Blockchain Technologies for Secure Multi-Tier Distributed Computing: A Comprehensive Survey

Shervin Sajadi
Department of Computer Engineering, University of Kurdistan, Sanandaj, Iran

Abstract

Multi-tier distributed computing is the key to solving the problem of high focus on complex mathematical operation problems that run through various layers. Despite this, the whole system is still insecure owing to the many types of threats that may be encountered such as data tampering, access to unauthorized persons, and distrust among the different layers. Getting defense in this manner from the traditional security solutions is not a guarantee to protect secure with a consistent transit time and jitter and scalable performance, and restricting access to the potential threat. In this case, the name of the technology is "agreed" and among these are the blockchain technologies, "society" with sceptics and non-believers, etc. At the same time, the coin that people doubt the most is known. This has brought about trust issues in the multi-tier architecture domain, which is addressed at last with blockchain.

The provided paper is to review other works in the literature on the blockchain topic as to the application of the blockchain technology used for secure network systems. We will classify the existing research into three main categories: direct use, where blockchain has been actively implemented; indirect use, where its potential has been studied but not deployed; and without implementation, focusing on theoretical perspectives. Our study sheds light on the fact that blockchain effectively plays the roles of data integrity preservation and single points of failures removal, and severe transparency. However, scalability, computational costs, and integration challenges are still prominent issues that obstruct its wide-ranging usage.

Keywords: Blockchain, Multi-Tier Distributed Computing, Security, Distributed Ledger Technology (DLT), Trust Management, Internet of Things (IoT).

۱. Introduction

Multi-tier distributed computing has appeared as a common strategy in the work distribution of modern computers, so that it is natural to distribute complex workloads among many processes known as multi-tier distributed computing. It is being increasingly used in cloud computing, edge computing, and the enterprise-scale architecture that is the technology in which the computation is divided into several levels of optimal performance, resource distribution, and scalability. Owing to the fact that multi-tier distributed computing is more advantageous in all aspects, security assurance remains one of the main challenges. Unauthorized access, data tampering, trust management, and single points of failure are the most popular concerns among hackers who use automated systems to attack those systems. common security elements such as central authentication, role-based access control, and cryptographic encryption are just the first step in the long road towards full safety in the end. They will still have to face the problem of bringing new problems, such as scalability limitations, efficiency overhead, and vulnerability to internal threats. Moreover, due to the decentralization and dynamics of multi-tier systems, the security system must be strong, transparent, and trust-extending without its effectiveness being jeopardized. Blockchain has arrived as a futuristic solution for alleviating the security threats in this area. Is it a decentralized system with cryptographic security and immutability, blockchain becomes a platform for secure data sharing, authentication of identity within decentralized systems, and production of tamper-evident audit logs in the distributed systems. As the blockchain becomes more advanced and functional, it will one day make single points of failure things of the past, thereby increasing trust and transparency. In the present paper, the phenomena of blockchain technologies in multi-tier secured computation are represented. In this way, we divide the existing approaches of research into three types:

- ✓ **Direct Use**: This is a kind of study that creates some form of the common blockchain security per multi-tier distributed computing.
- ✓ **Indirect Use**: A study that describes the possibility and usefulness of blockchain in theory while it is not really implemented.
- ✓ **Non-Implementation**: The theoretical-simulated research is what can be made with blockchain using multilevel computing in secure the system but not based on real data.

The objective of this survey is to explore the role of blockchain towards security in multi-tier distributed computing, identify the prevailing challenges and obstructions, and recommend future research direction. Organizing existing literature and analyzing the merits and limitations of blockchain in this field, this paper can hopefully provide a systematic overview that can serve as the foundation for possible future studies and application.

۲. Background & Key Concepts

This section is an introduction to the base ideas prevailing in multi-tier distributed computing, secure blockchain control of, and the coming of blockchain to multi-tier distributed systems, respectively. Basics of these concepts are necessary for checking how blockchain effects the security and functionality of distributed computing systems.

۲,۱ Multi-Tier Distributed Computing

Definition, Applications, Benefits, and Challenges: The concept of multi-tier distributed computing is the one in which computing work and data processing are spread across a network of many layers. The functionality of these layers can be edge devices, fog nodes, cloud servers, and decentralized networks that is all coordinated to provide effective processing, storage, and communication. Multi-tier computing is employed in the following areas:

- Cloud and Edge Computing: Processing is split between edge devices and the cloud servers to reduce latency.
- IoT Networks: Sensor data may be processed in multiple tiers before it is sent to the centralized system.
- Enterprise Systems: The databases, business logic, and user interfaces are handled independently through the deployment of multi-layer structures.
- Smart Cities and Autonomous Systems: The multi-tier structures are utilized on a large scale network for real-time data processing and analysis of data collected from a wide array of sources.

Advantages of Multi-Tier Distributed Computing:

- Scalability: The systems are able to handle the increasing amount of data with ease by transferring workload on different layers.
- Resource Optimization: One of the strategies to offloading the task is to avoid using a single central server instead of multiple intermediary nodes that does the job (like fog or edge computing).
- Performance Improvement: This technique reduces latency and thus the system gives a quicker response.
- Fault Tolerance: By the time one layer fails the others already continue to work, which is fault-tolerant.

۲,۲ Blockchain and Security: Consensus Mechanisms, Smart Contracts, and Cryptography

The blockchain, by being decentralized, immutable, and cryptographically sealed, represents an ideal infrastructure that ensures data accuracy, transparency, and the conduct of trust in a multiple-node network environment. These

intrinsic qualities of blockchain fortify its status as the right candidate solution for the protection of multi-tier computing systems.

Key Components of Blockchain for Security:

- Consensus Mechanisms: Build trust in a decentralized environment. The main consensus type include:
- Proof of Work (PoW): A Bitcoin option of conducting the cryptographic computations across the participants but with high energy demands.
- Proof of Stake (PoS): Thus the currency amount used to purchase a coin is what defines token ownership in the said system thereby reducing the energy footprints because this prevents the excessive use of slower but more energy-efficient solutions.
- Byzantine Fault Tolerance (BFT): Comes with faster finality and usage in blockchains like Hyperledger Fabric which is permissioned in nature.

The concept of secure access control is usually coupled with the smart contracts that are used for automatic transactions and the identity authentication in multi-tier computing.

- Cryptographic Techniques:
- Public-Key Cryptography: This method, a system to authenticate secure transactions along with encryption, is the leading technology used by blockchain to execute private transactions in the era of financial inclusion.
- Merkle Trees: They need to be efficiently performing and strong in setting data verification correctly among system layers.
- Zero-Knowledge Proofs (ZKP): Are the cryptographic system, which helps the user to verify himself without showing the sensitive information.

Blockchain security measures not only deal with the inherent shortcomings of the traditional multi-tier distributed computing but also regrettably bring some new ones along, mainly in the scalability and integration scope.

۲,۳ Importance of Blockchain Integration with Multi-Tier Distributed Computing

The integration of blockchain with multi-tier computing systems has its positives regarding the safety of it, however, it is also a deal with it.

