Future Generation Computer Systems 154 (2024) 59–71

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Blockchain and trusted reputation assessment-based incentive mechanism for healthcare services

Yanhua Liu [a], Zhihuang Liu [b,*], Qiu Zhang [a], Jinshu Su [b], Zhiping Cai [b], Xiaoyan Li [a]

[a] *College of Computer and Data Science, Fuzhou University, Fuzhou, 350108, China*
[b] *College of Computer, National University of Defense Technology, Changsha, 410073, China*

ARTICLE INFO

Keywords:
Blockchain
Healthcare Internet of Things
Reputation assessment
Consensus mechanism
PBFT algorithm
Incentive mechanism

ABSTRACT

Blockchain-based healthcare IoT technology research enhances security for smart healthcare services such as real-time monitoring and remote disease diagnosis. To incentivize positive behavior among participants within a blockchain-based smart healthcare system, existing efforts employ benefit distribution and reputation assessment methods to enhance performance. Yet, there remains a significant gap in multidimensional assessment strategies and consensus improvements in addressing complex healthcare scenarios. In this paper, we propose a blockchain and trusted reputation assessment-based incentive mechanism for healthcare services (BtRaI). BtRaI provides a realistic and comprehensive reputation assessment with feedback to motivate blockchain consensus node participation, thus effectively defending against malicious behavior in the healthcare service system. Specifically, BtRaI first introduces multiple moderation factors for comprehensive multidimensional reputation assessment and credibly records the assessment results on the blockchain. Then, we propose an improved PBFT algorithm, grounded in the reputation assessment, to augment blockchain consensus efficiency. Finally, BtRaI designs a token-based reward and punishment mechanism to motivate honest participation in the blockchain, inhibit potential misbehavior, and promote enhanced service quality in the healthcare system. Theoretical analysis and simulation experiments conducted across various scenarios demonstrate that BtRaI effectively suppresses malicious attacks in healthcare services, improves blockchain node fault tolerance rates, and achieves blockchain transaction processing efficiency within 0.5 s in a 100-node consortium chain. BtRaI's reputation assessment and token incentive mechanism, characterized by realistic differentiation granularity and change curves, are well-suited for dynamic and complex healthcare service environments.

1. Introduction

The Healthcare Internet of Things (H-IoT), emerging from the rapidly evolving Internet of Things technology and the era of personalized digital health, significantly facilitates people's lives. H-IoT has the capability to enhance disease monitoring, improve the quality of diagnosis and treatment, and reduce healthcare costs [1,2]. However, H-IoT faces troubling security and privacy issues due to the sensitivity of patient medical data [3,4]. Information breaches and data tampering resulting from improper management or malicious attacks during the sharing, transmission, and remote access of patient medical data frequently occur [5]. Therefore, ensuring the security and privacy of medical data has become a significant challenge for the modern healthcare industry [6,7].

Recently, research on tamper-proof and traceable healthcare IoT security technology combined with blockchain technology has become an emerging trend [8,9]. Researchers are continuously exploring to promote the application and development of blockchain-based IoT security technologies in healthcare. This includes enhancing the privacy of shared healthcare data [10–13] and improving the reliability of smart healthcare devices [14,15]. These efforts demonstrate the immense potential of blockchain technology in enhancing the security and reliability of H-IoT services, thereby contributing to the evolution of the blockchain-based smart healthcare system [16].

Although the introduction of blockchain systems provides data tampering resistance and privacy enhancement for H-IoT, the issues of collaboration and incentive among distributed entities have emerged as potential threats. Blockchain-based smart healthcare systems depend on the active collaboration and participation of distributed entities for the smooth and regular operation. However, in practice, the system

[*] Corresponding author.
E-mail addresses: lyhwa@fzu.edu.cn (Y. Liu), lzhliu@nudt.edu.cn (Z. Liu), 221027129@fzu.edu.cn (Q. Zhang), sjs@nudt.edu.cn (J. Su), zpcai@nudt.edu.cn (Z. Cai), xyli@fzu.edu.cn (X. Li).

https://doi.org/10.1016/j.future.2023.12.023
Received 21 June 2023; Received in revised form 20 December 2023; Accepted 21 December 2023
Available online 24 December 2023

performance is often challenged by the dynamically changing environment and unpredictable entity behavior [17]. For instance, malicious patient behavior could lead to wasteful utilization of remote healthcare resources, healthcare institutions might deliver low-quality medical services, and blockchain nodes could exhibit passive participation in system maintenance.

Effective incentives are an important way to prevent malicious services and system performance degradation. Through rewards and penalties, incentive mechanisms promote the provision of high-quality services by all participants, reduce the risk of data leakage and tampering, and prevent malicious competition and misuse of resources [18]. The sharing of medical data and the provision of healthcare services in the blockchain-based smart healthcare system are primarily driven by stakeholder interests and efficiency gains [19].

Existing incentive mechanisms partly focus on encouraging patients to proactively share medical data, ensuring the effective utilization of medical data [20,21]. However, these mechanisms do not address the issue of malicious attacks in distributed systems. Additional efforts have been made in multi-party collaboration platforms to consider the allocation of benefits among participants. For example, token rewards incentivize participants to enhance service quality and data reliability [19,22,23]. Furthermore, establishing a behavioral evaluation system that considers participants' historical behavior can create a dynamic reputation score. Service providers can be selected or rewarded based on their scores [24]. However, in practice, incentive mechanisms can be further enhanced to punish malicious behavior, ensure service quality, and promote the stable operation of the system. These enhancements have been widely applied and validated in other IoT domains [25–27].

Based on the aforementioned observations, with the increasing complexity and scale of application scenarios in blockchain-based smart healthcare systems, the main challenges in adequately utilizing the incentive mechanism are as follows:

- Existing research on incentive mechanisms in blockchain-based smart healthcare systems throughout the healthcare process has limitations in promoting reliable data sharing, on-chain transactions, and consensus mechanisms.
- The absence of a comprehensive, multidimensional approach in reputation assessment, crucial for incentive mechanism design, can undermine system fairness and reduce participants' motivation.
- Research is limited on how incentive mechanisms and blockchain efficiency mutually reinforce each other. The lack of improvements in consensus mechanisms leads to poor integration of reputation assessment with the blockchain system, which in turn reduces the motivation for user participation in consensus process [28].

Hence, in this paper, we propose a **B**lockchain and **t**rusted **R**eputation **a**ssessment-based **I**ncentive mechanism for healthcare services (BtRaI). It addresses the trusted reputation assessment challenge, which involves multiple entities and dimensions. Furthermore, BtRaI designs a reputation-based consensus algorithm and a token incentive mechanism. The contributions of this paper can be summarized as follows:

(1) We propose a comprehensive and credible reputation assessment method. Multifactor moderation and multidimensional assessment are used to suppress malicious or collusive scoring attacks, and reputation-based token rewards and penalties are designed to motivate service quality improvement.
(2) We design a consensus mechanism characterized by high fault tolerance and efficiency. Leveraging reputation assessment results, this mechanism dynamically interchange consensus nodes and validation nodes. It thus defends against both faulty and malicious nodes while encouraging positive behavior through incentive mechanisms.
(3) We validate the effectiveness of BtRaI through simulation experiments across various scenarios. BtRaI demonstrates comprehensive reputation assessment capabilities against attack interference and malicious behavior. The improved consensus algorithm significantly outperforms PBFT in efficiency. BtRaI can be effectively applied to healthcare service incentives in dynamic and complex scenarios.

The rest of this paper is organized as follows. Section 2 introduces the related work. In Section 3, we present the system model and design goals. In Section 4, we describe in detail the proposed BtRaI. We present the security and theoretical analysis of BtRaI in Section 5 and evaluate BtRaI in Section 6. Finally, a conclusion is drawn in Section 7.

2. Related work

In the service field, incentive mechanisms can motivate all parties to complete system tasks, guarantee the security of the service transaction process, and promote the quality of services [29]. The introduction of incentive mechanisms in blockchain-based service systems can enhance the motivation of nodes to participate in processes such as block validation and data sharing. This approach not only avoids the security risks associated with trusted third parties but also helps prevent issues such as trust deficits and privacy leakage, thereby further guaranteeing service quality [17,27]. Wang et al. [25] designed a smart contract-based incentive mechanism in a consortium chain-based vehicular edge computing system, which motivates vehicles to share computing resources with service requesters and prevents malicious behavior for selfish purposes. Noshad et al. [27] proposed a decentralized incentive and reputation mechanism for crowdsensing networks. Monetary rewards are employed to incentivize data collectors and encourage participation in network activities. Meanwhile, the reputation system addresses issues including data integrity, fake reviews, and conflicts among entities.

Similarly, trustworthy incentives for blockchain-based healthcare services can help promote regular operations and quality improvement. Gan et al. [21] designed an incentive mechanism in a blockchain-based e-health system, providing rewards to patients for sharing medical data, with the rewards contingent on data quality and the level of patient engagement. Zhu et al. [19] proposed a Shapley value-based scheme to incentivize collaboration in medical data sharing on the blockchain. This approach encourages participants to actively engage in cooperation by providing a mechanism for fair benefit distribution. Similarly, other works such as [22] and [23] also utilize benefit allocation as an incentive mechanism. Shen et al. [22] designed a blockchain-based Shapley value scheme to encourage data owners to share reliable data. Litchfield et al. [23] described incentives through token rewards in a blockchain-based healthcare service system. It is aimed at encouraging and engaging patients to participate in and use prescription management systems and mitigating the negative effects of inequality in healthcare services. There are also efforts to design incentives based on reputational assessments. Purohit et al. [24] proposed a health information-sharing system based on blockchain technology called HonestChain. HonestChain rates and determines the reputation of medical data requesters and providers based on their respective historical feedback and risk levels. Using these reputation results, it assesses the responsiveness to service requests and the likelihood of service provision, fostering incentive-driven and trust-based collaboration among organizations.

However, further exploration is needed to delve into the design of incentive mechanisms, particularly in the design of multidimensional reputation assessment and the improvement of blockchain consensus mechanisms, to enhance the efficiency and reliability of blockchain-based smart healthcare systems.

