis, but it is especially useful in certain scenarios. Below, we discuss these scenarios.

- Doing SA on a regular basis might become a standard practice for businesses. These audits may take place once or twice a year. For instance, a project manager might initiate an audit to review the current state of the project and verify that everything is running as intended;
- One of the first places SA may be put to use is during the onboarding process for a new team. Before starting a new project, it is important to have a complete picture of the current project scenario. This may not be an exhaustive investigation into the finer points of the project, such as whether or not the necessary permits have been acquired. However, SA is an important part of the onboarding process since it might reveal hidden details about the project;
- When things are not going as planned and certain components of the program are not functioning as expected, but the root cause is unknown, an audit might be conducted. Potential issues may be discovered during an audit, and obstacles that have been preventing the project from moving forward can be removed.

2.1.2. Advantages of Doing Software Audits

There are several advantages to conducting SA. Some of the most significant are described here.

- SA aid in maintaining software quality and identifying improvement opportunities. It allows an organization to maintain all programs functioning smoothly. The audit may reveal the necessity to acquire additional technologies that may further enhance the software's quality;
- During an audit, the status of existing licenses may be determined, allowing for more efficient software use. This will guarantee that the company maximizes the use of its existing licenses. The audit will also determine whether or not the licenses are current;

- If the program needs certain proprietary tools to work effectively, it is important to undertake a comprehensive audit to determine whether the tools you want to acquire will be compatible with all the ones already existing. An audit at this point will guarantee that you acquire products that are suitable for company objectives and improve business operations;
- During the audit, it is possible to determine whether the software conforms to industry standards, and if it does not, the audit may recommend improvements that would enhance the program.

2.1.3. Types of Software Audits

SA may examine the quality, security, usability, and accessibility of the software. The type of audit required depends on the audit's objectives. Some audits may concentrate just on the quality elements, while others will examine all three mentioned facets of the product. Below, we describe the common types of SA.

Software Quality Audits

This audit, as its name indicates, evaluates the quality of the software. Auditors confirm that all apps and programs are current and operational. In addition, they seek alternatives that might replace the present instruments with those that are more effective. Software quality audits may also check the user's licensing compliance. This audit seeks to guarantee that the tools used are of the greatest quality possible. This also takes into consideration continuous technological improvements, ensuring compliance with the most recent technical requirements and decreasing the likelihood of failure in the near future. The outcome of such an audit is the discovery of quality problems and recommendations for improvements [27,28].

Software Security Audits

In this era in which cyber assaults have grown commonplace, software security is a crucial issue. It is of the utmost importance to implement cybersecurity safeguards to protect software from security breaches and harmful assaults. Such assaults may result in severe problems, such as the disclosure of a company's private and sensitive information [29]. These breaches have grave consequences and might even harm the business's image. Owing to this, organizations worldwide take all safeguards required to protect their software. They invest in digital defenses such as current antivirus and malware protection, robust firewalls, SSL-encrypted data transport, etc. The primary objective of a software security audit is to ensure that all of the business's software is safe and protected [30–32].

Usability and Accessibility Audits

User-friendliness has become a crucial need for apps. Every organization spends a considerable amount of work ensuring that its apps are extremely accessible and straightforward for the ordinary user. The greater an application's usability, the less effort a user must use in order to execute a job. Before publishing an application, it is vital to perform these checks. Typically, some changes are necessary. The application's users may find some aspects unclear or difficult to comprehend, for instance. Usability and accessibility audits guarantee the deployment of a properly functional and user-friendly product. This audit may include heuristic assessment, user walkthroughs, user flow analysis, and so on [33,34].

2.2. Blockchain Technology

A blockchain is a digital ledger (DTL) designed to record network transactions involving many participants. It is a peer-to-peer, Internet-based DTL that records all transactions that have occurred from its inception. Each participant (person or organization) utilizing the shared database is a "node" linked to the blockchain that maintains an identical copy of the DTL [35–37]. Every record in a blockchain reflects a transaction in which participants exchange value. In practice, a variety of blockchain types are being built and evaluated.

However, the majority of blockchains adhere to this overall structure and methodology. Once a user initiates a transaction between two parties, the remaining nodes in the network will verify the legitimacy of the transaction via inter-node communication according to a set protocol. A consensus algorithm describes this kind of method. After a transaction is confirmed by the network, the DTL is automatically updated across all nodes. A "block" is a group of related transactions that is added to the DTL at once. All of the distributed copies of the blocks in the chain are connected to one another because each block includes information that links back to previous blocks. New transactions with timestamps may be added by participating nodes, but once they have been confirmed and approved by the network, neither they nor any other node can remove or change them. If a node were to make a change to an older block, it would be out of sync with the rest of the network and hence removed from the blockchain.

2.2.1. Smart Contracts: Evolution of Blockchain

Among the most significant advancements in the blockchain is the incorporation of smart contracts. Smart contracts are digital agreements written in code that may be kept on a DTL and triggered when certain conditions are met. With their help, counterparties may eliminate the need for intermediaries and automate formerly tedious processes. Smart contract technology has the potential to expedite company procedures, lessen the likelihood of human mistakes in operations, and lower associated costs [38–40].

2.2.2. Blockchain Use in Auditing

To improve efficiency in accounting, BCT may be used to automate both reporting and auditing. An audit group may now receive a wide range of electronic and manual forms. Auditors must spend considerable effort on audit preparation since each audit starts with unique data and timetables. For auditing purposes, an auditor in a blockchain environment might have access to data in near real-time via the use of read-only nodes. An auditor may be able to collect the necessary data for the audit in a reliable, repeatable manner if this is the case. By digitizing auditing processes with the help of BCT, auditors can better use automation, analytics, and machine learning to do things such as instantly notifying the appropriate people of any suspicious activity. Contracts and other supporting documents might be encrypted and securely kept on or linked to a blockchain. The auditors would benefit from having access to immutable audit evidence if it allowed them to work more quickly through financial reports and audits [41–43].

