**Blockchain-based Trust Management for IoT**

**Chapter 1**

*Introduction*

﻿ The Internet of Things (IoT) is revolutionizing our world, but its tremendous network of interconnected gadgets presents a challenge: trust. Securing information, ensuring device integrity, and enabling dependable verbal exchange are essential for achieving IoT packages. Traditional trust control techniques need to be revised to keep pace with the dynamic and ever-expanding nature of the IoT landscape.

This is where blockchain technology emerges as a game-changer. Blockchain's core strengths—its decentralized, tamper-proof nature and its capability to create a clear and immutable file—provide a powerful solution for achieving control in IoT. By leveraging blockchain, we will construct a more secure, reliable, and honest basis for the future of IoT.

*Background:*

Trust: The Cornerstone of Relationships

Trust is a fundamental concept that underpins our interactions with the sector around us. It's the sensation of confident reliance on the man or woman, ability, or truthfulness of a person or something. We region trust in friends and own family to maintain our secrets and techniques, in institutions to act with integrity, and in products to characteristic as advertised. Trust allows us to be susceptible, take risks, and collaborate successfully.

Managing Trust: Building and Maintaining Strong Bonds

Trust management is the continuing method of building, keeping, and repairing acceptance as true within relationships. This applies to both non-public and expert settings. Effective acceptance, as true with management, entails constant actions that demonstrate trustworthiness, including honesty, transparency, and accountability.

When considered damaged, accept it as true with control. Control specializes in rebuilding it through honest apologies, taking responsibility for errors, and demonstrating a commitment to alternate.

The Internet of Things (IoT): Connecting the Physical and Digital Worlds

The Internet of Things (IoT) refers to the community of physical gadgets embedded with sensors, software, and other technology that permit them to acquire and change information. These gadgets, ranging from smartphones to thermostats, connect to the Internet, permitting them to talk with each other and with us.

The IoT is swiftly transforming our world, growing more interconnected and automatic surroundings.

Applications of IoT: Transforming Everyday Life

The IoT programs are large and ever-evolving. In clever houses, IoT gadgets like related thermostats and home equipment can research our possibilities and modify robotically, improving consolation and performance. In cities, IoT sensors can reveal site visitors' float, manage waste series, and optimize power use. Businesses use IoT to tune stock, display the overall performance of gadgets, and improve delivery chain logistics. The opportunities are actually endless.

Blockchain: A Secure Foundation for the Digital Age

Blockchain is a disbursed ledger technology that allows for secure, obvious, and tamper-evidence recording of facts. Imagine a public document e-book, duplicated and allotted across a network of computers. Transactions are brought to the chain in chronological order, and each block is connected to the previous one, creating a permanent and verifiable file.

Blockchain offers considerable potential for numerous applications, including secure monetary transactions, transparent delivery chain management, and steady vote-casting systems.

*Security Challenges in IoT*

The Internet of Things (IoT) guarantees a world of convenience and automation. However, its fast boom has outpaced security concerns. This full-size network of interconnected gadgets, from smart audio systems to industrial manipulation structures, gives a unique set of protection-demanding situations. Let us explore some of the most critical:

Weak Security Measures: Many IoT gadgets come pre-configured with vulnerable default passwords or lack sturdy encryption, making them smooth targets for attackers. These gadgets often have constrained processing electricity and memory, making it hard to put into effect complicated safety answers.

Lack of Visibility and Control: The sheer quantity and diversity of IoT devices could make it difficult for groups to maintain a complete inventory and implement protection guidelines. These gadgets may be deployed outside of IT's purview, developing blind spots for potential vulnerabilities.

Insecure Communication Protocols: Some IoT devices rely on old or insecure conversation protocols, which are liable to eavesdropping and manipulation. This can disclose sensitive information or permit attackers to manipulate gadgets.

Software Vulnerabilities: The rapid development of IoT gadgets can result in insufficient security testing, leaving them susceptible to software bugs and recognized exploits. Patching these vulnerabilities can be difficult or may not be possible on positive devices, developing lengthy-term risks.

Botnet Formation: Large numbers of compromised IoT gadgets may be harnessed to form powerful botnets capable of launching large-scale denial-of-provider attacks or stealing significant quantities of statistics.

*Security Attacks*

These security challenges create a fertile floor for malicious actors. Here are a few commonplace safety attacks concentrated on IoT devices:

Denial-of-Service (DoS) Attacks: Attackers can crush IoT devices with requests, causing them to crash or become unavailable to valid users. Botnets shaped from compromised devices can launch devastating DoS assaults, disrupting crucial infrastructure or online services.

Man-in-the-Middle Attacks: Attackers can intercept conversations among IoT gadgets and steal sensitive records, such as login credentials or non-public information.

Malware and Ransomware: IoT gadgets can be inflamed with malware that allows attackers to take control of the device, secretly spy on users, or possibly hold their data hostage for ransom.

Physical Tampering: In some cases, attackers may gain a bodily advantage by getting admitted to IoT gadgets to steal data, set up malware, or disrupt their operation.

By understanding those protection challenges and assaults, we can take proactive measures to protect the future of IoT.