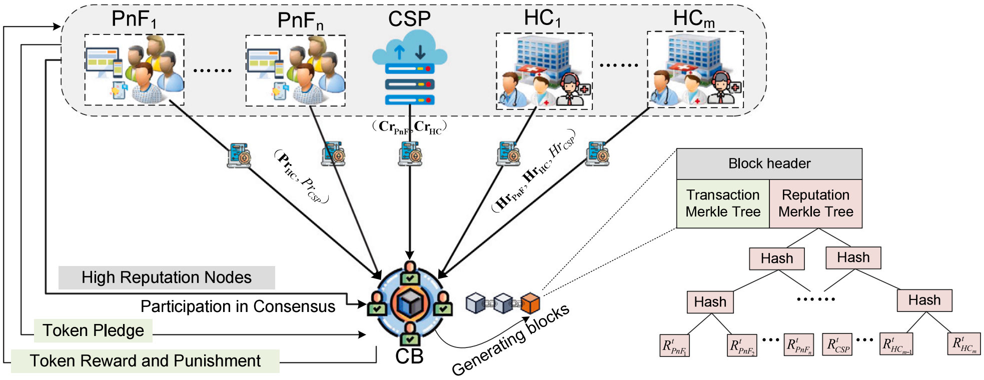


Fig. 1. System model.

3. System model and design goal

3.1. System model

The system model shown in Fig. 1 consists of PnF (Patient and patient's Family), HC (Healthcare Center), CSP (Cloud Service Platform), and CB (Consortium Blockchain), with the specific roles and functions of each entity described below:

(1) PnF, comprising patients and their family members, can proactively request a medical visit by sharing an EHR (Electronic Health Record) and submitting its summary to the blockchain for deposition. Also, PnF receives smart health diagnostics and healthcare education from HC while providing feedback and fee payments through smart contracts on CB.
(2) HC is responsible for providing diagnosis and education services to PnFs. HC initiates EHR access requests for PnFs from the CSP and uploads the updated diagnosis and education content to the CSP for storage. Additionally, HC publishes summary information, including hash value and service cost, on the blockchain for deposition.
(3) The CSP serves as a data storage platform with high capacity and performance, providing search functions and transmitting encrypted information to authorized entities. Additionally, it synchronously logs access to encrypted data on the consortium chain.
(4) CB, a permissioned blockchain, enables PnF and HC to securely share data in a trusted environment through a strict review and access mechanism. Smart contracts, deployed on CB, facilitate entity interactions. CB stores only lightweight data, ensuring tamper-proof and traceable capabilities.

The workflow of the BtRaI system model is described as follows:

(1) After receiving healthcare services from HCs, PnFs send $(\mathbf{Pr}_{\mathbf{HC}}, Pr_{CSP})$ to the consortium chain CB for feedback assessment via smart contract function, including the score matrix $\mathbf{Pr}_{\mathbf{HC}}$ for all HCs and the score Pr_{CSP} for CSPs. Similarly, CSPs compute the score $(\mathbf{Cr}_{\mathbf{PnF}}, \mathbf{Cr}_{\mathbf{HC}})$ for all PnFs and all HCs on the chain, and HCs compute the score $(\mathbf{Hr}_{\mathbf{PnF}}, \mathbf{Hr}_{\mathbf{HC}}, Hr_{CSP})$ for all PnFs, other peer HCs and CSPs on the chain.
(2) Based on the historical reputation of PnFs, CSPs, and HCs, as well as current ratings in various aspects, the smart contract on the CB calculates the comprehensive reputation of each entity at the present time. This information is accessible to the nodes participating in the CB.
(3) Nodes with higher reputations are eligible to participate directly in the consensus process of the blockchain, generating blocks containing transactions and reputation assessment results in each time period. The comprehensive reputation results of each node are recorded in the block using a Merkle tree structure.
(4) Throughout the healthcare service system, internode interactions, transaction requests, and smart contracts usage necessitate token pledges. A token-based reward and punishment mechanism encourages honest participation and active engagement in the blockchain's consensus process among nodes.

3.2. Threat model

Based on the system model described in Fig. 1, the following types of attacks may exist:

(1) False reputation assessment attacks: Providing unrealistic (low or high) ratings to an entity in an attempt to devalue or inflate its comprehensive reputation, which in turn disrupts the system's consensus and incentive mechanisms. These attacks may involve collusion among entities that exchange higher ratings while unfairly assigning low ratings to others.
(2) Short-term honest service attacks: To achieve higher reputational ratings and greater consensus opportunities, some entities attempt to achieve high long-term reputations and rewards by temporarily improving their healthcare performance.
(3) Temporary malicious attacks: Although some entities consistently maintain good performance and a high reputation over time, they may later engage in malicious healthcare service practices, using their previously established honesty to deflect scrutiny of their temporary misconduct.
(4) Byzantine attacks [30,31]: During block consensus, some nodes may encounter failures or exhibit malicious behavior by providing incorrect consensus or validation results, with the aim of deliberately undermining the efficiency and integrity of the consensus process.

3.3. Design goal

Based on the system model and threat model described above, the designed scheme should satisfy the following goals:

(1) Defending against malicious assessments and collusion attacks [32]: With the majority of nodes being honest, malicious assessments, including those from colluding nodes, should receive a correspondingly lower weighting in the final comprehensive reputation assessment to minimize their influence on the results.
(2) Trusted and practical reputation assessment: The reputation of each node is recorded in a trusted and fault-tolerant blockchain environment. The reputation accumulation mechanism is tailored for practical applications, where reputation increases gradually with good behavior but declines rapidly with malicious behavior.

(3) Effective differentiation in reward and punishment mechanisms: Assessment results should distinctly categorize nodes based on reputation levels, offering varied token rewards accordingly. The adopted reward and punishment mechanism should widen the gap in reputation and token rewards between constructive and malicious behavior.

(4) Resilience against other attacks: BtRaI should be capable of withstanding common attacks, including external and internal forgery, replay, repudiation, DDoS, and 51% attacks.

4. The proposed BtRaI

BtRaI first proposes a multidimensional reputation assessment method with multifactor moderation to measure the reputation of each entity more comprehensively and stably. Subsequently, an improved PBFT algorithm is proposed, which leverages the reputation assessment to enhance the efficiency of the consensus process. Finally, BtRaI encourages honest completion of blockchain maintenance tasks honestly through token rewards and penalties, thereby enhancing service quality among all involved parties.

4.1. Multidimensional comprehensive reputation assessment with multifactor moderation

The assessment method is based on the principle that reputation values are not easily accumulated but quickly degraded by malicious behavior, as a way to discourage malicious behavior of legitimate users in the system [33]. Reputation calculations are dynamically updated at regular intervals or upon reaching a threshold number of assessments, triggering an automatic update of the comprehensive reputation.

Let $PnF = \{PnF_1, PnF_2, PnF_3, \dots, PnF_n\}$ denote the set of PnFs, and $HC = \{HC_1, HC_2, HC_3, \dots, HC_m\}$ denote the set of HC. The comprehensive reputation scores of HC, PnF, and CSP are denoted by R_{HC}, R_{PnF}, and R_{CSP}, respectively. At time $t+1$, let $R^{t+1}_{HC_k}$, $R^{t+1}_{PnF_k}$, and $R^{t+1}_{CSP_k}$ denote the comprehensive reputation scores of the kth HC, PnF, and CSP, respectively. The reputation calculation processes for HC, PnF, and CSP are described below.

4.1.1. HC comprehensive reputation calculation

The factors affecting the comprehensive reputation of HC_k at the moment $t+1$ include:

(1) The historical reputation of HC $R^t_{HC_k}$. Scores initialized at the $t = 0$ moment for hospital rank, equipment resources, and proficiency in diseases that are given at registration after CB administrator verification.

(2) Assessment from PnFs. The direct reputation assessment from PnF_i, denoted as Pr_{ik}, considers indicators including the speed of response, satisfaction levels with diagnosis and education, and the extent of EHR tampering and data leakage. Pr^τ_{ik} is calculated as

$$Pr^\tau_{ik} = \frac{Q^\tau_{ik}}{\lambda^\tau_{ik}(Tam^\tau_{ik} + Le^\tau_{ik} + 1)}, \tag{1}$$

where $\tau = t+1$ only when the corresponding score has an update at the $t+1$ moment, otherwise $\tau = t$. The service quality, denoted by Q^τ_{ik}, includes PnF_i's satisfaction with diagnosis and education. Tam^τ_{ik} represents the degree of EHR tampering, and Le^τ_{ik} indicates the extent of data leakage in EHR_{ik}. If Tam^τ_{ik} and Le^τ_{ik} are not equal to 0, the CB administrator is responsible for verifying the correlation between the tampering or leakage and HC_k, and the penalty factor λ^τ_{ik} is assigned accordingly. There are uniform range criteria for Q^τ_{ik}, Tam^τ_{ik}, Le^τ_{ik}, and λ^τ_{ik} among different PnFs.

If there is no direct interaction between PnF_i and HC_k at $t+1$ moment, then $Pr^\tau_{ik} = Pr^{t+1}_{ik} = Pr^t_{ik}$, which means that the interaction assessment at the previous moment is used as the score at $t+1$ moment; if there has been no direct interaction between PnF_i and HC_k, then $Pr^\tau_{ik} = 0$. To mitigate malicious assessments from PnF, it is essential to compute the credibility of PnF's assessment, denoted as Pcr^τ_{ik}. Pcr^τ_{ik} is calculated as shown in Eq. (2), which represents the validity of the score Pr^τ_{ik} given by PnF_i within the context of all PnFs' assessments of HC_k.

$$Pcr^\tau_{ik} = 1 - \sqrt{\left(Pr^\tau_{ik} - \frac{\sum_{j=1}^{n'} Pr^\tau_{jk}}{n'}\right)^2}, \tag{2}$$

where n' represents the number of Pr^τ_{ik} with non-zero assessment values. Finally, the reputation assessments of all PnFs on HC_k at the moment $t+1$ are denoted by $PR^\tau_{HC_k}$, as shown in Eq. (3).

$$PR^\tau_{HC_k} = \left(\sum_{i=1}^{n'} Pcr^\tau_{ik} \times Pr^\tau_{ik}\right)/n', \tag{3}$$

(3) Assessment from peer HCs. Similar to the calculation of PnFs' reputation assessment of HCs, the reputation assessment $HR^\tau_{HC_k}$ of the remaining HCs on HC_k is calculated as

$$\begin{aligned} HR^\tau_{HC_k} &= \left(\sum_{i=1, i\neq k}^{m-1} Hcr^\tau_{ik} \times Hr^\tau_{ik}\right)/m-1, \\ Hcr^\tau_{ik} &= 1 - \sqrt{\left(Hr^\tau_{ik} - \frac{\sum_{j=1, j\neq k}^{m-1} Hr^\tau_{jk}}{m-1}\right)^2}, \end{aligned} \tag{4}$$

where $Hr^\tau_{ik} (i \neq k)$ denotes the peer reputation assessment of HC_i on HC_k, which is not 0 by default and takes values in the range $(0, 1]$. Hcr^τ_{ik} denotes the assessment credibility, which refers to the credibility of Hr^τ_{ik} in the context of all HC assessments of HC_k.