Accessing information on the blockchain is projected to become more efficient as more entities and processes switch to blockchain solutions. For instance, if a sizable subset of transactions in a given industry are recorded in a blockchain, an audit team may be able to write software for doing ongoing audits of businesses that use the blockchain [38,41–43]. Several time-consuming and labor-intensive data extraction and audit preparation tasks might be avoided if this were implemented. By completing routine audits in near real-time and freeing up management and auditors to concentrate on riskier and more complicated transactions, decreased lag time presents a chance to improve auditing efficiency and effectiveness.

2.3. Related Work

In order to determine whether or not blockchain technology may be useful for performing audits, the authors of paper [35] have compiled the most important ideas from existing research. This gives the reader a solid grounding in the work that has been performed so far in the field of accounting. The study [36] performs an SLR, including content and bibliometric analyses, of the effect of BCT on auditing to spot patterns, find new avenues of inquiry, and outline a framework for future studies. This study used the Scopus database of accounting journals to analyze research performed between 2010 and 2020, and it found 40 papers that focus on the intersection of BCT and auditing. According to SLR's findings, the disruption brought about by BCT in the auditing industry is still in its infancy, and more convincing empirical investigations and the possible participation of practitioners are needed. To better accommodate digitization and the widespread use of new communications technologies, auditing practices may need to be rethought. To adjust to and successfully meet the challenge that BCT will provide to auditing, researchers need to develop new standards, guidelines, and educational opportunities.

The study [39] aims to investigate the potential applications of artificial intelligence (AI) in auditing and to examine the implications of BCT for the auditing profession. Findings suggest that AI has great potential to improve accounting and audit processes by automating routine, rule-based procedures and freeing up professionals to concentrate on higher-value, more creative endeavors. More importantly, the results of this research suggest that BCT alters the auditing process by doing away with the need for samples, confirmations, and other conventional methods of acquiring data. All of BCT's features work together to usher in a whole new age of auditing predicated on constant assurance. Current developments may provide challenges to audit files and the overall performance of an audit's judgment if they are not accounted for in professional audit standards.

Paper [41] argues that although BCT could not entirely do away with the need for auditors to evaluate transactions, it might significantly alter how such evaluations are carried out, as well as how audits of systems and financial statements are conducted. Most blockchains are built with basic control features already implemented, freeing auditors to focus on more advanced forensic auditing techniques such as analytics, automation, AI, and machine learning. The time it takes to complete the cycle of financial reporting and auditing might be greatly shortened if auditors were given permission to make use of these technological capabilities.

Paper [42] highlighted the primary concerns about competencies and expertise, risks, and obstacles in conducting internal audits (IA) while using blockchains. It provided a structure for IA implementation in smart agriculture production organizations. The paper's authors argue that this paradigm presents a formidable obstacle to the study of novel methods of internal auditing and control. Their decisions should be influenced by the need to learn more about the technology itself, the risks that could affect the company as a whole, the modifications to the company's workflow and control procedures, the augmentation of its executive and management ranks, the revision of its risk management policies, the introduction of new laws and regulations, and so on. The research results showed that a bespoke IA execution strategy is required for each individual application. If a company is serious about successfully adopting new technology, it must take steps to mitigate the dangers that come with using it, particularly if that technology will be integrated into the backbone of the operation. Each blockchain-based solution comes with its own set of advantages and dangers that must be weighed throughout the course of an organization's internal audit and control procedures. In order to manage and reduce these risks, it is vital to have a firm grasp on what factors contribute to their occurrence, to build up the required skill sets and resources, and to learn from the experiences of others.

The article [44] aims to investigate how accountants and auditors in the UAE feel about BCT. The possible benefits and drawbacks of BCT on accounting and auditing processes in the UAE were discussed in a semi-structured interview with 19 accountants, internal auditors, auditors, and risk managers. The results demonstrate the blockchain's effects on the accounting profession via its use in transaction recording, evidence storage, and offering a safe platform for conducting commercial dealings. The research adds to the current literature in many ways. First, it provides actual evidence of the impact that BCT is having on the accounting and assurance industry, expanding our understanding of the ways in which BCT might enhance the delivery of auditing and consulting services. The second aim of this study is to investigate how accountants and financial auditors in the UAE see the impact that BCT may have on their industry. Lastly, the study analyzes potential variables for the efficacy of BCT and the next obstacles to BCT.

Paper [45] argues that blockchain solutions may have significant benefits for auditing in the form of reduced auditor workload, reduced risk of fraud, and enhanced efficiency of existing processes; however, it is important to keep in mind the role that other emerging technologies may play in this area. Although firms such as Factom, Libra, and Verady are working on blockchain solutions with potential auditing applications, there is still much ground to cover. Paper [46] provides a review of the effects of BCT on accounting in general and on auditing that makes use of AI in particular. This paper explores how accounting professionals may utilize blockchain data to increase openness and confidence in their work, as well as how they can make better decisions as a result. To further our understanding of how blockchain might be used to reduce information asymmetry and strengthen stakeholder partnerships, this study interprets its results via agency theory and stakeholder theory. A summary of the difficulties and an elaboration of the reasons why certain businesses are hesitant to implement BCT are also included in the study.

Existing studies performed so far mainly explore the use of BCT for financial transactions, and they provide the challenges and suggestions associated with the use of BCT in the accounting domain. Table 2 compares previous research that has attempted to address the issue of secure and fair auditing. As can be seen from the comparison provided in Table 2, BCT has not been adequately used for auditing purposes, especially for SA. Further, most of the existing studies are review papers that highlight the challenges of using BCT in auditing domains and provide suggestions for incorporating BCT and providing training to the accountants and auditors about its benefits. To the best of our knowledge, we did not find any study that explicitly explores the usage and benefits of using BCT in SA or provides a solution for it. To fill this gap, we provide a BCT-enabled framework for improving the SA process in the upcoming section.

Table 2. Comparison of existing studies.

