10.31341/jios.48.1.11 UDC 004.738.5:004.056:336
Open Access Survey Paper

A Review on Blockchain for Fintech using Zero Trust Architecture

Avinash Singh *mgcu2019csit6002@mgcub.ac.in*
Department of Computer Science and Information Technology
Mahatma Gandhi Central University,
Motihari, Bihar- 845401, India

Vikas Pareek *vikaspareek@mgcub.ac.in*
Department of Computer Science and Information Technology
Mahatma Gandhi Central University,
Motihari, Bihar- 845401, India

Ashish Sharma *ashishsharma.fitt@gmail.com*
Department of Computer Science and Engineering
Manipal University, Jaipur, Rajasthan 303007, India

Abstract

Financial Technology (FinTech) has sparked widespread interest and is fast spreading. As a result of its continual growth, new terminology in this domain has been introduced. The name 'FinTech' is one such example. This term covers a wide range of practices that are repeatedly used in the financial technology industry. This processes were typically accomplished in careers or organizations to supply required services through the use of information technology-based applications. The word covers a wide range of delicate subjects, including security, privacy, threats, cyberattacks, and others. Several cutting-edge technologies, including those associated with a mobile embedded system, mobile networks, mobile cloud computing, big data, data analytics techniques, and cloud computing, among others, must be mutually integrated for FinTech to thrive. To be approved by its users, this new technology must overcome serious security and privacy flaws. This research gives a thorough analysis of FinTech by discussing the present as well as expected confidentiality and safety problems facing the financial sector to protect FinTech. Finally, it examines potential obstacles to ensuring financial technology application security and privacy.

Keywords: FinTech, security, privacy, cyber security, threats, fraud detection, Internet of things

1. Introduction

Technology and finance are combined to form fintech. Finance is tied to managing money-related activities, and when aided by technology, these duties can be completed more easily and efficiently. The financial sector known as "FinTech"

(financial technology) uses technology to enhance financial operations. "Financial technology is a novel concept that improves financial service processes by recommending technical solutions based on numerous business solutions"[1].

Zero Trust is a paradigm for protecting framework & information that is appropriate for today's modern digital transformation. It specifically tackles today's business concerns about ransomware attacks, hybrid cloud infrastructures, and protecting remote workers [2]. There are a variety of standards from reputable bodies that can help you align Zero Trust with your firm, despite the fact that many suppliers have made their attempts to define it.

Accordingly, Online sources, the definition of a blockchain is a "distributed database that preserves a continuously increasing list of systematic records, called blocks," which are "connected using encryption. Every block has a timestamp, a cryptographic hash of the preceding one, and transaction data [3]. A blockchain is a decentralized, distributed, and open digital ledger employed to record transactions across many computers in a way that forbids the record from being transformed retrospectively without modifying all succeeding blocks and getting network consensus [4].

With the ideas of blockchain technology and zero trust architecture, we will conduct a literature review on financial technology (Fintech) in this review paper. In this paper, we'll also talk about the difficulties facing the fintech industry right now and its potential.

2. Architecture of Fintech

2.1. Zero Trust Architecture

Focusing on security based on access control is the foundation of the zero-trust concept. It is necessary to explicitly verify any external or internal entity wishing to access the fintech resource. The access control in the zero-trust security model is collected of a Policy enforcement point & a zero-trust engine [4-5].

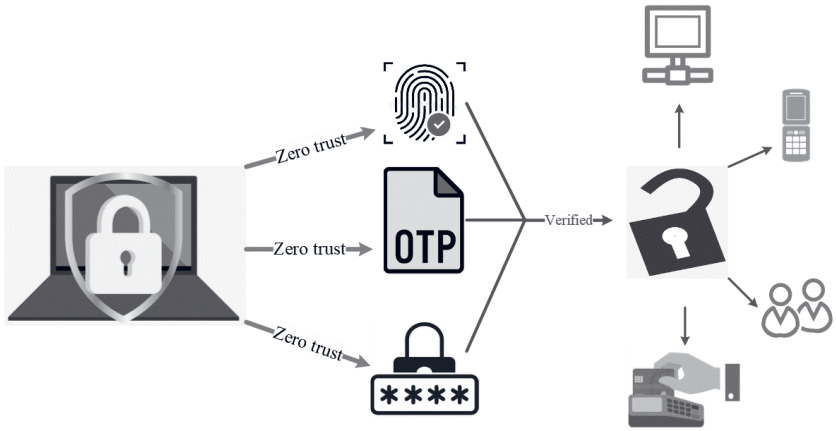

Figure 1. Workflow of Zero trust architecture

Zero trust policy enforcement points allow for communication between the given organization's resources and either internal or external users. The zero-trust policy enforcement point forwards user requests to the zero-trust engine whenever they are generated by company users, whether they are internal or external [6-7]. Additionally, the zero-trust engine verifies the user's request is valid based on various security parameters; if the security parameter is confirmed, the user or device is given access. Figure 1 shows the workflow of zero trust.

2.2. Block-Chain Architecture

Zero trust policy enforcement points allow for communication between a given organization's resources and either internal or external users. The zero-trust policy enforcement point forwards user requests to the zero-trust engine whenever they are generated by company users, whether they are internal or external. Additionally, the zero-trust engine verifies the user's request is valid based on various security parameters; if the security parameter is confirmed, the user or device is given access [8-9].

The one-way nature of cryptographic hash functions results in no one being able to find the input value that corresponds to the corresponding output. They provide a fixed-length output to a corresponding variable-size input [10]. The output value will change if the input value is slightly altered. Figure 2 represents the blockchain workflow procedure.