*Problem Statement*

﻿ The rapid growth of the Internet of Things (IoT) has revolutionized various elements of our lives. However, this good-sized network of interconnected devices affords a large assignment: agree with. Traditional acceptance as true with control approaches conflicts to hold pace with the dynamic and ever-increasing nature of the IoT landscape

***Objective of the study***

This thesis ambitions to explore the capacity of blockchain generation as a basis for belief control within the Internet of Things (IoT) panorama. The primary objective is to investigate how blockchain's precise characteristics, which include decentralization, immutability, and transparency, can cope with the crucial safety-demanding situations confronted by IoT gadgets and structures.

Specifically, they have a look at will recognition on:

* Analyzing the restrictions of conventional trust control processes in securing the incredible and dynamic environment of IoT.
* Identifying how the blockchain era can establish a secure data garage, ensure device integrity, and facilitate dependable conversation inside the IoT ecosystem.
* Evaluating capability applications of blockchain-based totally consider control answers in various IoT domain names, along with smart homes, commercial automation, and connected cities.
* Exploring the technical challenges and boundaries associated with imposing blockchain for IoT agrees with control.
* Proposing a framework or version for integrating the blockchain era into existing IoT architectures to beautify trust and protection.

***Organization o*f the thesis**

**Chapter 1: Introduction**

* Introduce the concept of consideration and its importance inside the IoT landscape.
* Highlight the safety-demanding situations confronted via IoT gadgets and traditionally agree with control barriers.
* Introduce blockchain generation and its ability advantages for trust management in IoT.

**Chapter 2: Background**

* Provide a comprehensive overview of control concepts and strategies.
* Explore the architecture and functionalities of the Internet of Things (IoT).
* Explain the center standards and mechanisms of blockchain technology.
* Discuss present protection answers and challenges in IoT environments.

**Chapter 3: Blockchain-primarily based Trust Management for IoT**

* Analyze the suitability of the blockchain era for addressing agreement with and protection issues in IoT.
* Explore how blockchain may be leveraged to obtain secure statistics storage, device integrity, and reliable communication.
* Discuss capacity programs of blockchain-based belief control answers in diverse IoT domain names.
* Evaluate the technical challenges and limitations associated with integrating blockchain into IoT structures.

**Chapter Four: Proposed Framework/Model**

* Propose a framework or model for integrating blockchain generation into existing IoT architectures to enhance acceptance as accurate and secure.
* Discuss the technical considerations for implementing the proposed framework/model.
* Analyze the potential benefits and boundaries of the proposed technique.

**Chapter 5: Evaluation and Future Research**

* Evaluate the proposed framework/version via simulations or proof-of-idea implementations.
* Discuss the limitations of the study and become aware of regions for future studies.
* Analyze the broader implications of blockchain-based total trust management for the destiny of IoT.

**Chapter 6: Conclusion**

* Summarize the key findings of the have a look at.
* Reiterate the ability of blockchain technology to grow a greater secure and straightforward IoT ecosystem.
* Discuss the future directions and capacity programs of blockchain-based belief management in IoT.

**Additional Sections**

* References: A complete listing of all assets mentioned throughout the thesis.
* Appendix (Optional): This can consist of extra technical information, assisting facts, or code samples used inside the examination.

**Chapter 2 Literature Review**

**Overview of Existing Techniques**

﻿ One technique involves reputation-based totally agrees with models (Braga et al., 2018). These fashions assign agree scores to devices based totally on their past interactions and behavior. Devices with an effective history of dependable conversation and data change earn better acceptance as true with scores, while those showing suspicious pastimes see their rankings decrease (Marr, 2016). This fosters collaboration amongst trusted devices and discourages malicious behavior. Another approach utilizes identity-based agreement with control. Here, devices are issued precise digital identities that can be validated on a steady platform. This permits authentication and authorization, making sure the simplest legal gadgets participate in the network and statistics alternate. These are just a few examples, and ongoing studies explore diverse techniques to set up agree inside the dynamic IoT panorama.

Luo et al. (2024) present a hybrid blockchain-based many-to-many cross-domain authentication mechanism for smart agriculture IoT networks. The work overcomes the issues created by centralised authentication systems by proposing a decentralized way to secure communication between agricultural devices across domains. The suggested technique enables simultaneous mutual authentication of different devices and data service providers from distinct agricultural systems. A group able batch verification algorithm is developed to improve the flexibility of cross-domain batch authentication by dynamically altering batch sizes for maximum efficiency. Furthermore, the technique includes a pseudonym updating process to protect device privacy and prevent unauthorized access by malevolent actors. The authors use security analysis and performance evaluation to illustrate the improved security characteristics and efficiency of their proposed authentication mechanism. The hybrid blockchain architecture protects secrecy through private chains while allowing for effective public verification among various agricultural entities. The study provides an important contribution by introducing a novel authentication method for IoT systems in smart agriculture, which combines the advantages of consortium and private blockchain to address the unique security requirements of cross-domain collaboration.

Asif et al. (2022) present a blockchain-based authentication and trust management method designed specifically for safeguarding smart cities within the Internet of Things (IoT) ecosystem. To address the limitations of traditional security architectures in resource-constrained IoT environments, the authors propose a solution that combines the ACE framework-based authorization blockchain with the Object Security Architecture for the Internet of Things (OSCAR) object security model. This mechanism ensures secure authorized access to smart city resources by providing a flexible and trustless authorization process. The study contains a practical implementation of the authorization blockchain on the ethereal network, using a node.js server and a Raspberry Pi B+ used to mimic a smart city. The authors' experimental results show that the system is feasible, with an authentication response time of less than 100 MS even with a rising number of clients, improving security in smart city deployments.