Potential Strengths:

- Decentralized Trust Model: The system of having no central authorities brings down the obstacles that arise from a single point of failure. This will ensure that the voting process is not only secure but also more reliable.
- Immutable Data Storage: The data is written in one peace and cannot be changed or deleted which means that it is easier to be audited.
- Secure Data Transmission: Cryptographic protocols guarantee confidentiality and integrity between the tiers of computing.

Potential Weaknesses and Open Challenges:

- High Computational Overhead: PoW and other consensus algorithms introduce latency and high energy consumption, which may be unsuitable for real-time processing.
- Interoperability Issues: The majority of multi-tier systems are developed over heterogeneous platforms, and blockchain integration is difficult.
- Regulatory and Compliance Issues: The difference as to whether blockchain networks are of permissioned or permissionless type creates challenges such as legal and governance for enterprise applications.

Blockchain is a powerful but very intricate way to secure multi-tier distributed computing. Even though, at its heart, it is about trust, integrity, and security, the scope of these problems, in fact, are computational limitations, interoperability issues, and scalability issues that should be dealt with at all costs. The article is about the way blockchain is used in two or more tier computing using the data from previous research, and dividing the works by means of direct use, indirect use, and theoretical discussion.

۳. Methodology for Categorization

A systematic and regular approach is recommended to this respect, including a review of blockchain technology adoption within secure multi-tier distributed computation. In this way, we place those studies into one of three categories: Direct Use, Indirect Use, and Without Implementation. This enables us to figure out the different ways in which QR has been used in multi-tier computing scenarios and spot research gaps that have to be explored.

۳,۱ Selection Criteria and Sources of Data

The scientific papers presented in this survey were obtained from peer-reviewed scientific databases, including IEEE Xplore, ACM Digital Library, ScienceDirect, Springer, and Google Scholar. The selection criteria applied are as follows:

Topic Relevance: Blockchain's aim is to improve the security, trust, and data integrity in a distributed computing environment at the multi-tier level.

Peer-Reviewed Conference or Journal Publication: Only the best pieces of important articles from authoritative sources were analyzed.
Implementation Focus: The papers were classified depending on the level of blockchain implementation—whether their technology was implemented, it was studied conceptually or just talked about philosophically.
Recent Work (2018-2024): Because of the speed of blockchain innovation, mostly the newest papers but also some basis papers were considered.

۳,۲ Categorization of Study

On the basis of blockchain deployment flexibility, studies were grouped into the following three categories:

A. Direct Use (Deployed Blockchain Solutions)

The articles under this type of research were the ones that extensively used blockchain technology right from the beginning at several distributed system levels. They usually were practical models, field implementations, or experimental results proved how blockchain can be used to increase the security and efficiency of the system. Examples of Direct Use Studies: Block-based authentication and access control was introduced as a service in the cloud-edge computing environment.Applying a blockchain solution to the security of cloud-resource by implementing security policies over multiple tiers. Developing a blockchain-based audit trail system to ensure the integrity of data in the distributed systems. This section presents the actual experiences and introspective analysis on blockchain for multi-tier architecture.

B. Indirect Use (Exploratory & Feasibility Studies Without Implementation)

This type of study comprises studies in which the use of blockchain is theoretical and does not lead to deployment. Such studies provide conceptual frameworks, security algorithms, and models but without experimental analysis and data gathering. Indirect Use Study Examples: What is the Network Use of Blockchain for Multi-Level Trust—An Overview? The blockchain solution is modeled for the security of identity verification from the various sides of a distributed system. Scalability problem discussions involving blockchain, and a series of possible enhancements on a trading style with a computing system in a pyramid structure. These types of investigations are useful in directing future research by specifying the theoretical advantages, expected drawbacks, and eventual improvements in the blockchain use for various level environments.

C. Without Implementation (Theoretical Analysis & Conceptual Frameworks)

The third category contains articles about the idea of blockchain in multi-tier computing systems. The articles include high-level communications, reviews, or conceptual frameworks on the theme of the matter along with the application of blockchain in multi-tier computing. They are viewed as no implementation researches, but assessments of the principle of security, trade-offs, and implications of the use of blockchain technology for distributed architectures are carried out. Examples of Without Implementation Studies: Abstracts and introductions published in journals explaining that the idea of insurance contracts powered by blockchain is a noticeable solution to the problem of insurance fraud. Discussion of the relation of technological innovation to governance and how blockchain might be used to address governance issues by ensuring transparency, security, and trust. However, they are quite the pivotal ones that contribute to the identification of knowledge gaps and facilitate the development of new frameworks that can guide future implementations.

۳,۳ The Justification of the Categorization Methodology

Being a formalized comparison among a cryptographic transaction it could be found that both the Direct, Indirect, and Without Implementation types of blockchain technologies in multilayer distributed computing provide dependable substitutes and are intended for similar enterprise deployment. This classification of blockchain uses allows us to: To examine the potential benefits, these blockchain technologies bring to a company versus the future cost of switching to them, to determine whether they are worth it. Reviewing the current availability of blockchain technologies and associated issues to extend their utilization in various computer architectures. These studies conclude that there is also a lack of consistency and completeness of solutions proposed, which can be illustrated by the case of event-driven microservices systems. The way we split the blockchain technology application field such as the sections afterwards will be as methods of our analysis. Here, we will assess the effect, limitations, and challenges of blockchain adoption in secure multi-tier distributed computing systems.

٤. Literature Review

The blockchain technology has been the subject of numerous research projects related to distributed multi-tiered computations with a focus on the security, trust, and data integrity problems. From the current literature, the research can be divided into the three that have involved blockchain in the management of multi-tier computing infrastructure. The third category includes the

١. **Direct Use**: Research studies that have implemented blockchain solutions in multi-tier computing systems.
٢. **Indirect Use**: Research studies that investigate blockchain's promise in this area but are not practically applicable.
٣. **Without Implementation**: Research studies that provide theoretical discussions, models, or conceptual frameworks of blockchain in multi-tier computing.

This section contributes a complete view of the major research contributions that correspond to each category of blockchain, their methodologies, the benefits and limitations as well as the multi-tier computing security

contribution. "**The numbering of tables in this paper follows the original source. As a result, some numbers may appear to be missing in the sequence. This approach ensures consistency with the main source. The original file containing the full set of tables is provided in the appendix. The articles listed in Tables ١, ٢, and ٣ are also cited alongside the paper's objectives, with full references provided at the end of the article.**"

٤,١ Direct Blockchain Implementation Studies

Blockchains have been practically implemented to ensure the integrity, trustworthiness, and transparency of multi-tier computer systems. On the other hand, in the direct application of blockchain, the focus is more on the actual uses that can solve the most significant tasks which include providing data integrity, decentralized authentication, consensus mechanisms, and secure transactions in distributed systems. **Table ١** shows a collection of research works with blockchain as a direct technology in various multi-tier computing applications. The works conducted explore different fields such as fog computing, IoT security, digital identity, supply chain tracing, electronic health records (EHR), and decentralized finance.

