sustainability

MDPI

Article

IoT: A Decentralized Trust Management System Using Blockchain-Empowered Federated Learning

Lirui Bi [1], Tasiu Muazu [2,*] and Omaji Samuel [3,*]

[1] School of Safety Science and Emergency Management, Wuhan University of Technology, Wuhan 430070, China
[2] College of Computer and Information, Hohai University, Nanjing 210098, China
[3] Department of Computer Science, Edo State University Uzairue, Iyamho 312101, Nigeria
* Correspondence: tmuazu@yahoo.com (T.M.); omaji.samuel@edouniversity.edu.ng (O.S.)

Abstract: We propose a decentralized medical trust management system using blockchain-based federated learning for large-scale Internet of Things (IoT) systems. The proposed system enables health institutions to share data without revealing the privacy of data owners. Health institutions form coalitions and the leader of each coalition is elected based on the proposed proof-of-trust collaboration (PoTC) consensus protocol. The PoTC consensus protocol is based on a weight difference game where trust scores, trust consistency value, and trust deviation are factors used for evaluating nodes in the blockchain. The trust of a node is obtained either through direct trust or recommended trust evaluations. Each leader elects an aggregator who has the most credibility to manage the proposed federated learning system. The leaders become the federated clients as well as validators while the aggregator is the federated server. To ensure the decentralization of nodes, a consortium blockchain is employed. Extensive simulations are performed, which show that the proposed system not only demonstrates scalability and credibility without compromising the accuracy, convergence, and resilience properties against malicious attackers but also outperforms existing trust management systems. A security analysis is also conducted, which shows that the proposed system is robust against trust-related attacks.

Keywords: blockchain; machine learning; IoT; proof-of-trust collaboration; trust evaluation

Citation: Bi, L.; Muazu, T.; Samuel, O. IoT: A Decentralized Trust Management System Using Blockchain-Empowered Federated Learning. *Sustainability* **2023**, *15*, 374. https://doi.org/10.3390/su15010374

Academic Editor: Manuel Fernandez-Veiga

Received: 23 November 2022
Revised: 7 December 2022
Accepted: 19 December 2022
Published: 26 December 2022

1. Introduction

Recently, there has been a tremendous improvement in the Internet of medical things (IoMT) devices, which efficiently meet and satisfy medical requests or services. Moreover, these IoMT devices may compete for resources, which means that some IoMT devices are resource constrained and cannot perform well in handling more complex computational tasks. Therefore, a recent work [1] has proposed solutions that not only resolved the computation problems of IoMT devices but address centralization and trust management issues. Trust issue occurs when the service providers have to find ways of selecting trustworthy devices that are connected to the Internet. However, the problem of centralization is not fully resolved.

Trust management is important to resolve the problems associated with a situation where IoMT device owners behave honestly at some points and maliciously at other points. The motive behind their behavior may be for financial gain or to exploit the vulnerability of the system. Another situation can be that malicious nodes in the system can collide with others to damage the system's integrity. Therefore, it is vital to provide service-oriented management systems that ensure trust between IoMT device owners [1]. Blockchain as a disruptive technology has been deployed for trust management in recent times [2]. Blockchain is known to accelerate transmission rates while maintaining reliability. The work in [3] proposed a trust management system that detects normal and abnormal behaviors in distributed control networks. Another work [4] proposed an auxiliary trust reputation system

and attribute-based access control for a decentralized IoT scenario. In another scenario, identity-based attacks are detected using a Bayesian inference method in the IoMT [5]. A reward/penalty scheme for scalable trust architecture is proposed in [6] to achieve trust between IoT devices. The architecture solves scalability problem in distributed trust systems, i.e., communication and storage can be scaled with several IoT devices. However, maintaining a consistent relationship between IoT devices becomes problematic because of the dynamism of the system. Therefore, the inconsistent relationship or interaction makes trust evaluation inaccurate. Furthermore, the amount of information generated collectively by IoT devices requires more computing resources while maintaining the privacy of the data owners. Based on the identified limitations of [6] in terms of maintaining consistent relationships between IoT devices, problems of centralization [3], and data privacy in decentralized systems, we are motivated to propose a decentralized trust management system that combines blockchain technology and federated learning without compromising the trust evaluation, privacy, and security of data owners in the system. For simplicity, we introduce an overview of blockchain technology, and, afterward, the federated learning system is discussed. Firstly, blockchain is a disruptive technology that can connect non-trusted entities. It is a distributed ledger that allows every entity (i.e., node) to have the same copy of the ledger. This property makes blockchain a shared, immutable ledger that facilitates the recording of transaction processes and ensures the tracking of assets in a business network. Note that assets used in blockchain can be tangible or intangible and the values of assets can be tracked and traded on the blockchain, which then reduces the risk and cost for all entities involved. Today, blockchain is a solution to the complexities, vulnerabilities, inefficiencies, and costs of traditional transaction systems. It is believed that the first blockchain technology was Bitcoin, which was introduced by Satoshi Nakamoto in 2009 [7]. Unlike conventional currency systems, Bitcoin does not have central monetary authority and it enables peer-to-peer communication. Bitcoin is cost-effective, which means that intermediaries are eliminated; it is efficient, which implies that transactions are recorded once and it is available to all entities within the distributed network; and it is secure, which means that transaction is tamper-proof. That is, the transaction cannot be altered but can be reversed with another transaction. Lastly, the idea of federated learning started from Google, where machine learning models used datasets that are distributed across multiple devices without disclosing private information [8]. Federated learning can be categorized into three types according to its operation and design: (1) horizontal federated learning allows the training of two datasets that share the same feature space but different sample spaces, (2) vertical federated learning allows the training of two datasets with the same sample identity but have different feature spaces, and (3) transfer learning allows the training of two datasets that do not only differ in sample spaces but also in feature spaces. To avoid the verbosity of explaining what federated learning is, we refer interested readers to read the work in [8].

In this study, a decentralized trust management system is proposed to achieve scalable trust-based service management for distributed IoMT devices. The objective of this study is to explore federated learning and blockchain technology while considering health institutions for data sharing and predictions. Data sharing and prediction become vital for combating, controlling, and monitoring infectious diseases (COVID-19, malaria, ebola, etc). Here, it is expected that each health institution trains local data using the global model update shared by the federated server. It helps to remove prediction inaccuracy, overfitting, and poor generalization. Because of data insufficiency, machine learning models become inefficient, which leads to inaccurate forecasting; thus, federated learning is necessary. In the process of data sharing, some health institutions may not trust data from other institutions, especially when the data are not regulated and validated. Therefore, blockchain technology and trust management systems are important to address the problem. The following are the contributions of this work.

1. We propose a decentralized trust management system using direct and indirect trust evaluation methods. Time progression is considered in the evaluation to avoid mis-

judgment and feedback sparseness. The results of the trust evaluation are further validated using the process of trust consistency and similarity.

2. A decentralized federated learning system is proposed in the study. In the federated learning system, the federated server, known as an aggregator, is elected by leaders of nodes in different coalition groups, while the federated client is the leader of a coalition group. The federated learning model is the convolutional neural network where the initial gradient parameter is initiated by the server and is updated via an iterative process. Every client updates the shared model using the gradient parameter that trains the model.
3. We propose a new blockchain-based consensus protocol, known as proof-of-trust collaboration (PoTC). Here, a trust collaboration value, which is obtained from the trust collaboration reward, is used in the formulation of the consensus protocol. The leader of the blockchain network is selected using the proposed weight difference game.
4. Security analysis of the proposed system is evaluated using the proposed security metrics. The results of the analysis show that the proposed trust management system is robust against trust inconsistency attacks, similarity attacks, double-spending attacks, on-off attacks, and Sybil attacks.

In theory, the proposed decentralized trust management based on federated learning and blockchain is employed to address major concerns usually faced when implementing conventional trust and machine learning models with data stored in a centralized location. In practice, every health institution engages in local model training without the fear that the data privacy and shared gradient of the model are compromised. This is because the proposed system ensures trustworthiness between different institutions while complying with data privacy regulations. Health institutions can benefit from the proposed system because it has scalable and distributed trust-based service management. Furthermore, experimental results have indicated that the proposed model can solve the trust management problem in decentralized federated learning models.

The remaining part of this paper is organized as follows. Section 2 presents the related work, which is concluded with a table summarizing the work; Section 3 provides detailed descriptions of the proposed system model and formulations and Section 4 presents the security analysis of the proposed system model while considering trust-related attacks. Section 5 provides the simulation result and discussion, while Section 6 concludes the paper with future work.

2. Literature Background

Nowadays, the Internet of things (IoT) is one of the means of integrating different devices via wireless sensor networks. In the IoT, several resource-constrained sensor nodes exist and they are prone to security and privacy attacks. For tackling the attacks, the authors of [9] proposed a trustworthy system that allows feedback from trust evaluation. The proposed system is based on blockchain, where the trustworthiness of the sensor nodes is evaluated by the edge nodes. Additionally, trust accuracy is analyzed while resiliency and convergence of the trust computation process were also investigated. However, the system does not address the concerns of data privacy. Additionally, feedback sparsity and internal credibility problems cannot be solved by trust computation alone. Therefore, there is a need for a system that considers the trust feedback sparsity and credibility management system. In retrospect, cryptographic primitives have been deployed for ensuring the trust of systems [10]. Moreover, access control mechanisms have also been used for granting access to resources by only trusted entities in the system. However, these access control mechanisms and cryptographic primitives are centralized-based and are vulnerable to a single point of failure attack. Additionally, the interaction among entities in a system needs to be considered for ensuring trust. Additionally, although each of them has distinct limitations, cryptographic primitives and trust management are both somewhat effective. Therefore, the authors of [11] proposed a hybrid system that is based on cryptography and a trust management scheme to secure the vehicular energy network (VANET). In the pro-

posed system, asymmetric identity-based digital signature, and symmetric hash message authentication codes were used. However, the computation overheads for combining these mechanisms are not minimized for resource-constrained vehicles. Additionally, the trust evaluation method requires further improvement. The authors of [12] proposed a trust evaluation method for a multi-agent system. The proposed method combines trust distortion, trust consistency, and trust reliability to evaluate the trust computation of different agents. A tit-3-for-tat strategy was proposed for ensuring cooperation between the agents. However, collaborative learning and privacy concerns for the agents were not considered. In collaborative systems, entities broadcast messages for the improvement of the systems. However, because of the non-trusted environment, some entities may not trust the messages they received from other entities. This creates a trust gap among the entities; thereby exposing the system to trust-related attacks. For example, in the Internet of vehicles (IoV), vehicles improve traffic safety via an adaptive traffic management system.