Kumar and Sharma (2022) give a comprehensive survey on the use of blockchain technology to ensure trust in Internet of Things (IoT) contexts. Recognising the security and privacy problems that IoT faces owing to resource restrictions, as well as the importance of data confidentiality and integrity, the authors highlight Blockchain’s potential as a secure and differentiated alternative. The poll opens with an overview of IoT and blockchain technologies, emphasising the security concerns with IoT and the potential answers provided by blockchain. The authors go into the complexities of merging blockchain with IoT while also exploring the benefits, such as decentralization, distributed ledgers, and increased trust. By conducting a comparative examination of traditional and blockchain-based trust management methodologies, the article emphasises the importance of blockchain in ensuring trust in the IoT ecosystem. The survey seeks to provide insights into the applications, vulnerabilities, and integration issues, serving as a helpful resource for understanding Blockchain’s role in protecting and improving trust in IoT systems.

Fan et al. (2022) address the important need for dependable time synchronization in Internet of Things (IoT) systems by providing a distributed and verifiable time synchronization strategy based on Network Time Protocol (NTP), trust management, and blockchain. The study emphasises the difficulties encountered by standard time synchronization technologies such as NTP and Precision Time Protocol (PTP), which are prone to crashes, power outages, and external attacks, resulting in potential single points of failure. To achieve accurate time synchronization, the suggested approach takes advantage of Blockchain’s transparency and immutability. Transactions on the blockchain indicate synchronization processes, and a consensus method is intended to resist Byzantine nodes, thereby improving trust management. The authors give simulation results that demonstrate the proposed scheme's efficiency and security, as well as its potential for dependable time synchronization in IoT scenarios. This work makes a significant contribution by providing a secure and verifiable time synchronization system that addresses the unique challenges and requirements of IoT applications.

Shala et al. (2020) investigated the use of blockchain technology and trust evaluation methodologies to build trust in decentralized IoT ecosystems. The authors evaluated various blockchain-based trust techniques, highlighting their advantages and disadvantages in decentralized IoT networks. They suggested an optimised trust model that includes a multi-layer adaptive and trust-based weighting method. The paper offered various trust metric parameters and mathematical models for trust evaluation, as well as a novel technique to rewarding players in the IoT marketplace using control loops and smart contracts. Experimental results confirmed the proposed trust model's dependability and increased resilience to various threats, establishing it as a strong option for safe and decentralized IoT service supply.

Oualhaj et al. (2020) suggested a decentralized trust management and cooperation paradigm based on blockchain technology. The approach intends to overcome issues in IoT systems such as heterogeneous system interconnection, decentralized object administration, robustness, and data access privacy. The authors looked into consensus techniques for updating the blockchain, proposing Proof of Trust (Pot) and Proof of Proof-of-Stake as alternatives to the energy-intensive Proof of Work (POW) scheme. The trust management model contains a trust update mechanism for detecting nodes that exhibit malicious behaviour and provide incorrect system information. The article emphasised the importance of blockchain in developing decentralized, transparent, and secure systems, as well as providing solutions to difficulties in the rising sharing economy and human-connected object interaction in the IoT context.

Putra et al. (2021) tackled the intricate challenges associated with access control in the Internet of Things (IoT) domain by introducing a novel decentralized attribute-based access control mechanism. This mechanism incorporated a Trust and Reputation System (TRS) grounded in blockchain technology. Traditional authorization systems within IoT often grapple with issues of overheads and centralization, prompting the authors to propose a solution emphasizing decentralization and flexibility. The system aimed at achieving dynamism by quantifying trust and reputation scores for each network node. To ensure privacy preservation, the authors ingeniously designed the system to operate on a public blockchain, supplemented by private sidechains for storing sensitive information securely. The implementation of their innovative solution was executed on a public Rinke by Ethereal test-network, seamlessly interconnected with a lab-scale testbed. Evaluations were conducted, encompassing a diverse set of performance metrics, effectively showcasing the practical applicability of the proposed mechanism in real-world IoT scenarios. The fusion of decentralized access control, attribute-based authorization, and a blockchain-driven Trust and Reputation System emerged as a promising avenue to address the evolving security and privacy concerns in IoT ecosystems.

Dharma Putra et al. (2021) addressed the critical challenges of access control in the context of the Internet of Things (IoT) by proposing a trust-based blockchain authorization mechanism. The authors recognized that common authorization systems in IoT, often relying on conventional schemes, face issues related to overheads and centralization. To overcome these challenges, the research leverages blockchain technology, which has shown potential in resolving access control problems in IoT environments. A significant contribution of the study lies in the design of a decentralized attribute-based access control mechanism, complemented by a Trust and Reputation System (TRS). The TRS serves as an auxiliary component, allowing for the progressive quantification of trust and reputation scores for each node within the IoT network. This dynamic scoring system is then integrated into the access control mechanism, enabling flexibility and adaptability. Notably, the authors implemented their proposed solution on a public Rinke by Ethereal test-network, connected with a lab-scale testbed, and conducted comprehensive evaluations using various performance metrics. The study underscores the importance of dynamic and flexible access control mechanisms in the IoT domain, emphasizing the potential of blockchain-based solutions for addressing these concerns.