(4) Assessment from CSP. The reputation assessment of CSP on HC_k, denoted as $CR^\tau_{HC_k}$, is calculated as $CR^\tau_{HC_k} = R^t_{CSP} \times Cr^\tau_k$. Here, Cr^τ_{ik} denotes the direct reputation assessment of HC_k by the CSP, based on interaction performance, with values in the range $(0, 1]$. The comprehensive reputation of the sole CSP in the system, R^t_{CSP}, is used as the credibility factor in this calculation.

(5) Historical maintenance on the consortium chain. Let $BR^\tau_{HC_k}$ denote the maintenance score of HC_k on the consortium chain. This score is influenced by various factors, including the number of correctly generated consensus blocks $acnum^\tau_k$, the average block generation speed $\bar{f}^\tau_k$ (with larger values indicating faster speed on a scale of 1–5), the number of correctly validated blocks $acval^\tau_k$, the number of incorrectly generated consensus blocks $wrnum^\tau_k$, and the number of incorrectly validated blocks $wrval^\tau_k$. The $BR^\tau_{HC_k}$ is calculated as

$$\begin{aligned} Beh^\tau_{HC_k} &= \frac{acnum^\tau_i \times \bar{f}^\tau_i + acval^\tau_i}{wrnum^\tau_i + wrval^\tau_i + 1}, \\ BR^\tau_{HC_k} &= \frac{1}{1 + e^{-\omega \times Beh^\tau_{HC_k}}}. \end{aligned} \tag{5}$$

By utilizing the sigmoid function $f(x) = 1/(1 + e^{-x})$, each $BR^\tau_{HC_k}$ is confined to the interval $[0.5, 1)$, where ω is referred to as the gap modifier. Thus, we obtain the HC comprehensive reputation $R^{t+1}_{HC_k}$ at $t+1$ moments calculated as

$$R^{t+1}_{HC_k} = (1-\gamma)R^t_{HC_k} + \gamma(\alpha_1 PR^\tau_{HC_k} + \alpha_2 HR^\tau_{HC_k} + \alpha_3 CR^\tau_{HC_k} + \alpha_4 BR^\tau_{HC_k}). \tag{6}$$

Here, $\gamma \in (0, 1)$ denotes the learning rate factor. α_1, α_2, α_3, and α_4 represent the weight percentages of PnF, HC, CSP assessment, and performance on consortium chain maintenance, respectively. Moreover, these weights must sum up to 1 ($\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 1$).

Furthermore, we adjust the value of the γ parameter based on the relationship between the historical reputation $R^t_{HC_k}$ and the current performance score, which is a weighted sum of four factors: $\alpha_1 PR^\tau_{HC_k} + \alpha_2 HR^\tau_{HC_k} + \alpha_3 CR^\tau_{HC_k} + \alpha_4 BR^\tau_{HC_k}$. If the historical reputation exceeds the current performance score, we set $\gamma = \gamma_1$. If it is lower, $\gamma = \gamma_2$, where $0 < \gamma_2 < \gamma_1 < 1$. This asymmetric approach to reputation calculation ensures that only long-term good behavior can gradually increase reputation, whereas malicious behavior result in more significant reputation damage, deterring potential malicious activities.

4.1.2. PnF comprehensive reputation calculation

Similar to the comprehensive reputation calculation of HC, the comprehensive reputation of PnF_k incorporates several factors: the historical reputation $R^t_{PnF_k}$, assessment from HC ($HR^\tau_{PnF_k}$), assessment from CSP ($CR^\tau_{PnF_k}$), along with performance scores in the consortium chain ($BR^\tau_{PnF_k}$). R_{PnF_k} is initialized at $t = 0$ as a score reflects PnF_k's size, average age, and average equipment resources. $R^{t+1}_{PnF_k}$ is calculated as

$$R^{t+1}_{PnF_k} = (1-\gamma)R^t_{PnF_k} + \gamma(\beta_1 HR^\tau_{PnF_k} + \beta_2 CR^\tau_{PnF_k} + \beta_3 BR^\tau_{PnF_k}), \tag{7}$$

where $\beta_1 + \beta_2 + \beta_3 = 1$. A penalty factor η^τ_{ik} is introduced in the calculation of $HR^\tau_{PnF_k}$, and when $\eta^\tau_{ik} > 1$ indicates that PnF_k has wasted HC_i medical resources or made invalid requests, as shown in Eq. (8).

$$\begin{aligned} HR^\tau_{PnF_k} &= \Big(\sum_{i=1}^{m'} Hcr^\tau_{ik} \times \frac{Hr^\tau_{ik}}{\eta^\tau_{ik}}\Big)/m', \\ Hcr^\tau_{ik} &= 1 - \sqrt{\Big(Hr^\tau_{ik} - \frac{\sum_{j=1}^{m'} Hr^\tau_{jk}}{m'}\Big)^2}, \end{aligned} \tag{8}$$

where Hr^τ_{ik} takes values in the range $[0, 1]$. Hr^τ_{ik} is equal to the score of the previous moment if there is no healthcare interaction at the current moment, and $Hr^\tau_{ik} = 0$ if there is never a healthcare relationship. m' represents the count of non-zero Pr^τ_{ik} assessment values.

4.1.3. CSP comprehensive reputation calculation

The comprehensive reputation of CSP_k is determined by several factors: its historical reputation $R^t_{CSP_k}$, assessment from PnF ($PR^\tau_{CSP_k}$) and HC ($HR^\tau_{CSP_k}$), and its performance scores in the consortium chain ($BR^\tau_{CSP_k}$). R_{CSP_k} is initialized at $t = 0$ as a score reflects CSP_k's resources, computing power, and performance in other services. R_{CSP_k} is calculated as

$$R^{t+1}_{CSP_k} = (1-\gamma)R^t_{CSP_k} + \gamma(\delta_1 PR^\tau_{CSP_k} + \delta_2 HR^\tau_{CSP_k} + \delta_3 BR^\tau_{CSP_k}),$$

$$\begin{aligned} PR^\tau_{CSP_k} &= \Big(\sum_{i=1}^{n} Pcr^\tau_{ik} \times Pr^\tau_{ik}\Big)/n, \\ Pcr^\tau_{ik} &= 1 - \sqrt{\Big(Pr^\tau_{ik} - \frac{\sum_{j=1}^{n} Pr^\tau_{jk}}{n}\Big)^2}, \\ HR^\tau_{CSP_k} &= \Big(\sum_{i=1}^{m} Hcr^\tau_{ik} \times Hr^\tau_{ik}\Big)/m, \\ Hcr^\tau_{ik} &= 1 - \sqrt{\Big(Hr^\tau_{ik} - \frac{\sum_{j=1}^{m} Hr^\tau_{jk}}{m}\Big)^2}, \end{aligned} \tag{9}$$

where $\delta_1 + \delta_2 + \delta_3 = 1$, and because every entity interacts with the CSP, Pr^τ_{ik} and Hr^τ_{ik} are usually non-zero. In the absence of current interactions, the score from the previous time step is used.

Throughout the healthcare service process, each entity's comprehensive reputation score is included as one of its attributes. For instance, when a PnF visits a doctor, a HC with a comprehensive reputation score of at least 0.9 can be specified as a condition. An entity falling below a specific comprehensive reputation score threshold will be excluded from the consortium chain. To rejoin, it must undergo a rigorous audit and re-registration process, administered by the CB administrator. Notably, a CSP is typically an entity with high credibility [34]. A continuous decrease or failure of reputation may lead to a change in the CSP service source, subject to audit confirmation.

4.2. Reputation-based RPBFT consensus

PBFT (Practical Byzantine Fault Tolerance) is a fault-tolerant and resilient consensus algorithm [35], employed in permissioned blockchains to reduce computational overhead and increase transaction throughput [36]. The basic flow of PBFT consensus is shown in Fig. 2, where the number of non-functional faulty or malicious nodes in the consensus nodes is f (node 3 is faulty in this example).

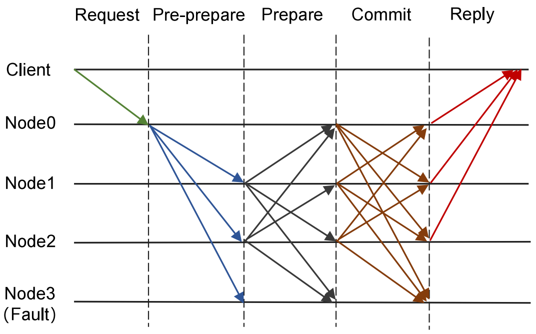


Fig. 2. PBFT consensus process.

PBFT is divided into the following five phases:

1. Request phase: The client submits a transaction request to the master node (node 0 at the current moment).
2. Pre-prepare phase: Master node 0 broadcasts a signature packet containing a summary of the request message to other consensus nodes in the network.
3. Prepare phase: Node 1 and node 2, functioning properly, verify the signature packet from master node 0. Upon validation, they cache the packets of the Pre-prepare message and broadcast their Prepare signature packets. They also verify and cache Prepare signature packets received from other nodes. If the node caches $2f+1$ signature packets (its own included) within the designated timeframe, it moves to the next phase.
4. Commit phase: After completing the Prepare phase, a normal node broadcasts its Commit packets and then verifies and caches Commit packets from other nodes. If the node collects at least $2f + 1$ Commit packets within a specified timeframe (its own included), it proceeds to execute the request and records the associated blocks in the database.
5. Reply phase: After the above processing, the node will reply to the client. Consensus is completed when the client collects $f+1$ valid messages from different nodes.

In a system containing f faulty or malicious nodes, when the total number of network nodes N exceeds $3f$ (i.e., $N \geq 3f + 1$), the normal operation of the distributed system can be guaranteed. This condition means that the maximum fault-tolerant number of PBFT is $(N - 1)/3$.

The algorithmic complexity of PBFT is $O(N^2)$. PBFT may suffer from performance issues, like significant network communication overhead, when handling many nodes and transactions, owing to the extensive communications and confirmations required [31]. To address these issues, in BtRaI, we propose a PBFT consensus mechanism based on the comprehensive reputation assessment, called RPBFT. The improved consensus mechanism is illustrated in Fig. 3.