Ref#	Paper Contribution	Solution Provided	Research Methods Used
[35]	Compiled existing research on the use of blockchain for accountants	Agenda for future research	Review
[36]	Categorizing prior research	Agenda for future research	SLR
[39]	Explored the role of AI and BCT in auditing	Implications of AI and BCT in auditing	Review
[41]	Explored the role of AI and BCT in auditing	Identified risks and limitations of using BCT for auditing	Review
[42]	Explored the role of BCT in internal auditing and internal control	Identified risks and limitations of using BCT for auditing	Review and framework
[44]	Explored BCT's impact on accounting professions	Identified challenges of blockchain use in the accounting and assurance profession	semi-structural interview
[45]	Explored the role of BCT in auditing	Dedicate innovation teams to use BCT to facilitate the move from standard auditing to optimized auditing	Review
[46]	Explored the role of AI and BCT in auditing	Identified challenges of blockchain use in auditing and provided suggestions	Agency theory and stakeholder theory

3. Proposed Methodology

Organizations rely heavily on SA because they check to see whether a software product or process is compliant with rules, norms, and policies. In contrast, BCT may cause a major shift in the auditing and controlling industry. In this part, we propose the SSFTA framework to offer a smart and secure audit procedure, bearing in mind the significance of both audit and BCT. Figure 3 provides a pictorial overview of SSFTA. According to SSFTA, software organizations create audit policies that include remediation procedures, remediators, and policy rules where particular breaches are defined by policy regulations. When an audit scan finds a breach of a policy rule, the remediation procedure is initiated, and remediators are appointed users with the authority to address the violation. Remediators can be a single user or a group of people appointed to address security violations. These policy rules are stored in the private cloud from which authorized persons can access them. Once the policy rules are defined, they are documented using a smart contract so that they may be immutable. Once the organization decides to conduct IA or external audit (XA), these policy rules are shared with the audit team.

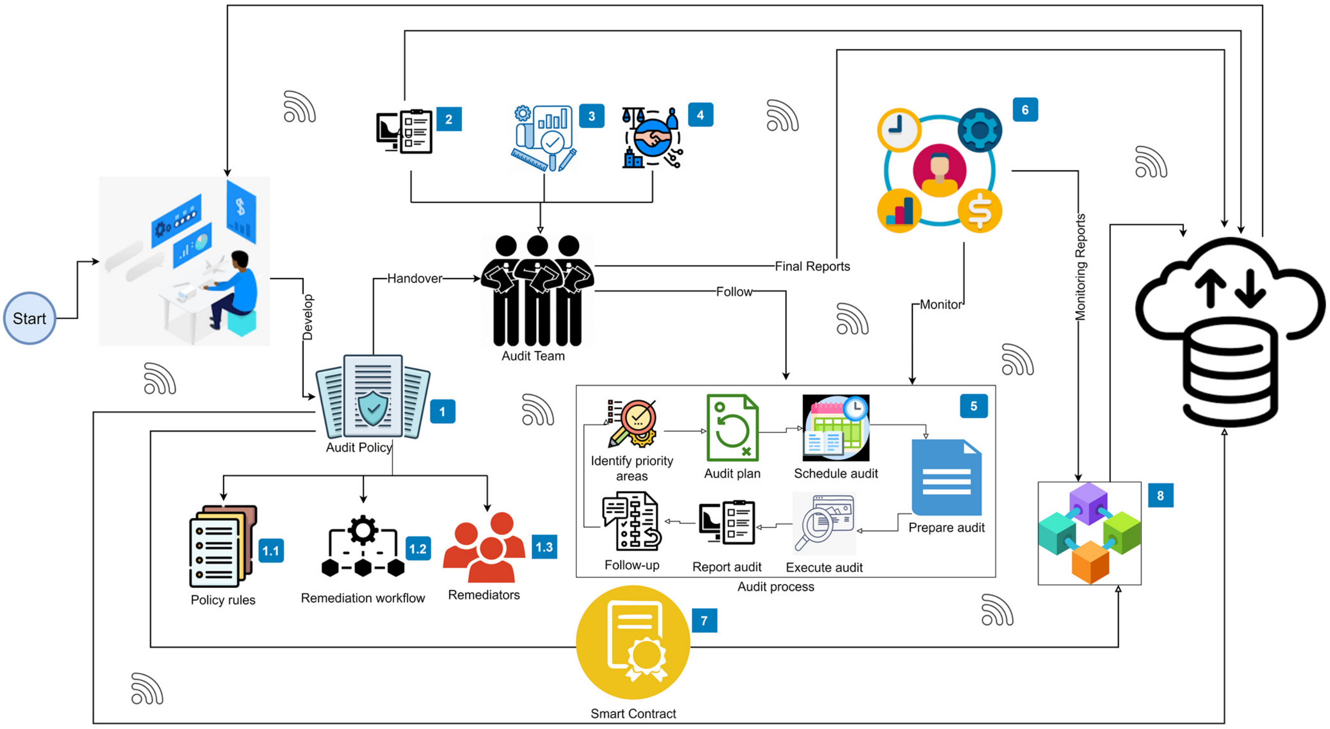

Figure 3. SSFTA: a smart and secure framework for transparent software auditing.

The organization defines the audit subject and criteria to the audit team, which is also written in the form of a smart contract and also stored in the private cloud to make it immutable and secure. The audit team collects information about the audit environment, collects audit logs, and uses automated audit tools to perform the audit process along with the manual auditing process. An audit log, sometimes referred to as an audit trail, is a record of the actions taken by the IT devices on a network in response to certain events. Event logs are recorded in audit logs and often relate to a single operation or a set of activities. They keep track of who performed an action, the action itself, and the reaction of the system. The procedures and technologies used by auditors to carry out audit processes are characterized by automation. The operational environment comprises a company's or organization's policies and processes, as well as the creation of protocols for the more efficient implementation of environmental laws and regulations. The audit team must make sure that they examine environmental compliance and implementation in great detail. After analyzing environmental parameters, getting audit logs, and selecting audit automation tools, the audit team starts the audit process by following the seven steps mentioned in SSFTA. During the audit process, the audit response team monitors the audit process and generates the monitoring reports that are stored in blockchain DTL and cloud. Once the audit process is complete, the results are stored in the cloud. The organization accesses the monitoring reports and audit results from the cloud using 5G to obtain insights into the audit result. The process of using BCT, DTL, and smart contracts is mentioned in Algorithm 1.