Kouicem et al. (2020) addressed the security challenges within the Internet of Things (IoT) by proposing a decentralized blockchain-based trust management protocol. In the context of IoT, where diverse nodes like connected devices, smart cars, and homes interact in distributed and dynamic environments, trust management becomes a crucial aspect. The existing trust management solutions were found lacking in meeting the specific requirements of IoT, including heterogeneity, mobility, and scalability. The authors presented a hierarchical and scalable blockchain-based trust management protocol designed to support mobility in massively distributed IoT systems. In their approach, mobile smart objects disseminate trust-related information about service providers to the blockchain. This ensures that all objects within the architecture gain a comprehensive view of each service provider, thereby expediting the trust evaluation process. Additionally, the protocol demonstrated resilience against various malicious attacks such as bad-mouthing, ballot-stuffing, and cooperative attacks. Through theoretical analysis and extensive simulations, the authors validated the efficiency of their proposal. The study highlighted the protocol's superiority over existing solutions, particularly in terms of scalability, mobility support, and reductions in communication and computation costs. The research contributes to the development of trust management mechanisms tailored for the unique challenges posed by the IoT environment.

Wu and Liang (2021) addressed security concerns in Internet of Things (IoT), particularly in wireless sensor networks with resource-constrained nodes. As IoT applications become widespread, security threats to these nodes increase. The authors emphasized the need for a trustworthy IoT environment based on the trustworthiness of sensor nodes. Existing research focused on trust management and evaluation in IoT but lacked exploration of ensuring the trustworthiness of feedback used in the evaluation process. Moreover, resource-constrained IoT nodes faced challenges in memory availability for trust computation and maintenance. The proposed solution, a Blockchain-based Trust Management Mechanism (BBTM), involved evaluating the trustworthiness of sensor nodes by mobile edge nodes. BBTM employed smart contracts for trust computation, enhancing transparency and security. Performance analysis of BBTM demonstrated its effectiveness in terms of trust accuracy, convergence, and resilience against attacks, showcasing its superiority compared to other methods.

Kumar and Sharma (2022) conducted a survey focusing on leveraging blockchain for ensuring trust in the Internet of Things (IoT). IoT, characterized by connected computing devices forming a network, faces security and privacy challenges due to factors such as limited computation power, heterogeneity, and resource constraints in its devices. The authors highlighted the critical parameters of data confidentiality and integrity in IoT scenarios and emphasized the significance of managing and maintaining trust in information exchange. Blockchain technology was explored as a solution, providing distinct and secure approaches. The survey covered an overview of IoT and blockchain technologies, challenges in trusted IoT, potential blockchain-based solutions, complications in integration, and a comparative analysis between traditional and blockchain-based trust management techniques. The study aimed to illustrate the importance of integrating blockchain in the IoT environment to ensure trust among IoT devices.

Wang et al. (2023) presented a blockchain-empowered framework for decentralized trust management in the Internet of Battlefield Things (IoBT). The IoBT faces security challenges due to malicious intrusions from external environments, making trust management crucial at the node level. In this decentralized and dynamic IoBT environment, where nodes lack predetermined trust relationships, the authors proposed a framework leveraging blockchain to achieve decentralized trust management. The framework integrates space and ground segments with portable ping-pong stations, forming a blockchain network for managing decentralized trusts among IoBT nodes. The proposed framework comprises three algorithmic components: Local Trust Computation, Global Trust Aggregation, and Blockchain Consensus Process. Simulations incorporating various attack models and system setups demonstrated the effectiveness of the blockchain-empowered trust management framework in suppressing the probability of successful attacks and enhancing IoBT security.

Corradini et al. (2022) introduced a two-tier Blockchain framework to enhance the security and autonomy of smart objects in the Internet of Things (IoT) by implementing a trust-based protection mechanism. The IoT paradigm faces challenges related to protecting smart objects and ensuring their autonomy. The authors emphasized the importance of trust and reputation mechanisms for addressing these challenges. The proposed framework organizes smart objects into communities, utilizing a two-tier Blockchain solution. The first-tier Blockchain is local and records probing transactions performed to evaluate trust within the same community or across different communities. Periodically, these transactions are aggregated, and the resulting values are stored in the second-tier Blockchain, representing the reputation of each object within its community and the trust between communities. The paper provides a detailed description of the framework, its behavior, the associated security model, and the conducted tests to evaluate correctness and performance.

Shala et al. (2020) explored the integration of blockchain technology and trust evaluation techniques for secure, end-user-based, and decentralized Internet of Things (IoT) service provision. The research begins by reviewing various blockchain-based trust approaches, highlighting their strengths and limitations in decentralized IoT communities. Recognizing the challenges faced by both blockchain and trust evaluation in the IoT, the authors propose an optimized trust model featuring a multi-layer adaptive and trust-based weighting system. The publication also introduces trust metric parameters and their mathematical models for trust evaluation. A novel approach to incentivization processes in the IoT marketplace is presented, leveraging control loops and smart contracts to motivate participants for continuous improvement in their behavior. The proposed trust model is validated through experiments in different scenarios, demonstrating its reliability and improved resiliency against various attacks compared to existing approaches. The traditional IoT ecosystem relies on centralized infrastructures and commercial service providers, but the authors advocate for the integration of end-users in service provision to enhance flexibility, decentralization, service variety, and energy efficiency in the marketplace. Trust management systems are proposed as a countermeasure to the lack of trustworthiness in decentralized IoT ecosystems.