Table ١: Key Studies with Direct Blockchain Use

No.	Authors & Study	Objective	Blockchain Use	Relevance to Our Topic
٣	Dewanta & Mambo (٢٠٢١)	BPT Scheme: Establishing Trusted Vehicular Fog Computing Service for Rural Area Based on Blockchain Approach [١٣]	Direct use; blockchain-based trust and transaction mechanism	Introduces a blockchain-based method for trusted fog computing in vehicular networks; relevant for secure multi-tier blockchain architectures in distributed computing.
١٣	Ahmad, Saad, Bassiouni & Mohaisen (٢٠١٨)	Towards Blockchain-Driven, Secure and Transparent Audit Logs [٥]	Direct use; blockchain-based audit log security system	Proposes BlockAudit, a blockchain based system for securing and maintaining tamper-proof audit logs using Hyperledger; highly relevant for secure multi-tier blockchain computing.
١٤	Rahman (٢٠٢١)	Privacy Enhancement of the Internet of Everything (PeIE) with the Integrated Blockchain Technology [٣٩]	Direct use; blockchain-based privacy and security framework	Proposes an integrated blockchain approach using Sidechain and Rootstock (RSK) to enhance security and privacy in IoE; relevant for secure multi-tier blockchain architectures in distributed computing.
١٦	Roy, Ashaduzzaman, Hassan & Chowdhury (٢٠١٨)	Blockchain for IoT Security and Management: Current Prospects, Challenges, and Future Directions [٤٢]	Direct use; blockchain-based security and management for IoT	Provides a comprehensive study on integrating blockchain with IoT for security, privacy, and management; highly relevant for multi-tier blockchain architectures in distributed computing.
١٧	Gopal & Omeleze-Baror (٢٠٢٤)	Using Blockchain to Secure Digital Identity and Privacy Across Digital Sectors [١٨]	Direct use; blockchain-based multi-layer identity management system	Proposes a multi-layer blockchain model for securing digital identities and preventing data breaches; relevant for secure identity management in multi-tier blockchain-based distributed computing.
١٨	Bashar (٢٠٢١)	Fair and Efficient Consensus Protocols for Secure Blockchain Applications [٩]	Direct use; focuses on improving blockchain consensus protocols	Proposes three novel blockchain consensus protocols: Proof of Queue (PoQ), ACCORD (for healthcare records), and Janus (for pharmaceutical supply chains), enhancing fairness, scalability, and security in multi-tier blockchain architectures.
١٩	Parjuangan & Suhardi (٢٠٢٠)	Systematic Literature Review of Blockchain-Based Smart Contracts Platforms [٣٥]	Direct use; focuses on blockchain-based smart contract platforms	Conducts a systematic review of blockchain-based smart contract platforms, identifying their characteristics and applications; relevant for understanding multi-tier blockchain architectures in distributed computing.
٢٠	Brau, Decampos, Gardner & Gardner (٢٠٢٣)	Blockchain in Supply Chain Management: A Feature-Function Framework for Future Research [١٠]	Direct use; blockchain-based supply chain management framework	Proposes a feature-function framework integrating blockchain features with supply chain functions, identifying future research directions; relevant for structuring blockchain integration in multi-tier distributed computing.
٢٢	Grünewald, Gürpinar, Culotta & Guderian (٢٠٢٤)	Archetypes of Blockchain-Based Business Models in Enterprise Networks [١٩]	Direct use; blockchain-based business model frameworks	Proposes a taxonomy and seven archetypes of blockchain-based business models in enterprise networks, offering insights into how blockchain enhances multi-tier distributed computing.
٢٣	Durigan Junior, Spinola, Gonçalves & Laurindo (٢٠٢٢)	Central Bank Digital Currencies: The Advent of Its IT Governance in the Financial Markets [١٥]	Direct use; blockchain-based CBDC governance model	Proposes a systematic literature review on IT governance for Central Bank Digital Currencies (CBDCs), discussing Distributed Ledger Technology (DLT), interoperability, and blockchain-based governance frameworks; relevant for secure multi-tier blockchain computing.
٢٦	Rogerson & Parry (٢٠٢٠)	Blockchain: Case Studies in Food Supply Chain Visibility [٤١]	Direct use; blockchain for supply chain transparency	Examines how blockchain enhances visibility and trust in food supply chains through real-world case studies; relevant for blockchain driven secure multi-tier distributed computing.
٢٧	Hastig & Sodhi (٢٠٢٠)	Blockchain for Supply Chain Traceability: Business Requirements and Critical Success factors [٢٢]	Direct use; blockchain for supply chain traceability	Identifies business requirements and critical success factors for implementing blockchain in supply chain traceability systems, making it relevant for secure multi-tier blockchain-based distributed computing.
٣٠	Ahmed & MacCarthy (٢٠٢١)	Blockchain-Enabled Supply Chain Traceability in the Textile and Apparel Supply chain: A case study of the fiber producer, Lenzing [٦]	Direct use; blockchain-based supply chain traceability	Analyzes blockchain's role in enhancing supply chain transparency and traceability in the textile and apparel industry; relevant for secure multi-tier blockchain architectures in distributed computing.

٣١	Peng, Zhang, Zhang, Wan, Chen & Xia (٢٠٢١)	A Secure Signcryption Scheme for Electronic Health Records Sharing in Blockchain [٣٦]	Direct use; blockchain-based EHR security model	Proposes an identity-based signcryption scheme with multiple authorities for secure sharing of electronic health records (EHRs) on blockchain; highly relevant for securing multi-tier blockchain architectures in distributed computing.
٣٢	Rangelov, Subudhi, Lämmel, Boerger,Tcholtchev & Khan (٢٠٢١)	Design and Specification of a Blockchain-Based P٢P Energy Trading Platform [٤٠]	Direct use; blockchain-based P٢P energy trading platform	Proposes a decentralized Ethereum based architecture for transparent, secure, and trustful peer-to-peer (P٢P) energy trading; highly relevant for secure multi-tier blockchain computing.
٣٣	Iyer (٢٠٢١)	Sustainable Education Management Blockchain: A Systematic Literature Review [٢٦]	Direct use; blockchain-based sustainable education framework	Investigates the role of blockchain in sustainable education management, analyzing its application for education-based information systems; relevant for secure and transparent multi-tier blockchain-based information management.
٣٤	Adeshina, Kalu & Abdullahi (٢٠٢١)	Blockchain-Based Fog Computing for Internet of Things: A Review of Trends and Challenges [٢]	Direct use; blockchain for securing fog computing in IoT	Reviews blockchain-based fog computing for IoT applications, identifying trends, challenges, and architectural improvements; relevant for multi-tier blockchain computing in secure distributed IoT networks.
٣٦	Chen & Chen (٢٠٢٣)	Blockchain-Enabled Supply Chain Internal and External Finance Model [١١]	Direct use; blockchain-based supply chain finance optimization	Proposes a Stackelberg game theory model to compare blockchain enabled vs. traditional financing scenarios, analyzing pricing, interest rates, and risk management; highly relevant for multi-tier blockchain based distributed computing in financial ecosystems.
٣٧	Khan, Ali, Ahmed, Marwat, Hamid & Tooba (٢٠٢٣)	Data Security in Smart Metering: A Blockchain-Based Approach [٢٨]	Direct use; blockchain for securing smart metering data	Proposes a blockchain-based framework to ensure the confidentiality, integrity, and availability of smart metering data, eliminating unauthorized access and providing a secure multi-tier distributed ledger system; highly relevant for multi-tier blockchain architectures in distributed computing.
٣٨	Ivanov (٢٠٢١)	Digital Supply Chain Management and Technology to Enhance Resilience by building and using end-to-end visibility during the COVID-١٩ pandemic [٢٥]	Direct use; blockchain for supply chain visibility	Explores the role of digital technologies, including blockchain, in enhancing supply chain resilience during the COVID-١٩ pandemic, making it highly relevant for secure multi-tier blockchain architectures in distributed computing.