Algorithm 1 Audit Process using blockchain DTL and smart contract

```
Let $\mathcal{PR}$ = Policy Rules; $\mathcal{AS}$ = Audit Subject; $\mathcal{AA}$ = Audit Assignment;
$\mathcal{AC}$ = Audit Criteria; $\mathcal{IR}$ = Inherent Risks; $\mathcal{AO}$ = Audit Objectives;
$\mathcal{SO}$ = Audit Sub Objectives; $\mathcal{AM}$ = Audit Methodologies; $\mathcal{AP}$ = Audit Program;
$\mathcal{ART}$ = Audit response team; $\mathcal{AR}$ = Audit Response; $DTL$ = digital ledger

Begin
Management $\rightarrow$ Define $\mathcal{PR}$
SmartContract $\rightarrow$ $\mathcal{PR}$
Store($\mathcal{PR}$) $\rightarrow$ $DTL$
Auditors $\rightarrow$ Recieve($\mathcal{AA}$) $\leftarrow$ Management
Collect Information ($\mathcal{AS}$)
Define($\mathcal{AC}$)
SmartContract $\rightarrow$ $\mathcal{AC}$
Store($\mathcal{AC}$) $\rightarrow$ $DTL$
Classify (ProblemDomain)
Identify($\mathcal{IR}$)
$Document(\mathcal{IR})$
Refine($\mathcal{AO}$)
Refine($\mathcal{SO}$)
Identify (Control, AccessControlRisks)
Choose($\mathcal{AM}$)
AllocateBudget $\rightarrow$ $\mathcal{AM}$
Formalize ($\mathcal{AP}$)
SmartContract $\rightarrow$ $\mathcal{AP}$
Store($\mathcal{AP}$) $\rightarrow$ $DTL$
Perform ($\mathcal{AM}$)
document($\mathcal{AM}$)
SmartContract $\rightarrow$ $\mathcal{AM}$
Store($\mathcal{AM}$) $\rightarrow$ $DTL$
Conclude
Draft findings
Finalize report
FinalizeReport $\rightarrow$ $\mathcal{ART}$
$Store(FinalizeReport) \rightarrow DTL$
$\mathcal{ART}$ $\rightarrow$ Compare( InternalAudit($\mathcal{AR}$), ExternalAudit($\mathcal{AR}$))
$if$ ($\mathcal{AR}$) does not match
IdentifyGaps
Else
Send($\mathcal{AR}$) $\rightarrow$ Management
End
```

Practical Implications of the Proposed Framework

Software auditing is the process of evaluating the conformance and quality of software to verify its correctness and fairness. The audit reports must accurately reflect a software's real status and functioning. When software is created domestically, there is a considerable danger of manipulation or fraud by insiders. There are several personal motivations for these manipulations; thus, auditing is essential to guarantee that nothing is misrepresented. Traditional auditing procedures make it difficult to provide transparency. Blockchain is a DTL that enables safe, transparent, and tamper-proof transactions. It may be used in the software audit process to build confidence amongst process participants and monitor changes. The whole software audit process, from audit planning to audit report creation, may be recorded using blockchain technology. The blockchain gives visibility over who made what modifications, when, how those changes were made, and where those finished changes went. This ensures that everyone participating in the process is informed of any changes or updates, preventing disagreements or misunderstandings. The advantages of using blockchain in software auditing include enhanced security, shorter project completion times owing to less paperwork, and more precision due to immutable data. The proposed framework not only uses BCT, but rather it also leverages the potentials of 5G and clouds for efficient data storage and transmission. To make the audit process transparent, everything is documented using DTL and smart contract; further, the role of the audit response and monitoring team is also highlighted to ensure the security and transparency of the whole process.

Further, the conventional type of audit evidence, which was proof produced by the firm or based on papers from outside sources, will be evolved into information that is communicated, processed, kept, or retrieved electronically using SSFTA. Technologies such as cloud computing, 5G, and blockchain used in SSFTA allow auditors to extract and evaluate the whole accounting data without the requirement for sampling in the big data environment of today. The dependability of this method is substantially greater than manual data collection because of automated data extraction. Blockchain also has the potential to improve the reliability of the evidence. Aggregating information will no longer be necessary since blockchain can store audit proof from many sources. Sampling is another stage of the audit process that has been modified by blockchain. Data analytics and storage are used to examine whole data sets rather than simply samples picked by auditors. With the continual sharing of data across 5G and the cloud, an effective internal control environment is produced. The audit process using SSFTA will be evolved from being utilized for testing and exams toward being a preventative one. Using the proposed SSFTA, the position of the auditor will be changed from one assurance to one of strategic partners and counselors.

4. Results and Discussion

Confidence and well-informed software marketplaces depend on audit reports that are both thorough and accurate. While audit findings contribute to successful root cause analysis, future planning, generating recommendations, and many more, it is crucial that audit quality and consistency of execution be improved to preserve trust in the independent assurance they provide. Both quantitative and qualitative approaches to audit process executions have flaws that are somewhat offset by the other's benefits. Quantitative evaluation of the audit process lends itself well to establishing cause-and-effect relationships, testing hypotheses, and determining the opinions, attitudes, and practices of a large population, whereas qualitative evaluation of the audit process lends itself well to developing hypotheses and theories and describing processes such as decision making and communication. Quantitative research creates factual, trustworthy result data that are typically generalizable to wider groups, while qualitative research generates rich, comprehensive, and valid process data based on the participant's viewpoints and interpretations rather than the investigator's. In this study, the qualitative approach was chosen for the evaluation of SSFTA due to several reasons: the majority of existing studies focus on financial audits, whereas there are few studies on software audits; since the software is developed for and by humans, the qualitative approach provides more insight into the proposed software audit process. Furthermore, qualitative approaches investigate the limits and flaws of a process more thoroughly. They provide a deeper comprehension of the richness and diversity of human experience in all-natural contexts. We used a case study as a qualitative assessment method for the SSFTA evaluation. A case study is a research method used to develop a comprehensive, multifaceted knowledge of a complicated subject in its real-world setting.