Gimenez-Aguilar et al. (2021) conducted a comprehensive survey focusing on the intersection of blockchain technologies and cybersecurity within decentralized systems, particularly in the context of the Internet of Things (IoT). In the contemporary landscape of extensive connectivity, cloud services, and the proliferation of IoT devices, decentralized approaches to trust management are gaining prominence. Blockchain technologies, renowned for their distributed ledger capabilities, have become a focal point for research across diverse application fields. However, it is crucial to recognize that blockchain alone does not inherently provide cybersecurity. The survey aims to offer a detailed review of techniques and elements proposed to enhance cybersecurity in blockchain-based systems. The authors highlight the exponential growth of Internet connectivity, the widespread use of cloud technologies, and the advent of the IoT.

Tu et al. (2022) address the security challenges posed by the increasing number of distributed Internet of Things (IoT) devices through the introduction of a Blockchain-based Trust and Reputation Model (BTRM). Recognizing the vulnerabilities associated with traditional Distributed Trust and Reputation Models (DTRMs), the proposed BTRM aims to enhance the security of IoT networks by leveraging blockchain's decentralized, traceable, and anonymous characteristics. The researchers specifically focus on the "network-to-device" TRM, emphasizing the assessment of user behavior at the network side to prevent malicious attacks. The paper introduces a novel Dynamic Evaluation Mechanism (DEM) as part of BTRM, designed to comprehensively evaluate user behavior and dynamically detect malicious attacks. Deploying DEM-BTRM in a prototype system of Hyperledger Fabric, the authors demonstrate its effectiveness in comparison to existing reputation evaluation methods.

Völter, Urbach, and Padget (2023) investigate the applicability of established Information Systems (IS) trust cues to blockchain technology and evaluate their effectiveness in influencing end-user trust. The study aims to fill the gap in understanding how existing trust cues, established for conventional IT, impact trust formation in the context of blockchain technology. Conducting a between-groups experiment, the researchers analyze the effectiveness of various IS trust formation factors on end-user trust in the blockchain. The findings suggest that trust signals emphasizing the underlying trust-building characteristics of blockchain technology are most effective. The study highlights the importance of contextualizing trust research for blockchain technology and provides insights for researchers and practitioners aiming to build trustworthy blockchain applications that facilitate trustless interactions in both theory and practice.

(Qiu et al., 2018), the challenges of deploying traditional Blockchain architecture in Internet of Things (IoT) systems and propose a dynamic scalable blockchain-based communication architecture for IoT networks. While traditional Blockchain architectures offer decentralized and trustworthy systems suitable for applications like cryptocurrencies, their direct deployment in IoT faces practical obstacles. The authors introduce a dynamic Blockchain-based trust system designed to overcome these challenges and provide a scalable communication architecture for IoT. They discuss the practical obstacles to deploying Blockchain in IoT, present the proposed dynamic trust system, and conduct a case study to explore security issues. The paper contributes insights to enable the integration of Blockchain technology into IoT networks, offering a dynamic and scalable solution with implications for future research.

Hassan et al. (2019) explore the integration of blockchain in Internet of Things (IoT) systems, focusing on privacy preservation. As modern IoT systems increasingly connect everyday objects, security, authentication, and maintenance become crucial. Blockchain, with its decentralized nature, addresses security concerns, leading to a surge in its applications in IoT. However, the authors emphasize that blockchain-based IoT networks, being public, expose transactional details and encrypted keys to all participants, raising privacy concerns. The paper discusses privacy issues resulting from the integration of blockchain in IoT applications and proposes five privacy preservation strategies: anonymization, encryption, private contract, mixing, and differential privacy. The article also outlines challenges and suggests future research directions for privacy preservation in blockchain-based IoT systems, offering valuable insights for researchers and practitioners in this evolving domain.