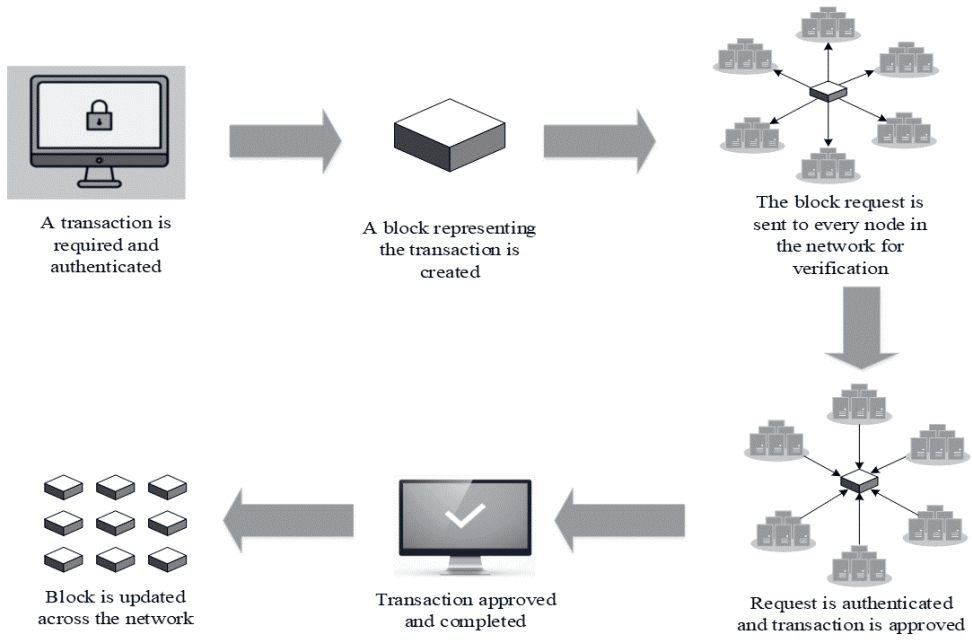

Figure 2. Workflow in the blockchain

3. Abbreviations

BcT	Blockchain Technology
DSR	Design Science Research
ZTX	Zero Trust eXtended
FTI	FAA Telecommunications Infrastructure
TBO	Trajectory Based Operations
NAS	National Airspace System
ZTF	Zero Trust Framework
FAA	Federal Aviation Administration
UAV	Unmanned Aerial Vehicle
ISR	Intelligence, Surveillance, and Reconnaissance
UTAUT	Unified Theory of Acceptance and Uses of Technology
DIMS	Decentralized Identity Management Solutions
DiD	Defense-in-Depth
ZT	Zero Trust
SAS	Spectrum access system
BD-SAS	Blockchain-based Decentralized SAS architecture
G-Chain	Global Block Chain
L-Chains	Local Block Chains
DeFi	Decentralized Finance
IoT	Internet of Things
IoV	Internet of Vehicles
ANT	Activity-Network-Things
A-A theory	Affordance-Actualization
BCM	Blockchain Managers
MAC	Mandatory Access Control
ZTA	Zero Trust Architecture

Table 1. Abbreviations

4. Survey on Blockchain for Financial Transactions in Zero Trust Architecture

Casimer DeCusatis et al [11] in this research, for blockchain apps that are hosted in the cloud, the author presents experimental test bed findings for a revolutionary user identity management solution. By adding cryptographic identity tokens to the initial packet using a Black Ridge Technology endpoint on a Windows host, the author initiates a novel session request. By enforcing security rules and preventing unauthorized access at or beneath the transport layer, a comparable gateway appliance in the cloud. However, compared to other models, this model takes less time to use. But for automation, a third-party program is necessary.

Mayra Samaniego et al [12] This paper presents Amatista, a blockchain-based middleware for IoT administration. With its innovative zero-trust hierarchical mining method, Amatista makes it possible to validate framework and transactions at changed

degrees of trust. This study evaluates the Amatista on Edison Arduino Boards. The evaluations' findings demonstrated Amatista's capacity to validate transactions as well as infrastructure in a hierarchical fashion. Transactions produced by sensors and blocks made in the block factory were verified by Amatista, it did so with an acceptable level of performance. On the foundation of Amatista, future research can provide additional levels of validation, consensus algorithms, and more specialized smart contracts for IoT.

Jungho Kang et al [13] The study will assess current trends in mobile Fintech payment services & categorize them in accordance with service forms to identify requirements and security challenges for future better and more secure service delivery. First, the study compared and contrasted existing payment methods with Fintech payment methods, after looking at current mobile Fintech payment methods, it divided mobile Fintech payment service providers into four groups—hardware manufacturers, operating system developers, payment platform providers, and financial institutions—to highlight their commonalities. It defined the standards that mobile Fintech payment services must meet as well as the security issues that both present and future mobile Fintech payment services would encounter in terms of mutual authentication, authorization, integrity, privacy, and availability. Consideration should be given to mutual authentication, authorization, integrity, privacy, and availability when defining secure and useful fintech payment systems. Future research will look into and analyze the mobile payment process, which is primarily developed in the TechFin financial organizations, which are IT-oriented.

Nir Kshetri [14] This research demonstrates the several ways that blockchain might help with the supply chain goals outlined above. Special attention has been made to the responsibilities of IoT integration in blockchain-based solutions, as well as the amount of blockchain deployment to verify the character of individuals and assets. The use of the blockchain and zero trust can boost trust and security. However, transaction costs and the requirement for third-party software are regarded as disadvantages.

Samuel Fosso Wamba et al [15] The objective of this research is to close a knowledge gap in the body of existing Bitcoin, Blockchain, and FinTech literature. It allows you to assess your degree of understanding of Bitcoin, Blockchain, and Fintech, as well as how they have evolved. The information shows that businesses are implementing these technologies to obtain a competitive advantage and that they are evolving. Therefore, businesses must take advantage of this research to better comprehend these technologies, improve their company strategy, & generate crucial insights for decision-making. Security and trust can be increased by using blockchain and zero trust. However, the software is prohibitively pricey.

Jesus Iglesias Garcia et al [16] This paper discusses Hyot, a blockchain-based method for monitoring IoT activity. Strange events associated with sensors are explicitly recorded using an authorized Blockchain on a Raspberry Pi 3 computer. A web-based system was made available for exploiting the real-time data that has been gathered like this. Compared to public BCs, it offers a substantially greater transaction rate.

Hye-Young Paik et al [17] The development goals to increase awareness of blockchain technology as a information repository and to encourage a logical approach to integrating it into large software systems. It is necessary to first establish the common architectural layers of a typical software system with data stores before we can conceptualize every layer in terms of a blockchain. Second, we examine the placement and movement of data within blockchain-based programs. The third section looks at blockchain data management difficulties, especially when utilized as a dispersed data store. Fourth, they discuss reliable data analytics enabled by blockchain technology and analytics of blockchain information. The privacy and quality assurance issues around data governance in blockchains are the last thing we examine. These methods do, however, have certain practical drawbacks, including greater transaction costs, the necessity of utilizing minors as witnesses, and the reliance on third-party software to enable communication between blockchains are all disadvantages.