In order to evaluate the proposed methodology, we conducted a case study with a well-known software industry. The subject organization is a market leader in the software industry. It commenced operations in 1977. The organization has competence in a wide range of software solutions and IT services. Digital commerce, application development and integration, business applications, cloud services, data analysis and management, application development and integration, IT infrastructure, and business process outsourcing are among their areas of specialization. An online appointment was scheduled with the company through some reference. In this online session, we elaborated on the working and potentials of SSFTA to the participants. In the end, they were requested to fill out a questionnaire to evaluate the SSFTA based on three key parameters, namely, ease of use, security, and structure of SSFTA. The questionnaire consists of three sections. Section one includes a detailed description of SSFTA. Section two was related to the demographics of respondents, and section three consisted of questions related to the three measurement parameters mentioned above. The respondents were asked to provide their feedback about SSFTA on a Likert scale as follows: Strongly Agree = 5, Agree = 4, Neutral = 3, Disagree = 2, and Strongly Disagree = 1. The 12 representatives from the organization participated in the questionnaire, and the total and average of the strongly agree and agree was calculated. Below we discuss the details of responses against each parameter.

Table 3 shows the questions that were asked by the respondents to evaluate the usability and ease of use of the SSFT. The respondents were asked to answer these questions using the Likert scale. Once all the responses were performed, the total of strongly agree and agree was calculated. A total of 70% was set as a threshold value, which means if 8 out of 12 respondents agree on a certain question, quality exists in the SSFT.

Table 3. The questions to evaluate SSFTA ease of learning.

Ease of Learning
It is easy to understand the end-to-end process of software audit from *SSFTA*
It is easy to understand the role of BCT/DTL and smart contracts in managing software audit
It is easy to use SSFTA to assess the role of 5G and the cloud for software audit
Each individual practice mentioned in SSFTA is easy to understand and unambiguous
Some training is required before using SSFTA
SSFTA is general and can be applied to most software companies for auditing

Figure 4 shows the statistics of respondents for each question related to ease of use. Most of the questions were ranked more than 8, which shows that SSFTA is easy to use for a software audit.

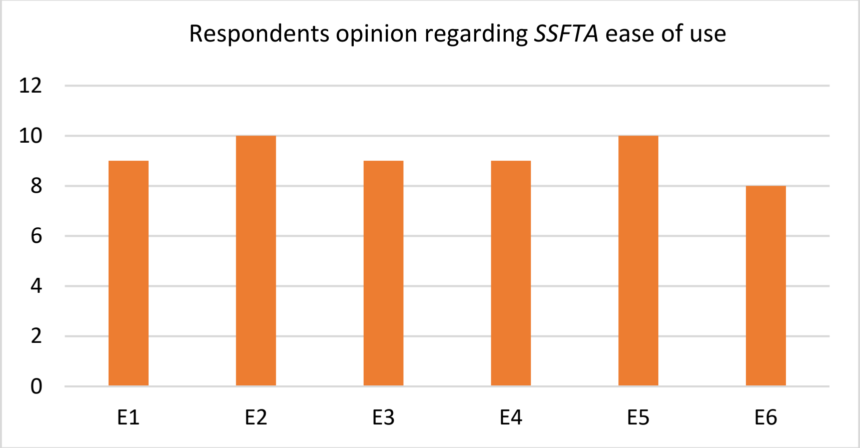

Figure 4. The evaluation of SSFTA for usability and ease of use.

Table 4 includes the four questions that were asked of the respondents to evaluate the security of SSFTA. The respondents' evaluation of the questions related to SSFTA security is depicted in the graph of Figure 5.

According to Figure 5, the total percentage of agreement was more than the threshold value for each question related to the security of the software audit process while using SSFTA. This shows that SSFTA is helpful in preventing software from audit fraud.

Table 5 lists three questions that were used to evaluate the structure of SSFTA. These questions aimed to evaluate whether the structure of SSFTA is self-explanatory and applicable.

Table 4. The questions to evaluate SSFTA secure auditing characteristics.

Secure Auditing
Using SSFTA will make the audit process transparent and secure
Using SSFTA would identify strong and weak areas in the company regarding secure software auditing
The use of BCT/DTL and smart contract in SSFTA helps to prevent audit fraud
Using SSFTA would improve our secure software audit processes

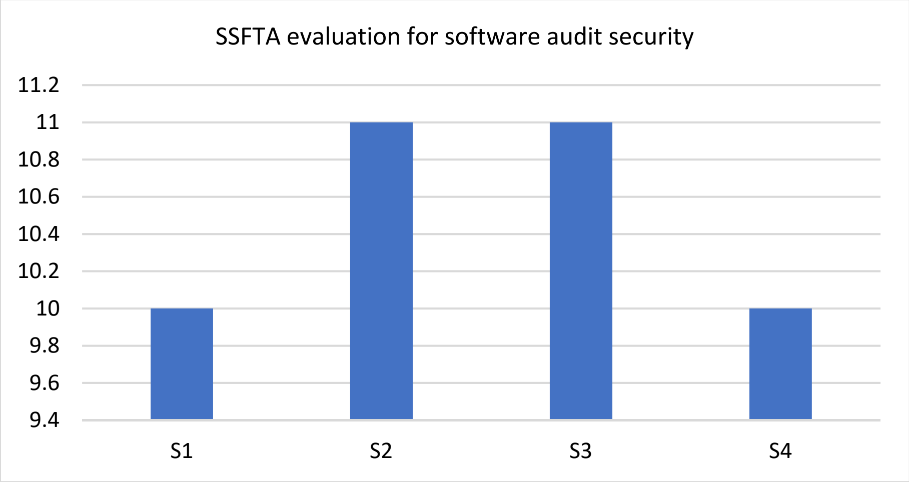

Figure 5. SSFTA evaluation for the security of software audit.