Here, vehicles broadcast messages to the management system. The establishment of trust management is vital means of ensuring security that is steadily limited by scalability challenges in IoV [13]. The authors of [13] presented a protocol that is based on blockchain technology to secure trusted vehicles and restrict malicious ones. The trust of vehicles is achieved by assigning unique identities while a certificate is used to preserve the privacy of vehicles. However, using identity alone as a means of ensuring the trust of a vehicle is not sufficient. Additionally, Sybil attacks are possible with the identity-based trust method. Furthermore, the credibility evaluation of each vehicle and internal security attacks are not considered. It is noted that internal security attacks are mitigated using trust management [14]. Considering the information-centric networks (ICN), an efficient trust management scheme is vital to address intelligent internal attacks. Another work in [15] stated that internal attacks cannot be solved using cryptographic primitives and authentication mechanisms. A Dirichlet-distribution-based trust management scheme (DDTMS) is designed by the authors of [15] to prevent internal attacks. A third-party recommendation trust method is employed to evaluate trust value more precisely. However, the Dirichlet distribution has a mean value for each variable while sharing a common variance parameter. The authors of [14] designed a fast and efficient trust management scheme, known as FETMS to prevent on-off attacks. Here, direct trust and indirect methods are applied to users in the ICN; however, trust credibility is not considered. Additionally, the openness characteristics of entities in ICN may create problems of privacy and security. The work in [7] addresses the openness characteristics of entities by proposing an anonymous announcement protocol for vehicles to transmit messages in a fully non-trusted environment. Moreover, a trust management model is developed using blockchain to achieve the credibility and reliability of vehicles based on their reputation scores. Conditional privacy is also obtained as malicious nodes can be traced by the trusted authority. However, the data privacy of the proposed system needs to be improved. Another work in [16] proposes an announcement protocol for preserving data privacy and anonymity using an identity-based group signature. Additionally, a trust management system is employed to ensure the authenticity of the disseminated messages. However, the credibility of the system is not considered.

Due to the decentralized structure of the Internet of medical things (IoMT), trust establishment is still a problem for efficient systems management. The behavior of nodes determines their trust evaluations which involve interactions with the environment. Therefore, trust management allows nodes in the IoMT to be evaluated via rating and recommendation based on feedback. Contrarily, most trust management systems [17–21] are centralized, which makes them vulnerable to a single point of attack or failure. However, decentralization is aimed to solve the problem encountered in centralization. In [22], the authors proposed a novel decentralized trust management system empowered by blockchain technology. The proposed system is a prototype that provides transparent trust evaluation as compared to the centralized trust management systems. However, data privacy is not considered. Another work in [23] stated that self-enforcing decentralized management

and privacy concerns without trusted third parties are some of the challenges of trust management systems. The work proposed a framework for calculating the trustworthiness of nodes in the self-enforcing network while relying on a trusted third party. Homomorphic encryption is employed to provide data privacy. However, the credibility of the trusted third-party node is not considered as the node can be compromised by malicious nodes. Table 1 shows the comparison of the existing systems with our proposed system in terms of application scenario, year, major contribution, techniques, and limitations.

Table 1. Summary comparison of previous articles on trust management systems with application scenario, year, major contributions, techniques, and limitations.

Ref.	Application Scenario	Year	Major Contributions	Techniques	Limitations
[9]	IoMT within COVID-19 pandemic	2021	A trustworthy system that allows feedback from trust evaluation. Analysis of both trust accuracy, resiliency, and convergence of the trust computation process	Blockchain and trust management system	The system does not address the concerns for data privacy. Additionally, feedback sparsity and internal credibility problems cannot be solved by trust computation alone
[11]	VANETs	2020	A hybrid system that is based on cryptography and a trust management scheme to secure the vehicular energy network (VANET)	Asymmetric identity-based digital signature and symmetric hash message authentication codes	The computation overheads for combining these mechanisms are not minimized for resource-constrained vehicles. Additionally, the trust evaluation method requires further improvement
[12]	Multi-agent system	2021	A trust evaluation method for a multi-agent system. The proposed method combines trust distortion, trust consistency, and trust reliability to evaluate the trust computation of different agents	A tit-3-for-tat strategy and blockchain	Collaborative learning and privacy concerns for the agents were not considered
[13]	IoV	2020	Protocol that is based on blockchain technology to secure trusted vehicles and restrict malicious ones. The trust of vehicles is achieved by assigning unique identities while a certificate is used to preserve the privacy of vehicles	Blockchain and trust management method	Using identity alone as a means of ensuring the trust of a vehicle is not sufficient. Additionally, Sybil attacks are possible with the identity-based trust method. Furthermore, the credibility evaluation of each vehicle and internal security attacks are not considered
[15]	IoT	2019	Designed a fast and efficient trust management scheme, known as FETMS to prevent on-off attacks. Here, direct trust and indirect methods are applied to users in the ICN	Dirichlet distribution	Dirichlet Distribution has a mean value for each variable while sharing a common variance parameter. Additionally, the openness characteristics of entities in ICN may create problems of privacy and security
[14]	IoT	2019	Designed a fast and efficient trust management scheme, known as FETMS to prevent on-off attacks	Direct trust and indirect methods	Trust credibility is not considered. Additionally, the openness characteristics of entities in ICN may create problems of privacy and security
[7]	VANETs	2019	An anonymous announcement protocol for vehicles to transmit messages in a fully non-trusted environment. Moreover, a trust management model is developed using blockchain to achieve credibility and reliability of vehicles based on their reputation scores	Blockchain, conditional privacy and trust management	Data privacy of the proposed system needs to be improved
[16]	IoV	2021	Data privacy, trust, and anonymity	Announcement protocol using identity-based group signature and trust management system	Credibility of nodes in the system is not considered

Table 1. *Cont.*

Ref.	Application Scenario	Year	Major Contributions	Techniques	Limitations
[22]	Intelligent transport system	2020	The authors proposed a novel decentralized trust management system	Blockchain and trust management	Data privacy is not considered
[23]	Social Internet of things	2020	A framework for calculating the trustworthiness of nodes in the self-enforcing network while relying on a trusted third party	Homomorphic encryption	Credibility of the trusted third-party node is not considered as the node can be compromised by malicious nodes
Our	IoMT	2022	Decentralized trust management system	Blockchain, federated learning, and trust management method	The scalability of the proposed PoTC consensus protocol will be evaluated for a large number of nodes. This will further enhance communication via minimization of latency and transmission cost

Motivated by the limitations of the existing literature [7,9–23], none of the authors consider application scenario based on IoMT for ensuring trust using blockchain, federated learning, and trust evaluation method. Additionally, the proposed system is aimed at addressing decentralized trust management and data privacy issues for health institutions. No case study of a particular country or system is considered. Moreover, as a future research direction, economic, organizational, and managerial factors regarding systems and countries will be considered.

3. Proposed System Model

Since the outburst of the COVID-19 pandemic in 2019 [24], health institutions have taken the responsibility of mitigating and controlling the spread of the COVID-19 virus by following the recommended standard of the world health organization (WHO). Moreover, some health institutions have failed to notify the center for disease control (CDC) in their country about the pandemic because of a lack of efficient communication, insufficient funding, etc. Thus, there is no sufficient feedback from health institutions to CDCs regarding the spread of the virus because of a lack of collaboration. To this end, COVID-19 patients are not given enough guidance on the mitigation, spread, and control of the virus. When there is a collaboration, different health institutions will provide the necessary skills and information to accomplish the shared goals that benefit both CDCs and WHO. Note that in the proposed system, collaboration among health institutions is not hierarchical, which means that health institutions have equal status, no matter their functionalities. Additionally, it means that biases are removed from health institutions by providing them with equal status to fully participate in federated learning and blockchain. However, in reality, there is a hierarchy between health institutions, and the hierarchy varies by country. Furthermore, in the future, we aim to consider hierarchical factors such as economic and spatial in the proposed problem formulation. The economic factor determines both the monetary and maintenance costs of health institutions for storing and sharing healthcare data; whereas the spatial factor determines the geographical separation of health institutions when sharing healthcare data. Moreover, collaboration is cost-effective for health institutions because data can be shared between them. It implies that during collaboration, resources are pooled and productivity is increased. However, without collaboration, individual health institutions will incur a high cost of model training for a large amount of data. Contrarily, in the proposed system, collaboration ensures that only a few nodes with more computing resources and high trust values are allowed to participate in the consensus and mining processes as well as global model training. Furthermore, collaboration cannot be possible if there is a lack of trust between health institutions, which is one of the motivations of this study. Currently, the regulatory status of the personal data of health institutions is not within the scope of this study. Additionally, as progressive research, we aim to take note of structures, and systems of relationships of health institutions (including private and public) for different countries.

Furthermore, ethics and data privacy restrictions will be investigated for ensuring more efficient collaboration between health institutions.