Cordeiro et al [18] To build interest and expertise in these areas, this article will examine recognized hazards, how they are identified, and their impact on systems, tactics to prevent them, as well as methods to control and resolve them, using an industry case study as a reference. The creation of innovative services with improved performance and added value, as well as the reduction of data acquisition costs for existing services and the opportunity to create new sources of income within the context of a sustainable business model, will be among the main advantages and benefits of IoT. However, the limits include data minimization and storage.

Wenyu (Derek) Du et al [19] the study suggests that the Blockchain technology that emerging fintech technology can cope with the business organization and business process. Since blockchain is new technology so most of the studies are about presenting a theoretical framework for business solutions. The real implementation of a blockchain-based framework is less. To solve this problem authors presented a process framework based on Actualization and affordance theory. The authors list three advantages of blockchain technology for the company as well as a method for achieving these advantages. The A-A theory, which states that blockchain use cases can be identified in transactions and other business processes, is supplemented by the process model in an experimentation stage. The paper discusses A-A theory, blockchain, and how to use the blockchain to solve transaction, business process-related problems. This research can also assist IT professionals in efficiently implementing blockchain and extracting value from their investments.

Yuri Bobbert et al [20] This research outlines the state of the art for using zero trust at the moment. In this article, ON2IT's "Zero Trust Innovators" assess the shortcomings of current methodologies and how they are addressed in the Zero Trust Framework. The key benefits of this strategy are that risk & technology can be matched with better accuracy and economic efficiency. However, portal technology must be incorporated in the future to improve security.

Larry Nace et al [21] in this research, the TBO infrastructure and application security in the NAS are addressed using a mixed ZTX approach. To guarantee TBO goals are met and to provide defensive depth to fend off any insider threats, the FAA must consider applying a hybrid ZTF theory method. This would entail using the ZTF

application on the NAS Zero Trust extended (ZTX) platform to reinforce the current boundary safeguards given by the FAA Telecommunications Infrastructure (FTI) network. By allowing data integration for this analysis, the security risk is increased due to sophisticated threats that can penetrate the NAS's secure perimeter and interfere with or jeopardize flight safety. Utilizing this platform significantly reduces data leakage.

Peiyun Zhang et al [22] A blockchain system confronts a variety of safety & trust challenges, includes attacks on the propagation & consensus processes, it could lead to erroneous data being stored or data dissemination being delayed. The fundamental design of blockchains is examined in the article along with potential security and trust issues at the data, network, consensus, smart contract, and application layers. Security has improved with data encryption while using the blockchain with zero trust architecture. But to develop the automatic detection of blockchain risks, new techniques are needed. This is essential to offer incentive-compatible consensus methods so selfish nodes in a decentralized blockchain system can handle block verification and accounting on their own.

Sobia Mehrban et al [23] Ever as the introduction of data sharing in e-health systems, data security has been a hotly debated and researched subject. Although data digitization has boosted productivity & speed, it has also made information more susceptible to cyberattacks. Medical records and data breach activities are frequently targeted by hackers. To defend the system, perimeter-based solutions such as firewalls, VPN utilization, and encryption techniques are used, however, their effectiveness is limited. The authors propose that the blockchain could be a viable option for preserving medical data (images) from the beginning to the end of the medical image transmission process. Blockchain technology, according to the research, maintains data integrity by keeping a record of transactions. The zero-trust principle, on the other hand, ensures that medical data is secure and that only verified persons and equipment can communicate with the network. The result reveals that the suggested system has higher security than the present one. A framework for legislative recommendations, however, might offer FinTech users a workable solution to security issues.

Ryan Randy Suryono et al [24] This study aims to: (1) evaluate the current state of the financial technology research sector; (2) recognize research needs, and (3) pinpoint obstacles and trends for prospective future research. This study's new proposal contains financial technology-related theoretical contributions. The results of this study offer a theoretical framework for information systems-based fintech research, including the definition and advancement of fintech technological concepts. To authenticate the caliber of the literature and analysis, this research used Kitchenham's method of systematic literature review together with theme analysis, meta-analysis, and observation. Finally, there are still a lot of benefits that may be derived from fintech research, such as advancements in legislation, security, monitoring, and even other technologies. This literature study can serve as a starting point for future studies to comprehend fintech. Future research in computer science can focus on AI, including algorithms, methods, and finance system strategies.

Nashirah Abu Bakar et al [25] This research developed a method to identify the transactional framework for the electronic wallet payment system in the digital economy. This study outlined the steps involved in a transaction, from the registration of users and service providers to the composition of payments and profit generation for the e-wallet provider's business model. To raise public awareness of the e-wallet transaction, this research offers a precise and trustworthy analysis. In the sectors of the digital economy, the structure employed in this study supports the growth of small and medium-sized firms.

Miguel Pincheira et al [26] The author of this study presents a software architecture designed specially for a trustless water management system, where a small number of IoT sensors can exchange sensed data directly over a public blockchain network. The author uses commercially available hardware to implement the suggested system and thoroughly tests its memory, program size, communication overheads, & power consumption. The findings demonstrate that conventional IoT devices may generally be utilized to communicate immediately and without unnecessary difficulty with a blockchain. More particular, these devices use just 6% more energy than they would normally use to interface with a gateway. The measurement of energy usage at the device level with greater accuracy will be the focus of future research. To achieve this, an accurate estimation of the daily energy budget that takes into account both the idle and sensing modes is required. The creation of the smart contracts that will support our proposal is a key component of this project's road plan.

Hayder M. Kareem Al Duhaidahawi et al [27] in this study, the author examines the definition of fintech and assesses how much fintech factors have an impact on the dependent variable of cyber security. In their study, all correlation coefficients demonstrated a positive relationship and were significant at the level of 0.01; additionally, they discovered that the influence factor between the research variables had a favorable effect when it was significant at the level of 0.05 for all sections of the independent variable. As a result, the authors accepted the correlation hypotheses. The study discovered that the effect coefficient had greatly grown to 0.908, which explains why the independent variable's portions complement one another.