٤,١,١ Key Findings of Direct Implementation Studies of Blockchain

Table ١ represents work that emphasizes various applications of blockchain in the multi-level computing system. These are some of the main elements that stand out in these cases:

Secure Multi-Level Authentication & Trust Management using Blockchain

By linking the blockchain technology with the process of offloading, they managed to get rid of the insecure and complex authentication. Besides this, they now can also attest to the identity of users by using this new technology (Dewanta & Mambo, ٢٠٢١) [١٣].

Furthermore, Gopal & Omeleze-Baror's (٢٠٢٤) [١٨] proposal of a technology for identity management employing blockchain in a multi-layer was overcoming the issues of the security evaluation of the identification verification by proving tamper-resistant and secure identification.

Blockchain for Secure Data Integrity & Audit Logs

Ahmad et al. (٢٠١٨) [٥] call the block-based system, BlockAudit, which is a system that can verify data via blocks against tampering. Data can be accessed only to authorized users, and the accesses are logged in the audit. Data is decrypted when it is accessed and remains encrypted during the time when the user is offline. In addition, the system exhibits immunity to attacks of ٥١٪ and provides good protection in the Ransomware case. Furthermore, signcryption suite offers to encrypt and a robust suite assists the user to decrypt the records to plaintext before sending Ethical Healthcare Data Records over a network (Peng et al., ٢٠٢١) [٣٦]. Perhaps, these technical innovations of secure patient data exchange might be of great help to patients who have chronic diseases or who are frequently changing doctors. Therefore, a new solution is coming up and thus, the time of the issues is becoming past tense. In addition, the validation process for the safe patient data exchange would become even longer through tamper-proof ledger secure time-lock. Even this encryption risk for the enemies might be the final solution to all of the above mentioned issues. Blockchain Security for Performance Measurements of IoT and Fog Computing

Roy and others (٢٠١٨) [٤٢] the sources for the writers have mentioned the fact, "Therefore, with the adoption of the new blockchain technology, the Internet of Things and Fog nodes are made to work together using a system of self-identification which is classified as secure and hack resistant" The most powerful characteristic of a blockchain-fog to IoT technology, in our opinion, is the ability to track a single product through its whole life-cycle. Capitalization of Adeshina is a mistake that potentially could be a disruptive technology. The authors of the paper Brau et al. (٢٠٢٣) [١٠] also put forward the idea of feature-function models implemented using blockchain to ensure a total traceability in the process of logistics and warehousing. Without any doubts, the introduction of blockchain to supply chain finance had improved the commercial operations of the chain. needmaker used approval protocol. The classical approach is taken from the descriptive taxonomy. The cumulative game compares the blockchain to the classical approach with a discount factor of a year. Ivanov (٢٠٢١) [٢٥] provides more insight on blockchain

technology and how it can be useful for the digital supply chain management that can make use of the distributed ledger technology for constructing a strong and open network. Blockchain for Secure Decentralized Transactions .Rangelov et al. (٢٠٢١) [٤٠] propose a novel energy trading model based on Blockchain P٢P consisting of Ehereum smart contracts that ensured tamper-evident and transparency to the trade. A blockchain security model was proposed in a research paper by Khan et al. (٢٠٢٣) [٢٨] on the application of blockchain technology to the field of smart metering data that, in return, balanced the technology, personalization of data, and the safety of the energy system.

٤,١,٢ Benefits of Direct Blockchain Utilization in Multi-Tier Computing

Therefore, in compliance with the studies looked at, blockchain technology can offer these main benefits in the realm to which it is applied security:

- Decentralized Security: Solid security approach prevention o one powerful player but at the same time, issues fatal weakness.
- Data Integrity & Tamper-Proof Storage: Blockchain technology is single-handedly capable of creating a secure and at the same time, legal data storing.
- Automated Access Control: Adjustment of security rules and conditions make operation simpler and reduces a chance of the human factor errors.
- Enhanced Transparency & Traceability: Supply chain handling, financial networks, healthcare, and even educational systems need real-time, automatically tracked and securely audited transactions.

٤,٢ Indirect Use of Blockchain Feasibility Studies

Although direct utilization of blockchain--studies assume live application to explain blockchain application relevancy, large scale studies, in reality, concentrate mainly on theoretical and feasibility problems of the blockchain in the multi-layer distributed computing environment. These studies take into account the advantages of the blockchain, the patterns of the safety of algorithms, and the problems of the connecting system without physical implementation. Table ٢ shows the meta-database with the most outstanding studies where blockchain is an indirect application.

Table ٢: Key Studies with Indirect Blockchain Use

No.	Authors & Study	Objective	Blockchain Use	Relevance to Our Topic
١	Estrada-Galinanes & Felber (٢٠١٣)	Helical Entanglement Codes: An Efficient Approach for Designing Robust Distributed storage systems [١٦]	Indirect use; suitable for blockchain integration	Highlights multi-layer trust mechanisms, fault tolerance, and scalability; relevant for designing multi-tier blockchain architectures
٢	Komathy, Ramachandran & Vivekanandan (٢٠٠٣)	Security for XML Messaging Services—A Component-Based Approach [٢٩]	Indirect use; focuses on secure messaging	Discusses a multi-tier security model for distributed web transactions; relevant for securing data in multi-tier blockchain architectures.
٤	Joshi, Hiltunen, Sanders & Schlichting (٢٠١١)	Probabilistic Model-Driven Recovery in Distributed Systems [٢٧]	Indirect use; focuses on fault-tolerant distributed computing	Presents a model-based approach using Bayesian estimation and Markov decision theory for automatic recovery in distributed systems; relevant for enhancing fault tolerance in blockchain-based multi tier computing.
٥	Abdulsalam, Olaniyi, Ahmed & Olaniyan (٢٠١٧)	Developing a Secure Distributed Electronic Health System Using Information Hiding Techniques [٣]	Indirect use; focuses on security in distributed computing	Proposes a secure electronic health system using steganography and watermarking techniques; relevant for securing multi-tier distributed computing environments, but lacks direct blockchain integration.
٦	Chen (٢٠١٤)	Model-Based Autonomic Security Management of Networked Distributed Systems [١٢]	Indirect use; focuses on security management in distributed systems	Introduces an autonomic security management framework for self-protection in distributed systems; relevant for securing multi-tier blockchain computing, but does not directly integrate blockchain.
٧	Baltopoulos & Gordon (٢٠٠٨)	Secure Compilation of a Multi-Tier Web Language [٨]	Indirect use; focuses on security in multi-tier web applications	Proposes a secure compilation strategy for multi-tier applications using authenticated encryption; relevant for securing blockchain-based multi-tier distributed computing architectures.
٨	Menaka, Banu & Ashadevi (٢٠١٦)	Survey on Signatured XML Encryption for Multi-Tier Web Services Security [٣٢]	Indirect use; focuses on securing XML-based multi-tier web services	Proposes XML encryption and signatures for securing multi tier web services; relevant for securing blockchain-based distributed computing environments through cryptographic methods.
٩	Islam & Abawajy (٢٠١٣)	A Multi-Tier Phishing Detection and Filtering Approach [٢٤]	Indirect use; focuses on multi-tier security classification	Proposes a multi-tier classification model for phishing detection using machine learning; relevant for security aspects in blockchain-based multi-tier distributed computing.
١٠	Swamy, Chen, Fournet, Strub, Bhargavan & Yang (٢٠١١)	Secure Distributed Programming with Value-Dependent Types [٤٤]	Indirect use; focuses on secure distributed programming	Proposes F⋆, a dependently-typed programming language for secure distributed computing; relevant for multi-tier blockchain security frameworks due to its verification mechanisms and modular reasoning about state.