In this study, we consider both direct and indirect trust evaluations (see the proposed system model in Figure 1). Different coalition groups are considered in our proposed scenario. Each coalition group denotes the CDC in a country that comprises several health institutions. Every institution performs direct trust evaluation with one another and elects a group aggregator based on the rating score. Any institution of a group whose rating score is the highest will immediately become the group aggregator, known as the leader. Aggregators of all groups perform direct trust evaluation and select the overall aggregator with the highest rating. Moreover, other factors such as trust reliability and trust consistency are considered to ensure the credibility of the aggregator (see Section 3.1). Additionally, when making decisions, trust factors might lessen the uncertainty and cost effect [12]. Note that every aggregator of a group becomes the validator node in the blockchain that participates in the consensus processes of creating and validating blocks. The aggregator is not necessarily a trusted third party but the node in the blockchain network with the highest rated score.

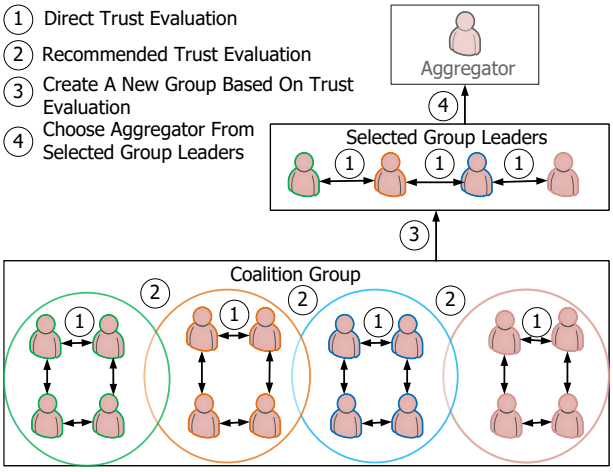

Figure 1. The proposed trust evaluation method.

Today, blockchain is known as a disruptive technology that is based on a distributed ledger [25]. Data in the blockchain are stored as transactions and they are validated by validator nodes. Blockchain has consensus protocols such as proof-of-work (PoW), proof-of-authority (PoA), and proof-of-stake (PoS), that are required to achieve the global state of the network. These consensus protocols ensure that both conflicts between nodes and fork node propagation are minimized. In this study, a new consensus protocol, known as proof-of-trust collaboration (PoTC), is proposed for block creation and validation (see Section 3.2). Blockchain provides the following security objectives: confidentiality, integrity, and availability. Additionally, the mutability of the blockchain ensures that transactions cannot be changed once they are written onto the blockchain.

3.1. The Proposed Trust Management System

In this study, a new trust management system is proposed for health institutions to achieve efficient collaboration. Trust management is the trustworthiness of estimation where there is high quality and reliable health institutions engagement management. In the existing literature [26], each trust mechanism has a different trust management phase. Some trust mechanisms recalculate trust values in light of the positive interactions between entities in the past, while others do so in light of the negative feedback an entity has collected from previous interactions. Even trust systems that update trust levels based on the progression of time exist. In [12], the authors presented direct and indirect trust evaluation mechanisms. The authors stated that the directed trust is affected by feedback

sparseness and misjudgment as time progression was not considered. Therefore, this study considers this limitation and provides a solution that allows a direct trust mechanism to employ in the collaboration of health institutions. The trust value v_t is defined as follows.

$$v_t = \tau_t \times \beta_t, \tag{1}$$

where $\tau_t \in [0, 1]$ is the trust rating of evaluatee by evaluator over tth period, which is arbitrarily chosen, and β_t is the trust factor of evaluatee over tth period. Note that $0 \leq \beta_t \leq 1$. If $\beta_t \geq 0.5$, then the evaluatee has high credibility in the past.

$$\beta_t = \frac{\tau_t}{\sum_{t=1}^{T} \tau_t}, \tag{2}$$

where T is number of periods and τ_t is directly proportional to β_t. In this study, the health institutions are underpinned by trust collaboration reward C_R, which is similar to the ether given in Ethereum [27]. This implies that data are shared between health institutions, which are recorded as transactions in the blockchain; hence, every health institution is paid with C_R. The trust collaboration value T_c is defined as follows.

$$T_c = \frac{C_R}{\sqrt{\sum_{i=1}^{N} \beta_i F_{i,j}}}, \tag{3}$$

$$F_{i,j} = \frac{\tau_i}{\beta_i - \tau_j}, \tag{4}$$

where N is the number of institutions in a coalition group, and indexes i and j denote the evaluatee and evaluator, respectively. To prevent feedback sparseness and misjudgment, this study measures the dissimilarity between two feedback F_p and F_q, of health institution (see Definition 1). Where the subscript p and q denote present and past feedback, respectively.

Definition 1 (Degree of consistency)**.** *The degree of consistency is a measure used to quantify the similarity of two feedback F_p and F_q. To normalize the consistency, we define trust consistency $\theta \in [0, 1]$, such that the higher the value of θ is, the greater the consistency of F_p and F_q.*

The similarity measure quantifies how closely related or distinct two data samples are to one another. $S(F_p, F_q) \in [0, 1]$ is a scalar and if $S(F_p, F_q) = 1$, it implies that feedback data F_p and F_q are related and very similar, and vice versa. The smaller the distance between F_p and F_q, the larger the similarity. A given similarity $S(.)$ is aimed to be a metric if and only if it satisfies the following conditions:

1. Non-negativity: $S(F_p, F_q) \geq 0$, for any two distinct feedback F_p and F_q of a health institution.
2. Symmetry: $S(F_p, F_q) = S(F_q, F_p)$, for all F_p and F_q.
3. Triangular inequality: $S(F_p, F_q) = S(F_p, F_r) + S(F_q, F_r)$, for all F_p, F_q, and F_r.
4. $S(F_p, F_q) = 0$, only if $F_p = F_q$.

The trust similarity is calculated as follows.

$$d_{p,q} = \frac{\sum_{n=1}^{N} \frac{F_{pn} - F_{qn}}{F_{qn}}}{N}, \tag{5}$$

$$S(F_p, F_q) = 2\left(d_{p,q}\right)^2 - 4|d_{p,q}| + 1, \tag{6}$$

Equation (6) is a modification of the work in [28]. The work in [28] uses a range value that does not use all of the elements in a data collection and is particularly sensitive to outliers. Moreover, trust distortion is checked by validators of nodes before any trust value is calculated (see Section 3.2). The trust distortion implies that the trust value has been tampered with by a malicious evaluator while the degree of distortion can only be

probabilistically given. It implies that a random distribution rate is added to the trust value. Thus, $d_{p,q}$ is best suitable in our proposed scenario. If $S(F_p, F_q) = 1$ it implies that a similarity exists between F_p and F_q. Otherwise, if $S(F_p, F_q) = 0$, there is no similarity between F_p and F_q. The trust consistency θ is calculated as follows.

$$\theta = \frac{\alpha}{\alpha + S(F_p, F_q)}, \tag{7}$$

where $\theta \in [0, 1]$, and α is the adjustable parameter that regulates the degree of feedback consistency. As stated earlier, if $S(F_p, F_q)$ is small, the closer F_p and F_q are. To determine the feedback accuracy, a reference value that defines the range of $S(F_p, F_q)$, is denoted as ϵ. If $S(F_p, F_q) < \epsilon$, the consistency degree of F_p and F_q can be quantified. If ϵ is big, it implies that there is an inconsistency between F_p and F_q, and should be disregarded.

Definition 2 (Strong consistency)**.** *F_p and F_q satisfy a strong consistency if feedback values are the same.*

Definition 2 clearly defines the strong consistency of the two feedbacks with the same values. Moreover, strong consistency feedback may come from the same evaluator, but with different time progressions. We define weak feedback consistency as follows.

Definition 3 (Weak consistency)**.** *F_p and F_q satisfy a weak consistency if there is a certain deviation in their values.*

In Definition 3, the evaluator may perform recommended trust evaluation of the evaluatee at different times based on cordial interaction. If the interaction is successful, a feedback will be sent to the blockchain. Other evaluators send their feedback values to the blockchain-based on established communication and interaction. The aggregator evaluates the evaluatee using the feedback values. Hence, there may be a certain deviation in the feedback values of the evaluators. We consider a complete consistency of the feedback such that there is a relationship between the two feedback. Additionally, if F_p and F_q obeys the same rule, a conditional consistency is established. Algorithm 1 illustrates the process of trust evaluation. The time complexity of the proposed system model tells us the amount of time required by the algorithm to run as a function of the size of the input. It takes a constant time for message authentication, i.e., O(1), in an average scenario it requires O(1), and in a worst-case scenario, it takes O(N). In the proposed system, the number of trust evaluations takes the time complexity of O(N) and the entire operation takes the time complexity in a worst-case scenario of log(N) + O(N).

Algorithm 1 Evaluation of the trust value.

1: $TrustCheck = false$

2: The requester of data calculates the hash of its request using the hash based message authentication code (HMAC) as

$$HC_{req} = HMAC_{req}(Sig_{req}, D, \{ID_{req}||Pk_{req}\}), \tag{8}$$

where Sig_{req} is the signature of the requester, D is the requested data, ID_{req} is the identity of the requester and Pk_{req} is the public key of the requester.

Algorithm 1 *Cont.*

3: Once aggregator receives a request of data from the requester in a coalition group G, it first authenticates by verifying the request such that the request req is defined as

$$Req = \{ID_{req}, Sig_{req}, D, Pk_{req}, t\}, \tag{9}$$

where t is the time when a request was initiated. The aggregator calculates the hash code HC_{agr} as

$$HC_{agr} = HMAC_{agr}(Sig_{req}, D, \{ID_{req}||Pk_{req}\}), \tag{10}$$

where the subscript agr denotes aggregator. Afterwards, aggregator verifies HC_{agr}.