Maliha Sultana et al [28] A relatively new technology called blockchain has shown to be an effective tool for safeguarding private data. The zero trust security paradigm mandates that security measures be taken at every level, including before, during, and even after the transmission of medical images, to guarantee the overall protection of medical information (pictures). A decentralized and trustless framework for secured medical information & image transfer and storage was developed by fusing these two concepts in this study, which looked at a range of works addressing these two concepts. According to the findings of the research, by preserving a record of every transaction, blockchain technology preserves data integrity. Zero trust principles, meanwhile, assure that medical data is protected and that only authorized people and equipment communicate with the network. As a consequence, a suggested methodology addresses a number of data security concerns. Finding ways to speed up and improve the system's usability is one of our future objectives.

Zhiyu Chen et al [29] This study creates a data protection architecture that addresses the device, data, & business layers, accomplishes high-level security protection of data flow in all power network channels, and enhances the system's safety monitoring and control capacity. This research suggests the use of BcT to improve data interaction safety and provide high-level data circulation protection in all power network links. The strategy described in this work tightly manages the application of control information, standardizes data use rights management and enhances the trustworthiness and interaction rate of corporate data. However, terminal software remains a threat.

Yuri Bobbert et al [30] The first section of the article summarises the limitations of current techniques and how they are dealt with in the ZTF created by ON2IT's 'Zero Trust Innovators.' The design and engineering of a Zero Trust object that resolves the current issues are then described, in accordance with Design Science Research (DSR). The design of an empirical validation using practitioner-oriented research to enhance the use of Zero Trust approaches is described in the study's concluding part, and how 73 security professionals participated in this validation in 2020. The result is a framework that is suggested and related to technology that, using Zero Trust principles, addresses various organizational layers to understand and align cyber security concerns, as well as comprehend the organization's readiness and fitness to counter cyber security hazards. However, the operating cost of this system is high.

Britta Hale et al [31] This article suggests a method depends on well-established security principles like Zero-Trust & defense-in-depth to assistance prohibit and mitigate security risks, including those arising from ML-based components. The demonstration of the methodology is based on an Unmanned Aerial Vehicle (UAV) case study with an advanced Intelligence, Surveillance, and Reconnaissance (ISR) module. However, this paradigm is lacking in a balance between mission performance, security, and resources.

Christopher A. Villareal [32] The goal of this design is to add to the body of information regarding trust-extended UTAUT studies and study which aspects matter when adopting DIMS expending the Unified Theory of Acceptance and Uses of Technology (UTAUT). This study provides IT decision-makers with acceptance-based information on whether to implement DIMS. The data inform DIMS developers that potential users rely on their DIMS adoption mainly on Trust and Performance Expectancy.

Sairath Bhattacharjya et al [33] The model has a zero-trust architecture, meaning that before being processed, all requests and replies are verified. This study presents a novel approach to efficiently generate a secret key for every user & device pair. The strategy establishes the foundation for end-to-end encrypted communication. One advantage of using the key is that the command and device response are hidden from all parties, including the gateway. With the others, each pair can safely communicate. The P3 connection paradigm automates the key generation and can assist ensure privacy during communication. However, this paradigm has a few drawbacks, including resource constraints, a lack of user authentication, and insufficient encryption.

Aleksandra Scalco et al [34] This study demonstrates how RA is used in the critical infrastructure vertical of the Healthcare and Public Health industry to investigate ideas like Zero Trust (ZT) and Defense-in-Depth (DiD) structure principles associated to policymaking. The benefits of the RA include improved decision-making and policy-making assistance for cyber security in control systems.

Hesam Hamledari et al [35] This study demonstrates that current payment programmes, even those that are computerised, cannot safely automate progress payments due to their reliance on centralised control systems and lack of execution guarantees. The study examines how these limitations might be handled by decentralised, blockchain-based smart contracts. It examines how smart contracts can reliably and autonomously condition cash flow on the state of a product flow and examines the theoretical foundation for the creation of an automated payment system. This project holds higher security and trust over other system. But this model is relay on centralized systems for command and control, as well as a lack of execution assurance.

Kris Oosthoek [36] this document provides the summary of DeFi security incidents that have occurred in the wild. Many of these exploits are market assaults, in which badly designed business logic in one protocol is combined with credit granted by another to increase appropriations. Attackers are increasingly utilizing DeFi's strength of permissionless composability against itself, rather than misusing individual protocols. DeFi is the first to provide a comprehensive examination of real-world security issues within the young financial ecosystem. According to the author, the enhanced Defi will give higher security than other model. However, because this is a developing approach, the Defi must be updated every 16 months.

Kwok-Yan Lam et al [37] In this paper, the author recommends a security reference architecture for identifying security threats, taking care of security requirements, and comprehending security challenges with intricate IoT systems. It offers a security reference architecture focused on Activity-Network-Things (ANT), which is built on the three architectural viewpoints for examining IoT systems: device, internet, and semantic. This structure is malleable enough to handle any IoT application, making it simple to apply to the scenario of SAGIN-enabled IoV.

Zachary A. Collier et al [38] The author of this article proposes the concept of a supply chain with zero trust. An ideology with a zero trust foundation is one that originated in the IT sector and cyber security and presupposes that all actors and activity are unreliable. In this paper, the author connects supply chain principles to zero trust and discusses the actions an organization may take to make the change. With this model, the service will be highly secured and the tread prevention will be improved. However, this model's transaction costs are considerable, and it only works with a few software applications.

Suparna Dhar et al [39] the author of this paper addresses the security concerns associated with IoT implementation and proposes a blockchain-based, zero-trust paradigm for IoT device security. The characteristics & communication protocols of IoT devices are becoming more similar thanks to risk-based segmentation of the IoT network. Zero Trust widens the trust's circle beyond the IT/OT network. The IoT network's device documentation and access control capabilities are enhanced by

blockchain. Both academic academics and practitioners will benefit from the IoT implementers will be able to address current security difficulties with the help of the suggested IoT security architecture. Future research will need to develop techniques for assessing the dependability of the suggested architecture in a real IoT network.

Sultan Algarni et al [40] In this study, a unique method for managing the delivery of decentralised, lightweight safe access control for an IoT system is provided, depends on a multi-agent system & blockchain. The primary purpose of the proposed technique is to build Blockchain Managers (BCMs) for securing IoT access control and enabling protected communication between local IoT devices. Additionally, technology permits safe connectivity between cloud computing, fog nodes, and IoT devices. The proposed framework will be used in subsequent studies to evaluate the degree to which the fundamental security objectives integrity through the use of digital signatures, the requirements for shared secret key authentication, MAC policy authorization, and public key encryption have been satisfied.