The specific process of RPBFT is described as follows:

1. Determine the node numbers of all consortium chain participating entities: Sort the $NodeID$ of each consensus node from 0 to $N - 1$. This sorting is based on the descending order of each entity's comprehensive reputation. N is defined as $n + m + 1$, representing the total number of nodes, where n is the number of PnFs and m is the number of HCs.
2. Divide consensus committee nodes and validation nodes: Nodes with number indexes from 0 to c_num-1 are selected as consensus committee nodes, and nodes with number indexes from c_num to $N - 1$ are selected as validation nodes.

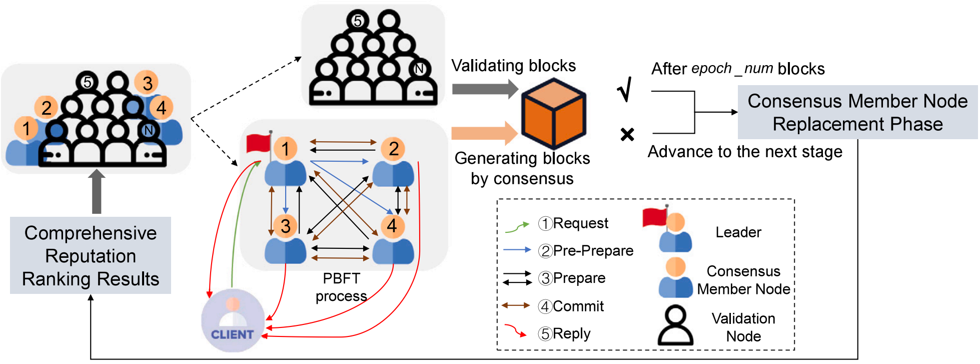


Fig. 3. RPBFT consensus mechanism based on reputation assessment.

(3) Block consensus and block validation: Consensus committee nodes use the PBFT algorithm for consensus, where the node with the highest reputation acts as the Leader and is responsible for packing transactions into blocks. Block generation authority rotates among these nodes based on reputation rank. The consensus committee node will participate in the consensus process of $epoch\_num$ blocks. Validation nodes retrieve, verify, and decide on the acceptance of new blocks. If a majority of validation nodes (exceeding the number of consensus committee nodes) reject a block, all consensus committee nodes suffer a collective reputation penalty of ϕ. Subsequently, the node replacement phase begins in advance, and the consensus process will be repeated.

(4) Consensus committee node replacement: After the consensus of $epoch\_num$ blocks, $NodeID$ will be re-ranked according to the comprehensive reputation to determine a new index, and then step (2) will be repeated. To prevent malicious groups or collusion attacks, if the new consensus committee nodes include more than $\lceil (c\_num - 1)/2 \rceil$ nodes from the previous round, the $\lceil (c\_num - 1)/2 \rceil$ nodes with the highest indices among them are replaced by $\lceil (c\_num - 1)/2 \rceil$ nodes with lower indices from the validation nodes. Then repeat step (3).

Since the calculation of the comprehensive reputation score is dynamically updated, the reputation-based RPBFT consensus committee nodes and validation nodes are also dynamically updated and have reputation-based trustworthiness guarantees. Combined with the incentive mechanism described in the next subsection, active and honest participation in the consortium chain is rewarded: HCs receive high reputation and tokens for EHR data requests; PnFs gains tokens for diagnostic and educational resources; the CSP earns token rewards and opportunities to provide services.

4.3. Reputation-based incentives

In the BtRaI system, based on the comprehensive reputation assessment, tokens (called CareCoin) are issued, paid, and rewarded as incentives. CareCoin is relevant to the interests of the entity and can be used to attract consensus participants and validators, thereby facilitating the operation of the consensus mechanism. The incentive mechanisms in each phase are outlined below:

(1) Initialization: CareCoin is issued for each registered entity based on their initial comprehensive reputation at the time of registration. If the Rp value falls below 0.6, the entity must undergo a review process for re-registration to regain CareCoin.

(2) Consensus reward and punishment: For the nodes participating in consensus, the CareCoin gain U_M obtained by generating correct blocks and invalid blocks is calculated by Eq. (10).

$$U_M = \begin{cases} \dfrac{Rp \times Rw_M}{1/(1+e^{T_s - T_f})} - \dfrac{K}{2Rp}, & \text{If the block is valid;} \\ -\ K, & \text{If the block is invalid.} \end{cases} \tag{10}$$

For the nodes involved in validation, the CareCoin gains U_V that generate correct and invalid validation are calculated by Eq. (11).

$$U_V = \begin{cases} \dfrac{Rp \times Rw_V}{1/(1+e^{T_s - T_f})} - \dfrac{V}{3Rp}, & \text{If the validation is valid;} \\ -\ V, & \text{If the validation is invalid.} \end{cases} \tag{11}$$

where Rp represents the entity's comprehensive reputation value calculated based on Section 4.1. Rw_M, Rw_V are the base values of the revenue earned by consensus committee nodes and validation nodes through contribution allocation, respectively. T_f and T_s represent the time of generating the transaction request and block confirmation, respectively. K and V are the CareCoin pledged by the bookkeeper (i.e., consensus committee node) and validator, respectively. It can be seen that the revenue of a participant in a consortium chain is closely related to its comprehensive reputation value. Additionally, after mapping via the sigmoid function, $T_f - T_s$ falls within the $(0.5, 1)$ interval. In this context, a smaller value results in a higher gain. This promotes faster block consensus and validation, reducing transaction time. Regarding maintenance costs, coefficients $K/2Rp$ and $V/3Rp$ mean that higher reputation leads to lower CareCoin pledges, and consensus participation costs more than validation.

5. Security and theoretical analysis

This section provides a security and theoretical analysis of the proposed BtRaI based on the threat model and design goals. We also compare BaRaI with related work. The details are analyzed below.

(1) Defending against false reputation assessment attacks

In the case of false assessment attacks, including collusion attacks, the impact of these false evaluations is mitigated by introducing a credibility factor into the evaluators' assessment process.

Taking the reputation assessment process of HC by PnF as an example, the credibility factor calculation $Pcr_{ik}^{\tau} = 1 - \sqrt{(Pr_{ik}^{\tau} - (\sum_{j=1}^{n'} Pr_{jk}^{\tau})/n')^2}$ in Eq. (2) reveals that a rating's credibility degree Pcr_{jk}^{τ} inversely relates to how much it deviates from the average rating. Therefore, for a given evaluated entity, if the majority of evaluators are honest and their scores are consistent, any false rating significantly deviating from reality will have reduced credibility. According to $PR_{HC_k}^{\tau} = (\sum_{i=1}^{n'} Pcr_{ik}^{\tau} \times Pr_{ik}^{\tau})/n'$ in Eq. (3), it can be inferred that false scores have lower weight in the final reputation assessment calculation.

Additionally, when a specific type of entity is infiltrated with false assessments, dishonesty can be mitigated by employing multidimensional constraints and adjusting the score weight for that entity. For example, when calculating HC reputation $R_{HC_k}^{t+1} = (1-\gamma)R_{HC_k}^{t} + \gamma(\alpha_1 PR_{HC_k}^{\tau} + \alpha_2 HR_{HC_k}^{\tau} + \alpha_3 CR_{HC_k}^{\tau} + \alpha_4 BR_{HC_k}^{\tau})$, some PnFs may assign scores that inaccurately represent the actual situation. To mitigate the influence of false assessments, BtRaI employs a multidimensional

Table 1
Comparative analysis of BtRaI with existing related work.

Scheme	Chain type	Reputation assessment	Consensus improvement	Incentive method
[21]	Private chain	×	×	Bonus rewards
[19]	Consortium chain	×	×	Revenue distribution
[22]	Consortium chain	×	×	Revenue distribution
[23]	Public chain	×	×	Token rewards
[24]	Consortium chain	Single dimensional	×	Reputation assessment + Service delivery rate
BtRaI	Consortium chain	Multidimensional	✓	Reputation assessment + Token reward and punishment

reputation calculation mechanism, integrating the HC's historical reputation, assessments from other HCs and the CSP, and consortium chain maintenance scores. Moreover, the score weight assigned to the PnF group (i.e., α_1) in the final comprehensive reputation calculation can be correspondingly reduced.

Therefore, BtRaI achieves robustness in the assessment process through multifactor moderation and multidimensional constraints. Consequently, malicious assessments, including collusion attacks, are suppressed. Hence, the first design goal is fulfilled.

(2) Defending against short-term honest service attacks and temporary malicious attacks

Robustness against short-term honest service attacks and temporary malicious attacks is achieved by measuring historical reputation impact and employing an adaptively varying reputation learning factor γ.

Specifically, the reputation learning factor γ determines how much the new reputation value will affect the historical reputation. Taking the HC comprehensive reputation calculation at the moment $t+1$ as an example, i.e., $R^{t+1}_{HC_k} = (1-\gamma)R^{t}_{HC_k} + \gamma(\alpha_1 PR^{\tau}_{HC_k} + \alpha_2 HR^{\tau}_{HC_k} + \alpha_3 CR^{\tau}_{HC_k} + \alpha_4 BR^{\tau}_{HC_k})$ in Eq. (6). Let the comprehensive score of the current performance obtained at the moment $t+1$ be $RC^{t+1}_{HC_k} = \alpha_1 PR^{\tau}_{HC_k} + \alpha_2 HR^{\tau}_{HC_k} + \alpha_3 CR^{\tau}_{HC_k} + \alpha_4 BR^{\tau}_{HC_k}$. Therefore, $R^{t+1}_{HC_k} = (1-\gamma)R^{t}_{HC_k} + \gamma RC^{t+1}_{HC_k}$. When γ approaches 0, it indicates that reputation assessment results found from the current moment will be disregarded; when γ approaches 1, it indicates that reputation assessment results derived from historical experience will be disregarded.

In BtRaI, the learning rate γ dynamically adjusts. It decreases when the current reputation $RC^{t+1}_{HC_k}$ exceeds the historical reputation $R^{t}_{HC_k}$, thereby moderating the pace of reputation improvement to discourage attackers from boosting their long-term reputation through short-term honest behavior. Conversely, if the current reputation falls below the historical level, γ increases, hastening the decline in reputation to penalize sporadic malicious behavior by attackers.