4: **if** $HC_{req} == HC_{agr}$ **then**

5: The request is authenticated successfully,

6: Aggregator evaluates the trust value of the requester by calculating

$$v_{agr} = \tau_t \times \beta_t. \tag{11}$$

7: **if** $v_{agr} == v_t$ **then**

8: The trust value is verified successfully. Afterwards, the aggregator calculates the similarity and acceptability of the trust value.

9: **if** $S(F_p, F_q) < \epsilon$ **then**

10: Consistency degree can be quantified.

11: $TrustCheck = true$

12: **else**

13: Trust acceptance is not successful.

14: $TrustCheck = false$

15: **end if**

16: **else**

17: Trust value is not successful and there is a possibility of manipulation.

18: $TrustCheck = false$

19: **end if**

20: After the trust value and acceptance test is successful, the aggregator forwards the request of data in an encrypted form to the coalition group leader.

21: The leader receives the encrypted request and decrypts it using its private key. Then, leader sends a broadcast to the nodes within the group.

22: On receiving the broadcast message, the concerned node acknowledges the request and sends the respond to the leader, which then forwards the encrypted respond message to the aggregator.

23: Aggregator decrypts the respond message and forwards it to the requester.

24: **else**

25: The requester is not authenticated; hence, aggregator drops the request of data and report it via broadcast in the blockchain.

26: **end if**

3.2. Proof-of-Trust Collaboration Consensus Protocol

In this study, nodes in the blockchain with the highest trust values take part in the consensus processes of block creation and mining. The PoTC consensus protocol is designed to sustain trust management between nodes in the blockchain. As compared to the PoW consensus protocol [29], the proposed PoTC consensus protocol is application intensive, which means that it is computationally cost-effective. The PoW consensus protocol requires

all nodes to participate in the cryptography hash puzzle that is easy to validate but difficult to be solved. This type of consensus protocol is not suitable for resource-constrained IoMT devices. According to [29], the stake of assets (i.e., PoS) is used instead of high computing resources of PoW to accomplish mining. Therefore, motivated by PoW and PoS consensus protocols, the PoTC is conceived. Here, CDCs prove the trust of collaboration by engaging in healthy interactions with one another. Additionally, there is no need for CDCs to solve complex mathematical puzzles to validate the proof of their work. Inspired by [29], the PoTC consensus is formulated as follows.

$$\begin{aligned} &\text{Find p} \\ &\text{subject to:} SHA256(SHA256(b,p)) < T_c \times target, \end{aligned} \tag{12}$$

where b denotes the content of the latest block, and $target$ represents mining difficulty. The smaller the value of $target$ is, the more difficult mining will be [29]. The leader among other nodes, known as the aggregator, is chosen based on the weight difference game. Three parameters are considered when playing the game and they are the trust consistency value θ, trust value v_t, and trust deviation $d_{p,q}$. Note that these parameters are recorded in the blockchain. The weight difference game is being played by leaders of coalition groups and the leader whose trust score is the highest among other leaders starts the game followed by the leader with the next score, and so on.

3.2.1. Strategy of the Game

The game comprises leaders of coalition groups, which reduces the boredom that has been established if all CDCs were to be evaluated using the above-mentioned trust evaluation parameters. The only strategy is that the trust values (scores), trust consistency, and trust deviation are computed accurately.

3.2.2. Winner of the Game

A winner is selected if the trust values, trust consistency, and trust deviation are compared for each coalition group leader. The leader with the highest trust score, trust consistency value, and lowest trust deviation value is declared the winner of the game; thus, it becomes the overall aggregator that propagates new a block. The game terminates when a winner is announced.

Theorem 1. *The proposed PoTC consensus protocol prevents the mining centralization problem.*

To prove Theorem 1, we consider the following assumptions.

1. Every CDC uses application-specific integrated circuits similar to users of Bitcoin.
2. The winner node is selected based on its computing resources. This implies that the winner node with the most computing resources is always selected.

In the proof of Theorem 1, mining centralization is addressed because assumptions (1) and (2) do not hold. Here, every aggregator in each group is evaluated and rated. It means not all CDCs of a group are involved in the consensus protocol, thereby minimizing the response time and latency. The proposed PoTC consensus protocol reduces the number of competitors via the proposed trust evaluation mechanism, thereby minimizing resource wastage as seen in the PoW consensus protocol. Note that reducing the number of competitors achieves consistency and prevents the double-spending attack. As time progresses, the leader of a group is selected based on its trust value. It implies that at a certain period, a leader is selected as the winner if it has the highest trust value, while at another period they might not be selected as the winner if it has the lowest trust value. Thus, the proposed PoTC consensus protocol prevents minimizing the centralization problem.

Theorem 2. *The proposed PoTC consensus protocol is robust against similarity attacks.*

In order to prove Theorem 2, we define a similarity attack. When a malicious user tries to take advantage of the proposed trust management system's flaw, it results in a similarity attack. The attack is possible if the malicious user collides with the aggregator to modify the trust values; thereby producing fake trust consistency values. The proposed PoTC consensus addresses similarity attacks because trust values are not used alone to evaluate nodes, other factors such as feedback consistency and trust deviation are considered. Feedback consistency ensures that modified trust values can be easily detected. Suppose that the attacker a has a trust consistency value denoted as θ_a; if $\theta_a > \theta$, the attacker successfully launches a similarity attack. However, it is difficult for the attacker to achieve $\theta_a > \theta$ because, for every period, F_p and F_q are evaluated by validators and the $S(F_p, F_q)$ of the attacker cannot satisfy the similarity metric. Thus, the proposed PoTC consensus protocol is robust against similarity attacks.

The proposed PoTC consensus protocol aims to provide fault tolerance in such as manner that the failure of a particular node does not affect the accuracy of the trust management system. All CDCs are placed in a coalition group, every group has a leader, and the leader with the most trust value becomes the aggregator while other group leaders serve as backup nodes. The aggregator node becomes the federated server (see Section 3.3 for the discussion of federated learning) that serves the requests of the clients' nodes (federated clients). It acts as an arbitrator between the backup nodes and the client nodes. The leaders of the coalition groups are capable of communicating with nodes within their coalition. Moreover, the leaders can reach a consensus for the general change in the network based on majority rule. The idea of the proposed PoTC consensus protocol is similar to the practical Byzantine fault tolerance algorithm [30] with the exception that trust values are used to assemble nodes in coalition groups. The federated clients send requests to the federated server and the leader node broadcast the requests to the backup nodes. All backup nodes act on the request and send the responses to the federated clients while the clients wait for $(f - 1)$ responses from all backup nodes with the same result. Note that f denotes the number of faulty nodes in the network. The proposed PoTC consensus protocol consists of the following phases as shown in Figure 2.

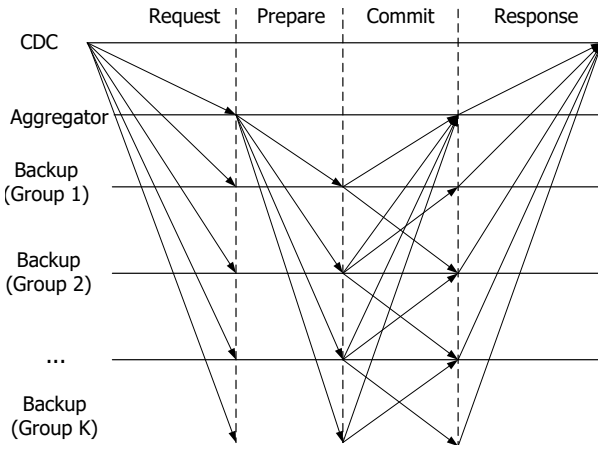

Figure 2. The working of the proposed PoTC consensus algorithm.

Request Phase

In this phase, the CDC sends a request for data to the aggregator, which then rebroadcasts the request to the backup nodes. The concern backup node that has the response to the CDC's request sends the reply to the aggregator.

Prepare Phase

After receiving the broadcast message from the aggregator, the backup nodes send the message as a reply to all nodes inclusive of the aggregator. A backup node is prepared

if it has received the message from the aggregator and has $(2f-1)$ number of broadcast messages from other nodes.

Commit Phase

The commit implies that the nodes are willing to respond to the aggregator and other nodes via acknowledgments. It means that the nodes send commit messages if they received $(f+1)$ commit messages by responding to the CDCs' requests. The entire process of verifying and validating messages follows the distributed system. Moreover, digital signatures are used to prevent the problem of non-repudiation. Non-repudiation means that the sender can deny sending a message to the receiver. Nevertheless, the sender and message are ensured using the sequence number.

3.3. The Proposed Federated Learning System

The federated learning model is used in this study to produce a decentralized trust management system and data training, as shown in Figure 3. Here, identical data samples are stored on numerous IoMT servers or devices without any modification. Additionally, because only the model and gradient parameters used to train the data are given, the privacy of the owners of each sample is maintained. On the other hand, a centralized system enables all local data to be processed and uploaded to the central server. Single points of failure can be a problem for this kind of system. Because diverse health institutions can create a similar and reliable machine learning model without sharing data, this study takes federated learning into account. As a result, important issues including data security, privacy, and access control privilege are dealt with. Decentralized federated learning is based on the ideas of local data sample training and parameter exchange amongst local nodes (federated clients) at a predetermined frequency to create a shared global model. The parameters are the model's weight and the machine learning algorithm's biases.

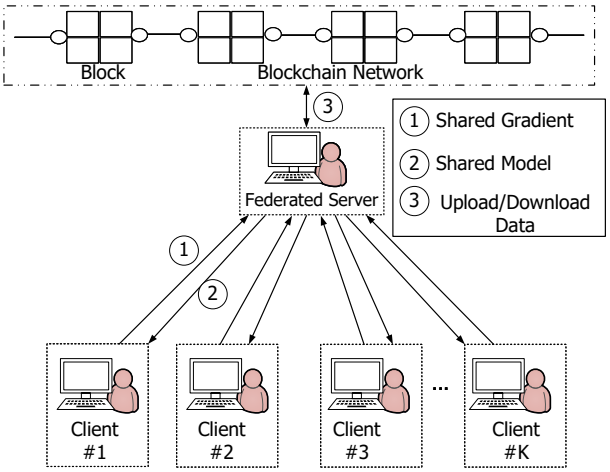

Figure 3. The federated learning system. Each client sends model gradient parameter to the server; afterwards, it receives the shared model from the server. The server uploads and downloads the shared global gradients and model parameters to blockchain.