Lampis Alevizos et al [41] The author looks into how ZTA can be added onto endpoints in the work due to the concurrence of ZTA with blockchain-based intrusion detection and prevention. In particular, the author conducts a cutting-edge analysis of ZTA models, actual designs that focus on endpoints, and intrusion detection systems based on blockchain. From the review, it is found that there is no need for tight resource integration. Adopting this technique is still hampered by issues with performance, computational costs, and choosing the appropriate blockchain implementation. Further research is required to adequately answer these questions.

Xiaohan Hao et al [42] In contrast to situations where one may rely on a trustworthy third party, sharing information is more challenging in zero-trust environments. They suggest a zero-trust information-sharing protocol that uses blockchain technology to address this problem. It can filter out fabricated information while preserving participant anonymity. The performance of our protocol is then assessed by a number of experiments, and the safety of our procedure is finally proved in the commonly compostable confident structure. The evaluation results demonstrate that our protocol's three crucial steps execute on average in 0.059 seconds, 0.060 seconds, and 0.032 seconds, indicating that it has the potential to be used in a real-world setting. Future improvements, however, will focus on strengthening our system's security by lowering the necessary communication, computation, and time overheads (against a wider variety of assaults).

Cyril Onwubiko [43] Protecting digital investments, ensuring a safe, secure, and favorable business environment, safeguarding a country's vital national infrastructures, and promoting citizen welfare are its three main objectives. The author of this research examines operational elements that affect CyberOps situational awareness, in particular, the features that deal with understanding and comprehension of operational and human factors aspects and that aid in providing insights on human operator decision-making. But this model requires a human operator.

Yang Xiao et al [44] The novel blockchain-based decentralised SAS architecture known as BD-SAS offers SAS services successfully and securely without depending on the dependability of any particular SAS server. G-Chain is a worldwide blockchain that BD-SAS utilises to comply with spectrum regulations. and local blockchains (L-

Chains) with smart contract functionality are created in each spectrum zone to automate spectrum access assignment based on user requests. A proposed strategy for fault-tolerant spectrum access management is a decentralized SAS architecture. But more automation, flexibility, and finer granularity are necessary.

José María Jorquera Valero et al [45] Adversaries in 5G-enabled environments can take advantage of resource-sharing flaws to launch lateral attacks against other tenant resources, interfere with the delivery of 5G services, or even damage infrastructure resources. Additionally, the multi-tenancy security problems or the dynamic nature of 5G infrastructure vulnerabilities cannot be addressed by the current security and trust models. As a result, a novel security and trust paradigm for 5G multi-domain circumstances is presented in this work. The author presents to demonstrate its value, a supporting 5G network framework is used with a threat model for multi-tenant scenarios. Additionally, the author provides a number of mitigation strategies, including enhancing security and trust levels through network security monitoring, threat analysis, and end-to-end trust configurations. The architecture is put to use in a real-world use case by the H2020 5GZORRO project, which envisions a multi-tenant system where domain owners can freely share resources. The proposed framework reduces the requirement for human interaction by establishing a protected environment with zero-touch automation capabilities.the systematic surevy on Block Chain for Financial Transaction in Zero Trust Architecture has been shown in Table 2.

Ref no	Publish On	Author	Technique	Significance	Limitation
11	2018	Casimer DeCusatis	In this article, for blockchain apps that are hosted in the cloud, the author presents experimental test bed results for a cutting-edge user identity management technique. To request a new session, they use a Black Ridge Technology endpoint on a Windows host to add cryptographic identity tokens to the initial packet.	This model requires less time to use than other models.	A third-party program is necessary
12	2018	Mayra Samaniego	In this study, they offer Amatista, a blockchain-based middleware for IoT administration. With its innovative zero-trust hierarchical mining method, Amatista makes it possible to authorize frameworks and transactions at different degrees of trust.	By using Amatista the performance is increased.	Algorithms in Amatista need to be updated.
13	2018	Jungho Kang	To indicate requirements and security concerns and the study will examine current trends in mobile Fintech payment services & classify in accordance with service methods to enable the provision of better and further secure services in the future.	Consider mutual authentication, authorization, integrity, privacy, and availability while developing	Future development should be done with different applications.

				fintech payment systems.	
14	2018	Nir Kshetri	Case examples of various stages of blockchain development for various applications are discussed	The use of the blockchain and zero trust can boost trust and security.	The transaction costs and the requirement for third-party software are regarded as disadvantages
15	2018	Samuel Fosso Wamba	The goal of this research is to close a knowledge gap in the body of existing Bitcoin, Blockchain, and FinTech literature.	Using blockchain & zero trust can improve security and trust.	The cost of the software is prohibitively high.
16	2019	Jesus Iglesias Garcia	In this paper, Hyot a blockchain-based Internet of Things (IoT) activity registration service is introduced.	Compared to public BCs, it has a substantially greater transaction rate.	Required third-party software
17	2019	HYE-YOUNG PAIK	The project intends to encourage a logical approach to implementing blockchain technology in big software systems and to raise awareness of blockchain technology as data storage.	This model gives higher Atomicity, concentricity, and isolation of troubles	This model required higher transaction costs and third-party software.
18	2019	Cordeiro	This paper will discuss recognized dangers, how they are identified, and how they are mitigated Its influence on systems, techniques to avoid them, and strategies to contain and resolve them to develop interest and understanding in these subjects, using an industry case study as a reference.	Data accusation cost is low	Data minimization and storage.
19	2019	Wenyu (Derek) Du	The article goes through A-A theory, blockchain, and how to use blockchain to solve transaction and business process challenges. This research can also help IT professionals adopt blockchain more efficiently and get the most out of their investments.	This model will give the result in the most efficient and cost-effective.	Blockchain needs to upgrade frequently.
20	2020	Yuri Bobbert	The study examines the limits of current techniques and how the ON2IT 'Zero Trust Innovators' Zero Trust Framework addresses them.	This system has higher precision and cost-effectiveness.	Lack of portal technology.