۱۱	Gamlo & Bamasak (۲۰۱۱)	A multi-tier framework for securing e-transactions in e-government systems of Saudi Arabia [۱۷]	Indirect use; focuses on multi-tier security frameworks for e-government	Proposes a structured security framework for e-government transactions, relevant for designing secure blockchain-based multi-tier distributed computing systems.
۱۲	Yavuz, Alagöz & Anarim (۲۰۱۰)	A new multi-tier adaptive military MANET security protocol using hybrid cryptography and signcryption [٤٥]	Indirect use; focuses on multi-tier security protocols	Proposes a hierarchical security model for military MANETs using hybrid cryptography and signcryption; relevant for secure communication in multi-tier distributed computing, but lacks direct blockchain integration.
۱۵	Rahman, Roy, Kaiser & Islam (۲۰۱۸)	A Lightweight Multi-tier S-MQTT Framework to Secure Communication between low-end IoT nodes [۳۷]	Indirect use; focuses on secure IoT communication	Proposes a multi-tier security model for IoT using an enhanced MQTT protocol with cryptographic security layers; relevant for securing communication in multi-tier blockchain-based distributed computing.
۲۱	Mohsan, Mazinani, Othman & Hussain (۲۰۲۲)	Towards the Internet of Underwater Things: A Comprehensive Survey [۳۳]	Indirect use; blockchain mentioned for securing IoUT systems	Reviews the concept of IoUT, its challenges, and applications, including blockchain as a potential security mechanism for underwater networks; relevant for multi-tier distributed computing but lacks direct blockchain implementation.
۲٤	Alahi, Sukkuea, Tina, Nag, Kurdthongmee, Suwannarat & Mukhopadhyay (۲۰۲۳)	Integration of IoT-Enabled Technologies and Artificial Intelligence (AI) for Smart city scenario: recent advancements and future trends [۷]	Indirect use; discusses potential blockchain integration for IoT security	Provides an extensive review of IoT and AI integration for smart cities, including security concerns where blockchain is suggested as a potential solution; relevant for secure multi-tier distributed computing environments.
۲۵	Otoum, Gottimukkala, Kumar & Nayak (۲۰۲٤)	Machine Learning in Metaverse Security: Current Solutions and Future Challenges [۳٤]	Indirect use; discusses blockchain as a security mechanism in Metaverse environments	Explores machine learning techniques for Metaverse security, covering AI, XR, ٦G, and blockchain; relevant for blockchain enabled multi-tier security in distributed computing.

٤,۲,۱ Key Findings of Indirect Implementation Studies of Blockchain

The research works on the ways of blockchain in various subjects such as IoT messaging, message security, and trust management. Here are some important results: Estrada-Galinanes & Felber (۲۰۱۳) [۱٦] proposed a multi-layer trust mechanism that was a part of the blockchain model, which was optimized to fault tolerance and scalability. Komathy et al. (۲۰۰۳) [۲۹] elaborated on secure XML-based web transactions, a topic that is relevant to blockchain-based secure message services. Baltopoulos & Gordon (۲۰۰۸) [۸] gave a transparently secure compilation strategy for multi-tier applications by using authenticated security layers; blockchain is the only way to do this. The Use of Blockchain in Secure IoT and Edge Computing. Rahman et al. (۲۰۱۸) [۳۷] brought up to date multi-tier MQTT architecture for IoT safety and recommending blockchain as an add-on to the solutions. Mohsan et al. (۲۰۲۲) [۳۳] addressed the topic of Internet of Underwater Things (IoUT) and mentioned blockchain as a solution that can be extended over the operation of USVs underwater. Alahi et al. (۲۰۲۳) [۷] encapsulated IoT and AI integration, and the potential of blockchain in secure IoT communications. Blockchain in a Decentralized Security Framework Gamlo & Bamasak (۲۰۱۱) [۱۷] developed a multi-leveled security framework for e-government transactions, in which trust management was singled out as the main stumbling block—an issue that blockchain is capable of solving. Yavuz et al. (۲۰۱۰) [٤٥] introduced a hierarchical security configuration for military networks that can be said to have some resemblance to the distributed trust mechanism of blockchain. Otoum et al. (۲۰۲٤) [۳٤] are pioneers in blockchain space security. They delve into the potential of the technology to enhance trust, and thus, identity and data security in the Metaverse, by providing its use-cases.

٤,۲,۲ Recognized Benefits & Challenges of Indirect Use Studies

Possible Benefits of Blockchain in Multi-Tier Computing

Improved Trust & Authentication: Multi-layer security research adds up with blockchain's decentralized trust model.
Scalability Implications: Secure and fault-tolerant solutions can be applied to blockchain for its scalability to the extent that security architectures allow research.
Interoperability & Data Sharing: The cross-platform software integration that blockchain aims to support requires the secure and tamper-evident data flow with blockchain.

Challenges & Research Gaps

Lack of Real-World Testing: The majority of the projects outline a framework for proposed blockchain framework without actual implementation.
Difficulty in Integration: The ability to add blockchain into an existing multi-tiered framework and have an overall system work without stress is another consideration.
Computational Overhead: Other research models study a trade-off regarding security and computational power which is a strong argument for the feasibility of blockchain.

٤,۳ Theoretical Studies on Blockchain & Multi-Tier Computing

By the way, direct and indirect blockchain studies concern the question of feasibility and the way of implementations. In addition, several works have considered conceptual models, theoretical frameworks, and strategical insights about the integration of the blockchain technology into a multi-tier distributed system. Table ۳

offers a summary of existing theoretical studies capable of comprehending blockchain security, quantum resistance, IoT integration, and even supply chain transparency but to indirect implementation.