This study takes into account the decentralized federated learning strategy, in which each node works together to obtain updates to the global model. By exchanging model updates among networked nodes without integrating a central server, this sort of method reduces the risks of single points of failure. The federated server has the same device attributes as the clients (see Figure 3). Keep in mind that the client's status as a federated server depends on the outcome of its trust evaluation (see Section 3.1). A heterogeneous federated learning system will be taken into consideration as advanced research to integrate a large number of heterogeneous clients, such as mobile devices and IoT devices [31].

An iterative process divided into client-server interactions, known as a learning round, is the foundation of decentralized federated learning. Each round starts with sending the current state of the global model to the participating nodes, followed by training the local model on the client to produce a number of model updates at each client node, then combining the local updates into a single global update and processing it to create the global model. The federated clients train the server's rule locally while the federated server handles the aggregate. The learning process is outlined as follows:

1. Initialization: A machine learning model is initially chosen using the input, that is, the parameters are set, to be trained on federated clients. Federated clients are then turned on and ready for the server to provide them with computing work.
2. Selection of clients: All backup nodes are the selected federated clients that will begin training the local data. While other nodes, or CDCs, wait for the subsequent learning round, and the leaders receive the most recent statistics from the model.
3. Configuration: The backup nodes are given instructions by the federated server to begin training on the local data in a predetermined way. The gradient descent's mini-batch update is set up here.
4. Documentation: The aggregated parameters and local model are saved in the blockchain while the backup nodes send their local models to the federated server for aggregation. The backup nodes receive model updates from the federated server, which aggregates the local models it has received. The latest model updates are handled by the server. The process of client selection is started in the following learning round.
5. Termination: The federated server collects the updates once the termination criterion is reached and completes the global model.

This study considers the procedure above to be synchronized model updates as exchange happens once the computations have been executed for all layers of the machine model.

4. Security Analysis

A threat model is designed to demonstrate the possible vulnerabilities of the proposed system model. Moreover, there is no universal design of threat model [32], which means that our proposed threat model interprets the possible solutions to the identified threats and attacks. The threat actors consider in this study are honest, malicious, and honest-but-curious. An honest actor is someone who legitimately provides accurate trust evaluations of the evaluatees while considering the trust factors. Contrarily, a malicious actor is someone who engages in activities that compromise the proposed system, which includes providing fake or inaccurate trust evaluations. An honest-but-curious actor is someone who at some point behaves honestly and at another point behaves maliciously or becomes curious to exploit the vulnerability of the proposed system. This study aims to mitigate the possible threats and attacks. Moreover, existing studies [10,12,33] discuss the following attacks: on-off attacks, bad-mouthing attacks, good-mouthing attacks, selective misbehavior attacks, time-varying attacks, self-promoting attacks, whitewashing attacks, and newcomer attacks.

Definition 4 (Trust malicious node detection)**.** *A trust malicious node detection happens when multiple trust relationships exist with their respective actions. The relationships can be indirect, direct, or recommendation trust. Then, the actions can be successful interactions or failed interactions. For every trust relationship, the trust actor performs the following actions:*

1. *Successful interactions:* $\Delta_s = v_s + 1$,
2. *Failed interactions:* $\Delta_f = v_f + 1$,
3. *No interactions :* $\Delta_s = \Delta_f = 0$,

where Δ_s *and* Δ_f *are the trust evaluation for successful and failed interactions, respectively, and* v_s *and* v_f *are the trust values for successful and failed interactions, respectively.*

Definition 5 (On-off attack)**.** *An honest actor may be made incompetent and changed into a malicious actor through compromise; whereas, an incompetent actor may become competent as a result of environmental changes [34].*

Theorem 3. *The proposed system is robust against on-off trust-related attacks.*

To prove Theorem 3, we introduce a forgetting factor $\omega \in (0, 1]$, which is used to mitigate the on-off attack. The on-off attack can be prevented if $\frac{ns}{ns+nf} \leq \omega$, where ns is the number of successful interactions and nf is the number of failed interactions. If $\omega = 1$, the malicious actor has a high trust value (honest behavior) while the system does not forget such behavior. This implies that the malicious actor can have honest trust value even when it behaves maliciously. On the other hand, if $\omega < 1$, the malicious actor regains its trust after behaving honestly. Note that an adaptive forgetting scheme can be employed [34]. This study assumes the possible on-off attack by considering the proposed scenario. Suppose that an actor A behaves honestly in a coalition group G_1 and another coalition group G_2, it behaves maliciously. Note that the aggregator of G_2 will rate A low while the aggregator of G_1 will rate A high. Suppose that $B \in G_2$ wants to recommend A, the outcome of it will be a low recommendation value or a disagreement to recommend, because A has been given a low trust score in G_2. Therefore, the on-off trust attack is mitigated using the proposed system.

Definition 6 (Bad-mouthing attack)**.** *A bad-mouthing attack happens when an actor provides a dishonest trust evaluation of the evaluatee [10].*

Theorem 4. *The proposed system is robust against bad-mouthing trust-related attacks.*

To prove Theorem 4, a trust malicious detection metric is formulated as $\frac{|CN|}{|TCN|} \leq \sigma$, where $|CN|$ is the number of compromised nodes, $|TCN|$ is the total number of compromised nodes and σ is the threat threshold. Note that σ can be regarded as the weighted factor of trust evaluation, such that $\sigma \leq 1$. As the value of σ approaches 1, the number of compromised nodes reduces and vice versa. Thus, the proposed system is robust against bad-mouthing trust-related attacks.

Theorem 5. *The proposed system is robust against Sybil attacks.*

To prove Theorem 5, we first define what a Sybil attack is. A Sybil attack [35] occurs when an attacker in the network creates multiple identities for financial gains or degrades the proposed system. Here, the attacker tries to masquerade using different group identities. In the proof of Theorem 5, we consider the probability of y successes when sampling without replacement n nodes from the coalition group of r successes and $(N - r)$ of failures. This is a hyper-geometry distribution where we determine the number of successes the attacker will make when launching the Sybil attack. The hyper-geometric function is formulated as follows.

$$P[y] = \frac{\binom{r}{y}\binom{N-r}{n-y}}{\binom{N}{n}}, \tag{13}$$

where $\binom{r}{y}$ is a binomial distribution coefficient. We define the threshold Θ for the attacker to successfully launch the Sybil attack. Additionally, the computational resource is taken into account when executing the Sybil attack, in which the attacker is thought to possess greater processing power than the authorized nodes in the network. It indicates that the attacker is able to mine and build a fake chain to spread fork nodes with fictitious identities throughout the network. Let *rho* represent the attacker's computational capabilities; if $\rho > \Theta$, the attacker will be successful in launching Sybil, and vice versa. This study mitigates the Sybil attack using the proposed PoTC consensus protocol. Before a block

is added to the blockchain, it must be validated by the majority of nodes in the network. Only the leaders of the coalition groups are responsible for the validation. This means that no other nodes in the network can participate in the consensus process. Here, even if the attacker has a computing resource advantage, he is unable to compromise the proposed system because a trust management system is employed to ensure the credibility of the nodes in the blockchain. Nodes with good credibility participate in the consensus protocol. Thus, the proposed system is robust against Sybil attacks.

Theorem 6. *The proposed PoTC consensus protocol is robust against double-spending attacks.*

A double-spending attack is used to prove Theorem 6. When an attacker propagates two transactions using the same token, such as ether in Ethereum, before broadcasting them throughout the network, this is known as a double-spending attack [36]. This indicates that the attacker will mine two blocks, one of which is real and the other not. As the genuine one is received by the validators, payment or incentive is given to the attacker, while the fake block and genuine blocks are mined together. This study formulates a mechanism that determines the success of the double-spending attack as follows

$$\Psi = \frac{\rho_i}{\sum_{i=1}^{M} \rho_i} \leq \Theta, \tag{14}$$

where $\Psi \in [0, 1]$ is the degree of compromise if the double-spending attack is successful and M is the number of successful double-spending attacks. If $\Psi > \Theta$, the double-spending attack is successful; otherwise, it is not successful. As a result, the double-spending attack cannot succeed against the proposed PoTC consensus mechanism.

5. Simulation Results

This study uses a laptop with an Intel i5 quad-core processor running at 1.60 GHz and 8 GB of RAM for implementing the proposed system model. The Ethereum platform, which is based on Python 3.6.1, is utilized to create the consortium blockchain system in health institution scenarios. Web3.py is made available for communicating between blockchain and IoMT applications, while solidity is used to create the smart contract. Ganache is also used as the blockchain environment that enables the emulation of the Ethereum blockchain and for executing smart contracts. The performance of the proposed model is evaluated and validated through extensive simulation experiments. The parameters used in this study are given in Table 2, while other parameters are taken from [1,37].

Table 2. Parameter descriptions and values.