(3) Defending against Byzantine attacks

In the reputation-based RPBFT consensus mechanism, c_num nodes with higher reputation become consensus committee nodes and complete the PBFT consensus process, with a complexity of $O(c\_num^2)$. The system can tolerate up to $\lfloor (c\_num - 1/3) \rfloor$ faulty or malicious nodes. The remaining $N - c\_num$ nodes serve as validators, and if more than half of the validation nodes are honest, the result is considered valid. Therefore, a maximum of $\lfloor (N - c\_num)/2 \rfloor$ faulty or malicious validators are permissible. Thus, RPBFT's maximum fault tolerance is $\lfloor (3N - c\_num - 1)/6 \rfloor$, exceeding the original PBFT's by $\lfloor (N - c\_num + 1)/6 \rfloor$. Moreover, due to the dynamic replacement method of consensus committee nodes and the reputation penalty for invalid consensus nodes, it can encourage long-term high-reputation nodes to become consensus committee nodes and prime candidates. This approach effectively reduces failure and malicious rates in the consensus process.

Thus, through the analysis of (2) and (3), it can be concluded that BtRaI is capable of providing trusted and practical reputation assessment, thereby fulfilling the second design goal.

(4) Effectiveness of incentive mechanism

The reputation-based incentive mechanism distributes token rewards and penalties to promote honest participation in the consensus and validation processes, which can effectively improve blockchain efficiency and reduce failures and errors. Additionally, the degree of these rewards and penalties drives nodes to continually improve their performance within the healthcare service system, aiming for a higher reputation and greater token reward. During medical data diagnosis and sharing services, the token pledged value is inversely proportional to the reputation value, encouraging participants to engage honestly and actively in medical consultation, data sharing, and service provision. This creates a beneficial cycle linking reputation and token incentives.

Furthermore, regarding reputation and token rewards and penalties with differentiation, we will specifically demonstrate it in the experiments to further illustrate that BtRaI satisfies the third design goal, i.e., effective differentiation in reward and punishment mechanisms.

(5) Resilience against other attacks

Within the consortium blockchain that strictly scrutinizes participant user identities, common attacks from untrusted and unauthorized third parties, like identity forgery, are prevented from affecting the BtRaI system.

In BtRaI's transactional interactions, measures are in place to prevent malicious participants from broadcasting already verified transactions or blocks, thus averting replay attacks. This is achieved through the use of unique timestamps and nonce values in the blockchain's transaction structure.

Moreover, each user's private key is used to sign transaction information, which is then published on the blockchain with the transaction details, including timestamps, further preventing replay attacks. In the case of repudiation attacks, where a participant denies a transaction, the signer's identity can be confirmed by revealing the public key associated with their private key, ensuring accountability for the transaction. In addition to the utilization of digital signature technology within the blockchain, the incorporation of secure hash functions further enhances BtRaI's resilience against tampering attacks.

Besides, BtRaI's admission and token collateralization mechanisms, tying tokens to economic incentives, serve as a barrier against distributed denial-of-service (DDoS) attacks. The RPBFT's consensus committee node selection and rotation mechanism also reduce the risk of 51% attacks by limiting and dynamically changing the subset of nodes participating in the consensus process.

(6) Comparison with related schemes

Further, we theoretically compare the proposed BtRaI scheme with other blockchain-based incentive mechanisms for healthcare services in Table 1. As shown in the table, most schemes use consortium chains or even private chains to restrict access from unauthorized users [37]. However, existing healthcare service incentive mechanisms are less likely to incorporate multidimensional reputation assessment methods and lack feedback facilitation for consensus mechanisms. In contrast, BtRaI records reputation assessment results on the consortium chain in a tamper-evident manner. Additionally, it establishes a beneficial cycle linking multidimensional reputation assessment, the improved consensus algorithm, and the incentive mechanism.

6. Experimental analysis

To evaluate the BtRaI proposed in this paper, we conducted simulation experiments using Python over Windows 11 on Intel(R) Core(TM) i7-12700H 2.30 GHz 16G RAM. The multi-entity multidimensional comprehensive reputation assessment, reputation-based RPBFT consensus algorithm, and reputation-based incentive mechanism proposed in this paper were evaluated, respectively.

6.1. Reputation assessment results

The parameter settings for the reputation assessment section are shown in Table 2, including some values that need to be dynamically adjusted for comparison during evaluation. We assume that each consortium blockchain consists of 50 patient groups, 6 healthcare centers, and 1 cloud service platform. The gap modifier factor ω is set to the default normal level of 1, and the initialized learning factors γ are $\gamma_1 = 0.6$ and $\gamma_2 = 0.4$. To emphasize the importance of providing high-quality services to PnFs, the weights in the HC comprehensive reputation calculation are assigned as follows: 0.4 for PnF assessments, and 0.2 each for HC, CSP assessments, and maintenance performance on the consortium chain. Similarly, in the comprehensive reputation calculation of CSP, the importance of PnF assessment is emphasized, with $\delta_1 = 0.5$. To explore the impact of weights factors on the final reputation assessment, in the comprehensive reputation calculation of PnF, three weight factors, β_1, β_2, and β_3, are varied between 0.1, 0.3, and 0.6 to form different combinations. Additionally, the learning rate factors, γ_1 and γ_2, are varied to investigate the effect of their varying gaps on the comprehensive reputation assessment.

Experiments on comprehensive reputation assessment in multiple scenarios follow.

(1) We use the results of HC's comprehensive reputation assessment to illustrate the changes in reputation for both normal service scenarios and scenarios with partial malicious service. Firstly, in the normal scenario, the set comprehensive reputation ranking is HC1, HC5, HC6, HC2, HC4, and HC3, as shown in Fig. 4. It can be seen that the set reputation of HC1-HC6 is maintained steadily around 0.96, 0.84, 0.74, 0.82, 0.88, and 0.88, respectively.

Based on this reputation assessment, we analyze a complex and dynamic change scenario. Specifically, HC1 starts displaying malicious behavior after 50 rounds of improved performance, leading to a drop in ratings and becoming a validation node with block validation misbehavior after 70 rounds. HC3 temporarily improves performance in rounds 40–49 for a higher score, then reverts to usual behavior. HC4 engages in block validation misbehavior, then normalizes. HC5 improves the quality of service after 50 rounds, enhancing scores. HC2 and HC6 consistently maintain normal behavior.

Fig. 5(a) shows the comprehensive reputation changes of HCs, and Fig. 5(b) compares the effects of the scheme [38] that combines the sigmoid function in the final reputation assessment. We observed that our scheme and Hu et al.'s scheme [38] are effective in quickly reducing the reputation of nodes engaging in malicious behavior, such as HC1 and HC4, mirroring the significant real-world impact of such actions. However, for nodes showing positive behavior, like HC3 and HC5, the sigmoid-based scheme [38] offers a quicker reputation increase. Our BtRaI scheme, with its dynamically changing learning rate, provides a more gradual reputation growth and finer differentiation between nodes, aligning closely with real-world dynamics.

(2) Using the reputation calculation results of PnF as an example, Fig. 6 shows the current comprehensive reputation assessment results under different weight distributions, with HR_{PnF}, CR_{PnF}, BR_{PnF}, and R^t_{PnF} scores of 0.88, 0.98, 0.5, and 0.9. The weight distributions are $\beta_1 = 0.6$, $\beta_2 = 0.1$, $\beta_3 = 0.3$ (denoted as $6\beta_1, 1\beta_2, 3\beta_3$); $\beta_1 = 0.3$, $\beta_2 = 0.6$, $\beta_3 = 0.1$ (denoted as $3\beta_1, 6\beta_2, 1\beta_3$); and $\beta_1 = 0.1$, $\beta_2 = 0.3$, $\beta_3 = 0.6$ (denoted as $1\beta_1, 3\beta_2, 6\beta_3$). In Fig. 6, the bar chart represents the scores of each sub-assessment item, and the line graph illustrates the comprehensive reputation results obtained under different weight distributions. Fig. 6 illustrates that, due to the dynamic adjustment of historical reputation R^t_{PnF} and the learning rate factor γ, the final results tend to converge around R^t_{PnF}, exhibiting a preference for components with greater weights in the reputation calculation.

Table 2
Reputation assessment parameter setting.

Parameter	Value	Parameter	Value
n, m	50, 6	$\beta_1, \beta_2, \beta_3$ (variable)	[0.1,0.3,0.6]
ω	1	$\delta_1, \delta_2, \delta_3$	0.5,0.2,0.3
γ_1, γ_2	0.6, 0.4	γ_1 (variable)	[0.9,0.7,0.5]
$\alpha_1, \alpha_2, \alpha_3, \alpha_4$	0.4, 0.2, 0.2, 0.2	γ_2 (variable)	[0.1,0.3,0.4]

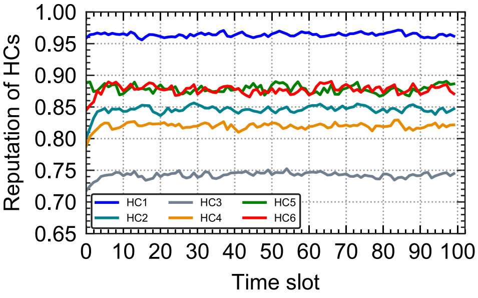
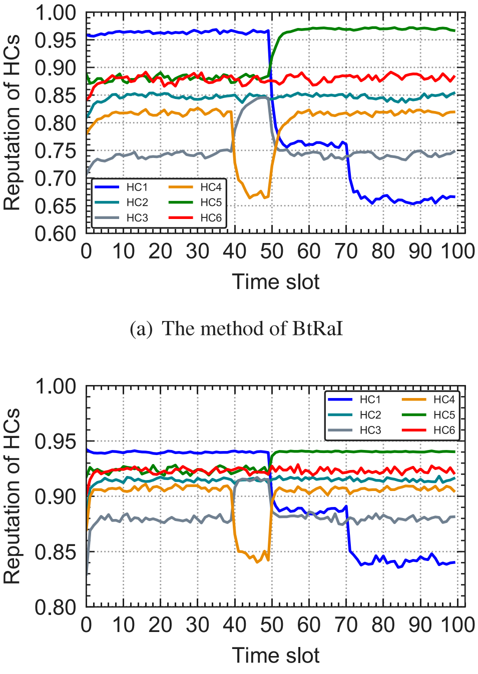


Fig. 4. HC comprehensive reputation assessment results.



(a) The method of BtRaI

(b) The method of Hu et al.

Fig. 5. Comparison of HC comprehensive reputation under dynamic changes in behavior.