Table ٣: Key Studies Mentioning Blockchain Without Implementation

No.	Authors & Study	Objective	Blockchain Use	Relevance to Our Topic
٤١	Guthoff, Anell, Hainzinger, Dabrowski, Krombholz (٢٠٢٣)	Perceptions of Distributed Ledger Technology Key Management – An Interview study with finance professionals [٢١]	Focuses on the key management challenges in Distributed Ledger Technology (DLT) for financial institutions	Investigates key management issues and adoption barriers in blockchain and DLT for financial applications, highly relevant for secure multi-tier distributed computing.
٤٢	Madan, Bhuniya, Kumar, Chauhan (٢٠٢٣)	Economic, Social & Environmental Benefits of Blockchain Adoption in Supply Management: An Indian Perspective [٣١]	Blockchain Technology (BCT) is used to address economic, social, and environmental challenges in supply chains, offering enhanced transparency, security, and efficiency.	This paper discusses the broad impacts of BCT on supply chain management in India, relevant to secure multi-tier blockchain applications and their role in improving distributed computing systems.
٤٣	Dietrich, Kuenster, Louw, Palm (٢٠٢٢)	Review Of Blockchain-based Tokenization Solutions For Assets In Supply Chains [١٤]	Blockchain is used for tokenizing physical and abstract assets in supply chains to enhance traceability, transparency, and disintermediation.	The paper provides insights into how blockchain can map assets in multi-tier supply chains and enhance transparency, which is crucial for secure multi-tier distributed computing.
٤٤	Rahman, Khalil, Atiquzzaman (٢٠٢١)	Blockchain Powered Policy Enforcement for Ensuring Flight Compliance in Drone-based service systems [٣٨]	Blockchain is used for policy enforcement and compliance tracking, ensuring drones adhere to predefined flight paths, avoid restricted areas, and comply with service policies.	This paper aligns with the topic of blockchain technologies in secure multi-tier distributed computing systems by addressing the need for secure, transparent policy enforcement in drone service systems, making it relevant for distributed computing environments.
٤٥	Tran Huy, Tran Thien, Tran, Le Chi (٢٠٢٢)	Monitoring, Detecting and Early Warning of Forest Fires using Blockchain in Wireless Sensor Network [٢٣]	Blockchain is used to secure routing, prevent data tampering, and ensure data integrity in the monitoring system for forest fires.	This paper contributes to secure distributed computing by integrating BC with WSN, ensuring the reliability and security of multi-tier distributed systems, particularly in the context of environmental monitoring.
٤٦	Gurzawska (٢٠٢٠)	Towards Responsible and Sustainable Supply Chains – Innovation, Multi-stakeholder Approach and governance [٢٠]	Blockchain is not explicitly mentioned in the title, but the paper highlights the role of innovation, stakeholder collaboration, and governance in supply chains. Blockchain can play a role in ensuring transparency, accountability, and security in these systems.	The focus on governance, multi stakeholder approaches, and innovation aligns with how blockchain can support secure, transparent, and decentralized management in multi-tier distributed systems, making it relevant to your topic.
٤٧	Abbas, Tawalbeh, Rafiq, Muthanna, Elgendy, Ahmed A. Abd El-Latif (٢٠٢١)	Convergence of Blockchain and IoT for Secure Transportation Systems in smart cities [١]	Blockchain is used to decentralize data management, enhance transparency, and secure communication within smart transportation systems by integrating IoT devices with blockchain for real-time tracking and secure transactions.	The integration of IoT and blockchain in smart transportation aligns with your topic of secure multi-tier distributed computing, showcasing the use of blockchain to enhance security and transparency in distributed IoT systems.
٤٨	Stavroulaki et al. (٢٠٢١)	DEDICAT ٦G - Dynamic Coverage Extension and Distributed Intelligence for human centric applicationswith assured security, privacy and trust: From ٥G to ٦G [٤٣]	Blockchain is used for trust management in ٦G networks, with an emphasis on private permissioned blockchain (Hyperledger Fabric) to provide security, privacy, and trust assurance.	The integration of blockchain in ٦G networks for trust and security management aligns with secure multi-tier distributed computing, enhancing the efficiency and security of future communication systems.
٤٩	Kumar, M., Mondal, B. (٢٠٢٤)	Quantum Blockchain Architecture using Cyclic QSCD and QKD [٣٠]	Introduces a new quantum blockchain framework using Cyclic Quantum State Computational Distinction (QSCD) and Quantum Key Distribution (QKD) to provide security against quantum computer threats, using a quantum voting consensus mechanism and multi-bit encryption.	The paper proposes a quantum resistant blockchain architecture, leveraging quantum cryptographic methods to ensure security and fault tolerance in distributed systems, aligning with secure multi-tier distributed computing in blockchain technologies.
٥٠	Abirami, P., Bhanu, S. V. (٢٠٢٠)	Enhancing cloud security using crypto-deep neural network for privacy preservation in trusted environment [٤]	Blockchain is not directly mentioned in the abstract but could be applied in securing cloud environments by integrating it with the crypto-deep neural network model to enhance data integrity and user authentication.	This paper's focus on security and privacy preservation in cloud computing is relevant for secure multi-tier distributed computing, particularly in environments requiring high trust and data protection.

٤,٣,١ Key Contributions of Theoretical Blockchain Research

Blockchain is a technology that has advanced fields such as: IoT, security of the AI-powered, supply chains and quantum computing, but the statistical data, in its current form, is not yet published.

- *Blockchain to Trust, Privacy, and Compliance in Distributed Systems*

Guthoff et al. (٢٠٢٣) [٢١] gives the most significant challenges to blockchain to be applied in banks. They mention security, convenience and compliance.

Rahman et al. (٢٠٢١) [٣٨] sanctioned the enforcement policy of the blockchain so that drones can be flown safely according to rules and offering private area surveillance alone.

Stavroulaki et al. (٢٠٢١) [٤٣] proposed the concept of trust management in next-generation cellular communications with blockchain-based security for private, permissioned, hybrid networks.
Kumar & Mondal (٢٠٢٤) [٣٠] demonstrated quantum computer safe nature of a blockchain model by implementing the Quantum Key Distribution (QKD) technique. Abirami & Bhanu (٢٠٢٠) [٤] proposed the concept of using a blockchain to secure the privacy of storage of cloud computing, thereby creating a blockchain on it.

- *Blockchain in Green & Safe Supply Chains*

Madan et al. (٢٠٢٣) [٣١] blockchain has been utilized for this reason that established economic, social, and environmental impacts in supply chains and brought transparency and efficiency. Dietrich et al. (٢٠٢٢) [١٤] have found that the use of blockchain technology is an alternative solution to governance, security and cost savings in supply chain management because it provides increased visibility and trust in supply chain operations and ensures efficient integration of digital and physical assets. Green supply chain governance based on blockchain is an eco-friendly model and is driven by all stakeholders.

- *Blockchain for IoT & Smart Transport Systems*

IoT is a highly secure topic in transport, data control and real-time tracing is what has been addressed by Abbas et al. (٢٠٢١) [١]. Blockchain has unlocked a new era to the smart evolution of transport systems embracing the tight security of data reception and data in real-time and also it is being controlled by Abbas et al. (٢٠٢١) [١]. Blockchain is the new approach to surveillance of the forest developed by Tran et al. (٢٠٢٢) [٢٣] and it supports data integrity as well as monitoring environmental protection in an untamperable form.