Parameters	Description	Values
N	Number of nodes	20
τ_t	Trust rating of evaluatee	[0, 1]
C_R	Trust collaboration reward	10
F_p and F_q	Current and past trust feedback	[0, 1]
α	Adjustable parameter of trust consistency	[0.6, 0.7, 0.8, 0.9]
ϵ	Reference value for trust similarity	[0.5, 0.6, 0.7, 0.8]
ns	Number of successful interactions	100
nf	Number of failed interactions	50
ω	Forgetting factor	[0, 1]
$\|CN\|$	Number of compromised nodes	3
$\|TCN\|$	Total number of compromised nodes	10
σ	Threat threshold	0.5

Evaluation of the Proposed Trust Management System

In this study, we consider 20 nodes for each coalition group. Note that this study is not limited to the number of nodes in a coalition group, but it can vary for different scenarios. The evaluators are expected to provide trust ratings of evaluatees within [0,1] over t period. Moreover, the same trust rating can be given to the same evaluatee by the evaluator if there is a cordial interaction between them. It implies that the trust rating of the evaluatee given by an evaluator remains the same over t period. However, the trust rating of the same evaluatee can be different for other evaluators. Thus, the trust management system can accommodate variations of the trust rating of evaluators. Note that a better trust rating, $\tau_t > 0.5$, is motivated by successful interactions between the evaluatee and evaluator, either in the past or current time horizon. Nevertheless, the trust value of an evaluatee is influenced by trust factor β_t, which means that even if an evaluatee gets $\tau_t > 0.5$, its trust value may be low if $\beta_t \leq 0.5$, and vice versa.

In Figure 4, it is observed that the trust factor varies for different probabilities. It means that the evaluatee with trust factor $\beta = 0.4$ has different probabilities. This depicts the different behaviors of the evaluatee at different t periods.

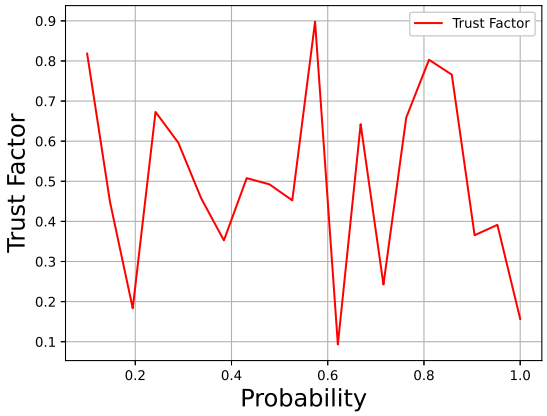

Figure 4. Evaluation of the trust factor.

The evaluation of trust-based collaboration is shown in Figure 5. The figure shows that the trust values and trust collaboration follow a similar pattern, with the initial trust collaboration incentive C_R being 10 and the number of nodes increasing. It indicates that trust value and trust collaboration are inversely correlated, meaning that trust value rises with trust collaboration and vice versa. This shows the different behaviors of evaluators regarding the trust collaboration reward. The trust collaboration reward is aimed to provide an incentive to the evaluator that provides honest trust evaluation of the evaluatees. The trust collaboration reward is used in the computation of the PoTC consensus protocol.

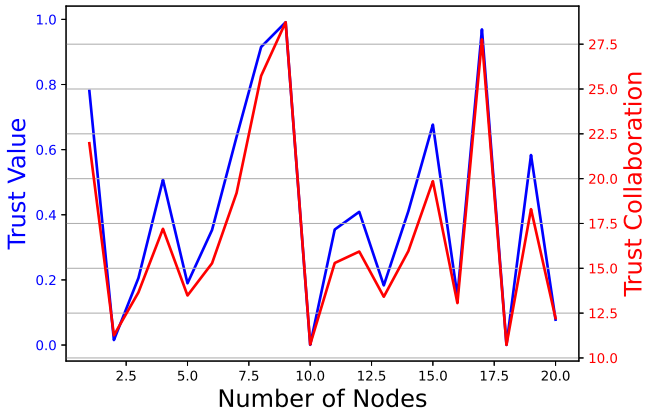

Figure 5. Evaluation of trust collaboration.

Figure 6 shows the evaluation of trust consistency based on different values of α. It is observed from the figure that the trust value approaches 1 for the different values of α. It implies that the trust feedback values of the evaluators are consistent, thereby leading to strong consistency. The adjustment parameter α denotes the different behaviors of the evaluators to provide either direct trust evaluation or recommended trust evaluation. The results in Figure 6 show the accuracy of the proposed trust management system, which means that the CDCs can share data without the fear of misleading. Every CDC that adopts the proposed trust management system is obliged to share information that is validated and authenticated by the majority of nodes whose trust evaluations are authentic.

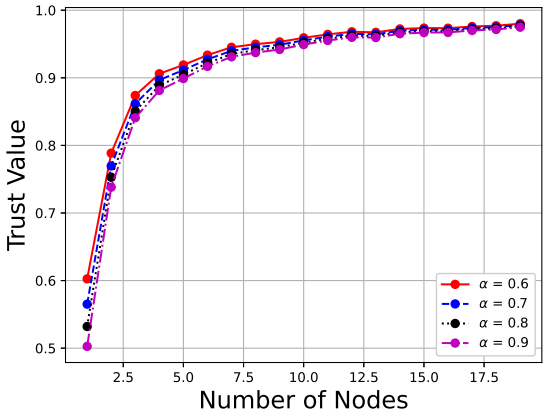

Figure 6. Evaluation of trust consistency based on different values of α.

To further demonstrate the performance of the proposed trust management system, we compare our results with two existing trust management systems, known as IoTHiTrust [1] and Adaptive trust [37], respectively.

We take into account an IoT environment with 400 different smart devices that are distributed randomly among 20 users [1]. The body area networks (BANs) are used to link the users. Data requests from evaluator i to evaluatee j are used to evaluate the direct trust between them. Epidemiological information that is helpful for disease prevention, surveillance, and diagnosis is the basis of the data request. Every node sends an exponentially distributed request for data to the desired device with a predetermined time interval [37]. Every two hours, the trust values are updated, but there is no direct trust update because the evaluation and other processes have been finished. To prevent long queues during service requests, we applied the time decay [1] until the service request is completed. Every process of evaluation takes at least 200 hours. Based on Figure 7, honest nodes follow the trust evaluation of our proposed system while malicious nodes provide inaccurate trust recommendations, which gave birth to badmouthing, on-off, and Sybil attacks for financial gains or other motives. In Figure 7, the similarity between our proposed system and existing schemes is also provided. It implies that our proposed scheme is adequate to deliver reliable and accurate trust assessments.

We further evaluate the performance of the proposed system in terms of execution time. The execution time of different functions of the proposed system is presented in Table 3. It is observed from the table that each function has a different execution time, which implies that the number of times it takes the algorithm to be executed is not the same.

The proposed system is compared to the current system's execution time in Table 4. It is clear from the table that the proposed system executes with the least amount of time when compared to the IoTHiTrust and adaptive systems, respectively. Because of how well the proposed approach performs, putting it into practice takes very little time. It becomes effective for IoT devices that have limited computing resources.

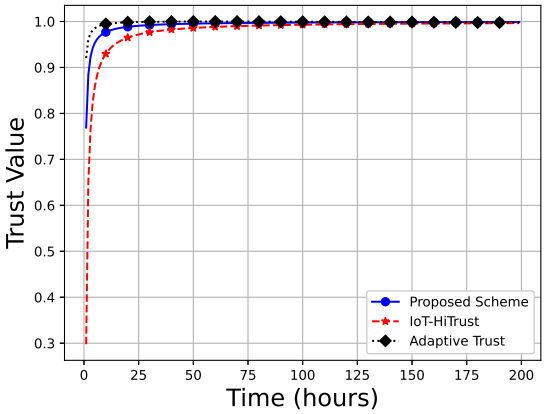

Figure 7. Comparison with existing schemes in terms of trust value.

Table 3. Evaluation of execution time for different functions.

Function	Execution Time (s)
Similarity Value	5.51
Trust Consistency	5.66
Degree Trust Similarity	190.18
Trust Reliability	254.26
Trust Deviation	254.83

Table 4. Evaluation of the proposed system and existing systems in terms of execution time.

Function	Execution Time (s)
Proposed System	284.83
IoTHiTrust	402.86
Adaptive	403.38

Security Analysis of the Proposed Trust Management System

The evaluation of trust similarity is shown in Figure 8. According to Equation (6), the similarity metric can be defined if $S(Fp, Fq) < \epsilon$. As the number of nodes rises, it is shown in Figure 8 that the values of trust dissimilarity decrease. It means that the trust similarity would not be calculated for compromised nodes if there are several of them. Therefore, the proposed trust management system aids in preventing the breach of similarity in trust. The trust similarity metric aids in determining how similar two trust feedback ratings are to one another. Any two trust feedback values that are not similar will be discarded by the proposed trust management system. We consider different values of ϵ to determine the behaviors of an attacker in exploiting the vulnerability of the trust similarity metric. It is also observed in Figure 8 that the values of ϵ increase, and the trust dissimilarity decreases. Suppose in this study that two or more nodes are compromised, the probability of trust dissimilarity is zero. It implies that the compromised nodes do not alter the trust credibility of the proposed system.

We can determine the dependability and consistency of two trust feedback ratings using trust consistency. It implies that the values for trust feedback are the same. We explore a case in which the proposed method has a lack of confidence. Figure 9 shows that the risk of trust inconsistency lowers as the number of nodes rises. It means that if more than one node is compromised, the probability of trust inconsistency is zero. For a few nodes, the probability of trust inconsistency is high, which can be easily detected by the proposed system. Our proposed system achieves strong consistency (see Definition 2) because the trust feedback F_p and F_q are the same. If there is any deviation in the trust feedback values, the probability of trust consistency will be 0.

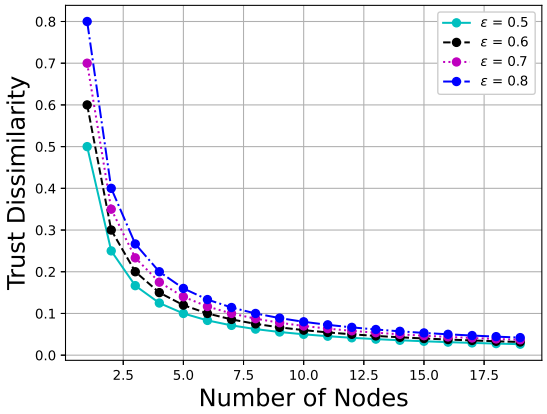

Figure 8. Evaluation of trust similarity.