Table 5. The questions to evaluate the SSFTA structure.

The Structure of SSFTA
SSFTA is self-explanatory and needs no further explanation for its efficient use
The process mentioned in SSFTA is practical and applicable in the software industry
SSFTA covers the end-to-end software audit process and the use of the latest tools and technologies

Figure 6 depicts the respondents' evaluation regarding the structure of SSFTA. The results of Figure 6 show that SSFTA is self-explanatory, applicable in real software settings, and uses the latest tools and technologies for software auditing.

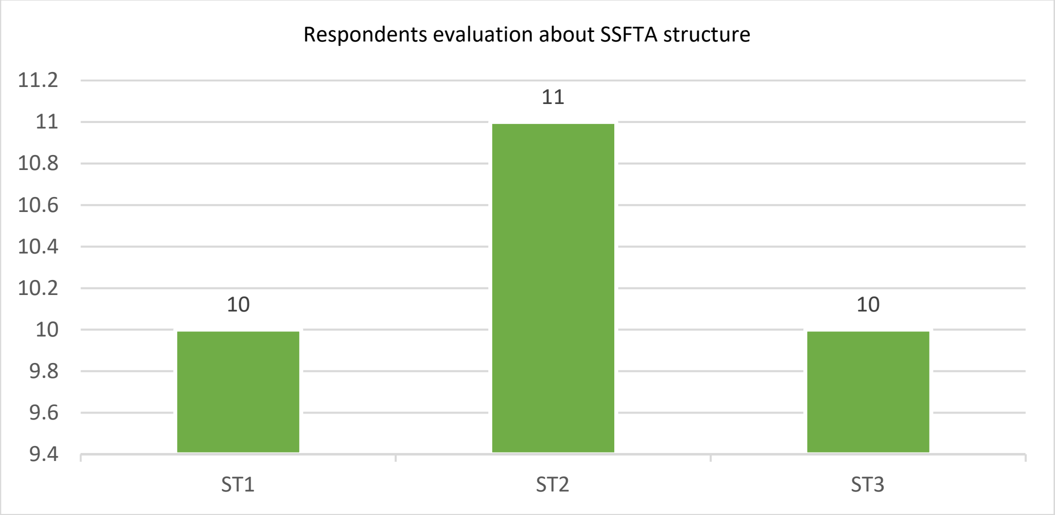

Figure 6. Evaluation of SSFTA structure.

a. Comparison with existing studies

Now, BCT has expanded well beyond bitcoin and is being tried out in a variety of corporate and financial contexts. However, a major obstacle to blockchain's disruptive potential is that the technology is still in its infancy and has not been demonstrated at the business size. Several accounting firms have launched blockchain projects to learn more about the potential of this technology, yet only a select number have used it in their audits. Much of the current research, as shown in Table 2, just investigate the possibilities and identifies the difficulties of using BCT in auditing. Moreover, not a single one of these investigations is dedicated to software audit rather than financial transaction audit. In addition, the proposed remedies in these studies are only suggestions and have not been subjected to any kind of empirical testing. The current studies on how BCT is used in auditing only use BCT to make the auditing process easier. They do not look at how other cutting-edge technologies could be used. Our proposed work is different from what has already been performed in many ways: First, it looks at the role of BCT in the process of auditing software. Second, SSFTA offers a complete auditing process with efficient ways to store, send, and protect audit data. SSFTA uses the power of 5G, cloud computing, and BCT to make the auditing process speedy and transparent.

b. Weaknesses and limitations of the proposed methodology
Following are the limitations and weaknesses of the proposed methodology

1. We did not find enough studies on software audit using blockchain, so it was difficult to find the parameters based on which proposed framework SSFTA may be compared with existing research
2. Blockchain technology is still new and has not been tested on a large scale yet, which is a big problem for its potential to change the world. Therefore, to implement SSFTA in real settings, much training and organizational support are required.
3. The proposed framework was evaluated using a case study with 12 respondents only (although the sample was representative), which is a small sample, and results cannot be fully generalized for the whole population.
4. Organizations need enough resources to implement the proposed framework.

c. Reliability of obtained observations

Targeting a sizable population was challenging because of the lack of adoption and understanding of blockchain technology in the healthcare industry. Nonetheless, we choose a representative sample to guarantee the accuracy of the results. To learn more about a certain population and make in-depth observations about it, a representative sample is one method that may be employed. A representative sample is a tiny subgroup group that aims to proportionately reflect defined traits demonstrated in a target population [47,48]. In order to ensure that our sample is representative of the whole, we asked the company in question to include members of the quality assurance/quality control team and the software audit team in our online session and survey evaluations. Twelve professionals with at least five years of expertise in quality assurance or software testing were surveyed and participated in an online session.

5. Conclusions and Future Work

BCT is already being discussed as one of the next megatrends. Researchers and organizations are beginning to comprehend the potential advantages of this technology and are investigating how its numerous uses might disrupt our current reality. The capacity to transfer BCT from idea to acceptance and manufacturing, however, has been limited so far. When it comes to auditing, BCT might provide significant advantages by lowering auditors' labor, minimizing fraud, and optimizing current procedures; nevertheless, little research has been conducted in this area. Current research on the use of blockchain technology in auditing focuses mostly on the auditing of financial transactions and the use of BCT to optimize the auditing process. We were unable to locate any research evaluating the usage of BCT in software audits. To address this deficiency, we suggested the SSFTA blockchain-enabled framework to investigate the function of BCT in software audits. A case study was conducted to assess the usability, security, and structure of SSFTA. The questionnaire was created to collect experts' opinions on SSFTA, and the findings indicate that the proposed framework provides an end-to-end simple, secure, and transparent software auditing procedure.