**Table 1: overview of existing approaches**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Problem Addressed** | **Approach** | **Strengths/Weaknesses** | **Implementation** | **Evaluation** | **Dataset Used** | **Implementation** |
| Challenges in traditional trust management for IoT due to openness, heterogeneity, and dynamicity. | Proposes evaluation criteria for IoT trust management, introduces taxonomy of trust systems, and focuses on blockchain-based trust management (BC-TM). | Strengths: Comprehensive overview, valuable insights. Weaknesses: Not specified. | Experimental results demonstrating reliability and resiliency. | Evaluation involves assessing the effectiveness of BC-TM criteria but lacks specific metrics or scenarios. |  |  |
| Challenges with centralized authentication, secure communication among agricultural devices. | Introduces a hybrid blockchain-based authentication scheme with group able batch verification and pseudonym update mechanisms. | Strengths: Superior security features, efficiency. Weaknesses: Not specified. | Security analysis and performance evaluation. | Demonstrates superior security features and efficiency through security analysis and performance evaluation. |  |  |
| Limitations of conventional security in resource-constrained IoT, secure authorized access to smart city resources. | Combines ACE framework-based authorization blockchain with OSCAR object security model. | Strengths: Feasibility demonstrated, flexible and trustless authorization. Weaknesses: Not specified. | Implemented on the Ethereal network using a node.js server and a Raspberry Pi B+. | Achieves authentication response time of less than 100 MS in smart city simulation, enhancing security in smart city deployments. |  |  |
| Security and privacy challenges in IoT, role of blockchain for secure and distinct approach. | Comparative analysis between traditional and blockchain-based trust management techniques. | Strengths: Highlights advantages of blockchain. Weaknesses: Not specified. | Experimental results demonstrating reliability and resiliency. | Insights into applications, vulnerabilities, and challenges, valuable for understanding blockchain's role in securing IoT. |  |  |
| Challenges with traditional time synchronization methods, vulnerability to failures and attacks. | Proposes a scheme based on NTP, trust management, and blockchain for secure and verifiable time synchronization. | Strengths: Secure and verifiable time synchronization. Weaknesses: Not specified. | Simulation results demonstrating efficiency and security. | Offers a secure and verifiable time synchronization solution for IoT scenarios. |  |  |
| Review of various blockchain-based trust approaches, proposed optimized trust model. | Introduces an optimized trust model with adaptive and trust-based weighting system, control loops, and smart contracts. | Strengths: Reliable trust model, enhanced resiliency. Weaknesses: Not specified. | Experimental results demonstrating reliability and resiliency. | Robust solution for secure and decentralized IoT service provision demonstrated through experiments. |  |  |
| Challenges in IoT systems, interconnection of heterogeneous systems, administration, resilience, and privacy. | Proposes a model utilizing blockchain with Proof of Trust and Proof of Proof-of-Stake as consensus mechanisms. | Strengths: Decentralized, transparent, and secure systems. Weaknesses: Not specified. | Simulation results demonstrating efficiency and security. | Utilizes Proof of Trust and Proof of Proof-of-Stake as alternatives to Pow in blockchain, emphasizing the significance of blockchain. |  |  |
| Challenges of access control in IoT, flexible access control system with trust and reputation scores. | Proposes a decentralized access control mechanism based on blockchain with Trust and Reputation System. | Strengths: Dynamic and flexible access control. Weaknesses: Not specified. | Implemented on a public Rinkeby Ethereum test-network. | Evaluations considering various performance metrics highlight the applicability in IoT contexts. |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Dharma Putra et al., 2021 | Trust-based blockchain authorization mechanism for IoT access control. | Challenges in common authorization systems in IoT, overheads, and centralization. | Proposes a decentralized attribute-based access control mechanism complemented by a Trust and Reputation System (TRS). | Strengths: Dynamic and flexible access control, trust and reputation quantification. Weaknesses: Not specified. | Implemented on a public Rinkeby Ethereum test-network connected to a lab-scale testbed. | Comprehensive evaluations using various performance metrics, highlighting the potential of blockchain-based solutions. |
| Kouicem et al., 2020 | Decentralized blockchain-based trust management protocol for IoT. | Security challenges in IoT, trust management in distributed and dynamic environments. | Introduces a hierarchical and scalable blockchain-based trust management protocol supporting mobility in massively distributed IoT systems. | Strengths: Hierarchical and scalable protocol, resilience against malicious attacks. Weaknesses: Not specified. | Theoretical analysis and extensive simulations. | Validated efficiency through simulations, superior scalability, mobility support, and reductions in costs. |
| Wu and Liang, 2021 | Blockchain-based Trust Management Mechanism (BBTM) for IoT nodes' trustworthiness. | Security concerns in IoT, trustworthiness of sensor nodes, challenges in memory availability. | Proposes BBTM for evaluating trustworthiness of sensor nodes by mobile edge nodes, employing smart contracts for trust computation. | Strengths: Transparent and secure trust computation. Weaknesses: Not specified. | Performance analysis showcasing trust accuracy, convergence, and resilience against attacks. | Demonstrates effectiveness in trust accuracy, convergence, and resilience against attacks compared to other methods. |
| Kumar and Sharma, 2022 | Survey on leveraging blockchain for trust in IoT. | Security and privacy challenges in IoT, importance of trust in information exchange. | Explores blockchain as a solution, covers IoT and blockchain technologies, challenges, potential solutions, integration complications. | Strengths: Importance of integrating blockchain in IoT for trust. Weaknesses: Not specified. | Experimental results demonstrating reliability and resiliency. | Aims to illustrate the importance of integrating blockchain in the IoT environment to ensure trust among IoT devices. |
| Wang et al., 2023 | Blockchain-empowered framework for decentralized trust management in IoBT. | Security challenges in IoBT, decentralized trust management in a dynamic environment. | Presents a framework leveraging blockchain to achieve decentralized trust management in IoBT. | Strengths: Effective in suppressing the probability of successful attacks. Weaknesses: Not specified. | Simulations incorporating various attack models and system setups. | Demonstrates the effectiveness of the blockchain-empowered trust management framework in enhancing IoBT security. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Corradini et al., 2022 | Two-tier Blockchain framework for security and autonomy of smart objects in IoT using trust-based protection. | Challenges in protecting smart objects and ensuring their autonomy in IoT. | Introduces a two-tier Blockchain solution, organizing smart objects into communities, emphasizing trust and reputation mechanisms. | Strengths: Local and global trust management, framework behavior and security model detailed. Weaknesses: Not specified. | Detailed tests to evaluate correctness and performance. | Provides a detailed overview of the framework, its behavior, the associated security model, and tests to evaluate correctness and performance. |
| Shala et al., 2020 | Integration of blockchain and trust evaluation techniques for secure, end-user-based, and decentralized IoT service provision. | Challenges in decentralized IoT communities, strengths and limitations of blockchain-based trust approaches. | Proposes an optimized trust model with multi-layer adaptive weighting, introducing trust metric parameters and mathematical models. | Strengths: Improved resiliency against attacks. Weaknesses: Not specified. | Validation through experiments in different scenarios. | Demonstrates the proposed trust model's reliability and improved resiliency against various attacks in comparison to existing approaches. |
| Gimenez-Aguilar et al., 2021 | Survey on the intersection of blockchain technologies and cybersecurity in decentralized systems, especially IoT. | The need for enhanced cybersecurity in decentralized systems, focusing on IoT. | Conducts a comprehensive survey on techniques and elements proposed to enhance cybersecurity in blockchain-based systems. | Strengths: Detailed review of techniques and elements. Weaknesses: Not specified. | Overview and analysis of techniques proposed in the literature. | Provides a detailed review of techniques and elements proposed to enhance cybersecurity in blockchain-based systems. |
| Tu et al., 2022 | Blockchain-based Trust and Reputation Model (BTRM) for enhancing security in distributed IoT networks. | Security challenges in IoT, vulnerabilities of traditional Distributed Trust and Reputation Models (DTRMs). | Proposes BTRM leveraging blockchain's characteristics for network-to-device trust management, including a Dynamic Evaluation Mechanism (DEM). | Strengths: Enhanced security with blockchain, introduction of DEM. Weaknesses: Not specified. | Deployment of DEM-BTRM in a prototype system of Hyperledger Fabric. | Demonstrates the effectiveness of DEM-BTRM in comparison to existing reputation evaluation methods. |
| Völter, Urbach, Padget, 2023 | Investigating the applicability of established IS trust cues to blockchain technology for influencing end-user trust. | Applicability of IS trust cues to blockchain, effectiveness in influencing end-user trust. | Conducts a between-groups experiment to analyze the effectiveness of IS trust formation factors on end-user trust in blockchain. | Strengths: Identifies effective trust signals for blockchain. Weaknesses: Not specified. | Experimental results demonstrating reliability and resiliency. | Highlights the importance of contextualizing trust research for blockchain and provides insights for building trustworthy blockchain applications. |
| Qiu et al., 2018 | Dynamic scalable blockchain-based communication architecture for IoT networks. | Challenges of deploying traditional Blockchain architecture in IoT, practical obstacles in IoT systems. | Proposes a dynamic Blockchain-based trust system, providing a scalable communication architecture for IoT. | Strengths: Addresses practical obstacles in IoT, dynamic and scalable solution. Weaknesses: Not specified. | Case study to explore security issues. | Offers insights to enable the integration of Blockchain technology into IoT networks, providing a dynamic and scalable solution. |
| Hassan et al., 2019 | Privacy preservation in blockchain-based IoT systems: Integration issues, prospects, challenges, and future research directions. | Privacy issues in blockchain-based IoT systems, challenges, privacy preservation strategies. | Proposes five privacy preservation strategies: anonymization, encryption, private contract, mixing, and differential privacy. | Strengths: Addresses privacy issues in blockchain-based IoT. Weaknesses: Not specified. | Experimental results demonstrating reliability and resiliency. | Offers privacy preservation strategies and highlights challenges and future research directions for blockchain-based IoT systems. |