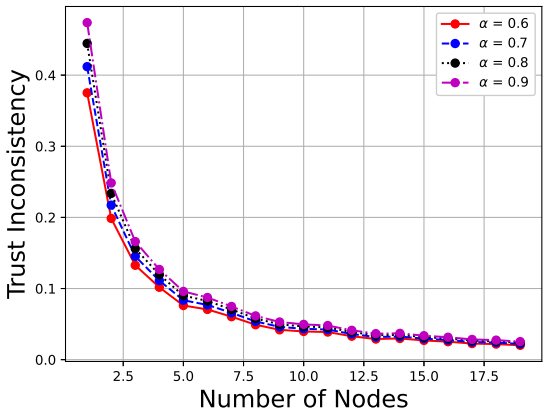

Figure 9. Evaluation of trust consistency.

We evaluate the efficiency of our proposed trust management system against malicious nodes' behavior for performing on-off, badmouthing, and Sybil attacks, by selecting at random certain nodes as malicious with a 0.3 percent probability of successfully launching the attacks. A malicious node takes advantage of the trust system's weakness based on the aforementioned threats, whereas an honest node performs the proposed trust management system honestly. In Figure 10, it is observed that as time increases, trust inconsistency reduces for all schemes. This means that the proposed system can mitigate trust-related attacks even when the malicious node has time advantages over the honest node.

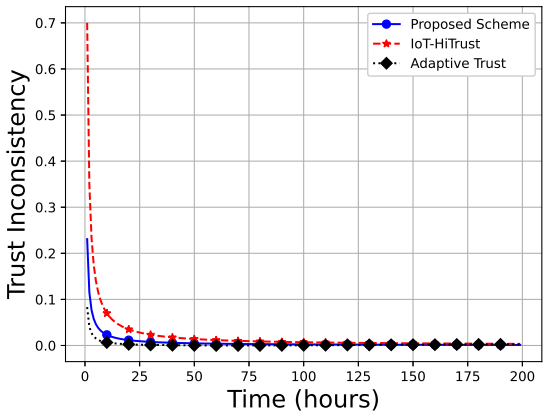

Figure 10. Comparison with existing schemes in terms of trust consistency.

Figure 11 shows the evaluation of an on-off attack. We consider the different values of ω to ascertain the performance of the proposed trust management system. It has been

found that as time passes, the likelihood of an on-off attack declines, meaning that even if the attacker has the benefit of time, they will not be able to launch the attack effectively. It is anticipated that the attacker will have an advantage over the honest nodes in terms of computation and time before the attack is conducted. It implies that the attacker with computational and time advantage can successfully mine a block, thereby creating fork nodes in the network. Additionally, a fake chain can be created by the attacker, thereby deceiving other honest nodes to join the chain. For example, when $\omega = 0.5$, it means there is a 50% chance that the on-off attack can be successfully launched. However, from the results, it is obvious as the attacker takes a longer time, the probability of a successful on-off attacker is zero. The proposed trust management mechanism is hence resistant to the on-off attack.

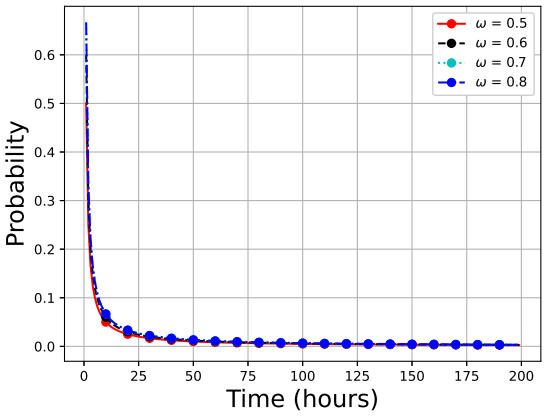

Figure 11. Evaluation of on-off attack considering ω.

Figure 12 shows the evaluation of the on-off attack in terms of the number of failed interactions. In this study, we consider $ns = 100$ and $nf = 50$ for the evaluation of on-off attacks. According to Figure 12, the likelihood of a successful on-off attack declines as attack duration increases for different values of nf. The various values of nf illustrate the attacker's behavior. The findings also indicate a decreasing likelihood of a successful on-off attack as the number of failed exchanges rises.

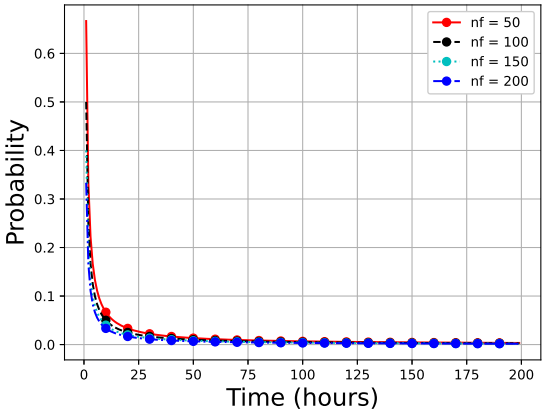

Figure 12. Evaluation of on-off attack considering the number of failed interactions.

The evaluation of a double-spending attack is shown in Figure 13. When an attacker has an advantage over honest nodes in terms of both time and computational resources, a double-spending attack occurs. We consider the computational cost ρ as gas generated from Ethereum blockchain. Note that computation cost comprises transactional cost and executional cost measure in gas (i.e, Ethereum blockchain). Additionally, the gas price generated by the Ethereum blockchain is different for each opcode. The computational cost against time is shown in Figure 14. The figure shows that the computational cost changes

for each time period. This means that the cost of mining a block differs with respect to time. Moreover, the probability of a successful double-spending attack is calculated using Equation (14) and its results are depicted in Figure 13. The findings unequivocally demonstrate that there is no chance of a successful double-spending attack as the number of time slots increases. This demonstrates that the probability remains 0 for all possible values of θ. If the probability approaches 1, it means that the attacker successfully launched a double-spending attack. Otherwise, if the probability approaches zero, the attacker could not launch the double-spending attack. The proposed approach is hence resistant to the double-spending attack.

Table 5 shows the comparison between the double-spending attack and the on-off attack. It is observed from the table that the double-spending attack has more execution time than the on-off attack. This is due to the process of determining the degree of compromise according to Equation (14). Moreover, the execution time of the double-spending attack comprises the block mining time of propagating two transactions and broadcasting them over the network.

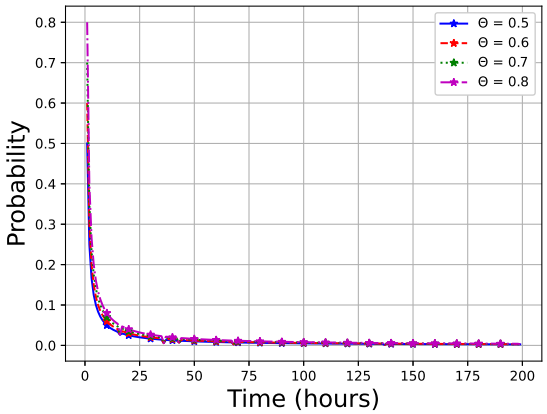

Figure 13. Evaluation of double-spending attack considering Θ.

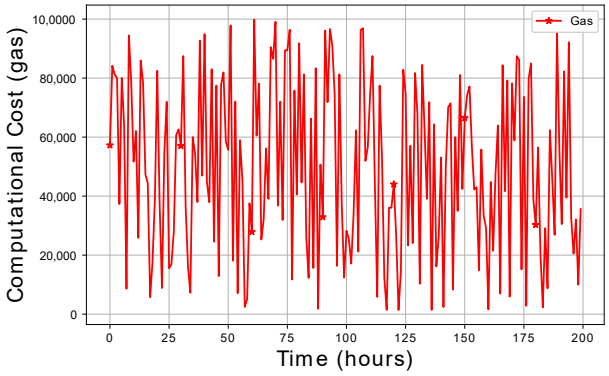

Figure 14. Evaluation of computational cost against double-spending attacks.

Table 5. Evaluation of the different attacks in terms of execution time.

Function	Execution Time (s)
On-off attack	407.39
Double-spending attack	416.49

6. Conclusions

In this study, we analyze the importance of a trust management system for large-scale IoMT systems. Additionally, the privacy of data owners is preserved using the proposed blockchain and federated learning systems. Health institutions are grouped into several

coalition groups for scalability and management. Leaders of coalition groups are elected using the proposed PoTC consensus protocol and the aggregator is chosen from leaders based on the weight difference game while considering the following factors: trust scores, trust consistency, and trust deviation. Direct and recommended trust evaluations are considered in this study. Extensive simulations are performed to evaluate the efficacy of the proposed system. The results show that the proposed system not only achieves scalability, and credibility without compromising the accuracy, convergence, and resilience against trust-related attacks but outperforms existing systems: IoT-HTrust and Adaptive trust. Security analysis shows that the proposed system is robust against on-off attacks, badmouthing attacks, Sybil attacks, and double-spending attacks.

In the future, we hope to test the robustness of the proposed PoTC consensus protocol to improve the network throughput. Additionally, we aim to collaborate with health institutions for the implementation of the proposed prototype system. This will enable us to evaluate its real-world application more accurately. Moreover, the proposed system is aimed to be applied in heterogeneous scenarios where different clients will be integrated.

Author Contributions: All authors agreed on the main idea. L.B. and T.M. implemented the proposed schemes and also wrote the proposed system models and results. L.B., T.M. and O.S. wrote rest of the paper, organized and refined the refined the paper as well. All authors together responded the reviewers' comments. O.S. supervised the overall work. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data available on request from the authors.