In the future, we are planning to perform a survey with diverse and vast software experts to better evaluate the applicability of the proposed framework.

Author Contributions: Formal analysis, M.A. and M.H.; Funding acquisition, M.A.; Methodology, M.A. and M.H.; Writing—original draft, M.H.; Writing—review and editing, M.H. All authors have read and agreed to the published version of the manuscript.

Funding: This project was supported by the Deanship of Scientific Research at Prince Sattam bin Abdulaziz University under research project # (PSAU-2022/01/19836).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Li, H.; Dai, J.; Gershberg, T.; Vasarhelyi, M.A. Understanding usage and value of audit analytics for internal auditors: An organizational approach. *Int. J. Account. Inf. Syst.* **2018**, *28*, 59–76. [CrossRef]
2. Adamyk, O.; Adamyk, B.; Khorunzhak, N. Auditing of the software of computer accounting system. In Proceedings of the 14th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer, Kyiv, Ukraine, 14–17 May 2018; pp. 251–262.
3. Moffitt, K.C.; Rozario, A.M.; Vasarhelyi, M.A. Robotic process automation for auditing. *J. Emerg. Technol. Account.* **2018**, *15*, 1–10. [CrossRef]
4. Omoteso, K. The application of artificial intelligence in auditing: Looking back to the future. *Expert Syst. Appl.* **2012**, *39*, 8490–8495. [CrossRef]
5. Curtis, M.B.; Payne, E.A. Modeling voluntary CAAT utilization decisions in auditing. *Manag. Audit. J.* **2014**, *29*, 304–326. [CrossRef]
6. Bradford, M.; Henderson, D.; Baxter, R.J.; Navarro, P. Using generalized audit software to detect material misstatements, control deficiencies and fraud: How financial and IT auditors perceive net audit benefits. *Manag. Audit. J.* **2020**, *35*, 521–547. [CrossRef]
7. Ahmi, A.; Kent, S. The utilisation of generalized audit software (GAS) by external auditors. *Manag. Audit. J.* **2012**, *28*, 88–113. [CrossRef]
8. Pham, Q.T.; Truong, T.H.D.; Ho, X.T.; Nguyen, Q.T. The role of supervisory mechanisms in improving financial reporting quality by Vietnam public non-business unit. *Cogent Bus. Manag.* **2022**, *9*, 2112538. [CrossRef]
9. Mökander, J.; Axente, M. Ethics-based auditing of automated decision-making systems: Intervention points and policy implications. *AI Soc.* **2021**, *38*, 153–171. [CrossRef]
10. Christ, M.H.; Eulerich, M.; Krane, R.; Wood, D.A. New frontiers for internal audit research. *Account. Perspect.* **2021**, *20*, 449–475. [CrossRef]
11. Al-ahdal, W.M.; Hashim, H.A. Impact of audit committee characteristics and external audit quality on firm performance: Evidence from India. *Corp. Gov. Int. J. Bus. Soc.* **2022**, *22*, 424–445. [CrossRef]
12. Boskou, G.; Kirkos, E.; Spathis, C. Classifying internal audit quality using textual analysis: The case of auditor selection. *Manag. Audit. J.* **2019**, *34*, 924–950. [CrossRef]
13. Krichene, A.; Baklouti, E. Internal audit quality: Perceptions of Tunisian internal auditors an explanatory research. *J. Financ. Rep. Account.* **2021**, *19*, 28–54. [CrossRef]
14. Kaban, I. Central Audit Activities as a Continuous Audit Approach in the Turkish Banking Sector: A Case Study about Frauds in Savings Accounts. *Öneri Derg.* **2020**, *15*, 254–275. [CrossRef]
15. Zakiah, A.N.; Agustini, D.; Twinarti, X. Application of Accounting Information System to Auditor Responsibility in Fraud Prevention. *ASEAN J. Econ. Econ. Educ.* **2022**, *1*, 19–26.
16. Awuah, B.; Onumah, J.M.; Duho, K.C.T. Determinants of adoption of computer-assisted audit tools and techniques among internal audit units in Ghana. *Electron. J. Inf. Syst. Dev. Ctries.* **2022**, *88*, e12203. [CrossRef]
17. Siew, E.-G.; Rosli, K.; Yeow, P.H. Organizational and environmental influences in the adoption of computer-assisted audit tools and techniques (CAATTs) by audit firms in Malaysia. *Int. J. Account. Inf. Syst.* **2020**, *36*, 100445. [CrossRef]