21	2020	Larry Nace	In this research, a hybrid ZTX method for TBO infrastructure and application security in the NAS is proposed.	Data leaking is decreased.	The algorithm needs to be more strong
22	2020	Peiyun Zhang	The fundamental architecture of a blockchain is examined, as well as potential issues with trust and security at the application, data, network, consensus, and smart contract layers.	Using blockchain and zero trust the security and data encryption has been improved.	A new mechanism is required for the automatic detection of data leakage.
23	2020	SOBIA MEHRBAN	This article presents a detailed examination of FinTech by evaluating current and potential privacy and security issues in the banking sector. It offers a complete overview of contemporary security challenges, detection, and prevention. FinTech has been proposed with mechanisms and security options.	This model gives higher security than other system	To handle security challenges a policy recommendation using a framework can be a workable solution.
24	2020	Ryan Randy Suryono	This study's goals are to: (1) evaluate the state of the art in financial technology research; (2) recognize research gaps in the area; and (3) recognize roadblocks and trends for potential future scope.	This model has high security and monitoring.	The Foundation of FinTech needs to make strong
25	2020	Nashirah Abu Bakar	This study outlined the steps involved in a transaction, from the registration of users and service providers to the composition of payments & profit generation for the e-wallet provider's business model.	This model can be used in small-scale businesses.	This model needs to be updated frequently
26	2020	Miguel Pincheira	In this study, the author presents a software architecture designed for a trustless water management system where constrained IoT devices can directly exchange sensed data on a public blockchain network.	This model consumes very less energy when compared with other models.	Budget is high
27	2020	Hayder M. Kareem Al_Duhaidahawi	In this study, the author examines the definition of fintech and assesses how much fintech factors affect cyber security, the dependent variable.	The coefficient significantly increased to 0.908	It was compactable with limited software
28	2020	Maliha Sultana	The zero trust security paradigm ensures that security measures are put in place at every level, from the beginning, during, and even after medical image transmission, to offer overall protection of medical data (images).	This method to improves the security of medical data transfer.	The processing speed is low

29	2021	Zhiyu Chen	This study recommends using BcT to increase data interaction security and provide high-level data circulation protection in all power network lines.	The credibility & engagement rate of business data were both enhanced by this method.	Terminal software remains a threat.
30	2021	Yuri Bobbert	The definition of asset owners' participation from a commercial perspective is one of the main objectives of the ON2IT ZTF design, leading to more clear interpretations of concepts like risk appetite and recovery time objectives.	It gives higher security protection	The cost of this system is high
31	2021	Britta Hale	This paper proposes a method for preventing and mitigating security threats, including those originating from ML-based components, depends on accepted security principles like Zero-Trust and defense-in-depth.	The security of the system is enhanced.	This paradigm is deficient in terms of balancing mission performance, security, and resources.
32	2021	Christopher A. Villareal	The goal of this design is to study which aspects matter when adopting DIMS using the unified theory of acceptance (UTAUT) & to advance the corpus of information around trust-extended UTAUT investigations.	Trust and Performance of this model is high	It is required to pay exorbitant fees for carrying out transactions.
33	2021	Sairath Bhattacharjya	This study presents a novel approach to efficiently generate a secret key for every user and device pair.	Device responses are hidden from all parties.	There are a few limitations to this paradigm, including resource limits, a lack of user authentication, and insufficient encryption.
34	2021	Aleksandra Scalco	The use of RA in the healthcare and public sectors is highlighted in this paper. Critical infrastructure in the healthcare industry is assessing policymaking ideas like Zero Trust (ZT) and Defense-in-Depth (DiD) design principles.	Better cyber security decision-making and policy-making	The introduction of a context-aware environment has been abandoned.
35	2021	Hesam Hamledari	The paper examines how decentralized smart contracts built on the blockchain can get around these limitations. An automated payment system's theoretical underpinnings are investigated, as well as the usage	Higher levels of security and trust than other systems	This model relies on centralized execution and control systems with

			of smart contracts to enable reliable & autonomous conditioning of cash flow on product flow status.		no assurance of proper execution.
36	2021	Kris Oosthoek	The first overview of real-world DeFi security incidents is presented in this study. The study noticed that many of these exploits are market attacks that use credit granted by another protocol to weaponize poorly designed business logic in one protocol and inflate appropriations.	More security will be provided by Defi than by any other model.	The Defi must be updated every 16 months.
37	2021	Kwok-Yan Lam	In this research, the author describes a method for comprehending complicated IoT system security concerns and for identifying security threats and addressing security needs, offering a security reference architecture.	This system is more flexible than other models	Fine-grained access controls to resources or applications are no longer available.
38	2021	Zachary A. Collier	In this article, the author connects supply chain principles to zero trust and discusses the actions a firm may take to make the change.	A high level of security will be provided for the service, and tread prevention will be enhanced.	This architecture only functions with a limited number of software applications and has high transaction costs.
39	2021	Suparna Dhar	The author of this paper examines the security issues related to IoT implementation and suggests a paradigm for IoT device security based on blockchain and zero trust.	The security feature has been enhanced.	This model is lack reliability.
40	2021	Sultan Algarni	Creating Blockchain Managers (BCMs) for securing IoT access control & enabling safe communication between local IoT devices is the major objective of the proposed approach.	The encryption is high in this model.	This model is lacking digital signature and authentication via a secret key.
41	2021	Lampis Alevizos	Motivated by the integration of ZTA with intrusion detection and prevention using blockchain, researchers investigate how ZTA can be added to endpoints in this work.	There is no requirement for tight resource integration.	Performance and computing cost is high
42	2021	Xiaohan Hao	In contrast to situations where we may rely on a trustworthy third party, sharing information is more challenging in zero-trust environments. We suggest a zero-trust information-sharing protocol that uses blockchain technology to address this problem. It can filter out fabricated information while preserving participant anonymity.	The execution time is very low	The communicatio n and calculation time need to improve.

43	2022	Cyril Onwubiko	This study examines operational characteristics that affect CyberOps situational awareness, in particular, the elements that contribute to understanding operational and human factors components and provide insights into how human operators make decisions.	The security treads are minimized.	Human operator is required.
44	2022	Yang Xiao	BD-SAS is a unique blockchain-based decentralized SAS architecture that gives SAS services securely & effectively without depending on the reliability of any one SAS server.	It gives a promising technique for fault-tolerant and resilient spectrum access management	More automation, flexibility, & granularity are required.
45	2022	José María Jorquera Valero	The multi-tenancy security challenges or the dynamic nature of threats to 5G framework cannot be addressed by the current security and trust paradigms. In this study, the author so suggests a novel safety and trust paradigm for 5G multi-domain scenarios.	This model minimizes human intervention by offering zero-touch automation possibilities.	The framework needs to be updated regularly.