٤,٣,٢ Key Takeaways & Theoretical Contributions

Blockchain Potential Benefits for Multi-Tier Computing
Quantum-Resistant Security: There is newly discovered architecture research that makes their efficiency in quantum quantum computers and distributed lottery rigged impossible to be broken.
Trust & Governance Models: Blockchain technology over time has innovated the potential uses of blockchain applications which includes compliance and transparency of IoT, supply chain as well as AI and other systems
AI-Blockchain Integration: Some other researchers are more faithful in their ideas. Not only the simple issues of security, pricing and energy efficiency are discussed but they also emphasize on other issues that are of more complex nature and also discuss how human errors can be to successfully prevent the attacks. Some other scholars who are more excited come up with new ideas and argue that not only the security and price issues are discussed but there are also other issues of more complex nature and include human errors that can be prevented.
Challenges & Open Research Questions
Risks of Quantum Computing: What are the future concerns regarding the quantum blockchain protocols?: The future of the current technique of blockchain and maybe cash also will need the improvement of the quantum-resistant cryptography
Scalability in Large-Scale Distributed Networks: Miscellaneous tools are experimented within the framework of blockchain technology with the aim of crossrefining them.

٥. Conclusion

This review presents a comprehensive summary of blockchain technologies for secure multi-tier distributed computing, a two-layer cloud topology that offers better trust and security and a faster response in the case of disaster events. This systematic review further examined advanced blockchain research pointing out existing ones dealing with direct, indirect and theoretical questions. Hence, the main findings of this study can be summarized as blockchain offers security, trust management, and data integrity in multi-tier systems by providing tamper-proof transactions, decentralized authentication, and immutable audit trails. Thus, there are still some problems that are not addressed in the literature, scalability is the main one, the next is the computational overhead and integration with current multi-tier computing systems. With direct implementations of blockchain, even with transparent security benefits, there are still some performance trade-offs. Quite the opposite, the indirect and theoretical aspects mostly explain the advantages of blockchain in an abstract and non-emirical manner. Prospects for further studies on blockchain in the context of multi-tier computing include: Developing energy-efficient and scalable consensus protocols to optimize blockchain for distributed environments. Integrating blockchain with AI and cloud computing to offer such security solutions as automation, real-time monitoring, and adaptive threat detection. Designing cross-platform interoperability frameworks that bridge the gap in the integration of blockchain into multi-tier infrastructures.The benefits of this technological advancement can be seen from the results of the research conducted most importantly how to deal with the scalability, computation, and governance issues in order to sustain and succeed in the future.

Acknowledgment
The author declare that this research was conducted independently, without any financial support or institutional affiliation. No funding, sponsorship, or grants were received for this study.

References

[۱] Abbas, K., Tawalbeh, L.A.A., Rafiq, A., Muthanna, A., Elgendy, I.A. and Abd El-Latif, A.A., ۲۰۲۱. Convergence of blockchain and IoT for secure transportation systems in smart cities. *Security and Communication Networks*, *2021*(۱), p.۵۵۹۷۶۷۹.

[۲] Abdullahi, I., Adeshina, S. and Kalu, F., ۲۰۲۱, July. Blockchain-Based Fog Computing For Internet of Things: A Review of Trends and Challenges. In *2021 1st International Conference on Multidisciplinary Engineering and Applied Science (ICMEAS)* (pp. ۱-٤). IEEE.

[۳] Abdulsalam, Y.S., Olaniyi, O.M., Ahmed, A. and Olaniyan, O.M., ۲۰۱۷. Developing a Secure Distributed Electronic Health System using Information Hiding Techniques.

[٤] Abirami, P. and Bhanu, S.V., ۲۰۲۰. RETRACTED ARTICLE: Enhancing cloud security using crypto-deep neural network for privacy preservation in trusted environment. *Soft Computing*, *24*(۲٤), pp.۱۸۹۲۷-۱۸۹۳۶.

[۵] Ahmad, A., Saad, M., Bassiouni, M. and Mohaisen, A., ۲۰۱۸, November. Towards blockchain-driven, secure and transparent audit logs. In *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services* (pp. ٤٤۳-٤٤۸).

[٦] Ahmed, W.A. and MacCarthy, B.L., ۲۰۲۱. Blockchain-enabled supply chain traceability in the textile and apparel supply chain: A case study of the fiber producer, Lenzing. *Sustainability*, *13*(۱۹), p.۱۰٤۹٦.

[۷] Alahi, M.E.E., Sukkuea, A., Tina, F.W., Nag, A., Kurdthongmee, W., Suwannarat, K. and Mukhopadhyay, S.C., ۲۰۲۳. Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: recent advancements and future trends. *Sensors*, *23*(۱۱), p.۵۲۰٦.

[۸] Baltopoulos, I.G. and Gordon, A.D., ۲۰۰۹, January. Secure compilation of a multi-tier web language. In *Proceedings of the 4th international workshop on Types in language design and implementation* (pp. ۲۷-۳۸).

[۹] Bashar, G.D., ۲۰۲۱. *Fair and Efficient Consensus Protocols for Secure Blockchain Applications*. Boise State University.

[۱۰] Brau, J.C., Gardner, J., DeCampos, H.A. and Gardner, K., ۲۰۲۳. Blockchain in supply chain management: a feature-function framework for future research. *Supply Chain Management: An International Journal*, *29*(۱), pp.۲۷-٤۹.

[۱۱] Chen, Q. and Chen, X., ۲۰۲۳. Blockchain-enabled supply chain internal and external finance model. *Sustainability*, *15*(۱۵), p.۱۱۷٤۵.

[۱۲] Chen, Q., ۲۰۱٤. *Model-based autonomic security management of networked distributed systems*. Mississippi State University.

[۱۳] Dewanta, F. and Mambo, M., ۲۰۲۱. BPT scheme: Establishing trusted vehicular fog computing service for rural area based on blockchain approach. *IEEE Transactions on Vehicular Technology*, *70*(۲), pp.۱۷۵۲-۱۷٦۹.

[۱٤] Dietrich, F., Kuenster, N., Louw, L. and Palm, D., ۲۰۲۲. Review of blockchain-based tokenization solutions for assets in supply chains.

[۱۵] Durigan Junior, C.A., Spinola, M.D.M., Gonçalves, R. and Laurindo, F.J.B., ۲۰۲۲. Central Bank Digital Currencies: The Advent of Its It Governance in the Financial Markets. In *19th CONTECSI–INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGY MANAGEMENT| DEC* (pp. ۱۹-۲۱).

[۱٦] Estrada Galinanes, V. and Felber, P., ۲۰۱۳, November. Helical entanglement codes: An efficient approach for designing robust distributed storage systems. In *Symposium on Self-Stabilizing Systems* (pp. ۳۲-٤٤). Cham: Springer International Publishing.

[۱۷] Gamlo, A. and Bamasak, O., ۲۰۱۱. A multi-tier framework for securing e-transactions in e-government systems of Saudi Arabia. *International Journal of Electronic Finance*, *5*(۲), pp.۱۲٦-۱٤۹.

[۱۸] Gopal, J. and Omeleze-Baror, S., ۲۰۲٤, March. Using Blockchain to Secure Digital Identity and Privacy Across Digital Sectors. In *International Conference on Cyber Warfare and Security* (pp. ۵۱۹-۵۲٦). Academic Conferences International Limited.

[۱۹] Grünewald, A., Gürpinar, T., Culotta, C. and Guderian, A., ۲۰۲٤. Archetypes of blockchain-based business models in enterprise networks. *Information Systems and e-Business Management*, *22*(٤), pp.٦۳۳-٦٦۵.