Fig. 7 compares the variation curves of PnF reputation over time in three different cases, each based on the previously described weight distributions. The fundamental assumption is that the score derived from CSP is higher than that derived from HC, and both score intervals exhibit stability. However, given that PnF occurs randomly in the consortium chain with correct and incorrect validation, the performance score of CB experiences fluctuations. As shown in Fig. 7, the larger decrease in scores for the weight distributions of "$6\beta_1, 1\beta_2, 3\beta_3$" and "$1\beta_1, 3\beta_2, 6\beta_3$" is due to the occurrence of PnF block validation

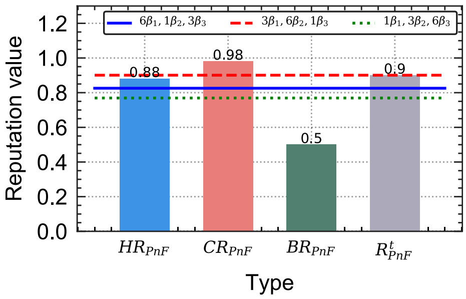


Fig. 6. Results of PnF reputation assessment with different weight distributions.

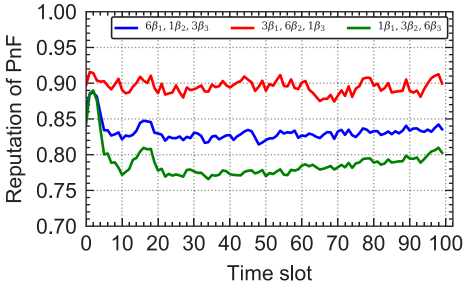


Fig. 7. Changes in the comprehensive reputation of PnF under different weight distributions.

errors, with a higher proportion of scores being allocated to HR_{PnF} and BR_{PnF} in the comprehensive reputation assessment. In contrast, “$3\beta_1, 6\beta_2, 1\beta_3$” has the smallest weight for BR_{PnF} and the largest weight for CR_{PnF}, resulting in greater stability and the highest score.

(3) Taking the reputation assessment results of CSP as an example, Fig. 8 shows the effect of adjusting the learning rate parameter on the final reputation calculation. The CSP is evaluated based on two scenarios with high and low initial reputations. The CSP scores higher PR_{CSP}, HR_{CSP}, and BR_{CSP} during the periods 0–20, 40–60, and 80–100, but scores lower in the 20–40 and 60–80 intervals due to poorer performance. The learning rate factor γ is varied across three different combinations: $\gamma_1 = 0.9$, $\gamma_2 = 0.1$ (denoted as γ9-1), $\gamma_1 = 0.7$, $\gamma_2 = 0.3$ (denoted as γ7-3), and $\gamma_1 = 0.5$, $\gamma_2 = 0.4$ (denoted as γ5-4).

In Fig. 8, the vertical axis on the left represents the comprehensive reputation values of the CSP reputation change curve under three combinations of learning rate factors. The right vertical axis corresponds to specific γ values per time slot, but only the γ9-1 combination is shown for clarity. As shown, γ takes on the value of γ_2 for most of the time, indicating that the current comprehensive score is higher than the historical reputation score, especially in phases of good performance and rising reputation. From the comparison of the three curves, we observe that as the gap between γ_1 and γ_2 increases, the rate of reputation enhancement in the rising stage gradually slows down. Specifically, in the γ9-1 case, the outcome more accurately reflects real-world reputation dynamics, where positive behavior slowly builds reputation while negative behavior rapidly diminishes it. Therefore, we suggest widening the gap between γ_1 and γ_2 for a more realistic representation.

(4) Furthermore, we evaluated the effectiveness of the BtRaI scheme in resisting collusion attacks. Specifically, we examined a scenario where HC3 and some PnFs colluded, exchanging high assessments and unfairly lowering HC1's ratings. To launch the collusion attack more stealthily, HC3 assessed HC1 normally. The experimental results for this scenario are presented in Fig. 9.

Fig. 9(a) illustrates that collusion attacks have a more significant impact on the average assessment score PR_{HC} derived from PnFs. In the scenario where the vast majority of PnFs collude with HC3, HC1's PR_{HC} scores are severely impacted, becoming lower than HC3's PR_{HC}. However, as shown in Fig. 9(b), our BtRaI scheme is resilient to such attacks, resulting in a higher reputation score for HC1 and a lower reputation score for HC3, despite collusion attempts by most PnFs with HC3. This resilience stems from the scheme's integration of scores from peer HCs, the CSP, consortium chain maintenance, and historical reputation, effectively countering collusive PnF ratings. Furthermore, if similar attacks are detected over time, the influence of malicious assessment groups can be mitigated by reducing the α_1 weight assigned to PnFs.

Table 3
Average transaction latency of RPBFT against PBFT (s).

$N = n + m + 1$	RPBFT-1	RPBFT-2	RPBFT-3	PBFT
4	0.011	0.013	0.013	0.013
10	0.015	0.024	0.015	0.051
20	0.024	0.049	0.040	0.148
30	0.038	0.054	0.084	0.302
40	0.058	0.087	0.159	0.579
50	0.087	0.118	0.214	0.849
60	0.111	0.151	0.328	2.316
70	0.144	0.213	0.453	3.325
80	0.160	0.262	0.560	6.759
90	0.234	0.322	0.733	9.482
100	0.281	0.465	3.025	11.607

In summary, BtRaI's multidimensional comprehensive reputation assessment method, based on multifactor moderation, is capable of resisting various threats such as long-term malicious service attacks, short-term honest service attacks, and collusion attacks. It achieves trusted and practical reputation assessment, aligning with real-world application needs.

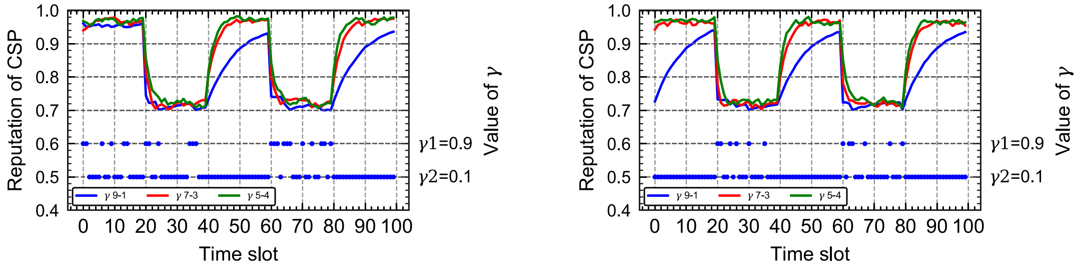
6.2. RPBFT efficiency

To simulate the implementation of RPBFT, we utilized multithreaded concurrency to simulate different nodes and employed Socket communication to simulate network communication between blockchain nodes. We conducted several experiments to compare the efficiency of the reputation-based RPBFT consensus algorithm with the PBFT algorithm. In these experiments, we varied $N = n + m + 1$ and c_num dynamically. Specifically, the consortium chain nodes N were assigned values in the range of [4, 10, 20, 30, 40, 50, 60, 70, 80, 90, 100]. In RPBFT, if $c\_num \leq 10$, make c_num equal to 4. For larger networks, c_num is calculated as $4 + \lfloor (N - 10)/4 \rfloor$ for RPBFT-1, $4 + \lfloor (N - 10)/3 \rfloor$ for RPBFT-2, and $4 + \lfloor (N - 10)/2 \rfloor$ for RPBFT-3.

The time from a client's transaction submission to the completion of its block's writing to the blockchain by all nodes is defined as the transaction completion process, termed as transaction delay or block generation time. Fig. 10 and Table 3 present experimental comparisons of the average transaction latency of RPBFT and PBFT for different N values. Meanwhile, Fig. 11 and Table 4 measure network traffic, quantified by message exchanges among nodes, comparing RPBFT and PBFT for different N values.

Fig. 10 and Table 3 demonstrate that transaction latency increases as the number of consortium chain nodes N rises. PBFT's performance significantly drops at larger node scales, averaging 11.607 s for block consensus at $N = 100$. In contrast, RPBFT consistently shows lower transaction latency than PBFT across all c_num settings. As c_num increases, RPBFT's transaction latency grows faster with N. At $N = 100$, RPBFT-3 takes 3.025 s for block generation, whereas RPBFT-1 and RPBFT-2 complete the block consensus and validation in under 0.5 s.

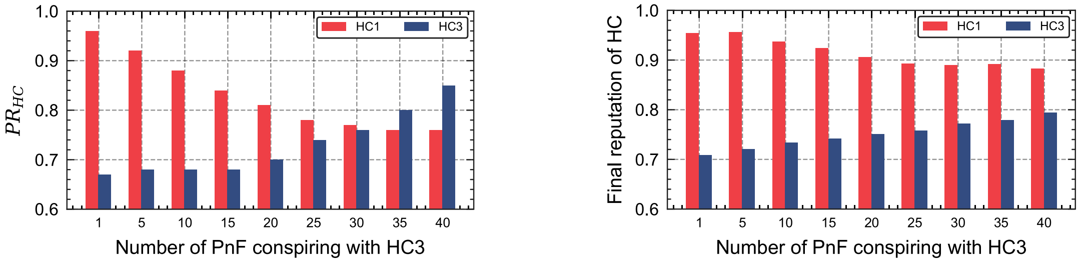
Fig. 11 and Table 4 demonstrate that communication overhead increases as the number of participating nodes increases. PBFT shows a rapidly increasing communication trend, hitting 3000 internode exchanges before $N = 50$. In contrast, RPBFT-3 exceeds 3000 exchanges only after $N = 90$. RPBFT-1 and RPBFT-2 exhibit the lowest communication overhead and growth. Notably, RPBFT-1 maintains a low



(a) High initial reputation

(b) Low initial reputation

Fig. 8. Reputation assessment results at different learning rates.



(a) Average assessment score obtained from PnF

(b) Comprehensive reputation assessment results

Fig. 9. Reputation assessment results under different levels of collusion attacks.

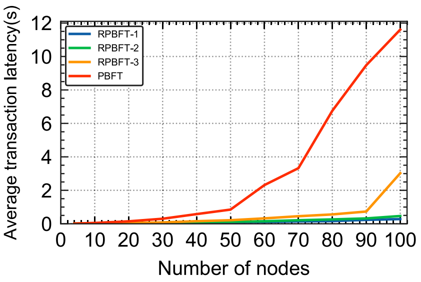


Fig. 10. Change in average transaction latency.