Table 2. Systematic Review on Block Chain for Financial Transaction in Zero Trust Architecture

5. Summary

Fintech security is a significant concern in the fintech ecosystem, according to the literature review. Embedded systems, mobile networks, cloud computing, big data analysis, & other technologies are included in fintech. Online banking, wallets, and other services are just a few of the fintech industry's many applications. However, issues with security, privacy, risks, and cyber-attacks exist in the fintech sector.

In contrast, the idea of "never trust, always verify" is the foundation of the zero-trust approach to safeguarding network devices and other entities. Zero trust security solutions are based on policy enforcement engines and are used in a variety of industries, including Google's Beyond Corp, Forrester NGFW/ZTX, and others. Zero-trust is also utilized in wireless networks, the IoT, cloud computing, & edge computing.

Blockchain technology is a novel fintech technology with characteristics such as immutability, availability, and consensus. The majority of blockchain research is concentrated on creating and implementing frameworks.

According to the survey, FinTech with zero trust architecture can increase security with high encryption. However, every technological advancement has a few drawbacks that must be addressed before more effective and secure financial transactions can be conducted.

6. Challenges and Future Scope

According to the results of the survey, there are a few limitations in current technology that must be addressed to achieve greater security encryption and cost-effectiveness. Some limitations are listed below.

- The model has a very high-cost factor.
- Effective communication necessitates the use of third-party software.
- Human intervention is still required to monitor the process.

6.1. Future Scope

The solution for the challenges facing

- To complete the process, third-party software is required. Reduce the use of third-party software in the future, and once the third-party software is terminated, the cost factor will also decrease.
- Human supervision is always required in financial transactions; however, if we can create an update in an automatic process, the need for human supervision will be reduced.

7. Conclusion

The financial industry and its related services are significantly impacted by a recent disruptive technological trend. As a result, technology has fundamentally changed how the financial sector functions. Though its shape and contours are still unclear, research on this quickly spreading trend has already begun. At this point, it is necessary to gain an understanding of the information being offered on this new technology.

The goal of this study is to increase awareness by reviewing and classifying the material. After offering a thorough analysis of FinTech and assessing recent research on security and privacy issues in the financial industry, this paper provided a taxonomy of current security difficulties, detection mechanisms, and security solutions for FinTech. This article goes into great detail about the suggested plans for the security and privacy of financial technologies. Finally, to propose future directions for this new technological era, future research issues are explored.

Funding

The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Conflict of interest

The authors declare that they have no conflict of interest.

Author Contributions

All authors read and approved the final manuscript

Data Availability Statement

Data sharing not applicable to this article, because it's confidential.

Ethical Approval

The article does not contain any studies with Human Participants or animals performed by any of the Authors.

References

[1] B. B. Pena, "Understanding and designing technologies for everyday financial collaboration," University of Northumbria at Newcastle (United Kingdom), 2021.

[2] S. Kak, "Zero Trust Evolution & Transforming Enterprise Security (Doctoral dissertation, California State University San Marcos)," 2022.

[3] M. Kaur & S. Gupta, "Blockchain technology for convergence: an overview, applications, and challenges," Blockchain and AI Technology in the Industrial Internet of Things, pp.1-17, 2021.

[4] S. Berlato, R. Carbone, A. J. Lee & S. Ranise, "Formal modelling and automated trade-off analysis of enforcement architectures for cryptographic access control in the cloud," ACM Transactions on Privacy and Security, Vol. 25, No.1, pp.1-37, 2021.

[5] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen & E. Dutkiewicz, "Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities," IEEE access, Vol. 7, pp.85727-85745, 2019.

[6] T. Hardjono & N. Smith, "Towards an attestation architecture for blockchain networks," World Wide Web, Vol. 24, No.5, pp.1587-1615, 2021.

[7] J. J. O'Hare, A. Fairchild & U. Ali, "Money & Trust in Digital Society, Bitcoin and Stablecoins in ML enabled Metaverse Telecollaboration," arXiv preprint arXiv:2207.09460, 2022.

[8] C. Buck, C. Olenberger, A. Schweizer, F. Völter & T. Eymann, "Never trust, always verify: A multivocal literature review on current knowledge

and research gaps of zero-trust," Computers & Security, Vol. 110, p.102436, 2021.

[9] M. Pace, "Zero Trust networks with Istio (Doctoral dissertation, Politecnico di Torino)," 2021.

[10] A. John, A. Reji, A. P. Manoj, A. Premachandran, B. Zachariah & J. Jose, "A novel hash function based on hybrid cellular automata and sponge functions," In Asian Symposium on Cellular Automata Technology, pp.221-233, 2022, March. Singapore: Springer Nature Singapore.

[11] C. DeCusatis, M. Zimmermann & A. Sager, "Identity-based network security for commercial blockchain services," In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), pp.474-477, 2018, January. IEEE.

[12] M. Samaniego & R. Deters, "Zero-trust hierarchical management in IoT," In 2018 IEEE international congress on Internet of Things (ICIOT), pp.88-95, 2018, July. IEEE.

[13] J. Kang, "Mobile payment in Fintech environment: trends, security challenges, and services," Human-centric Computing and Information sciences, Vol. 8, No.1, pp.1-16, 2018.

[14] N. Kshetri, "1 Blockchain's roles in meeting key supply chain management objectives," International Journal of information management, Vol. 39, pp.80-89, 2018.

[15] S. Fosso Wamba, J. R. Kala Kamdjoug, R. Bawack & J. G Keogh, "Bitcoin, blockchain, and FinTech: a systematic review and case studies in the supply chain," Production Planning and Control, Forthcoming, 2018.

[16] J. Iglesias García, J. Diaz & D. Arroyo, "Hyot: Leveraging Hyperledger for Constructing an Event-Based Traceability System in IoT," In International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on EUropean Transnational Education (ICEUTE 2019) Seville, Spain, May 13th-15th, 2019 Proceedings, Vol. 12, pp.195-204, 2020. Springer International Publishing.

[17] H. Y. Paik, X. Xu, H. D. Bandara, S. U. Lee & S. K. Lo, "Analysis of data management in blockchain-based systems: From architecture to governance," IEEE Access, Vol. 7, pp.186091-186107, 2019.

[18] C. Cordeiro & H. Barbosa, "Digital Privacy and Security Conference."