[۲۰] Gurzawska, A., ۲۰۲۰. Towards responsible and sustainable supply chains–innovation, multi-stakeholder approach and governance. *Philosophy of Management*, *19*(۳), pp.۲٦۷-۲۹۵.

[۲۱] Guthoff, C., Anell, S., Hainzinger, J., Dabrowski, A. and Krombholz, K., ۲۰۲۳, May. Perceptions of distributed ledger technology key management-an interview study with finance professionals. In *2023 IEEE Symposium on Security and Privacy (SP)* (pp. ۵۸۸-٦۰۵). IEEE.

[۲۲] Hastig, G.M. and Sodhi, M.S., ۲۰۲۰. Blockchain for supply chain traceability: Business requirements and critical success factors. *Production and Operations Management*, *29*(٤), pp.۹۳۵-۹۵٤.

[۲۳] Huy, L.T., Thien, C.T., Tran, H.T. and Le Chi, Q., ۲۰۲۲. Monitoring, Detecting and Early Warning of Forest Fires using Blockchain in Wireless Sensor Network.

[۲٤] Islam, R. and Abawajy, J., ۲۰۱۳. A multi-tier phishing detection and filtering approach. *Journal of Network and Computer Applications*, *36*(۱), pp.۳۲٤-۳۳۵.

[۲۵]Ivanov, D., ۲۰۲۱. Digital supply chain management and technology to enhance resilience by building and using end-to-end visibility during the COVID-۱۹ pandemic. *IEEE Transactions on Engineering Management*.
[۲۶]Iyer, S.S., Sustainable Education Management Blockchain: A Systematic Literature Review.
[۲۷]Joshi, K.R., Hiltunen, M.A., Sanders, W.H. and Schlichting, R.D., ۲۰۱۰. Probabilistic model-driven recovery in distributed systems. *IEEE Transactions on Dependable and Secure Computing*, *8*(٦), pp.۹۱۳-۹۲۸.
[۲۸]Khan, W.U., Ali, B., Ahmed, S., Marwat, S.N.K. and Hamid, I., Data Security in Smart Metering: A Blockchain based Approach.
[۲۹]Komathy, K., Ramachandran, V. and Vivekanandan, P., ۲۰۰۳. Security for XML messaging services—a component-based approach. *Journal of network and computer applications*, *26*(۲), pp.۱۹۷-۲۱۱.
[۳۰]Kumar, M. and Mondal, B., ۲۰۲٤. Quantum blockchain architecture using cyclic QSCD and QKD. *Quantum Information Processing*, *23*(۳), p.۱۰۱.
[۳۱]Madan, A.K., Bhuniya, A., Kumar, A. and Chauhan, A.A., ۲۰۲۳. Economic, Social & Environmental Benefits of Block chain Adoption in Supply Chain Management: An Indian Perspective. *American Journal of Multidisciplinary Research & Development (AJMRD)*, *5*(۰٤), pp.۳۹-٤۷.
[۳۲]Menaka, R., Banu, R.S.D.W. and Ashadevi, B., ۲۰۱٦. Survey on Signatured Xml Encryption for Multi-Tier Web Services Security. *Indian Journal of Science and Technology*, *9*(۱٦), pp.۲-۱۰.
[۳۳]Mohsan, S.A.H., Mazinani, A., Othman, N.Q.H. and Amjad, H., ۲۰۲۲. Towards the internet of underwater things: A comprehensive survey. *Earth Science Informatics*, *15*(۲), pp.۷۳٥-۷٦٤.
[۳٤]Otoum, Y., Gottimukkala, N., Kumar, N. and Nayak, A., ۲۰۲٤. Machine learning in metaverse security: Current solutions and future challenges. *ACM Computing Surveys*, *56*(۸), pp.۱-۳٦.
[۳٥]Parjuangan, S., ۲۰۲۰, October. Systematic literature review of blockchain based smart contracts platforms. In *2020 International Conference on Information Technology Systems and Innovation (ICITSI)* (pp. ۳۸۱-۳۸٦). IEEE.
[۳٦]Peng, X., Zhang, J., Zhang, S., Wan, W., Chen, H. and Xia, J., ۲۰۲۱. A Secure Signcryption Scheme for Electronic Health Records Sharing in Blockchain. *Computer Systems Science & Engineering*, *37*(۲).
[۳۷]Rahman, A., Roy, S., Kaiser, M.S. and Islam, M.S., ۲۰۱۸, December. A lightweight multi-tier S-MQTT framework to secure communication between low-end IoT nodes. In *2018 5th International Conference on Networking, Systems and Security (NSysS)* (pp. ۱-٦). IEEE.
[۳۸]Rahman, M.S., Khalil, I. and Atiquzzaman, M., ۲۰۲۱. Blockchain-powered policy enforcement for ensuring flight compliance in drone-based service systems. *IEEE Network*, *35*(۱), pp.۱۱٦-۱۲۳.
[۳۹]Rahman, Z., Privacy Enhancement of the Internet of Everything (PeIE) with the Integrated Blockchain Technology.
[٤۰]Rangelov, D., Subudhi, B.S.K., Lämmel, P., Boerger, M., Tcholtchev, N. and Khan, J., ۲۰۲۱, December. Design and Specification of a Blockchain-based P۲P Energy Trading Platform. In *2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C)* (pp. ٦۳٦-٦٤۳). IEEE.
[٤۱]Rogerson, M. and Parry, G.C., ۲۰۲۰. Blockchain: case studies in food supply chain visibility. *Supply Chain Management: An International Journal*, *25*(٥), pp.٦۰۱-٦۱٤.
[٤۲]Roy, S., Ashaduzzaman, M., Hassan, M. and Chowdhury, A.R., ۲۰۱۸, December. Blockchain for IoT security and management: Current prospects, challenges and future directions. In *2018 5th International Conference on Networking, Systems and Security (NSysS)* (pp. ۱-۹). IEEE.
[٤۳]Stavroulaki, V., Strinati, E.C., Carrez, F., Carlinet, Y., Maman, M., Draskovic, D., Ribar, D., Lallet, A., Mößner, K., Tosic, M. and Uitto, M., ۲۰۲۱, June. DEDICAT ٦G-Dynamic coverage extension and distributed intelligence for human centric applications with assured security, privacy and trust: From ٥G to ٦G. In *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)* (pp. ٥٥٦-٥٦۱). IEEE.Swamy, N., Chen, J., Fournet, C., Strub, P.Y., Bhargavan, K. and Yang, J., ۲۰۱۱. Secure distributed programming with value-dependent types. *ACM SIGPLAN Notices*, *46*(۹), pp.۲٦٦-۲۷۸.
[٤٤]Yavuz, A.A., ALAGÖZ, F. and Anarim, E., ۲۰۱۰. A new multi-tier adaptive military MANET security protocol using hybrid cryptography and signcryption. *Turkish Journal of Electrical Engineering and Computer Sciences*, *18*(۱), pp.۱-۲۲.

Appendix: Full List of Reviewed Articles

This study reviewed **۲۸۱ research papers** related to blockchain technologies in secure multi-tier distributed computing. The categorized analysis of these papers is provided in **Tables ۱, ۲, and ۳** within the main body of this paper. For full transparency, the complete list of reviewed articles, including additional metadata and classification details, is available in an external document accessible via the following link:
Full List of Reviewed Articles