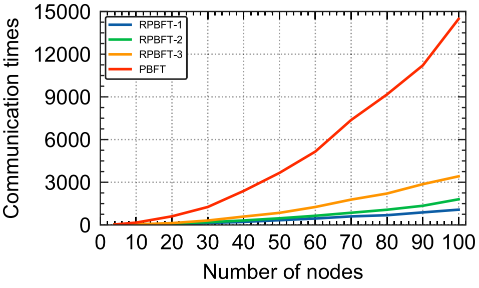


Fig. 11. Change in average communication overhead.

overhead of around 1000 internode message exchanges even at N = 100.

Since RPBFT selects consensus committees based on high reputation, *c_num* remains within a narrow range. Therefore, the high-performance RPBFT-1 and RPBFT-2 models are well-suited to the practical needs of our proposed healthcare service system based on reputation assessment.

Table 4
Average communication overhead of RPBFT against PBFT (times).

$N = n + m + 1$	RPBFT-1	RPBFT-2	RPBFT-3	PBFT
4	33	33	33	33
10	41	39	40	165
20	73	100	131	606
30	138	190	311	1263
40	214	316	588	2389
50	333	467	850	3659
60	451	644	1261	5155
70	600	856	1781	7375
80	684	1069	2207	9170
90	882	1347	2866	11 212
100	1074	1803	3418	14 480

6.3. Service incentive effect

The fundamental parameters of the incentive mechanism for healthcare services are shown in Table 5. The base profit values for consensus committee nodes serving as Leaders, Rw_M(Leader), are set to 4, while for other consensus committee nodes, Rw_M(Others), it is set to 3. The base profit value for validation nodes, Rw_V, is set to 2. The required CareCoin pledged for bookkeepers and validators in a consensus round is 10 and 5, respectively. The block generation time interval, $T_f - T_s$, ranges from 0.01 to 3.03 s.

To illustrate the incentive effect of HC participation in the consortium chain, we consider the scenario where: (1) 'Normal' HC1 always has a high reputation, while 'abnormal' HC1 sees a reputation decline post-50th round and block validation error post-70th round. (2) The normal HC6 and HC3 have decreasing reputations in order, but HC6 starts enhancing its reputation post-50th round and participates in block generation honestly. (3) Normal nodes in the consortium chain consistently generate valid consensus and validation results. Each time slot completes a round of block consensus and validation in this experiment.

Table 5
Basic parameter setting of incentive mechanism.

Parameter	Value
Rw_M(Leader), Rw_M(Others), Rw_V	4, 3, 2
K, V	10, 5
$T_f - T_s$	(0.01, 3.03)

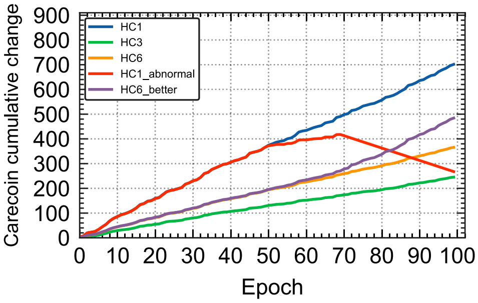


Fig. 12. Variation of Carecoin in incentives.

Fig. 12 shows the variation in Carecoin accumulation by different entities across 100 rounds, starting from 0. The accumulation for entities like HC1, HC6, and HC3 reflects their reputation levels, with HC1 (high reputation) accumulating about 500 more Carecoins than HC3 (low reputation) after 100 rounds. The significant disparity between high-reputation consensus nodes and low-reputation validation nodes serves as a stronger incentive for active and honest participation in healthcare services, encouraging entities to strive for consensus node status for better revenue.

In particular, a reduced HC1_abnormal reputation results in slower Carecoin accumulation. Its validation misbehavior after 70 rounds further reduces Carecoin as a penalty. On the other hand, HC6_better, with a higher reputation after 50 rounds, shows an initial slow increase in Carecoin accumulation, accelerating after becoming a consensus node. It is observed that nodes with high reputation lose reputation and Carecoin upon malicious behavior (trend 1), while those with low reputation gain higher reputation and more Carecoin for good performance (trend 2). Trend 1 is more pronounced than trend 2, reflecting real-world scenarios where good behavior needs sustained demonstration while malicious behavior are quickly penalized.

7. Conclusion

In this paper, we propose a healthcare service incentive mechanism based on blockchain and trusted reputation assessment to motivate all participants in the healthcare service system. We use multidimensional comprehensive reputation assessment method with multifactor moderation to calculate reputation scores that are resistant to malicious behavior. Using the reputation assessment results, we design a highly fault-tolerant and efficient consensus mechanism, RPBFT. We also introduce a reputation-related token reward and punishment incentive mechanism to promote system stability and active entity participation. Theoretical analyses and extensive experimental evaluations show that the proposed BtRaI is well-suited for incentivizing healthcare services in dynamic and complex scenarios.

In the future, we will explore practical applications in real healthcare environments, as well as simulate attack scenarios and collect actual operational data to evaluate and improve BtRaI, responding to more increasingly complex scenarios and evolving service requirements.

CRediT authorship contribution statement

Yanhua Liu: Conceptualization, Funding acquisition, Methodology, Writing – review & editing. **Zhihuang Liu:** Data curation, Formal analysis, Methodology, Software, Validation, Writing – original draft, Writing – review & editing. **Qiu Zhang:** Data curation, Investigation, Writing – review & editing. **Jinshu Su:** Supervision, Validation, Writing – review & editing. **Zhiping Cai:** Funding acquisition, Supervision, Validation, Writing – review & editing. **Xiaoyan Li:** Funding acquisition, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

This work is supported by the National Key Research and Development Program of China (2022YFF1203001), the National Natural Science Foundation of China (Grant No. 62072109, No. 62002062, and No. U1804263), the Natural Science Foundation of Fujian Province, China (Grant No. 2021J01625, No. 2021J01616, and No. 2022J05029), and the Major Science and Technology project of Fujian Province, China (Grant No. 2021HZ022007). The authors would like to thank the editor-in-chief, editor, and reviewers for their valuable comments and suggestions.

References

[1] M. Adil, J. Ali, M.M. Jadoon, S.A. Otaibi, N. Kumar, A. Farouk, H. Song, COVID-19: secure healthcare internet of things networks, current trends and challenges with future research directions, ACM Trans. Sens. Netw. 19 (3) (2023) 54:1–54:25, http://dx.doi.org/10.1145/3558519.

[2] S. Wang, H. Wang, J. Li, H. Wang, J. Chaudhry, M. Alazab, H. Song, A fast CP-ABE system for cyber-physical security and privacy in mobile healthcare network, IEEE Trans. Ind. Appl. 56 (4) (2020) 4467–4477, http://dx.doi.org/10.1109/TIA.2020.2969868.

[3] J.A.A. Alzubi, Blockchain-based Lamport Merkle Digital Signature: Authentication tool in IoT healthcare, Comput. Commun. 170 (2021) 200–208, http://dx.doi.org/10.1016/j.comcom.2021.02.002.

[4] M. Majhi, A.K. Pal, J. Pradhan, S.H. Islam, M.K. Khan, Computational intelligence based secure three-party CBIR scheme for medical data for cloud-assisted healthcare applications, Multimedia Tools Appl. 81 (29) (2022) 41545–41577, http://dx.doi.org/10.1007/s11042-020-10483-7.

[5] A.P. Singh, N.R. Pradhan, A.K. Luhach, S. Agnihotri, N.Z. Jhanjhi, S. Verma, Kavita, U. Ghosh, D.S. Roy, A novel patient-centric architectural framework for blockchain-enabled healthcare applications, IEEE Trans. Ind. Inform. 17 (8) (2021) 5779–5789, http://dx.doi.org/10.1109/TII.2020.3037889.

[6] J.A.A. Alzubi, O.A. Alzubi, A. Singh, M. Ramachandran, Cloud-IIoT-based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning, IEEE Trans. Ind. Inform. 19 (1) (2023) 1080–1087, http://dx.doi.org/10.1109/TII.2022.3189170.

[7] M.A. Jan, F. Khan, S. Mastorakis, M. Adil, A. Akbar, N. Stergiou, LightIoT: Lightweight and secure communication for energy-efficient IoT in health informatics, IEEE Trans. Green Commun. Netw. 5 (3) (2021) 1202–1211, http://dx.doi.org/10.1109/TGCN.2021.3077318.

[8] M.S. Rahman, M.A. Islam, M.A. Uddin, G. Stea, A survey of blockchain-based IoT eHealthcare: Applications, research issues, and challenges, Internet Things 19 (2022) 100551, http://dx.doi.org/10.1016/j.iot.2022.100551.

[9] H.M. Hussien, S.M. Yasin, N.I. Udzir, M.I.H. Ninggal, S. Salman, Blockchain technology in the healthcare industry: Trends and opportunities, J. Ind. Inf. Integr. 22 (2021) 100217, http://dx.doi.org/10.1016/j.jii.2021.100217.

[10] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, N. Yu, Healthchain: A blockchain-based privacy preserving scheme for large-scale health data, IEEE Internet Things J. 6 (5) (2019) 8770–8781, http://dx.doi.org/10.1109/JIOT.2019.2923525.

[11] J. Su, L. Zhang, Y. Mu, BA-RMKABSE: blockchain-aided ranked multi-keyword attribute-based searchable encryption with hiding policy for smart health system, Future Gener. Comput. Syst. 132 (2022) 299–309, http://dx.doi.org/10.1016/j.future.2022.01.021.

[12] Z. Wang, N. Luo, P. Zhou, GuardHealth: Blockchain empowered secure data management and Graph Convolutional Network enabled anomaly detection in smart healthcare, J. Parallel Distrib. Comput. 142 (2020) 1–12, http://dx.doi.org/10.1016/j.jpdc.2020.03.004.

[13] O.A. Alzubi, J.A.A. Alzubi, K. Shankar, D. Gupta, Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in Internet of Things, Trans. Emerg. Telecommun. Technol. 32 (12) (2021) http://dx.doi.org/10.1002/ett.4360.

[14] G.K. Verma, B.B. Singh, N. Kumar, O. Kaiwartya, M.S. Obaidat, PFCBAS: pairing free and provable certificate-based aggregate signature scheme for the e-healthcare monitoring system, IEEE Syst. J. 14 (2) (2020) 1704–1715, http://dx.doi.org/10.1109/JSYST.2019.2921788.

[15] G. Dong, Y. Chen, J. Fan, D. Liu, Y. Hao, Z. Wang, A privacy-user-friendly scheme for wearable smart sensing devices based on blockchain, in: 15th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2018, Chengdu, China, October 9-12, 2018, IEEE Computer Society, 2018, pp. 481–486, http://dx.doi.org/10.1109/MASS.2018.00073.