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

Abbreviations

The following abbreviations are used in this paper:

CDC	Center for Disease Control
DDTMS	Dirichlet Distribution-Based Trust Management Scheme
ICN	Information-Centric Networks
IoMT	Internet of Medical Things
IoT	Internet of Things
IoV	Internet of Vehicles
PoA	Proof-of-Authority
PoS	Proof-of-Stake
PoTC	Proof-of-Trust-Collaboration
PoW	Proof-of-Work
VANET	Vehicular Energy Network
WHO	World Health Organization

References

1. Chen, R.; Guo, J.; Wang, D.C.; Tsai, J.J.; Al-Hamadi, H.; You, I. Trust-based service management for mobile cloud IoT systems. *IEEE Trans. Netw. Serv. Manag.* **2018**, *16*, 246–263. [CrossRef]
2. Hao, W.; Zeng, J.; Dai, X.; Xiao, J.; Hua, Q.S.; Chen, H.; Li, K.-C.; Jin, H. Towards a trust-enhanced blockchain P2P topology for enabling fast and reliable broadcast. *IEEE Trans. Netw. Serv. Manag.* **2020**, *17*, 904–917. [CrossRef]
3. Wang, J.; Zhang, Z.; Wang, M. A Trust Management Method against Abnormal Behavior of Industrial Control Networks under Active Defense Architecture. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 2549–2572. [CrossRef]
4. Putra, G.D.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R.; Ignjatovic, A. Trust-based blockchain authorization for iot. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 1646–1658. [CrossRef]
5. Meng, W.; Choo, K.K.R.; Furnell, S.; Vasilakos, A.V.; Probst, C.W. Towards Bayesian-based trust management for insider attacks in healthcare software-defined networks. *IEEE Trans. Netw. Serv. Manag.* **2018**, *15*, 761–773. [CrossRef]

6. Battah, A.; Iraqi, Y.; Damiani, E. A Trust and Reputation System for IoT Service Interactions. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 2987–3005. [CrossRef]
7. Liu, X.; Huang, H.; Xiao, F.; Ma, Z. A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs. *IEEE Internet Things J.* **2019**, *7*, 4101–4112. [CrossRef]
8. Yang, Q.; Liu, Y.; Chen, T.; Tong, Y. Federated machine learning: Concept and applications. *ACM Trans. Intell. Syst. Technol. (TIST)* **2019**, *10*, 1–19. [CrossRef]
9. Wu, X.; Liang, J. A blockchain-based trust management method for Internet of Things. *Pervasive Mob. Comput.* **2021**, *72*, 101330. [CrossRef]
10. Samuel, O.; Javaid, N.; Khalid, A.; Imrarn, M.; Nasser, N. A trust management system for multi-agent system in smart grids using blockchain technology. In Proceedings of the GLOBECOM 2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6.
11. Tangade, S.; Manvi, S.S.; Lorenz, P. Trust management scheme based on hybrid cryptography for secure communications in VANETs. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5232–5243. [CrossRef]
12. Khalid, R.; Samuel, O.; Javaid, N.; Aldegheishem, A.; Shafiq, M.; Alrajeh, N. A secure trust method for multi-agent system in smart grids using blockchain. *IEEE Access* **2021**, *9*, 59848–59859. [CrossRef]
13. Javaid, U.; Aman, M.N.; Sikdar, B. A scalable protocol for driving trust management in internet of vehicles with blockchain. *IEEE Internet Things J.* **2020**, *7*, 11815–11829. [CrossRef]
14. Fang, W.; Xu, M.; Zhu, C.; Han, W.; Zhang, W.; Rodrigues, J.J. FETMS: Fast and efficient trust management scheme for information-centric networking in Internet of Things. *IEEE Access* **2019**, *7*, 13476–13485. [CrossRef]
15. Fang, W.; Zhang, W.; Shan, L.; Ji, X.; Jia, G. DDTMS: Dirichlet-distribution-based trust management scheme in Internet of Things. *Electronics* **2019**, *8*, 744. [CrossRef]
16. Zhao, Y.; Wang, Y.; Wang, P.; Yu, H. PBTM: A privacy-preserving announcement protocol with blockchain-based trust management for IoV. *IEEE Syst. J.* **2022**, *16*, 3422–3432. [CrossRef]
17. Zhang, C.; Li, W.; Luo, Y.; Hu, Y. AIT: An AI-enabled trust management system for vehicular networks using blockchain technology. *IEEE Internet Things J.* **2020**, *8*, 3157–3169. [CrossRef]
18. Junejo, A.K.; Komninos, N.; Sathiyanarayanan, M.; Chowdhry, B.S. Trustee: A trust management system for fog-enabled cyber physical systems. *IEEE Trans. Emerg. Top. Comput.* **2019**, *9*, 2030–2041. [CrossRef]
19. Wang, B.; Li, M.; Jin, X.; Guo, C. A reliable IoT edge computing trust management mechanism for smart cities. *IEEE Access* **2020**, *8*, 46373–46399. [CrossRef]
20. Awan, K.A.; Din, I.U.; Almogren, A.; Guizani, M.; Altameem, A.; Jadoon, S.U. Robusttrust—A pro-privacy robust distributed trust management mechanism for internet of things. *IEEE Access* **2019**, *7*, 62095–62106. [CrossRef]
21. Singh, S.; Chawla, M.; Prasad, D.; Anand, D.; Alharbi, A.; Alosaimi, W. An Improved Binomial Distribution-Based Trust Management Algorithm for Remote Patient Monitoring in WBANs. *Sustainability* **2022**, *14*, 2141. [CrossRef]
22. Chen, X.; Ding, J.; Lu, Z. A decentralized trust management system for intelligent transportation environments. *IEEE Trans. Intell. Transp. Syst.* **2020**, *23*, 558–571. [CrossRef]
23. Azad, M.A.; Bag, S.; Hao, F.; Shalaginov, A. Decentralized self-enforcing trust management system for social Internet of Things. *IEEE Internet Things J.* **2020**, *7*, 2690–2703. [CrossRef]
24. Salvio, G.; Gianfelice, C.; Firmani, F.; Lunetti, S.; Ferroni, R.; Balercia, G.; Giacchetti, G. Remote management of osteoporosis in the first wave of the COVID-19 pandemic. *Arch. Osteoporos.* **2022**, *17*, 1–9. [CrossRef] [PubMed]
25. Kucukaltan, B.; Kamasak, R.; Yalcinkaya, B.; Irani, Z. Investigating the themes in supply chain finance: The emergence of blockchain as a disruptive technology. *Int. J. Prod. Res.* **2022**, 1–20. [CrossRef]
26. Antonopoulos, N.; Exarchakos, G.; Li, M.; Liotta, A. (Eds.) *Handbook of Research on P2P and Grid Systems for Service-Oriented Computing: Models, Methodologies and Applications: Models, Methodologies and Applications*; IGI Global: United States of America by Information Science Reference: Hershey, PA, USA, 2010.
27. Vujicic, D.; Jagodic, D.; Randic, S. Blockchain technology, bitcoin, and Ethereum: A brief overview. In Proceedings of the 2018 17th International Symposium Infoteh-Jahorina (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 21–23 March 2018; pp. 1–6.
28. Zhao, K.; Tang, S.; Zhao, B.; Wu, Y. Dynamic and privacy-preserving reputation management for blockchain-based mobile crowdsensing. *IEEE Access* **2019**, *7*, 74694–74710. [CrossRef]
29. Xu, C.; Wang, K.; Li, P.; Guo, S.; Luo, J.; Ye, B.; Guo, M. Making big data open in edges: A resource-efficient blockchain-based approach. *IEEE Trans. Parallel Distrib. Syst.* **2018**, *30*, 870–882. [CrossRef]
30. Xu, X.; Zhu, D.; Yang, X.; Wang, S.; Qi, L.; Dou, W. Concurrent practical byzantine fault tolerance for integration of blockchain and supply chain. *ACM Trans. Internet Technol. (TOIT)* **2021**, *21*, 1–17. [CrossRef]
31. Wang, J.; Liu, Q.; Liang, H.; Joshi, G.; Poor, H.V. A novel framework for the analysis and design of heterogeneous federated learning. *IEEE Trans. Signal Process.* **2021**, *69*, 5234–5249. [CrossRef]
32. Samuel, O.; Omojo, A.B.; Onuja, A.M.; Sunday, Y.; Tiwari, P.; Gupta, D.; Shamshirband, S. IoMT: A COVID-19 Healthcare System driven by Federated Learning and Blockchain. *IEEE J. Biomed. Health Inform.* **2022**, 1–12. [CrossRef]
33. Wang, Y.; Zen, H.; Sabri, M.F.M.; Wang, X.; Kho, L.C. Towards Strengthening the Resilience of IoV Networks—A Trust Management Perspective. *Future Internet* **2022**, *14*, 202. [CrossRef]

34. Sun, Y.; Han, Z.; Liu, K.R. Defense of trust management vulnerabilities in distributed networks. *IEEE Commun. Mag.* **2008**, *46*, 112–119. [CrossRef]
35. Pu, C.; Choo, K.K.R. Lightweight Sybil attack detection in IoT based on bloom filter and physical unclonable function. *Comput. Secur.* **2022**, *113*, 102541. [CrossRef]
36. Wang, J.; Liu, Q.; Song, B. Blockchain-based multi-malicious double-spending attack blacklist management model. *J. Supercomput.* **2022**, *78*, 14726–14755. [CrossRef]
37. Chen, R.; Guo, J.; Bao, F. Trust management for SOA-based IoT and its application to service composition. *IEEE Trans. Serv. Comput.* **2014**, *9*, 482–495. [CrossRef]