**Comparative Analysis**

Comparative Analysis: Traditional Trust Management vs. Blockchain-based Totally Trust Management for IoT

While conventional agree with management tactics have performed a role in securing interactions, their obstacles grow to be obvious in the dynamic and complicated world of IoT. Here is a breakdown of the way they examine:

|  |  |
| --- | --- |
| Traditional Trust Management | Blockchain-primarily based Trust Management |
| Centralized Control: This system relies on a government to set up, control, and accept true relationships. This creates a single factor of failure and potential vulnerabilities. | Decentralized Network: This distributes acceptance as true throughout a community of contributors, disposing of a single factor of failure and improving security. |
| Limited Scalability: Struggles to conform to the ever-developing number and variety of gadgets within the IoT ecosystem.  Opaque Data Management: Data storage and access management might need to be more transparent, making it tough to affirm the integrity of information. | Scalable Infrastructure: Blockchain's inherent scalability can accommodate the sizeable and growing range of gadgets inside the IoT landscape. |
| Static Trust Models: Often rely upon pre-defined agree with ranges, which may not adapt to converting situations or device conduct within the dynamic IoT surroundings. | Dynamic Trust Management: Allows trust levels to be installed and changed based on actual-time records and device behavior, imparting an extra adaptable technique. |
|  |  |

This comparative evaluation highlights blockchain generation's capacity to deal with the constraints of traditional trust management within the context of IoT. By leveraging its decentralized nature, secure statistics management, and dynamic trust models, blockchain offers a promising direction toward building a steadier and more truthful basis for the future of IoT.