[16] G. Wu, S. Wang, Z. Ning, B. Zhu, Privacy-preserved electronic medical record exchanging and sharing: A blockchain-based smart healthcare system, IEEE J. Biomed. Health Inform. 26 (5) (2022) 1917–1927, http://dx.doi.org/10.1109/JBHI.2021.3123643.

[17] R. Han, Z. Yan, X. Liang, L.T. Yang, How can incentive mechanisms and blockchain benefit with each other? a survey, ACM Comput. Surv. 55 (7) (2023) 136:1–136:38, http://dx.doi.org/10.1145/3539604.

[18] R. Zhao, L.T. Yang, D. Liu, X. Deng, Y. Mo, A tensor-based truthful incentive mechanism for blockchain-enabled space-air-ground integrated vehicular crowdsensing, IEEE Trans. Intell. Transp. Syst. 23 (3) (2022) 2853–2862, http://dx.doi.org/10.1109/TITS.2022.3144301.

[19] L. Zhu, H. Dong, M. Shen, K. Gai, An incentive mechanism using Shapley value for blockchain-based medical data sharing, in: 5th IEEE International Conference on Big Data Security on Cloud, BigDataSecurity/HPSC/IDS 2019, Washington, DC, USA, May 27-29, 2019, IEEE, 2019, pp. 113–118, http://dx.doi.org/10.1109/BigDataSecurity-HPSC-IDS.2019.00030.

[20] P. Esmaeilzadeh, T. Mirzaei, Role of incentives in the use of blockchain-based platforms for sharing sensitive health data: Experimental study, J. Med. Internet Res. 25 (2023) e41805, http://dx.doi.org/10.2196/41805.

[21] C. Gan, A. Saini, Q. Zhu, Y. Xiang, Z. Zhang, Blockchain-based access control scheme with incentive mechanism for eHealth systems: patient as supervisor, Multimedia Tools Appl. 80 (20) (2021) 30605–30621, http://dx.doi.org/10.1007/s11042-020-09322-6.

[22] M. Shen, J. Duan, L. Zhu, J. Zhang, X. Du, M. Guizani, Blockchain-based incentives for secure and collaborative data sharing in multiple clouds, IEEE J. Sel. Areas Commun. 38 (6) (2020) 1229–1241, http://dx.doi.org/10.1109/JSAC.2020.2986619.

[23] A.T. Litchfield, A. Khan, BlockPres: A novel blockchain-based incentive mechanism to mitigate inequalities for prescription management system, Sensors 21 (15) (2021) 5035, http://dx.doi.org/10.3390/s21155035.

[24] S. Purohit, P. Calyam, M.L. Alarcon, N.R. Bhamidipati, A.S.M. Mosa, K. Salah, HonestChain: Consortium blockchain for protected data sharing in health information systems, Peer-to-Peer Netw. Appl. 14 (5) (2021) 3012–3028, http://dx.doi.org/10.1007/s12083-021-01153-y.

[25] S. Wang, D. Ye, X. Huang, R. Yu, Y. Wang, Y. Zhang, Consortium blockchain for secure resource sharing in vehicular edge computing: A contract-based approach, IEEE Trans. Netw. Sci. Eng. 8 (2) (2021) 1189–1201, http://dx.doi.org/10.1109/TNSE.2020.3004475.

[26] L. Vishwakarma, D. Das, SmartCoin: A novel incentive mechanism for vehicles in intelligent transportation system based on consortium blockchain, Veh. Commun. 33 (2022) 100429, http://dx.doi.org/10.1016/j.vehcom.2021.100429.

[27] Z. Noshad, A.U. Khan, S. Abbas, Z. Abubaker, N. Javaid, M. Shafiq, J. Choi, An incentive and reputation mechanism based on blockchain for crowd sensing network, J. Sens. 2021 (2021) 1798256:1–1798256:14, http://dx.doi.org/10.1155/2021/1798256.

[28] E.K. Wang, Z. Liang, C. Chen, S. Kumari, M.K. Khan, PoRX: A reputation incentive scheme for blockchain consensus of IIoT, Future Gener. Comput. Syst. 102 (2020) 140–151, http://dx.doi.org/10.1016/j.future.2019.08.005.

[29] Y. Yi, Y. Yang, K. Cheng, Y. Wu, X. Wang, Information dissemination with service-oriented incentive mechanism in Industrial Internet of Things, IEEE Internet Things J. 9 (18) (2022) 16897–16907, http://dx.doi.org/10.1109/JIOT.2022.3147840.

[30] G. Zhang, H. Jacobsen, Prosecutor: an efficient BFT consensus algorithm with behavior-aware penalization against Byzantine attacks, in: K. Zhang, A. Gherbi, N. Venkatasubramanian, L. Veiga (Eds.), Middleware '21: 22nd International Middleware Conference, Québec City, Canada, December 6 - 10, 2021, ACM, 2021, pp. 52–63, http://dx.doi.org/10.1145/3464298.3484503.

[31] G. Xu, H. Bai, J. Xing, T. Luo, N.N. Xiong, X. Cheng, S. Liu, J.X. Zheng, SG-PBFT: A secure and highly efficient distributed blockchain PBFT consensus algorithm for intelligent Internet of vehicles, J. Parallel Distrib. Comput. 164 (2022) 1–11, http://dx.doi.org/10.1016/j.jpdc.2022.01.029.

[32] M. Rezvani, A. Ignjatovic, E. Bertino, S.K. Jha, Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks, IEEE Trans. Dependable Secur. Comput. 12 (1) (2015) 98–110, http://dx.doi.org/10.1109/TDSC.2014.2316816.

[33] M. Wang, G. Wang, Y. Zhang, Z. Li, A high-reliability multi-faceted reputation evaluation mechanism for online services, IEEE Trans. Serv. Comput. 12 (6) (2019) 836–850, http://dx.doi.org/10.1109/TSC.2016.2638812.

[34] Z. Yan, X. Li, M. Wang, A.V. Vasilakos, Flexible data access control based on trust and reputation in cloud computing, IEEE Trans. Cloud Comput. 5 (3) (2017) 485–498, http://dx.doi.org/10.1109/TCC.2015.2469662.

[35] M. Du, X. Ma, Z. Zhang, X. Wang, Q. Chen, A review on consensus algorithm of blockchain, in: 2017 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2017, Banff, AB, Canada, October 5-8, 2017, IEEE, 2017, pp. 2567–2572, http://dx.doi.org/10.1109/SMC.2017.8123011.

[36] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, M.A. Imran, A scalable multi-layer PBFT consensus for blockchain, IEEE Trans. Parallel Distrib. Syst. 32 (5) (2021) 1146–1160, http://dx.doi.org/10.1109/TPDS.2020.3042392.

[37] S. Nazir, M. Kaleem, H. Hamdoun, J. Alzubi, H. Tianfield, Blockchain of things for healthcare asset management, in: V. Jain, J. Chatterjee, P. Kumar, U. Kose (Eds.), Healthcare Monitoring and Data Analysis using IoT: Technologies and Applications, in: Heathcare Technologies Series 38, Institution of Engineering and Technology (IET), 2022, pp. 199–209, http://dx.doi.org/10.1049/PBHE038E_ch.

[38] Q. Hu, H. Cheng, X. Zhang, C. Lin, Trusted resource allocation based on proof-of-reputation consensus mechanism for edge computing, Peer-to-Peer Netw. Appl. 15 (1) (2022) 444–460, http://dx.doi.org/10.1007/s12083-021-01240-0.

Yanhua Liu received his B.S. and M.S. degrees from the College of Computer and Data Science, Fuzhou University, China, in 1996 and 2003 respectively. He received his Ph.D. degree from the College of Physics and Information Engineering, Fuzhou University, China, in 2016. He is currently working as an associate professor and researcher at the Fujian Key Laboratory of Network Computing and Intelligent Information Processing at Fuzhou University. His research interests are intelligent computing, computer security, and big data. His research work has won several government awards.

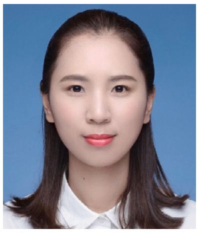
Zhihuang Liu received his B.E. and M.S. degrees from the College of Computer and Data Science, Fuzhou University, in 2020 and 2023, respectively. He is currently pursuing a Ph.D. degree in the College of Computer at the National University of Defense Technology. His research interests include blockchain, IoT security, and machine learning.

Qiu Zhang received his B.E. degree in Chemical Engineering from Fuzhou University in 2022. He is now pursuing his M.S. degree in the College of Computer and Data Science at Fuzhou University. His research interests are machine learning and federated learning.

Jinshu Su received the B. Sc degree in Mathematics from Nankai University and the M.S. and Ph.D. degrees in computer science from the National University of Defense Technology, Changsha, China. He is a professor with the College of Computer, National University of Defense Technology. He currently leads the Distributed Computing and High Performance Router Laboratory and the Computer Networks and Information Security Laboratory, which are both key laboratories of National 211 and 985 Projects, China. He is a CCF fellow, and he serves as the chair of the Internet Committee of CCF. He has published more than 200 papers in international journals and conferences, including

JSAC, TVT, FGCS, MobiHoc, INFOCOM, ICDCS, etc. His current research interests include Internet architecture, Internet routing, security, and wireless networks.

Zhiping Cai received the B.Eng., M.A.Sc., and Ph.D. degrees in computer science and technology from the National University of Defense Technology (NUDT), China, in 1996, 2002, and 2005, respectively. He is a full professor in the College of Computer, NUDT. His current research interests include artificial intelligence, network security, and big data. He is a senior member of the CCF and a member of the IEEE.



Xiaoyan Li received her Ph.D. degree in computer science from Soochow University, Suzhou, China, in 2019. She was a visiting scholar in the Department of Computer Science, the City University of Hong Kong, Hong Kong, from June 2018–June 2019. She is currently an associate professor with the College of Computer and Data Science, Fuzhou University, China. She has published more than 30 papers in research-related journals and conferences, such as IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, IEEE/ACM TRANSACTIONS ON NETWORKING, IEEE TRANSACTIONS ON COMPUTERS, JOURNAL OF PARALLEL AND DISTRIBUTED COMPUTING, and AAAI. She has served at some conferences as Session Chair and Program Committee Member, including IEEE BIBM 2020, IEEE TrustCom 2020 Workshop, WWW 2021, AAAI 2022 Workshop. Her research interests include graph theory, data center networks, parallel and distributed systems, design and analysis of algorithms, and fault diagnosis.