18. Al-Okaily, M.; Alqudah, H.M.; Al-Qudah, A.A.; Alkhwaldi, A.F. Examining the critical factors of computer-assisted audit tools and techniques adoption in the post-COVID-19 period: Internal auditors perspective. *VINE J. Inf. Knowl. Manag. Syst.* **2022**. [CrossRef]
19. Hu, Q.; Asghar, M.R.; Zeadally, S. Blockchain-based public ecosystem for auditing security of software applications. *Computing* **2021**, *103*, 2643–2665. [CrossRef]
20. Humayun, M. Industrial revolution 5.0 and the role of cutting edge technologies. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*. [CrossRef]
21. Humayun, M.; Jhanjhi, N.Z.; Niazi, M.; Amsaad, F.; Masood, I. Securing drug distribution systems from tampering using blockchain. *Electronics* **2022**, *11*, 1195. [CrossRef]
22. Pedrosa, I.; Costa, C.J.; Aparicio, M. Determinants adoption of computer-assisted auditing tools (CAATs). *Cogn. Technol. Work* **2020**, *22*, 565–583. [CrossRef]
23. Smidt, L.; Ahmi, A.; Steenkamp, L.; Van der Nest, D.; Lubbe, D. A Maturity-level Assessment of Generalised Audit Software: Internal Audit Functions in Australia. *Aust. Account. Rev.* **2019**, *29*, 516–531. [CrossRef]
24. Holt, T.P.; Loraas, T.M. Using Qualtrics panels to source external auditors: A replication study. *J. Inf. Syst.* **2019**, *33*, 29–41. [CrossRef]
25. Čular, M.; Slapničar, S.; Vuko, T. The effect of internal auditors' engagement in risk management consulting on external auditors' reliance decision. *Eur. Account. Rev.* **2020**, *29*, 999–1020. [CrossRef]
26. Balios, D.; Kotsilaras, P.; Eriotis, N.; Vasiliou, D. Big data, data analytics and external auditing. *J. Mod. Account. Audit.* **2020**, *16*, 211–219.
27. Mkoba, E.; Marnewick, C. Conceptual framework for auditing agile projects. *IEEE Access* **2020**, *8*, 126460–126476. [CrossRef]
28. Thottoli, M.M.; Thomas, K.; Ahmed, E.R. Qualitative analysis on information communication technology and auditing practices of accounting professionals. *J. Inf. Comput. Sci.* **2019**, *9*, 529–537.
29. Humayun, M.; Niazi, M.; Almufareh, M.F.; Jhanjhi, N.; Mahmood, S.; Alshayeb, M. Software-as-a-Service Security Challenges and Best Practices: A Multivocal Literature Review. *Appl. Sci.* **2022**, *12*, 3953. [CrossRef]
30. Marín-López, A.; Chica-Manjarrez, S.; Arroyo, D.; Almenares-Mendoza, F.; Díaz-Sánchez, D. Security information sharing in smart grids: Persisting security audits to the blockchain. *Electronics* **2020**, *9*, 1865. [CrossRef]
31. Schreiber, A.; Sonnekalb, T.; Heinze, T.S.; von Kurnatowski, L.; Gonzalez-Barahona, J.M.; Packer, H. Provenance-based security audits and its application to COVID-19 contact tracing apps. In Proceedings of the Provenance and Annotation of Data and Processes: 8th and 9th International Provenance and Annotation Workshop, IPAW 2020 + IPAW 2021, Virtual, 19–22 July 2021; Proceedings 8. pp. 88–105.
32. Husain, T. An analysis of modeling audit quality measurement based on decision support systems (DSS). *Measurement* **2019**, *275*, 310–326.
33. Auda, R.; Subriadi, A.; Tjahyanto, A.; Wulandari, A. Measuring software quality with usability, efficiency, and portability characteristics. *IOP Conf. Ser. Earth Environ. Sci.* **2021**, *704*, 012039.
34. García-Berná, J.A.; Sobrino-Duque, R.; Carrillo de Gea, J.M.; Nicolás, J.; Fernández-Alemán, J.L. Automated Workflow for Usability Audits in the PHR Realm. *Int. J. Environ. Res. Public Health* **2022**, *19*, 8947. [CrossRef] [PubMed]
35. Bonyuet, D. Overview and impact of blockchain on auditing. *Int. J. Digit. Account. Res.* **2020**, *20*, 31–43. [CrossRef] [PubMed]
36. Lombardi, R.; de Villiers, C.; Moscariello, N.; Pizzo, M. The disruption of blockchain in auditing–a systematic literature review and an agenda for future research. *Account. Audit. Account. J.* **2022**, *35*, 1534–1565. [CrossRef]
37. Gajendran, N. Blockchain-Based secure framework for elearning during COVID-19. *Indian J. Sci. Technol.* **2020**, *13*, 1328–1341.
38. Rozario, A.M.; Thomas, C. Reengineering the audit with blockchain and smart contracts. *J. Emerg. Technol. Account.* **2019**, *16*, 21–35. [CrossRef]
39. Zemánková, A. Artificial intelligence and blockchain in audit and accounting: Literature review. *Wseas Trans. Bus. Econ.* **2019**, *16*, 568–581.
40. Bonsón, E.; Bednárová, M. Blockchain and its implications for accounting and auditing. *Meditari Account. Res.* **2019**, *27*, 725–740. [CrossRef]
41. Cangemi, M.P.; Brennan, G. Blockchain auditing–accelerating the need for automated audits! *EDPACS* **2019**, *59*, 1–11. [CrossRef]
42. Popchev, I.; Radeva, I.; Velichkova, V. The impact of blockchain on internal audit. In Proceedings of the 2021 Big Data, Knowledge and Control Systems Engineering (BdKCSE), Sofia, Bulgaria, 28–29 October 2021; pp. 1–8.
43. Popchev, I.; Radeva, I.; Velichkova, V. Auditing blockchain smart contracts. In Proceedings of the 2022 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 6–8 October 2022; pp. 276–281.
44. Abdennadher, S.; Grassa, R.; Abdulla, H.; Alfalasi, A. The effects of blockchain technology on the accounting and assurance profession in the UAE: An exploratory study. *J. Financ. Rep. Account.* **2022**, *20*, 53–71. [CrossRef]
45. Abreu, P.W.; Aparicio, M.; Costa, C.J. Blockchain technology in the auditing environment. In Proceedings of the 2018 13th Iberian Conference on Information Systems and Technologies (CISTI), Caceres, Spain, 13–16 June 2018; pp. 1–6.
46. Han, H.; Shiwakoti, R.K.; Jarvis, R.; Mordi, C.; Botchie, D. Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. *Int. J. Account. Inf. Syst.* **2023**, *48*, 100598. [CrossRef]

47. De Mello, R.M.; Travassos, G.H. September. Surveys in software engineering: Identifying representative samples. In Proceedings of the 10th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement, Ciudad Real, Spain, 8–9 September 2016; pp. 1–6.
48. Baltes, S.; Ralph, P. Sampling in software engineering research: A critical review and guidelines. *Empir. Softw. Eng.* **2022**, *27*, 94. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.