Table 2 Comparison of IoT Security Attacks

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Technique | Attack 1 | Attack 2 | Attack 3 | .. | Attack N |
| [] | Yes | No | yes |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# References

Braga, D. D. S., Niemann, M., Hellingrath, B., & Neto, F. B. D. L. (2018). Survey on Computational Trust and Reputation Models. *ACM Computing Surveys*, *51*(5), 1–40. https://doi.org/10.1145/3236008

Marr, B. (2016). Big Data in Practice: How 45 Successful Companies Used Big Data Analytics to Deliver Extraordinary Results. In *Google Books*. John Wiley & Sons. https://books.google.co.ke/books?hl=en&lr=&id=wAOmCgAAQBAJ&oi=fnd&pg=PA1&dq=Devices+with+an+effective+history+of+dependable+conversation+and+data+change+earn+better+acceptance+as+true+with+scores

Liu, Y., Wang, J., Yan, Z., Wan, Z. and Jäntti, R., 2023. A survey on blockchain-based trust management for Internet of Things. IEEE Internet of Things Journal, 10(7), pp.5898-5922.

Luo, F., Huang, R. and Xie, Y., 2024. Hybrid blockchain-based many-to-many cross-domain authentication scheme for smart agriculture IoT networks. Journal of King Saud University-Computer and Information Sciences, p.101946.

Asif, M., Aziz, Z., Bin Ahmad, M., Khalid, A., Waris, H.A. and Gilani, A., 2022. Blockchain-based authentication and trust management mechanism for smart cities. Sensors, 22(7), p.2604.

Kumar, R. and Sharma, R., 2022. Leveraging blockchain for ensuring trust in IoT: A survey. Journal of King Saud University-Computer and Information Sciences, 34(10), pp.8599-8622.

Fan, K., Shi, Z., Su, R., Bai, Y., Huang, P., Zhang, K., Li, H. and Yang, Y., 2022. Blockchain-based trust management for verifiable time synchronization service in IoT. Peer-to-Peer Networking and Applications, 15(2), pp.1152-1162.

Shala, B., Trick, U., Lehmann, A., Ghita, B. and Shiaeles, S., 2020. Blockchain and trust for secure, end-user-based and decentralized IoT service provision. IEEE Access, 8, pp.119961-119979.

Oualhaj, O.A., Mohamed, A., Guizani, M. and Erbad, A., 2020, June. Blockchain based decentralized trust management framework. In 2020 international wireless communications and mobile computing (IWCMC) (pp. 2210-2215). IEEE.

Putra, G.D., Dedeoglu, V., Kanhere, S.S., Jurdak, R. and Ignjatovic, A., 2021. Trust-based blockchain authorization for iot. IEEE Transactions on Network and Service Management, 18(2), pp.1646-1658.

Dharma Putra, G., Dedeoglu, V., Kanhere, S.S., Jurdak, R. and Ignjatovic, A., 2021. Trust-based Blockchain Authorization for IoT. ArXiv e-prints, pp.arXiv-2104.

Kouicem, D.E., Imine, Y., Bouabdallah, A. and Lakhlef, H., 2020. Decentralized blockchain-based trust management protocol for the Internet of Things. IEEE Transactions on Dependable and Secure Computing, 19(2), pp.1292-1306.

Wu, X. and Liang, J., 2021. A blockchain-based trust management method for Internet of Things. Pervasive and Mobile Computing, 72, p.101330.

Kumar, R. and Sharma, R., 2022. Leveraging blockchain for ensuring trust in IoT: A survey. Journal of King Saud University-Computer and Information Sciences, 34(10), pp.8599-8622.

Wang, H., Wang, T., Shi, L., Liu, N. and Zhang, S., 2023. A blockchain-empowered framework for decentralized trust management in Internet of Battlefield Things. Computer Networks, 237, p.110048.

Corradini, E., Nicolazzo, S., Nocera, A., Ursino, D. and Virgili, L., 2022. A two-tier Blockchain framework to increase protection and autonomy of smart objects in the IoT. Computer Communications, 181, pp.338-356.

Shala, B., Trick, U., Lehmann, A., Ghita, B. and Shiaeles, S., 2020. Blockchain and trust for secure, end-user-based and decentralized IoT service provision. IEEE Access, 8, pp.119961-119979.

Gimenez-Aguilar, M., De Fuentes, J.M., Gonzalez-Manzano, L. and Arroyo, D., 2021. Achieving cybersecurity in blockchain-based systems: A survey. Future Generation Computer Systems, 124, pp.91-118.

Tu, Z., Zhou, H., Li, K., Song, H. and Yang, Y., 2022. A blockchain-based trust and reputation model with dynamic evaluation mechanism for IoT. Computer Networks, 218, p.109404.

Völter, F., Urbach, N. and Padget, J., 2023. Trusting the trust machine: Evaluating trust signals of blockchain applications. International Journal of Information Management, 68, p.102429.

Qiu, H., Qiu, M., Memmi, G., Ming, Z. and Liu, M., 2018. A dynamic scalable blockchain based communication architecture for IoT. In Smart Blockchain: First International Conference, SmartBlock 2018, Tokyo, Japan, December 10–12, 2018, Proceedings 1 (pp. 159-166). Springer International Publishing.

Hassan, M.U., Rehmani, M.H. and Chen, J., 2019. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. Future Generation Computer Systems, 97, pp.512-529.

Qiu, H., Qiu, M., Memmi, G., Ming, Z., & Liu, M. (2018). A Dynamic Scalable Blockchain Based Communication Architecture for IoT. *Smart Blockchain*, 159–166. https://doi.org/10.1007/978-3-030-05764-0\_17