[19] W. D. Du, S. L. Pan, D. E. Leidner & W. Ying, "Affordances, experimentation and actualization of FinTech: A blockchain implementation study," The Journal of Strategic Information Systems, Vol. 28, No.1, pp.50-65, 2019.

[20] Y. Bobbert & J. Scheerder, "Zero trust validation: from practical approaches to theory," Sci. J. Res. Rev, Vol. 2, No.5, 2020.

[21] L. Nace, "Securing Trajectory based Operations through a Zero Trust Framework in the NAS," In 2020 Integrated Communications Navigation and Surveillance Conference (ICNS), pp.1B1-1, 2020, September. IEEE.

[22] P. Zhang & M. Zhou, "Security and trust in blockchains: Architecture, key technologies, and open issues," IEEE Transactions on Computational Social Systems, Vol. 7, No.3, pp.790-801, 2020.

[23] S. Mehrban, M. W. Nadeem, M. Hussain, M. M. Ahmed, O. Hakeem, S. Saqib ... & M. A. Khan, "Towards secure FinTech: A survey, taxonomy, and open research challenges," IEEE Access, Vol. 8, pp.23391-23406, 2020.

[24] R. R. Suryono, I. Budi & B. Purwandari, "Challenges and trends of financial technology (Fintech): a systematic literature review," Information, Vol. 11, No.12, p.590, 2020.

[25] N. A. Bakar, S. Rosbi & K. Uzaki, "E-wallet transactional framework for digital economy: a perspective from Islamic financial engineering," International Journal of Management Science and Business Administration, Vol. 6, No.3, pp.50-57, 2020.

[26] M. Pincheira, M. Vecchio, R. Giaffreda & S. S. Kanhere, "Exploiting constrained IoT devices in a trustless blockchain-based water management system," In 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp.1-7, 2020, May. IEEE.

[27] H. M. K. Al Duhaidahawi, J. Zhang, M. S. Abdulreza, M. Sebai & S. A. Harjan, "Analysing the effects of FinTech variables on cybersecurity: Evidence form Iraqi Banks," International Journal of Research in Business and Social Science, No.6, pp.123-133, 2020.

[28] M. Sultana, A. Hossain, F. Laila, K. A. Taher & M. N. Islam, "Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology," BMC Medical Informatics and Decision Making, Vol. 20, No.1, pp.1-10, 2020.

[29] Z. Chen, L. Yan, Z. Lü, Y. Zhang, Y. Guo, W. Liu & J. Xuan, "Research on zero-trust security protection technology of power IoT based on blockchain," In Journal of Physics: Conference Series, Vol. 1769, No.1, p.012039, 2021. IOP Publishing.

[30] Y. Bobbert & J. Scheerder, "On the design and engineering of a zero trust security artefact," In Advances in Information and Communication: Proceedings of the 2021 Future of Information and Communication Conference (FICC), Vol. 1, pp.830-848, 2021. Springer International Publishing.

[31] B. Hale, D. L. Van Bossuyt, N. Papakonstantinou & B. O'Halloran, "A zero-trust methodology for security of complex systems with machine learning components," In International design engineering technical conferences and computers and information in engineering conference, Vol. 85376, p.V002T02A067, 2021, August. American Society of Mechanical Engineers.

[32] C. A. Villareal, "Factors Influencing the Adoption of Zero-Trust Decentralized Identity Management Solutions (Doctoral dissertation, Capella University)," 2021.

[33] S. Bhattacharjya & H. Saiedian, "Establishing and validating secured keys for IoT devices: using P3 connection model on a cloud-based architecture," International Journal of Information Security, Vol. 21, No.3, pp.427-436, 2022.

[34] A. Scalco, D. Flanigan & S. Simske, "Control Systems Cyber Security Reference Architecture (RA) for Critical Infrastructure: Healthcare and Hospital Vertical Example," Journal of Critical Infrastructure Policy 2.2 (2021): 125-43. Print, 2021.

[35] H. Hamledari & M. Fischer, "Role of blockchain-enabled smart contracts in automating construction progress payments," Journal of legal affairs and dispute resolution in engineering and construction, Vol. 13, No.1, p.04520038, 2021.

[36] K. Oosthoek, "Flash crash for cash: Cyber threats in decentralized finance," arXiv preprint arXiv:2106.10740, 2021.

[37] K. Y. Lam, S. Mitra, F. Gondesen & X. Yi, "ANT-centric IoT security reference architecture—Security-by-design for satellite-enabled smart cities," IEEE Internet of Things Journal, Vol. 9, No.8, pp.5895-5908, 2021.

[38] Z. A. Collier & J. Sarkis, "The zero trust supply chain: Managing supply chain risk in the absence of trust," International Journal of Production Research, Vol. 59, No.11, pp.3430-3445, 2021.

[39] S. Dhar & I. Bose, "Securing IoT devices using zero trust and blockchain," Journal of Organizational Computing and Electronic Commerce, Vol. 31, No.1, pp.18-34, 2021.

[40] S. Algarni, F. Eassa, K. Almarhabi, A. Almalaise, E. Albassam, K. Alsubhi & M. Yamin, "Blockchain-based secured access control in an IoT system," Applied Sciences, Vol. 11, No.4, p.1772, 2021.

[41] L. Alevizos, V. T. Ta & M. H. Eiza, "Augmenting zero trust architecture to endpoints using blockchain: A systematic review," arXiv preprint arXiv:2104.00460, 2021.

[42] X. Hao, W. Ren, R. Xiong, T. Zhu & K. K. R. Choo, "Asymmetric cryptographic functions based on generative adversarial neural networks

for Internet of Things," Future Generation Computer Systems, Vol. 124, pp.243-253, 2021.

[43] C. Onwubiko, "CyberOps: Situational Awareness in Cybersecurity Operations," arXiv preprint arXiv:2202.03687, 2022.

[44] Y. Xiao, S. Shi, W. Lou, C. Wang, X. Li, N. Zhang ... & J. H. Reed, "Decentralized spectrum access system: Vision, challenges, and a blockchain solution," IEEE Wireless Communications, Vol. 29, No.1, pp.220-228, 2022.

[45] J. M. Jorquera Valero, P. M. Sánchez Sánchez, A. Lekidis, J. Fernandez Hidalgo, M. Gil Pérez, M. S. Siddiqui ... & G. Martínez Pérez, "Design of a security and trust framework for 5G multi-domain scenarios," Journal of Network and Systems Management, Vol. 30, No.1, p.7, 2022.